KEBIJAKAN PENANGGULANGAN TINDAK PIDANA TEKNOLOGI INFORMASI MELALUI HUKUM PIDANA

TESIS

DISUSUN DALAM RANGKA MEMENUHI PERSYARATAN PROGRAM MAGISTER ILMU HUKUM

Oleh:
Philemon Ginting,SIK

PEMBIMBING:
Prof.Dr.H. Barda Nawawi Arief,SH.

Program Magister Ilmu Hukum
Universitas Diponegoro
Semarang
2008

KEBIJAKAN PENANGGULANGAN TINDAK PIDANA TEKNOLOGI INFORMASI MELALUI HUKUM PIDANA

Disusun Oleh:

Philemon Ginting,SIK
No Mhs B04.007.030

Dipertahankan di depan Dewan Penguji
Pada Tanggal 22 Desember 2008

Tesis ini telah diterima
Sebagai persyaratan untuk memperoleh gelar
Magister Ilmu Hukum

Pembimbing	Mengetahui
Magister Ilmu Hukum	Ketua Program
Prof.Dr.Barda Nawawi Arief,SH	Prof.Dr.PaulusHadisuprapto,SH.MH.
NIP.130.350.519	NIP.130. 531.702

PERNYATAAN KEASLIAN KARYA ILMIAH

Dengan ini saya , PHILEMON GINTING, SIK menyatakan bahwa Karya Ilmiah/Tesis ini adalah asli hasil karya sendiri dan Karya Ilmiah ini belum pernah diajukan sebagai pemenuhan persyaratan untuk memperoleh gelar kesarjanaan Strata Satu (S1) maupun Magister (S2) dari Universitas Diponegoro maupun Perguruan Tinggi lain.

Semua informasi yang dimuat dalam Karya Ilmiah ini yang berasal dari penulis lain baik yang di publikasikan atau tidak, telah diberikan penghargaan dengan mengutip nama sumber penulis secara benar dan semua isi dari karya Ilmiah/Tesis ini sepenuhnya menjadi tanggung jawab Saya sebagai penulis.

Semarang, 22 Desember 2008
Penulis

PHILEMON GINTING SIK
N I M . B 4 A. 0 0 7. 0 3 0

KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Tuhan YESUS KRISTUS, karena atas limpahan karunia-Nya sehingga tesis ini bisa diselesaikan. Tesis berjudul **"Kebijakan Penanggulangan Tindak Pidana Teknologi Informasi Melalui Hukum Pidana"** disusun untuk memenuhi salah satu persyaratan dalam memperoleh gelar Magister Hukum (MH) setelah menyelesaikan pendidikan Strata-2 di Universitas Diponegoro, Semarang.

Dalam penulisan ini, Penulis sadar bahwa banyak hambatan dan kesulitan, namun berkat bantuan dan dorongan banyak pihak, akhirnya penulis dapat menyelesaikannya. Untuk itu, perkenankanlah Penulis menyampaikan penghargaan dan terima kasih yang sebesar-besarnya kepada:

1. Prof. Dr. Paulus Hadisuprapto, SH, MS, selaku Ketua Program Magister Hukum Universitas Diponegoro beserta seluruh dosen di Universitas Diponegoro yang telah membina penulis selama mengikuti pendidikan di Universitas Diponegoro, Semarang.
2. Prof. Dr. Barda Nawawi Arief, SH, selaku dosen pembimbing, yang telah berkenan meluangkan waktu dan tenaganya untuk memberikan bimbingan dan arahan dalam penyusunan tesis ini.
3. Kombes.Pol.Dr.Petrus Reinhard Golose,Msi atas masukan dan ilmu yang diberikan untuk memperluas wawasan terhadap penanggulangan tindak pidana teknologi informasi.
4. Istri ku tercinta drg.Sylvia Fransisca br Sitepu dan Joyce Callita Monica bayi kami yang telah memberikan kebahagiaan, inspirasi, motivasi, dan semangat dalam penulisan tesis ini hingga dapat selesai.

5. Kepada kedua Orang tuaku, Mertua, Kakak, Abang, Adik, dan Adik ipar serta Keponakanku yang telah memberikan semangat juga motivasi di dalam penyelesaian tesis ini.
6. Rekan-rekan mahasiswa Universitas Diponegoro, yang telah memberikan dukungan selama penulis mengikuti pendidikan di Universitas Diponegoro.
7. Bapak Kakortarsis, Kadentar RS, dan Rekan-rekan pengasuh Ex Den “PR” dan Den “RS” di Akademi Kepolisian yang telah memberikan dukungan dan kesempatan dalam penulisan tesis ini.

Penulis menyadari bahwa penulisan tesis ini masih jauh dari sempurna dan masih terdapat banyak kekurangan karena segala keterbatasan yang dimiliki Penulis. Oleh karena itu, Penulis sangat menghargai dan mengharapkan apabila pembaca dapat memberikan koreksi, kritik dan saran untuk lebih menyempurnakan tesis ini dimasa yang akan datang.

Akhirnya penulis berharap semoga tesis ini dapat memberikan manfaat dan memiliki nilai guna. Semoga Tuhan Yang Maha Esa, selalu mengiringi, melindungi dan mengabulkan segala keinginan dan doa kita semua, Amin.

Semarang, Januari 2009

Penulis

ABSTRAK

Globalisasi teknologi informasi yang telah mengubah dunia ke era *cyber* dengan sarana internet yang menghadirkan *cyberspace* dengan realitas virtualnya menawarkan kepada manusia berbagai harapan dan kemudahan. Akan tetapi di balik itu, timbul persoalan berupa kejahatan yang dinamakan *cybercrime*, kejahatan ini tidak mengenal batas wilayah (*borderless*) serta waktu kejadian karena korban dan pelaku sering berada di negara yang berbeda. *Cybercrime* dapat dilakukan melalui sistem jaringan komputernya itu sendiri yang menjadi sasaran dan komputer itu sendiri yang menjadi sarana untuk melakukan kejahatan. 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. Produk hukum yang berkaitan dengan ruang siber *(cyber space)* atau mayantara ini dibutuhkan untuk memberikan keamanan dan kepastian hukum dalam pemanfaatan teknologi informasi, media, dan komunikasi agar dapat berkembang secara optimal.

Berdasarkan latar belakang permasalahan tersebut untuk melakukan penelitian terhadap Kebijakan Penanggulangan Tindak Pidana Teknologi Informasi Melalui Hukum Pidana maka dalam tesis ini dibatasi dalam 3 (tiga) permasalahan yaitu: Bagaimana kebijakan formulasi hukum pidana terhadap tindak pidana teknologi informasi saat ini?; Bagaimana kebijakan aplikatif yang dilakukan oleh aparat penegak hukum dalam upaya penanggulangan tindak pidana teknologi informasi?, serta ; Bagaimana sebaiknya kebijakan formulasi dan kebijakan aplikatif hukum pidana dalam penanggulangan tindak pidana teknologi informasi di masa yang akan datang?.

Permasalahan-permasalahan tersebut bertujuan untuk mengetahui dan memahami kebijakan formulasi hukum pidana terhadap tindak pidana teknologi informasi saat ini. Mengetahui kebijakan aplikatif yang dilakukan oleh aparat penegak hukum dalam upaya penanggulangan tindak pidana teknologi informasi, serta menggambarkan dan menganalisa kebijakan formulasi dan kebijakan aplikatif hukum pidana dalam menanggulangi tindak pidana teknologi informasi di masa yang akan datang.

Kajian penelitian ini bersifat yuridis normatif sebagai pendekatan utama, mengingat pembahasan didasarkan pada peraturan perundang-undangan dan prinsip hukum yang berlaku dalam masalah tindak pidana teknologi informasi. Pendekatan yuridis dimasudkan untuk melakukan pengkajian terhadap bidang hukum, khususnya hukum pidana. Pendekatan yuridis komparatif juga dilakukan untuk melakukan perbandingan dengan negara-negara yang sudah mempunyai peraturan perundang-undangan (*statute approach*) dan pendekatan konsepsi (*conceptual approach*) tentang tindak pidana teknologi informasi. Sifat dari penelitian ini adalah deskriptif analitis yang menggunakan data sekunder sebagai data utama dengan menggunakan teknik penelitian kualitatif.

Hasil analisa yang dapat dijadikan sebagai kesimpulan dalam tesis ini terhadap kebijakan formulasi hukum pidana terhadap tindak pidana teknologi informasi saat ini adalah, sebelum disahkannya UU ITE terdapat beberapa ketentuan perundang-undangan yang berhubungan dengan penanggulangan tindak pidana teknologi informasi, tetapi kebijakan formulasinya berbeda-beda terutama dalam hal kebijakan kriminalisasi-nya belum mengatur secara tegas dan jelas terhadap tindak pidana teknologi informasi, kebijakan formulasi dalam UU ITE masih membutuhkan harmonisasi/sinkronisasi baik secara internal maupun secara eksternal terutama dengan instrumen hukum internasional terkait dengan teknologi informasi.

Upaya penegakan hukum tidak hanya terbatas terhadap peningkatan kemampuan, sarana dan prasarana aparat penegak hukum tetapi juga diiringi kesadaran hukum masyarakat yang didukung dengan kerjasama dengan penyedia layanan internet. Dalam hal kebijakan formulasi tindak pidana teknologi informasi pada masa yang akan datang hendaknya berada dalam sistem hukum pidana yang berlaku saat ini, hal ini juga harus didukung dengan meningkatkan komitmen strategi/prioritas nasional terutama aparat penegak hukum dalam penanggulangan tindak pidana teknologi informasi.

Kata Kunci : Kebijakan, Teknologi Informasi , Hukum Pidana.

ABSTRACT

Globalization of information technology has changed the world to the cyber era with the facilities that bring the reality of cyberspace virtual offer hope to the human variety and convenience. But behind that, a problem arises, called cybercrime, this crime does not recognize boundaries (borderless), and the incident because the victim and the perpetrator is often in different countries. Cybercrime can be done through the computer network system itself which is the target and the computer itself which is the means to commit a crime. The development of information technology is so rapid to be anticipated in the law that set. The negative impact should be anticipated by others and with the law related to the utilization of information and communication technology. Products related to the legal space siber (cyber space) or mayantara this is required to provide security and legal certainty in the use of information technology, media, and communication in order to develop optimally.

Based on the background issues to do research on Criminal Policy Follow Through Information Technology in the Criminal Law thesis is limited in three (3) the problem is: How the policy formulation of criminal law against the crime of information technology at this time?; What is the policy applied by law enforcement in the efforts of information technology crime, and; How should the policy formulation and policy applied in the criminal law of criminal information technology in the future?.

Problems is aimed to know and understand the policy formulation of criminal law against the crime of information technology at this time. Knowing the policies applied by law enforcement in the efforts of criminal information technology, and describes and analyzes the policy formulation and policy in criminal law applied in tackling the crime of information technology in the future.

This research study is normative juridical as the main approach, given that the discussion is based on laws and legal principles that apply in the criminal information technology. Dimasudkan juridical approach to conduct the review of the law, especially criminal law. Juridical comparative approach is also done to make a comparison with the countries that already have laws and regulations (statute approach) concept and approach (Conceptual approach) on information technology crime. The nature of this research is descriptive analytical data using the secondary as the main data using qualitative research techniques.

Results of analysis can serve as the conclusion of this thesis in the policy formulation of the criminal law against criminal information technology is at this time, before the ITE regulation being legalice, there are several provisions of the legislation related to the handling of information technology crime, but policies vary formulasinya especially in terms of its criminalization policies have not set a firm and clear to the criminal information technology, policy formulation in the law still requires harmonization ITE / synchronization both internally and externally, especially with the international legal instruments related to information technology.

The efforts of law enforcement is not only limited to the capacity, facilities and infrastructure, law enforcement, but also accompanied the community's awareness of law are supported with the cooperation with the internet service provider. In the case of policy formulation criminal information technology in the future should be in the system of criminal

law applicable at this time, it also must be supported with a commitment to improve the strategy / national priorities, especially in law enforcement for criminal information technology.

Keywords: Policy, Information Technology, Criminal Law.

DAFTAR ISI

Halaman

BAB I

PENDAHULUAN

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 dari 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 sebagi 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.[1]

Sebagai mana ditulis dalam *International Review of Law Computer and Technology* :[2]

> *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 and*

---

[1] Didik J.Rachbini,*"Mitos dan Implikasi Globalisasi"* : Catatan Untuk Bidang Ekonomi dan Keuangan, Pengantar edisi Indonesia dalam Hirst, Paul dan Grahame Thompson, Globalisasi adalah Mitos, Jakarta, Yayasan Obor,2001,hal. 2.

[2] *International Review of law Computers and Technology, 'Insider Cyber-Threat: Problems and Perspectives'*, Volume 14, 2001, Pages 105-113.

vulnerable to an expanding array of computer security risks or harm and inevitably to various kinds of cumputer misuse.

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 aktifitas 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).[3]

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 perilaku manusia dalam berinteraksi dengan manusia lain, baik secara individual maupun secara kelompok. Di samping itu, kemajuan teknologi tentunya akan berjalan bersamaan dengan munculnya perubahan-perubahan di bidang kemasyarakatan.

Sebagaimana dikatakan oleh Satjipto Raharjo[4], ”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

---

[3] Agus Rahardjo,. *Cybercrime pemahaman dan upaya pencegahan kejahatan berteknologi*, PT.Citra Aditya Bakti, Bandung, 2002,hal.20.

[4] Satjipto Raharjo, *Hukum dan Masyara*kat,Angkasa, Bandung,1980,hal.96.

sosial, pola-pola perikelakuan,organisasi, susunan lembaga-lembaga masyarakat dan wewenang interaksi sosial dan lain sebagainya.

Kemajuan teknologi informasi khususnya media *internet*, dirasakan banyak memberikan manfaat seperti dari segi keamanan, kenyamanan dan kecepatan. Contoh sederhana, dengan dipergunakan *internet* sebagai sarana pendukung dalam pemesanan/reservasi tiket (pesawat terbang,kereta api), hotel, pembayaran tagihan telepon,listrik, telah membuat konsumen semakin nyaman dan aman dalam menjalankan aktivitasnya. Kecepatan melakukan transaksi perbankan melalui *e-banking*, memanfaatkan *e-commerce* untuk mempermudah melakukan pembelian dan penjualan suatu barang serta menggunakan *e-library* dan *e-learning* untuk mencari referensi atau informasi ilmu pengetahuan yang dilakukan secara *on line* karena dijembatani oleh teknologi *internet* baik melalui komputer atau pun *hand phone*.

Pemanfaatan teknologi *internet* juga tidak dapat dipungkiri membawa dampak negatif yang tidak kalah banyak dengan manfaat positif yang ada. *Internet* membuat kejahatan yang semula bersifat konvensional seperti pengancaman, pencurian, pencemaran nama baik, pornografi, perjudian, penipuan hingga tindak pidana terorisme kini melalui media *internet* beberapa jenis tindak pidana tersebut dapat dilakukan secara *on line* oleh individu maupun kelompok dengan resiko tertangkap yang sangat kecil dengan akibat kerugian yang lebih besar baik untuk masyarakat maupun negara.[5]

Fenomena tindak pidana teknologi informasi merupakan bentuk kejahatan yang relatif baru apabila dibandingkan dengan bentuk-bentuk kejahatan lain yang sifatnya konvensional. Tindak pidana teknologi informasi muncul bersamaan dengan lahirnya revolusi teknologi

---

[5] Petrus Reinhard Golose, *Perkembangan Cybercrime dan Upaya Penanganannya di Indonesia Oleh Polri*, Makalah pada Seminar Nasional tentang "Penanganan Masalah *Cybercrime* di Indonesia dan Pengembangan Kebijakan Nasional yang Menyeluruh Terpadu", diselenggarakan oleh Deplu,BI, dan DEPKOMINFO, Jakarta, 10 Agustus 2006, hal.5.

informasi. Sebagaimana dikemukakan oleh Ronni R.Nitibaskara bahwa :[6] *"Interaksi sosial yang meminimalisir kehadiran secara fisik, merupakan ciri lain revolusi teknologi informasi. Dengan interaksi semacam ini, penyimpangan hubungan sosial berupa kejahatan (crime) akan menyesuaikan bentuknya dengan karakter tersebut."*

Sebagai contoh saat ini, bagi mereka yang senang akan perjudian dapat melakukannya dari rumah atau di kantor hanya dengan mengakses situs www.indobetonline.com atau www.tebaknomor.com dan banyak lagi situs sejenis yang menyediakan fasilitas tersebut dan memanfaatkan fasilitas *internet bangking* untuk pembayarannya tanpa harus bertemu secara fisik.

Dunia perbankan melalui *Internet* (*ebanking*) Indonesia, dikejutkan oleh ulah seseorang bernama Steven Haryanto, seorang *hacker* dan jurnalis pada majalah Master Web. Lelaki asal Bandung ini dengan sengaja membuat situs asli tapi palsu layanan *Internet* banking Bank Central Asia, (BCA). Steven membeli *domain-domain* dengan nama mirip www.klikbca.com (situs asli *Internet* banking BCA), yaitu *domain* wwwklik-bca.com, kilkbca.com, clikbca.com, klickca.com. dan klikbac.com. Isi situs-situs plesetan inipun nyaris sama, kecuali tidak adanya security untuk bertransaksi dan adanya formulir akses (*login form*) palsu. Jika nasabah BCA salah mengetik situs BCA asli maka nasabah tersebut masuk perangkap situs plesetan yang dibuat oleh Steven sehingga identitas pengguna (user id) dan nomor identitas personal (PIN) dapat di ketahuinya. Diperkirakan, 130 nasabah BCA tercuri datanya. Menurut pengakuan Steven pada situs bagi para *webmaster* di Indonesia, www.webmaster.or.id.[7]

Selain *carding*, masih banyak lagi kejahatan yang memanfaatkan *Internet*. Seorang hacker bernama Dani Hermansyah, pada tanggal 17 April 2004 melakukan *deface* (*Deface* disini

---

[6] Tubagus Ronny Rahman Nitibaskara,*Ketika Kejahatan Berdaulat: Sebuah Pendekatan Kriminologi, Hukum dan Sosiologi*,Peradaban, Jakarta,2001,hal.38.

[7] Majalah *CyberTECH* , dengan judul "Steven Haryanto" ,6 November 2002,hal.51.

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 diatas 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 dari 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.[8] Sejalan dengan istilah tersebut Barda Nawawi Arief menyatakan :[9] "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[10] 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. Permasalahan

---

[8] Penjelasan Undang-Undang No.11 tahun 2008 tentang Informasi dan Transaksi Elektronik, diundangkan pada 28 April 2008, Lembaran Negara No.58.

[9] Barda Nawawi Arief, *Sari Kuliah: Perbandingan Hukum Pidana,* PT.Raja Grafindo Persada, Jakarta,2006, hal.268

[10] Mas Wigrantoro Roes Setiyadi dan Mirna Dian Avanti Siregar, Naskah Akademik Rancangan Undang-Undang Tindak Pidana di Bidang Teknologi Informasi,,November,2003.hal.25,dalam <http//www.gipi.or.id> di akses tanggal 13 Mei 2008.

hukum yang seringkali dihadapi adalah ketika terkait dengan penyampaian informasi, komunikasi, dan/atau transaksi secara elektronik, khususnya dalam hal pembuktian dan hal yang terkait dengan perbuatan hukum yang dilaksanakan melalui sistem elektronik.

Kejahatan dalam bidang Teknologi Informasi secara umum terdiri dari dua kelompok. Pertama, kejahatan biasa yang menggunakan Teknologi Informasi sebagai alat bantunya. Dalam kejahatan ini, terjadi peningkatan modus dan operandi dari semula menggunakan peralatan biasa, sekarang telah memanfaatkan Teknologi Informasi. Dampak dari kejahatan biasa yang telah menggunakan Teknologi Informasi ternyata cukup serius, terutama bila dilihat dari jangkauan dan nilai kerugian yang ditimbulkan oleh kejahatan tersebut. Pencurian uang atau pembelian barang menggunakan kartu kredit curian melalui media *Internet* dapat menelan korban di wilayah hukum negara lain, suatu hal yang jarang terjadi dalam kejahatan konvensional.

Kelompok kedua, kejahatan yang muncul setelah adanya *Internet*, di mana sistem komputer sebagai korbannya. Jenis kejahatan dalam kelompok ini makin bertambah seiring dengan kemajuan teknologi informasi itu sendiri. Salah satu contoh yang termasuk dalam kejahatan kelompok kedua adalah perusakan situs *Internet*, pengiriman virus atau program – program komputer yang tujuannya merusak sistem kerja komputer tujuan.

Indonesia saat ini merupakan salah satu negara yang telah terlibat dalam penggunaan dan pemanfaatan teknologi informasi, yang dibuktikan juga dengan sebanyak 20 juta pengguna *internet* pada tahun 2007, banyaknya pengguna *internet* dalam pengertian positif disamping banyaknya juga penyalahgunaan *internet* itu sendiri. Sesuai dengan catatan Asosiasi Penyelenggaraan Jasa *Internet* Indonesia, kejahatan dunia *cyber* hingga pertengahan 2006 mencapai 27.804 kasus. Itu meliputi *spam* (penyalahgunaan jaringan teknologi informasi), *open proxy* (memanfaatkan kelemahan jaringan) dan *carding* (menggunakan kartu kredit orang lain

untuk memesan barang secara *on line*) yang memiliki urutan ke dua di dunia setelah Ukraina. Data dari Asosiasi Kartu Kredit Indonesia (AKKI) menunjukkan, sejak tahun 2003 hingga kini, angka kerugian akibat kejahatan kartu kredit mencapai Rp. 30 Milyar per tahun.[11]

Sehubungan dengan tindak pidana di dunia maya yang terus berkembang, 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 konsumen, 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. Pada saat seminar dan sosialisasi Undang-Undang Informasi dan Transaksi Elektronik yang diadakan BEM Fasikom Universitas Indonesia[13] , beberapa masalah yang diangkat oleh para peserta seminar seperti pasal tentang penghinaan dan pencemaran nama baik yang dianggap membelenggu kebebasan berekspresi,

---

[11] Majalah Gatra No.23 Tahun XIV17-23 April 2008,hal.91

[12] Undang-Undang No.11 tahun 2008 tentang inforamsi dan Transaksi Elektronik, Diundangakan tanggal 28 April 2008, Lembaran Negara No.58.

[13] Diakses dari http://www.detik.com pada tanggal 20 Mei 2008.

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. [14]

Menurut Barda Nawawi Arief (BNA) 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 dari 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

[14] Naskah Akademik Rancangan Undang-Undang Tentang Informasi dan Transaksi Elektronik, Departemen Komunikasi dan Informatika Republik Indonesia,2006,hal.3.

itu disusun dalam satu kesatuan sistem hukum pidana (kebijakan legislatif) yang harmonis dan terpadu.[15]

Kebijakan penanggulangan *cybercrime* secara teknologi, diungkapkan juga dalam IIIC (*Internatonal Information Industry Congress*) yang menyatakan :[16]

> *The IIIC recongnizes that goverment action and international traties to harmonize laws and coordinate legal procedures are key in the fight against cybercrime, but warns that these should not be relied upon as the only instuments. Cybercrime is enabled by technology and requires a healty reliance on technology for its solution.*

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*).

---

[15] Barda Nawawi Arief, *Kapita Selekta Hukum Pidana*, PT.Citra Aditya Bakti, Bandung,2003,hal.259.

[16] ITAC,*" IIIC Common Views Paper On: Cybercrime"*, IIIC 2000 Millenium congress, September 19th, 2000, hal.5. Lihat dalam Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*, Kencana Prenada Media Group, Jakarta, 2007 ,hal.240.

B. Permasalahan

Berdasarkan latar belakang tersebut diatas maka permasalahan yang akan diteliti dapat dirumuskan sebagai berikut :

1. Bagaimana kebijakan formulasi hukum pidana terhadap tindak pidana teknologi informasi saat ini ?
2. Bagaimana kebijakan aplikatif yang dilakukan oleh aparat penegak hukum dalam upaya penanggulangan tindak pidana teknologi informasi ?
3. Bagaimana sebaiknya kebijakan formulasi dan kebijakan aplikatif hukum pidana dalam penanggulangan tindak pidana teknologi informasi di masa yang akan datang?

C.Tujuan Penelitian

Bertitik tolak pada permasalahan-permasalahan di atas, penelitian ini bertujuan untuk :

1. Mengetahui dan memahami kebijakan formulasi hukum pidana terhadap tindak pidana teknologi informasi saat ini.
2. Mengetahui kebijakan aplikatif yang dilakukan oleh aparat penegak hukum dalam upaya penanggulangan tindak pidana teknologi informasi .
3. Menggambarkan dan menganalisa kebijakan formulasi dan kebijakan aplikatif hukum pidana dalam menanggulangi tindak pidana teknologi informasi di masa yang akan datang.

D. Kontribusi Penelitian

Penelitian ini diharapkan dapat memberikan kontribusi berupa :

1. Kontribusi Teoritis

- Penelitian ini diharapkan dapat memberikan gambaran dan menambah pengetahuan mengenai tindak pidana teknologi informasi .
- Memberikan sumbangan pemikiran kepada pihak-pihak terkait dengan upaya pembaharuan hukum pidana di era teknologi informasi.

2. Kontribusi Praktis
   - Hasil penelitian ini diharapkan dapat memberikan informasi yang berupa bahan pertimbangan dalam menentukan kebijakan (pembuat atau *policy*) yang dipakai dalam penegakan hukum khususnya yang berkaitan dengan pembuatan maupun penyempurnaan peraturan dan kebijakan-kebijakan mengenai tindak pidana teknologi informasi di Indonesia.
   - Penelitian ini diharapkan dapat dipergunakan sebagai sumbangan pemikiran mengenai tindak pidana teknologi informasi karena hukum pidana bukan semata untuk meminimalisir kejahatan dan perilaku jahat lainnya, namun lebih luas juga untuk menciptakan kesejahteraan masyarakat.

E. Kerangka Pemikiran

Hukum merupakan suatu kebutuhan masyarakat sehingga ia bekerja dengan cara memberikan petunjuk tingkah laku kepada manusia dalam memenuhi kebutuhannya. Ia merupakan pencerminan kehendak manusia tentang bagaimana seharusnya masyarakat itu dibina dan kemana harus diarahkan. Arah dan pembinaan hukum secara garis besar meliputi pencapaian suatu masyarakat yang tertib dan damai, mewujudkan keadilan, serta untuk mendatangkan kemakmuran dan kebahagian atau kesejahteraan.

Kebijakan sosial (*social policy*) bertujuan untuk kesejahteraan sosial (*sosial welfare policy*) dan untuk perlindungan masyarakat (*social defence policy*). Sebagaimana yang tertulis di dalam Deklarasi No.3 Caracas yang dihasilkan oleh Kongres PBB ke-6 tahun 1980 :[17]

> *It is matter of great importance and priority that programmes for crime preventoin and the treatment of offenders should be based on the social, cultural, political and economic circumstances of each country, in a climate of freedom and respect for human right, and that member states should develop and effective capacity for formulation and planning of criminal policy, co-ordinated with strategies for social, economic, political and cultural development.*

Bertolak dari Kongres PBB di atas maka kebijakan sosial dan kebijakan pembangunan terkait politik hukum dari masing-masing negara. Politik hukum mengandung penentuan pilihan atau pengambilan sikap terhadap tujuan-tujuan yang dianggap paling baik termasuk di dalamnya usaha-usaha untuk mencapai tujuan-tujuan tersebut. Banyak sarjana hukum yang memberikan pengertian tentang politik hukum. Masing-masing sarjana memberikan pengertian bergantung pada sudut pandangnya masing-masing yang tentunya sangat dipengaruhi oleh latar belakang keilmuannya.

Mahfud yang mempelajari mengenai politik hukum di Indonesia menjelaskan ”*Definisi politik hukum juga bervariasi, namun dengan menyakini adanya persamaan substantif antar berbagai pengertian yang ada*. Politik hukum menurut Mahfud sebagai *legal policy* yang akan atau telah dilaksanakan secara nasional oleh pemerintah Indonesia yang meliputi:[18]

a. Pembangunan hukum yang berintikan pembuatan dan pembaharuan terhadap materi-materi hukum agar dapat sesuai dengan kebutuhan;
b. Pelaksanaan ketentuan hukum yang telah ada termasuk penegasan fungsi lembaga dan pembinaan para penegak hukum.

Dari pengertian politik hukum dari Mahfud di atas terlihat politik hukum mencakup proses pembuatan dan pelaksanaan hukum yang dapat menunjukkan sifat dan ke arah mana

---

[17] Laporan Kongres PBB ke-6,tahun 1981,lihat dalam Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana*, PT. Citra Aditya Bakti, Bandung, 2005, hal.5.

[18] Moh.Mahfud,MD,*Pergulatan Politik dan Hukum di Indonesia*, Gama Media, Yogyakarta,1999,hal.9.

hukum akan dibangun dan ditegakkan agar memenuhi kebutuhan hidup masyarakat. Definisi politik hukum menurut Bellefroid dalam bukunya yang berjudul *"Inleideg tot de Rechtswetenshap in Nederland* (Pengantar Ilmu Hukum di Nederland) mengutarakan :[19]

> Politik hukum merupakan salah satu cabang (bagian) dari ilmu hukum, yang menyatakan politik hukum bertugas untuk meneliti perubahan-perubahan mana yang perlu diadakan, terhadap hukum yang ada agar memenuhi kebutuhan-kebutuhan baru di dalam kehidupan masyarakat. Politik hukum tersebut merumuskan arah perkembangan tertib hukum, dari *"jus constitutum"* yang telah ditentukan oleh kerangka landasan hukum yang dahulu, maka politik hukum berusaha untuk menyusun *"jus constituendum"* atau hukum pada masa yang akan datang.

Mengacu pada dua pendapat di atas, maka pengertian politik hukum difahami sebagai suatu kajian terhadap perubahan yang harus dilakukan dalam hukum yang berlaku *"ius constitutum"* agar dapat memenuhi kebutuhan kehidupan masyarakat pada masa yang akan datang *"ius constituendum"*. Dengan demikian politik hukum mengandung arti, bagaimana mengusahakan atau membuat dan merumuskan suatu perundang-undangan yang baik.

Upaya penanggulangan kejahatan secara garis besar dapat dibagi 2 (dua), yaitu lewat jalur "*penal*" (hukum pidana) dan lewat jalur "*non-penal*" (bukan/diluar hukum pidana).[20] Penerapan hukum pidana (*criminal law application*) tidak terlepas dari adanya peraturan perundang-undangan pidana, menurut Sudarto[21] usaha mewujudkan peraturan perundang-undangan pidana yang sesuai dengan keadaan dan situasi pada suatu waktu dan untuk masa-masa yang akan datang berarti melaksanakan politik hukum pidana.

Politik hukum pidana dalam kepustakaan asing sering dikenal dengan *"penal policy"*. *Penal policy* menurut Marc Ancel,[22] adalah upaya menanggulangi kejahatan dengan pemberian

---

[19] Bellefroid, *Inleidag tot de Rechtswetenschap in Nederland*, 1953.pg.17.Lihat dalam Moempoeni Martojo, *Politik Hukum dalam Sketsa*, Fakultas Hukum Undip, Semarang, 2000.hal.35.

[20] Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana*, *Op.Cit*.hal.42

[21] Sudarto,Hukum dan Hukum Pidana, Penerbit Alumni, ,Bandung , 1977,hal.38.

[22] *Ibid.*

sanksi pidana atau *penal*. sebagai *"suatu ilmu sekaligus seni yang bertujuan untuk memungkinkan peraturan positif dirumuskan secara lebih baik*".

Kebijakan hukum dengan sarana *"penal"* (pidana) merupakan serangkaian proses yang terdiri atas tiga tahap yakni:[23]

a. Tahap kebijakan legislatif/formulatif;

b. Tahap kebijakan yudikatif/aplikatif;

c. Tahap kebijakan eksekutif/administratif.

Tahapan formulasi dalam proses penanggulangan kejahatan memberikan tanggung jawab kepada aparat pembuat hukum (aparat legislatif) menetapkan atau merumuskan perbuatan apa yang dapat dipidana disusun dalam satu kesatuan sistem hukum pidana (kebijakan legislatif) yang harmonis dan terpadu.

Berkaitan dengan peran legislatif tersebut Nyoman Serikat Putra Jaya,[24] menyatakan lembaga legislatif berpartisipasi dalam menyiapkan kebijakan dan memberikan kerangka hukum untuk memformulasikan kebijakan dan menerapkan program kebijakan yang telah diterapkan. Keselurahannya itu, merupakan bagian dari kebijakan hukum atau politik hukum yang pada hakikatnya berfungsi dalam tiga bentuk, ialah:

1. Politik tentang pembentukan hukum ;
2. Politik tentang penegakan hukum:dan
3. Politik tentang pelaksanaan kewenangan dan kompetensi.

Walaupun ada keterkaitan erat antara kebijakan formulasi/legislasi (*legislative policy* khususnya *penal policy*) dengan *law enforcement policy* dan *criminal policy*, namun dilihat

---

[23] Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*, *Op.Cit* ,hal.78-79.

[24] Nyoman Serikat Putra Jaya, *Bahan Kuliah Sistem Peradilan Pidana*, Program Magister Ilmu Hukum, Undip,2006,Hal.13.

secara konseptual/teoritis dan dari sudut realitas, kebijakan penanggulangan kejahatan tidak dapat dilakukan semata-mata hanya dengan memperbaiki/memperbaharui sarana undang-undang (*law reform* termasuk *criminal law/penal reform*). Namun evaluasi tetap diperlukan sekiranya ada kelemahan kebijakan formulasi dalam perundang-undangan yang ada. Evaluasi terhadap kebijakan formulasi mencakup tiga masalah pokok dalam hukum pidana yaitu masalah perumusan tindak pidana (kriminalisasi), pertanggungjawaban pidana, dan aturan pidana dan pemidanaan.[25]

Kriminalisasi terhadap perbuatan dunia mayantara muncul ketika dihadapkan pada suatu perbuatan yang merugikan orang lain atau masyarakat yang sebelumnya belum diatur oleh hukum pidana. Hukum selalu berkembang dan semakin diperluas untuk mencakup situasi atau perubahan teknologi informasi yang terus berkembang dalam kehidupan masyarakat, perubahan hukum akan menuntut masyarakat dunia maya untuk menyesuaikan dengan hukum yang baru tersebut. Akan tetapi pada kenyataannya hukum sendiri belum dapat mengatasi secara riil terhadap permasalahan-permasalahan yang ditimbulkan oleh teknologi khususnya teknologi informasi. Salah satu bukti konkretnya adalah timbulnya berbagai kejahatan di dunia virtual yang ternyata belum bisa diatasi sepenuhnya oleh hukum.

Dalam perspektif lain, teknologi informasi menjadi mungkin dalam formatnya saat ini karena difasilitasi oleh komputer yang didalamnya terdapat dua komponen pokok yaitu perangkat keras (*hardware*) dan perangkat lunak *(software)*. Wujud *hardware* berupa antara lain namun tidak terbatas pada :personal komputer,komputer mini dan *mainframe, note book, palmtop*, printer, modem, dan lain sebagainya. Adapun *software* antara lain terdiri dari

[25] Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan, Op.Cit* ,hal.214-215.

kelompok: sistem operasi, data base, sistem aplikasi, dan bahasa pemrogaman (*progamming language*).[26]

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.[27]

Pada tahun 1986 *The Organization for Economic Co-operation and Development* (OECD) telah membuat *guidelines* bagi para pembuat kebijakan yang berhubungan dengan *computer related crime* , dimana OECD telah mempublikasikan laporannya yang berjudul "*computer related crime: analysis of legal policy*". Laporan ini berisi hasil survei terhadap peraturan perundang-undangan negara-negara anggota beserta rekomendasi perubahannya dalam menanggulangi *computer related crime* tersebut, yang mana diakui bahwa sistem telekomunikasi juga memiliki peran penting didalam kejahatan tersebut.[28]

Melengkapi laporan OECD, *The Council of Europe* (CE) berinisiatif melakukan studi mengenai kejahatan tersebut. Studi ini memeberikan *guidelines* lanjutan bagi para pengambil kebijakan untuk menentukan tindakan-tindakan apa yang seharusnya dilarang berdasarkan hukum pidana negara-negara anggota dengan tetap memperhatikan keseimbangan antara hak-hak

---

[26] Pasal 1 huruf 3 Undang-Undang No.11 tahun 2008 tentang Informasi dan Transaksi Elektronik dan lihat juga dalam penjelasan Undang-Undang No.11 tahun 2008 tentang Informasi dan Transaksi Elektronik.

[27] Naskah akademik RUU tindak pidana di bidang Teknologi Informasi disusun oleh Mas Wigantoro Roes Setiyadi , Cyber Policy Club dan Indonesia Media Law and Policy Center,2003.

[28] Ari Juliano Gema, *Cybercrime: Sebuah Fenomena di Dunia Maya*, www.bisnisindonesia.com ,hal.8. Diakses pada tanggal 20 Mei 2008.

sipil warga negara dan kebutuhan untuk melakukan proteksi terhadap *computer related crime* tersebut. Pada perkembangannya, CE membentuk *Committee of Experts on Crime ini Cyber space of The Committee on Crime problem*, yang pada tanggal 25 April 2000 telah mempublikasikan draft *Convension on Cybercrime* sebagai hasil kerjanya, yang menurut Susan Brenner dari University of Daytona *School of Law*, merupakan perjanjian internasional pertama yang mengatur hukum pidana dan aspek proseduralnya untuk berbagai tipe tindak pidana yang berkaitan erat dengan penggunaan komputer, jaringan atau data, serta berbagai penyalahgunaan sejenis.[29]

Negara-negara yang tergabung dalam Uni Eropa pada tanggal 23 Nopember 2001 di kota Budapest, Hongaria telah membuat dan menyepakati *Convention on Cybercrime* yang kemudian dimasukkan dalam *European Treaty Series* dengan Nomor.185. Konvensi ini akan berlaku secara efektif setelah diratifikasi oleh minimal 5 (lima) negara, termasuk diratifikasi oleh 3 (tiga) negara anggota *Council of Europe*. Substansi konvensi mencakup area yang cukup luas, bahkan mengandung kebijakan kriminal (*criminal policy*) yang bertujan untuk melindungi masyarakat dan *cybercrime*, baik melalui undang-undang maupun kerja sama internasional.[30]

Berkaitan dengan kebijakan kriminalisasi terhadap perbuatan yang masuk dalam kategori tindak pidana teknologi informasi telah dibahas secara khusus dalam kongres PBB mengenai *The Prevention of Crime and The Treatment of Offender* ke-8 tahun 1990 di Havana (Cuba), yang memandang perlu dilakukan usaha-usaha penanggulangan kejahatan yang berkaitan dengan komputer (*computer related crimes*).Dalam lokakarya *workshop on crimes to computer*

---

[29] Ari Juliano Gema, *Cybercrime: Sebuah Fenomena di Dunia Maya*, www.bisnisindonesia.com ,hal.8. Diakses pada tanggal 20 Mei 2008.

[30] *EU Convention on Cybercrime*, lihat dalam Naskah Akademik Undang-Undang Informasi dan Transaksi Elektronik, hal.28.

networks yang diorganisir oleh UNAFEI selama kongres PBB X di Wina pada bulan April 2000 yang menghasilkan :[31]

b. CRC (*computer-related crime*) harus dikriminalisasikan ;
c. Diperlukan hukum acara yang tepat untuk melakukan penyidikan dan penuntutan terhadap penjahat *cyber* ;
d. Harus ada kerjasama antara pemerintah dan industri terhadap tujuan umum pencegahan dan penanggulangan kejahatan komputer agar *internet* menjadi tempat yang aman ;
e. Diperlukan kerjasama internasional untuk menelusuri/mencari para penjahat di *internet* ;
f. PBB harus mengambil langkah/tindak lanjut yang berhubungan dengan bantuan dan kerjasama teknis dalam penanggulangan CRC.

Walaupun kongres PBB tersebut telah menghimbau negara anggota untuk menanggulangi *cybercrime* dengan sarana *penal*, namun kenyataannya tidaklah mudah. Dokumen kongres tersebut mengakui bahwa ada beberapa kesulitan untuk menanggulangi *cybercrime* dengan sarana *penal*, antara lain :[32]

a. Perbuatan kejahatan yang dilakukan berada di lingkungan elektronik. Oleh karena itu, penanggulangan *cybercrime* memerlukan keahlian khusus, prosedur investigasi dan kekuatan/dasar hukum yang mungkin tidak tersedia pada aparat penegak hukum di negara yang bersangkutan.
b. *Cybercrime* melampaui batas-batas negara, sedangkan upaya penyidikan dan penegakan hukum selama ini dibatasi dalam wilayah teritorial negaranya sendiri.
c. Struktur terbuka dari jaringan komputer internasional memberikan peluang kepada pengguna untuk memilih lingkungan hukum (negara) yang belum mengkriminalisasikan *cybercrime*. Terjadinya data *havens* (negara tempat berlindung atau singgahnya data, yaitu negara yang tidak memprioritaskan pencegahan penyalahgunaan jaringan komputer) dapat menghambat usaha negara lain untuk memberantas kejahatan itu.

Permasalahan penegakan hukum di dunia virtual/maya, yurisdiksi dan hukum yang berlaku terhadap suatu sengketa multi-yurisdiksi akan bertambah penting dan kompleks. Hal ini

---

[31] Dokumen kongres PBB X,A/CONF.187/L.10, tgl 16 April 2000, "*Report of Commeitte II*" Mengenai "*Workswhop on Crimes Related to The Computer Network*",yang kemudian dimasukkan dalam "*Report of the Tenth United Nations Congrss on the Prevention of Crime and the Treatment of Offenders*", A/CONF.187/15,tgl 19 Juli 2000,paragraf 161-174, Dikutip dari Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*, Op.Cit, hal.241-242

[32] Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan, Op.Cit*, hal.243-244.

penting untuk diperhatikan mengingat seringkali disatu sisi kewenangan aparat penegak hukum dalam melakukan penegakan hukum dibatasi oleh wilayah suatu negara yang berdaulat penuh sebagai batas dari yurisdiksi hukum yang dimilikinya, disisi lain para pelaku kejahatan dapat bergerak bebas melewati batas negara selama dilengkapi dokumen keimigrasian yang memadai, akibatnya sangat sulit bagi negara untuk mengungkap sekaligus menangkap pelaku kejahatan tersebut.

Yurisdiksi adalah kekuasaan atau kompetensi hukum negara terhadap orang, benda atau peristiwa (hukum).Yurisdiksi ini merupakan refleksi dari prinsip dasar kedaulatan negara, kesamaan derajat negara dan prinsip tidak campur tangan. Yurisdiksi juga merupakan suatu bentuk kedaulatan yang vital dan sentral yang dapat mengubah, menciptakan atau mengakhiri suatu hubungan kewajiban hukum.[33]

Berdasarkan asas hukum umum dalam hukum internasional, setiap negara memiliki kekuasaan tertinggi atau kedaulatan atas orang dan benda yang ada dalam wilayahnya sendiri. Oleh karena itu, suatu negara tidak boleh melakukan tindakan yang bersifat melampaui kedaulatannya (*act of sovereignty*) di dalam wilayah negara lain, kecuali dengan persetujuan negara itu sendiri. Sebab tindakan demikian itu dipandang sebagai intervensi atau campur tangan atas masalah-masalah dalam negeri lain, yang dilarang menurut hukum internasional.[34]

Yurisdiksi suatu negara yang diakui Hukum Internasional dalam pengertian konvensional, didasarkan pada batas-batas geografis, sementara komunikasi multimedia bersifat internasional, multi yurisdiksi, tanpa batas, sehingga sampai saat ini belum dapat dipastikan

---

[33] Shaw, *Internatonal law*, London: Butterworths,1986,hal.342, sebagaimana dikutip oleh Didik M.Arif Mansur dan Alistaris Gultom, , *Cyber Law;Aspek Hukum Teknologi Informasi*, Refika Aditama,Bandung,2005,hal.30.

[34] I Wayan Parthina, *Ekstradisi dalam Hukum Internasional dan Hukum Nasional Indonesia*, Mandar Maju, Bandung, 1990,hal.10-11.

bagaimana yurisdiksi suatu negara dapat diberlakukan terhadap komunikasi multimedia sebagai salah satu pemanfaatan teknologi informasi.[35]

Terkait dengan yurisdiksi dan digunakan sarana *penal* oleh satu negara (yang melakukan kriminalisasi dengan menggunakan perundang-undangan pidana), bukan berarti *cybercrime* dapat tertanggulangi. Karena masalahnya bukan sekedar bagaimana membuat kebijakan hukum pidana yaitu kebijakan legislasi atau formulasi atau kriminalisai. Namun sebagaimana dikemukakan oleh Barda Nawawi Arief [36] bahwa perlu ada harmonisasi, kesepakatan, dan kerjasama antar negara mengenai yurisdiksi serta kebijakan *penal* (hukum pidana) dalam penanggulangan *cybercrime* diberbagai negara.

F. Metode Penelitian

1. Metode Pendekatan

Kajian penelitian ini bersifat yuridis normatif sebagai pendekatan utama, mengingat pembahasan didasarkan pada peraturan perundang-undangan dan prinsip hukum yang berlaku dalam masalah tindak pidana teknologi informasi. Pendekatan yuridis dimasudkan untuk melakukan pengkajian terhadap bidang hukum, khususnya hukum pidana.

Pendekatan yuridis komparatif juga dilakukan untuk melakukan perbandingan dengan negara-negara yang sudah mempunyai peraturan perundang-undangan (*statute approach*) dan pendekatan konsepsi (*conceptual approach*) tentang tindak pidana teknologi informasi. Perbandingan dilakukan dengan negara-negara yang telah memiliki pengaturan terhadap tindak pidana teknologi informasi untuk mencari kesempurnaan pembuatan perundang-undangan di Indonesia.

2. Spesifikasi Penelitian

---

[35] Tien S, Saefulah, Jurisdiksi sebagai Upaya Penegakan Hukum dalam Kegiatan *Cyberspace*, artikel dalam Cyberlaw: Suatu Pengantar, Pusat Studi Cyber Law Fakultas Hukum UNPAD,ELIPS,2002,hal.96.

[36] Barda Nawawi Arief, , *Tindak Pidana Mayantara*, Raja Grafindo Persada, Jakarta, 2006,hal. 10-11.

Sifat dari penelitian ini adalah deskriptif analitis yang mana melalui penelitian ini akan diperoleh gambaran utuh dan menyeluruh perihal kebijakan penanggulangan tindak pidana teknologi informasi melalui hukum pidana yang pada akhirnya akan ditemukan solusi dalam kesempurnaan kebijakan penanggulangan tindak pidana tersebut di Indonesia.

3. Jenis dan Sumber Data

Dalam penelitian yang menggunakan pendekatan yuridis, dilihat dari cara memperoleh dan mengumpulkan data dibedakan ke dalam 2 (dua) macam yaitu data primer dan data sekunder.[37]

Data sekunder berupa kepustakaan baik berupa tulisan atau pendapat sarjana yang sesuai dan terkait dengan permasalahan dan berguna untuk analisa tesis ini. Penelitian kepustakaan ini mencakup : (1) penelitian terhadap asas-asas hukum; (2) penelitian terhadap sistematika hukum; (3) penelitian terhadap taraf sinkronisasi vertikal dan horizontal; (4) perbandingan hukum; dan (5) sejarah hukum.[38]

4. Metode Pengumpulan Data

Mengingat penelitian ini memusatkan perhatian pada data sekunder, maka pengumpulan data terutama ditempuh dengan penelitian kepustakaan dan studi dokumen. Penelitian kepustakaan dilakukan dengan tahapan: Melakukan inventarisasi terhadap peraturan perundang-undangan; Melakukan penggalian berbagai asas-asas dan konsep-konsep hukum yang relevan dengan permasalahan yang akan diteliti; Melakukan kategorisasi hukum dalam hubungannya dengan permasalahan yang diteliti.

---

[37] Rianto Adi, *Metode Penelitian Sosial dan Hukum*, PT Grafika, Jakarta, 2004, hal. 56.

[38] Soerjono Soekanto dan Sri Mamuji, *Penelitian Hukum Normatif 'Suatu Tinjauan Singkat'*, PT.. Raja Grafindo Persada, Jakarta, 2004, hal 14.

Penelitian dokumen ini diperlukan untuk memperjelas informasi yang telah diperoleh dan mencari tambahan informasi yang diperlukan melalui sumber lain.[39] Hal tersebut dilakukan dengan cara mencari dan mengumpulkan data-data baik yang bersifat primer maupun sekunder yang berkenaan dengan kebijakan penanggulangan tindak pidana teknologi informasi melalui hukum pidana. Disamping itu juga dilengkapi dengan studi lapangan di Bareskrim Mabes Polri, Kejaksaan Negri Jakarta Selatan dan Mahkamah Agung serta terhadap aparat penegak hukum dan ahli hukum yang memiliki perhatian terhadap kejahatan teknologi informasi .

5. Metode Analisis Data

Analisis data adalah suatu proses untuk mengorganisasikan dan meletakkan data menurut pola atau kategori dan satuan uraian dasar sehingga peneliti dapat mengadakan evaluasi dan menyeleksi terhadap data yang relevan atau tidak relevan. Dalam penelitian ini penulis menggunakan analisis deskriptif terhadap data kualitatif yang pada dasarnya menggunakan pemikiran secara logis dengan induksi, deduksi, komparasi dan interprestasi.[40]

G. Sistematika Penulisan

Sistematika penulisan thesis ini secara sistematis akan disusun ke dalam 4 (empat) bab yang mana masing-masing bab terdiri dari beberapa sub-bab .

Setelah uraian PENDAHULUAN dalam BAB I yang memuat latar belakang, perumusan masalah, metode penelitian, dan sistematika penulisannya, maka selanjutnya dalam BAB II dikemukakan TINJAUAN PUSTAKA yang membahas mengenai Kebijakan penanggulangan kejahatan melalui hukum pidana dan mengenai masalah tindak pidana teknologi informasi.

BAB III. HASIL PENELITIAN DAN ANALISIS. Bab ini membahas penelitian dan pembahasan terhadap permasalahan-permasalahan yang diangkat, meliputi : Kebijakan formulasi

---

[39] Farouk Muhammad Dan H. Djaali, *Metodologi Penelitian Sosial (Bunga Rampai*), Penerbit PTIK Press, Jakarta, 2003, hal.110.

[40] Rianto Adi,*op.cit.*,hal. 73.

hukum pidana terhadap tindak pidana teknologi informasi saat ini; kebijakan penegakan hukum (kebijakan aplikatif) yang dilakukan oleh aparat penegak hukum dalam upaya penanggulangan tindak pidana teknologi informasi, dan kebijakan formulasi dan kebijakan aplikatif hukum pidana dalam menanggulangi tindak pidana teknologi informasi masa yang akan datang.

BAB IV. PENUTUP dalam bab ini penulis memberikan kesimpulan dari hasil penelitian dan pembahasan serta memberikan saran-saran yang sifatnya operasional.

BAB II

TINJAUAN PUSTAKA

A. KEBIJAKAN PENANGGULANGAN KEJAHATAN MELALUI HUKUM PIDANA.

A.1 Pengertian dan Landasan Pemahaman Kebijakan Penanggulangan Kejahatan.

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 dibidang hukum, yang dikenal dengan istilah pembaharuan hukum (*law reform*). Pembaharuan hukum nasional sebagai bagian dari 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 dari 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 dari keduanya tidak selalu bertemu *(converge)* bahkan seringkali tidak sama dan sebangun *(incongruent)*.

Istilah kebijakan berasal dari bahasa Inggris *policy* atau dalam bahasa Belanda *politie*. *Black's Law Dictionary* mengidentifikasikan *Policy* sebagai:

> *The general principles by which a government is guided in its management of public afairs, ...or principles and standard regarded by the ligislature or by the*

courts as being of fundamental concern to the state and the whole of society in measures, as applied to a law, ordinance, or rule of law, denotes its general purpose or tendency considered as directed to the welfare or prosperity of the state comunity. [81]

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).[82]

Upaya perlindungan masyarakat (*social defence*) dan upaya mencapai kesejahteraan masyarakat (*social welfare*) pada hakikatnya merupakan bagian integral dari kebijakan atau upaya penanggulangan kejahatan .[83] Kongres PBB ke-4 mengenai *Prevention of Crime and The Treatment of Offender* tahun 1970 yang tema sentralnya membicarakan masalah "*Crime and Development*" menegaskan keterpaduan tersebut: *"any dichotomy between a country's policies for social defence and its planning for national development was unreal by defenitions"*.[84]

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*

---

[81] Henry Campbell Black,"*Black's Law Dictionary", Seventh Edition*, St.Paulmin West Publicing,Co.,1999,hal.117

[82] Wisnusubroto, *Kebijakan Hukum Pidana dalam Penanggulangan Penyalahgunaan Komputer* Universitas Atmajaya, Yogyakarta, 1999,hal. 3.

[83] Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana*, *Op.Cit*.hal.2.

[84] Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana*, *Op.Cit*.hal.5.

policy should be coordinated and the whole should be integrated into a general social policy of each country."[85]

Kebijakan penanggulangan kejahatan atau yang biasa dikenal dengan istilah "politik kriminal" menurut Sudarto merupakan suatu usaha yang rasional dari masyarakat dalam menanggulangi kejahatan.[86] Definisi ini diambil dari definisi Marc Ancel yang merumuskan politik kriminal sebagai "*the rational organization of the control of crime by society*".[87]

Tujuan penanggulanggan kejahatan yaitu perlindungan masyarakat untuk mencapai kesejahteraan masyarakat. Perumusan tujuan dari politik kriminal yang demikian dinyatakan dalam salah satu laporan kursus latihan ke-34 yang diselenggarakan oleh UNAFEI di Tokyo tahun 1973 sebagai berikut:[88]

> *Most of group members agreed some discussion that "protection of the society" could be accepted as the final goal of criminal policy, although not the ultimate aim of society, which might perhaps be described by terms like "happiness of citizens", "a wholesome and cultural living", "social welfare" or "equality".*

Kesepakatan dari hasil kursus tersebut dapat menjadi landasan dalam dalam kebijakan kriminal sebagai upaya penanggulangan kejahatan untuk kesejahteraan sosial (*sosial welfare)* dan untuk perlindungan masyarakat (*social defence*).

A.2 Upaya Penanggulangan Kejahatan melalui Hukum Pidana

---

[85] *Fifth UN Congres, Report*,1976,hal 4.Lihat dalam Nyoman Serikat Putra Jaya, *Beberapa Pemikiran ke Arah Pengembangan Hukum Pidana*, PT.Citra Aditya Bakti, Bandung, 2008, hal.190.

[86] Sudarto,*Hukum dan Hukum Pidana*, *Op.Cit*. ,hal.38.

[87] Marc Ancel, *Social Defence* (terjemahan dari *La Nouvelle Defence Sociale*),London, 1965,hal.209. Lihat dalam Sudarto, Hukum dan Hukum Pidana,*Op.Cit*,hal .38.

[88] *Summary Report, Resource Material Series* No.7,UNAFEI,1974,hal.95, lihat dalam Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana, Op.Cit*.hal.2.

Penggunaan hukum pidana dalam mengatur masyarakat (lewat peraturan perundang-undangan pidana) pada hakekatnya merupakan bagian dari suatu langkah kebijakan (*policy*). Selanjutnya untuk menentukan bagaimana suatu langkah (usaha) yang rasional dalam melakukan kebijakan tidak dapat pula dipisahkan dari tujuan kebijakan pembangunan itu sendiri secara integral. Dengan demikian dalam usaha untuk menentukan suatu kebijakan apapun (termasuk kebijakan hukum pidana) selalu terkait dan tidak terlepaskan dari tujuan pembangunan nasional itu sendiri yaitu bagaimana mewujudkan kesejahteraan bagi masyarakat.

Kebijakan penanggulangan kejahatan atau yang biasa dikenal dengan istilah ”politik kriminal” Menurut GP Hoefnagles dapat ditempuh dengan:[89]

a. Penerapan hukum pidana (*criminal law application*)
b. Pencegahan tanpa pidana (*prevention without punishment*)
c. Mempengaruhi pandangan masyarakat tentang kejahatan dan pemidanaan melalui mass media (*influencing views of society on crime and punishment*)

Untuk kategori pertama dikelompokkan ke dalam upaya penanggulangan kejahatan lewat jalur *penal*, sedangkan kedua dan ketiga termasuk upaya penanggulangan kejahatan melalui jalur *non penal*. Terhadap ke-2 (dua) sarana tersebut Muladi berpendapat:[90]

> Kebijakan kriminal adalah usaha rasional dan terorganisasi dari suatu masyarakat untuk menanggulangi kejahatan. Kebijakan kriminal di samping dapat dilakukan secara represif melalui sistem peradilan pidana (pendekatan *penal*) dapat pula dilakukan dengan sarana “*non penal*” melalui pelbagai usaha pencegahan tanpa harus menggunakan sistem peradilan pidana, misalnya usaha penyehatan mental masyarakat, penyuluhan hukum, pembaharuan hukum perdata dan hukum administrasi, dan sebagainya.

---

[89] Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana*, *Op.Cit*,hal.42

[90] Muladi, Demokratisasi,*Hak Asasi Manusia dan Reformasi Hukum di Indonesia*, The Habibie Center, Jakarta,2002, hal.182.

Pendekatan dengan cara *non penal* mencakup area pencegahan kejahatan (*crime prevention*) yang sangat luas dan mencakup baik kebijakan maupun praktek. Sarana *non penal* pada dasarnya merupakan tindakan preventif, mulai dari pendidikan kode etik sampai dengan pembaharuan hukum perdata dan hukum administrasi. Kebijakan tersebut bervariasi antara negara yang satu dengan negara yang lain sesuai dengan latar belakang kultural, politik dan intelektual yang ada pada masing-masing masyarakat.

Berbicara tentang kebijakan kriminal (*criminal policy*) yang mencakup pendekatan *penal* melalui sistem peradilan pidana, dengan sendirinya akan bersentuhan dengan kriminalisasi yang mengatur ruang lingkup perbuatan yang bersifat melawan hukum, pertanggungjawaban pidana, dan sanksi yang dapat dijatuhkan, baik berupa pidana (*punishment*) maupun tindakan (*treatment*).[91] Sarana kebijakan penanggulangan kejahatan dilakukan dengan menggunakan sarana *penal* (hukum pidana), maka ”kebijakan hukum pidana” (”*penal policy*”) harus memperhatikan dan mengarah pada tercapainya tujuan dari kebijakan sosial berupa *social welfare* dan *social defence.*[92]

Penanggulangan kejahatan harus ada keseimbangan antara sarana *penal* dan *non penal* (pendekatan integral) . Dilihat dari sudut politik kriminal, kebijakan paling strategis melalui sarana *non penal* karena lebih bersifat preventif.[93] Walaupun demikian kebijakan *penal* tetap diperlukan dalam penanggulangan kejahatan, karena hukum pidana merupakan salah satu sarana kebijakan sosial untuk menyalurkan ”ketidaksukaan masyarakat” (*social dislike*) atau pencelaan/kebencian sosial (*social disapproval/social*

---

[91] Muladi, *Hak Asasi Manusia dan Reformasi Hukum di Indonesia,* The Habibie Center, Jakarta,2002,hal.201.

[92] Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan, Op.Cit* ,hal.77.

[93] Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan, Op.Cit.*,hal.78.

abhorrence) yang sekaligus juga diharapkan menjadi sarana perlindungan sosial (*social defence*).[94]

Sarana *"penal"* merupakan *"penal policy"* atau *"penal law enforcement policy"* sangat vital perannya dalam proses penegakan hukum untuk menanggulangi kejahatan. Seminar kriminologi ke-3 tahun 1976 dalam salah satu kesimpulannya menyebutkan:

> Hukum pidana hendaknya dipertahankan sebagai salah satu sarana untuk *sosial defence* dalam arti melindungi masyarakat terhadap kejahatan dengan memperbaiki atau memulihkan kembali (*rehabilitatie*) si-pembuat tanpa mengurangi keseimbangan kepentingan perorangan (pembuat) dan masyarakat.[95]

Politik kriminal yang dilakukan dengan menggunakan sarana *penal* berarti penggunaan sistem peradilan pidana, mulai dari kriminalisasi sampai dengan pelaksanaan pidana. Pendekatan dengan sarana *penal* harus terus menerus dilakukan melalui pelbagai usaha untuk menyempurnakan sistem peradilan pidana, baik dari aspek legislasi (kriminalisasi, dekriminalisasi dan depenalisasi), perbaikan sarana-prasarana sistem, peningkatan kualitas sumber daya manusia, dan peningkatan partisipasi masyarakat dalam sistem peradilan pidana. Secara sistemik, sistem peradilan pidana ini mencakup suatu jaringan sistem peradilan (dengan sub sistem kepolisian, kejaksaan, pengadilan dan pemasyarakatan) yang mendayagunakan hukum pidana sebagai sarana utamanya. Hukum pidana dalam hal ini mencakup hukum pidana materiil, formil dan hukum pelaksanaan pidana.[96]

---

[94] Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan, Op.Cit*,hal.176

[95] Muladi dan Barda Nawawi Arief, *Teori-Teori dan Kebijakan Pidana*, Alumni, Bandung, 1998,hal.92.

[96] Muladi, Demokratisasi,*Hak Asasi Manusia dan Reformasi Hukum di Indonesia*, *Op.Cit*., hal.156 dan hal.182.

Operasionalisasi kebijakan hukum dengan sarana *"penal"* (pidana) dapat dilakukan melalui proses yang terdiri atas tiga tahap yakni:[97]

d. Tahap formulasi (kebijakan legislatif)

e. Tahap aplikasi (kebijakan yudikatif/yudisial)

f. Tahap eksekusi (kebijakan eksekutif/administratif).

Berdasarkan tiga uraian tahapan kebijakan penegakan hukum pidana tersebut terkandung didalamnya tiga kekuasaan/kewenangan, yaitu kekuasaan legislatif/formulatif berwenang dalam hal menetapkan atau merumuskan perbuatan apa yang dapat dipidana yang berorientasi pada permasalahan pokok dalam hukum pidana meliputi perbuatan yang bersifat melawan hukum, kesalahan/pertanggungjawaban pidana dan sanksi apa yang dapat dikenakan oleh pembuat undang-undang. Tahap aplikasi merupakan kekuasaan dalam hal menerapkan hukum pidana oleh aparat penegak hukum atau pengadilan dan tahapan eksekutif/administratif dalam melaksanakan hukum pidana oleh aparat pelaksana/eksekusi pidana.

A.2.1 Kebijakan Formulasi

Dilihat dari 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

---

[97] Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan, Op.Cit* ,hal.78-79.

Sebagaimana ditulis oleh Barda Nawawi Arief, [98] kebijakan formulasi merupakan tahapan yang paling strategis dari ”*penal policy*” karena pada tahapan tersebut legislatif berwenang dalam hal menetapkan atau merumuskan perbuatan apa yang dapat dipidana yang berorientasi pada permasalahan pokok hukum pidana meliputi perbuatan yang bersifat melawan hukum, kesalahan, pertanggungjawaban pidana dan saksi apa yang dapat dikenakan. Oleh karena itu upaya penanggulangan kejahatan bukan hanya tugas aparat penegak hukum tetapi juga tugas aparat pembuat undang-undang (aparat legislatif).

Perencanaan *(planning)* dalam penanggulangan kejahatan dengan sistem hukum pidana pada tahapan formulasi pada intinya menurut Nils Jareborg mencakup tiga masalah pokok struktur sistem hukum pidana, yaitu masalah:[99]

1. Perumusan tindak pidana/Kriminalisasi dan Pidana yang diancamkan *(criminalization and threatened punishment)*
2. Pemidanaan *(adjudication of punishment sentencing)*
3. Pelaksanaan pidana *(execution of punishment)*

Sejalan dengan hal di atas konsep rancangan KUHP baru disusun dengan bertolak pada 3 (tiga) materi/substansi/ masalah pokok dalam hukum pidana, yaitu:[100]

1. Masalah tindak pidana
2. Masalah kesalahan atau pertanggungjawaban pidana.
3. Masalah pidana dan pemidanaan.

---

[98] Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan, Op.Cit* ,hal.78-79.

[99] Nils Jareborg,”*The Coherence of the Penal System”, dalam Criminal Law in Action, Arnhem, page*.239, lihat dalam Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan, Op.Cit* ,hal.215.

[100] Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana, Op.Cit*.hal.77.

Semua hukum pidana materiil/substantif, hukum pidana formal dan hukum pelaksanaan pidana dapat dilihat sebagai satu kesatuan sistem pemidanaan (*the sentencing system*). L.H.C Hulsman mengemukakan pengertian sistem pemidanaan sebagai;[101] ”aturan perundang-undangan yang berhubungan dengan sanksi pidana dan pemidanaan” (*the statory rules relating to penal sanctions and punishment*).

Dari pengertian di atas Barda Nawawi Arief memberikan pengertian pemidanaan secara luas sebagai suatu proses pemberian atau penjatuhan pidana oleh hakim, maka dapatlah dikatakan bahwa sistem pemidanaan mencakup pengertian:[102]

- Keseluruhan sistem (aturan perundang-undangan) untuk pemidanaan;
- Keseluruhan sistem (aturan perundang-undangan) untuk pemberian/penjatuhan dan pelaksanaan pidana.
- Keseluruhan sistem (aturan perundang-undangan) untuk fungsionalisasi/operasionalisasi/konkretisasi pidana;
- Keseluruhan sistem (perundang-undangan) yang mengatur bagaimana hukum pidana itu ditegakkan atau dioperasionalisasikan secara konkret sehingga seseorang dijatuhi sanksi (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 :[103]

a. Penggunaan 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.

---

[101] L.H.C Hulsman. *The Dutch Criminal Justice System From A Comparative Legal Perspective*, lihat dalam Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana*, *Op.Cit*.hal.135.

[102] Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana*, *Op.Cit*.hal.136.

[103] Sudarto, *Hukum dan Hukum Pidana, Op.Cit.*, hal.23.

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 dari badan-badan penegak hukum yaitu jaringan sampai ada kelampauan beban tugas (*overbelasting*).

Berdasarkan pertimbangan di atas, dapat disimpulkan bahwa alasan kriminalisasi pada umumnya adalah:[104]

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 sentral 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 (*over-criminalization*), yang justru mengurangi wibawa hukum. Kriminalisasi dalam hukum

[104] Teguh Prasetyo dan Abdul Halim Barkatullah, *Politik Hukum Pidana: Kajian Kebijakan Kriminalisasi dan Dekriminalisasi*, Pustaka Pelajar, Yogyakarta, 2005,hal.51.

pidana materiil akan diikuti pula oleh langkah-langkah pragmatis dalam hukum pidana formil untuk kepentingan penyidikan dan penuntutan.[105]

A.2.2 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 dari Negara berdasarkan atas hukum.[106] Peran aparat penegak hukum dalam Negara berdasarkan hukum juga dinyatakan oleh Satjipto Rahardjo[107] yang menyatakan, *"hukum tidak memiliki fungsi apa-apa, bila tidak diterapkan atau ditegakkan bagi pelanggar hukum, yang menegakkan hukum dilapangan adalah aparat penegak hukum."*

Istilah penegakan dalam bahasa Inggris dikenal dengan istilah *enforcement* dalam *black law dictionary* diartikan *the act of putting something such as a law into effect, the execution of a law.* Sedangkan penegak hukum (*law enforcement officer*) artinya adalah *those whose duty it is to preserve the peace.*[108] Dalam kamus besar bahasa Indonesia,

---

[105] Muladi, *Kebijakan Kriminal terhadap Cybercrime*, Majalah Media Hukum, Vol.1 No.3 tanggal 22 Agustus 2003,hal.1

[106] Muladi, Kapita Selekta Sistem Peradilan Pidana, UNDIP,Semarang,1995,hal.25-26.

[107] Satjipto Rahardjo, Ilmu Hukum, PT.Citra Aditya Sakti, Bandung, 1991,hal.153.

[108] Henry Campbell Black,"*Black's Law Dictionary*",*Seventh Edition,St.Paulminn West Publicing*,C.O.,1999,hal.797.

penegak adalah yang mendirikan/menegakkan. Penegak hukum adalah yang menegakkan hukum,dalam arti sempit hanya berarti polisi dan jaksa.[109] Di Indonesia istilah ini diperluas sehingga mencakup pula hakim , pengacara dan lembaga permasyarakatan.[110]

Sudarto,[111] memberi arti penegakan hukum adalah perhatian dan penggarapan, baik perbuatan-perbuatan yang melawan hukum yang sungguh-sungguh terjadi (*onrecht in actu*) maupun perbuatan melawan hukum yang mungkin akan terjadi (*onrecht in potentie*). Sedangkan menurut Soerjono Soekanto,[112] secara konsepsional, maka inti dari penegakan hukum terletak pada kegiatan menyerasikan hubungan nilai-nilai yang terjabarkan di dalam kaidah-kaidah yang mantap dan mengejawantah dan sikap tindak sebagai rangkaian penjabaran nilai tahap akhir, untuk menciptakan, memelihara, dan mempertahankan kedamaian pergaulan hidup.

Sebagai bagian dari *social policy*, kebijakan penegakan hukum ini meliputi proses apa yang dinamakan sebagai kebijakan kriminal atau *criminal policy*. Konsepsi dari kebijakan penegakan hukum inilah yang nantinya akan diaplikasikan melalui tataran instutisional 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 dari Sistem Peradilan Pidana inilah yang nantinya akan melaksanakan kebijakan penegakan hukum berupa pencegahan dan penanggulangan terjadinya suatu kejahatan dimana peran-peran dari sub-sistem ini akan

---

[109] Anton M.Moelijono, (et.al).Kamus Besar Bahasa Indonesia, Balai Pustaka, Jakarta,1998, hal.912.

[110] Marjono Reksodiputro, *Kemajuan Pembangunan Ekonomi dan Kejahatan. Kumpulan karangan buku kesatu*, Pusat Pelayanan Keadilan dan Pengabdian Hukum, Jakarta, 1994,hal.91.

[111] Sudarto, Kapita Selekta Hukum Pidana, Alumni, Bandung, 1986, hal.32.

[112] Soerjono Soekanto, *Faktor-faktor yang Mempengaruhi Penegakan Hukum*, PT.Raja Grafindo Persada, Jakarta, 2005, hal.5.

menjadi lebih akseptabel bersama-sama dengan peran masyarakatnya. Tanpa peran masyarakat, kebijakan penegakan hukum akan menjadi tidak optimalistis sifatnya.[113]

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:[114]

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 dari 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. [115]

Penegakan hukum sangat terikat dengan hukum acara pidana dan pembuktian. M Yahya Harahap[116] menyatakan bahwa 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-

---

[113] Indriyanto Seno Adji, *Korupsi Sistematik dan Kendala Penegak Hukum di Indonesia,* Jurnal Studi Kepolisian Perguruan Tinggi Ilmu Kepolisian, CV.Restu Agung, 2005,hal.9.

[114] Soerjono Soekanto, *Faktor-faktor yang Mempengaruhi Penegakan Hukum*, *Op.Cit*., hal.8.

[115] Soerjono Soekanto, *Faktor-faktor yang Mempengaruhi Penegakan Hukum.Op.Cit*. hal.69.

[116] M.Yahya Harahap, *Pembahasan Permasalahan Dan Penerapan KUHAP: Pemeriksaan Sidang Pengadilan, Banding, Kasasi, dan Peninjauan Kembali*, Edisi Kedua, Sinar Grafika, Bandung,2000, hal.252

undang ”tidak cukup” membuktikan kesalahan yang didakwakan kepada terdakwa, terdakwa ”dibebaskan” dari hukuman. Sebaliknya, kalau kesalahan terdakwa dapat dibuktikan dengan alat-alat bukti yang disebut Pasal 184 KUHAP terdakwa dinyatakan ”bersalah”. Kepadanya akan dijatuhkan hukuman.

Berkaitan dengan membuktikan sebagaimana diuraikan di atas, dalam hukum acara pidana (KUHAP) secara tegas disebutkan beberapa alat-alat bukti yang dapat diajukan oleh para pihak yang berperkara di muka persidangan. Berdasarkan Pasal 184 KUHAP,[117] alat-alat bukti ialah :

a. Keterangan saksi;

b. Keterangan ahli;

c. Surat;

d. Petunjuk;

e. Keterangan terdakwa.

Sedangkan penjelasan Pasal 184 KUHAP dijelaskan ; [118] “Dalam acara pemeriksaan cepat, keyakinan hakim cukup di dukung satu alat bukti yang sah”. Bertolak dari Pasal 184 dan penjelasannya tersebut, berarti kecuali pemeriksaan cepat, untuk mendukung keyakinan hakim diperlukan alat bukti lebih dari satu atau sekurang-kurangnya dua alat bukti yang sah. Untuk hal ini Pasal 183 KUHAP[119] secara tegas dirumuskan bahwa” Hakim tidak boleh menjatuhkan pidana kepada seseorang kecuali apabila dengan sekurang-kurangnya dua alat bukti yang sah ia memperoleh keyakinan

---

[117] M.Yahya Harahap, *Pembahasan Permasalahan Dan Penerapan KUHAP: Pemeriksaan Sidang Pengadilan, Banding, Kasasi, dan Peninjauan Kembali Op.Cit.*,hal.807

[118] Penjelasan Pasal 184 Undang-Undang No.8 Tahun 1981 tentang Kitab Undang-Undang Hukum Acara Pidana Lembaran Negara Republik Indonesia Nomor 76.

[119] Pasal 183 Undang-Undang No.8 Tahun 1981 tentang Kitab Undang-Undang Hukum Acara Pidana Lembaran Negara Republik Indonesia Nomor 76.

bahwa suatu tindak pidana benar-benar terjadi dan bahwa terdakwalah yang bersalah melakukannya". Dengan demikian dalam KUHAP secara tegas memberikan legalitas bahwa di samping berdasarkan unsur keyakinan hakim, pembuktian dengan sekurang-kurangnya dua alat bukti yang sah adalah sangat diperlukan untuk mendukung unsur kesalahan dalam hal menentukan seseorang benar-benar terbukti melakukan tindak pidana atau tidak.

A.3 Pengertian Kebijakan Hukum Pidana

Perkembangan globalisasi serta kemajuan teknologi informasi menuntut pembaharuan hukum pidana sebagai bagian dari kebijakan hukum pidana yang berlaku sesuai dengan nilai-nilai masyarakat Indonesia. Penanggulangan terhadap tindak pidana teknologi informasi perlu diimbangi dengan pembenahan dan pembangunan sistem hukum pidana secara menyeluruh, yakni meliputi pembangunan kultur, struktur dan subtansi hukum pidana. Dalam hal ini kebijakan hukum pidana menduduki posisi yang strategis dalam pengembangan hukum pidana modern.

Kebijakan hukum *(legal policy)* dalam arti kebijakan negara *(public policy)* di bidang hukum harus dipahami sebagai bagian kebijakan sosial yaitu usaha setiap masyarakat/pemerintah untuk meningkatkan kesejahteraan warganya di segala aspek kehidupan. Hal ini bisa mengandung dua dimensi yang terkait satu sama lain, yaitu kebijakan kesejahteraan sosial *(social welfare policy)* dan kebijakan perlindungan sosial *(social defence policy).*[120]

Sedangkan definisi hukum pidana menurut Sudarto adalah memuat aturan-aturan hukum yang mengikatkan kepada perbuatan-perbuatan yang memenuhi syarat tertentu

---

[120] Muladi, *Demokratisasi,Hak Asasi Manusia dan Reformasi Hukum di Indonesia, Op.Ci.t,*hal.269.

suatu akibat yang berupa pidana.[121] Pemberian pidana dalam arti umum itu merupakan bidang dari pembentuk undang-undang yang berdasarkan azas legalitas, yang berasal dari zaman Aufklarung, yang singkatnya berbunyi: *nullum crimen, nulla poena, sine praevia lege (poenali).* Secara singkat *nullum crimen sine lege* berarti tidak ada tindak pidana tanpa undang-undang dan *nulla poena sine lege* berarti tidak ada pidana tanpa undang-undang. Jadi undang-undang menetapkan dan membatasi perbuatan mana dan pidana (sanksi) mana yang dapat dijatuhkan kepada pelanggarnya. Jadi untuk mengenakan *poena* atau pidana diperlukan undang-undang (pidana) terlebih dahulu.[122]

Pengertian kebijakan hukum dan hukum pidana di atas memberikan definisi kebijakan hukum pidana (*penal policy/criminal law policy/strafrechtspolitiek*) sebagai, bagaimana mengusahakan atau membuatan merumuskan suatu perundang-undangan pidana yang baik.[123] Pengertian demikian terlihat pula dalam definisi "*penal policy*" yang dikemukakan oleh Marc Ancel,[124] bahwa *penal policy* adalah suatu ilmu sekaligus seni yang pada akhirnya mempunyai tujuan praktis untuk memungkinkan peraturan hukum positif dirumuskan secara lebih baik dan untuk memberi pedoman tidak hanya kepada pembuat undang-undang, tetapi juga kepada pengadilan yang menerapkan undang-undang dan juga kepada para penyelenggara atau pelaksana putusan pengadilan.

Sejalan dengan pemikiran demikian Barda Nawawi Arief menyatakan bahwa upaya melakukan pembaharuan hukum pidana pada hakikat nya termasuk bidang " *penal*

---

121 Sudarto, *Hukum dan Hukum Pidana, Op.Cit.*,hal.100.

122 Sudarto, *Hukum dan Hukum Pidana, Op.Cit.*, hal.50.

123 Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana*, *Op.Cit*.hal.25.

124 Marc Ancel, *Social Defence, A Modern Approach to Criminal Problem* (London, Routledge & Kegan Paul,1965,hal.4-5), lihat dalam Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana*, *Op.Cit.*,hal.21.

policy" yang merupakan bagian dan terkait dengan "*Law enforcement policy*" , "*Criminal policy*" dan " *Sosial Policy*". Ini berarti pembaharuan hukum pidana pada hakikat nya :

a. Merupakan bagian dari kebijakan (upaya rasional) untuk memperbaharui substansi hukum (legal substansi) dalam rangka lebih mengefektifkan penegakan hukum ;
b. Merupakan bagian dari kebijakan (upaya rasional) untuk memberantas/menanggulangi kejahatan dalam rangka perlindungan masyarakat ;
c. Merupakan bagian dari kebijakan (upaya rasional) untuk mengatasi masalah sosial dan masalah kemanusiaan dalam rangka mencapai/menunjang tujuan nasional (yaitu "*Sosial defennce*" dan "*sosial welfare*") ;
d. Merupakan upaya peninjauan dan penilaian kembali ("reorientasi dan re - evaluasi") pokok-pokok pemikiran, ide-ide dasar, atau nilai sosio-filosofik, sosio-politik, dan sosio kultural yang melandasi kebijakan kriminal dan kebijakan (penegakan) hukum pidana selama ini. Bukanlah pembaharuan ("*reformasi*") hukum pidana, apabila orientasi nilai dari hukum pidana yang dicita-citakan sama saja dengan orientasi nilai dari hukum pidana lama warisan penjajah (KUHP lama atau WvS). [125]

Pembaharuan hukum pidana di atas dipengaruhi oleh sistem hukum pidana, Marc Ancel mengkemukakan bahwa sistem hukum pidana abad XX masih tetap harus diciptakan. Sistem demikian hanya dapat disusun dan disempurnakan oleh usaha bersama semua orang yang beritikad baik dan juga oleh semua ahli di bidang ilmu-ilmu sosial.[126] Sistem hukum pidana tersebut terdiri dari:

1. peraturan-peraturan hukum pidana dan sanksinya;
2. suatu prosedur hukum pidana; dan
3. suatu mekanisme pelaksanaan (pidana).[127]

Pengertian "sistem hukum pidana" dari Marc Ancel memberikan landasan A.Mulder dalam memberikan pengertian kebijakan atau politik hukum pidana. (*penal policy*/*Strafrechtspolitiek*), untuk menentukan :[128]

---

[125] Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana*, *Op.Cit*.hal.28.
[126] Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana*, *Op.Cit*.,hal..28-29.
[127] A.Mulder ,"*Strafrechtspolitiek" Delikt en Delinkwent* ,Mei 1980,hal.333,lihat dalam Barda Nawawi Arief ,*Bunga Rampai Kebijakan Hukum Pidana, Op.Cit*.hal.26.

1. Seberapa jauh ketentuan-ketentuan pidana yang berlaku perlu diubah atau diperbaharui
   (*in welk opzicht de bestaande straf bepalingen herzien dienen te worden*);
2. Apa yang dapat diperbuat untuk mencegah terjadinya tindak pidana
   (*wat gedaan kan worden om strafrechtelijk gedrad verkomen*);
3. Cara bagaimana penyidikan, penuntutan, peradilan dan pelaksanaan pidana harus dilaksanakan
   (*hoe de opsporing, vervolging, berechting en tenuitvoerlegging van straffen dient te verloppen*).

Bertolak dari kebijakan tersebut di atas, usaha dan kebijakan untuk membuat peraturan hukum pidana yang pada pada hakikatnya tidak dapat dilepaskan dari tujuan penanggulangan kejahatan. Jadi, kebijakan atau politik hukum pidana juga merupakan bagian dari politik kriminal. Dengan perkataan lain, dilihat dari sudut politik kriminal, maka politik hukum pidana identik dengan pengertian kebijakan penanggulangan kejahatan dengan hukum pidana.[129]

---

[128] Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana*, *Op.Cit*. ,hal.25-26

[129] Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana*, *Op.Cit*.hal.26.

B. TINDAK PIDANA TEKNOLOGI INFORMASI

B.1 Teknologi Informasi dan Perkembangannya.

Revolusi yang dihasilkan oleh teknologi informasi biasanya dilihat dari sudut pandang penurunan jarak geografis, penghilangan batas-batas negara dan zona waktu, dan peningkatan efisiensi dalam memanipulasi pengumpulan, penyebaran, analisis, dan mungkin juga penggunaan data. Munculnya keseluruhan dunia sebagai satu komunitas ekonomi global dan komplikasi lebih lanjut dari operasi bisnis telah mengakibatkan suatu konsekuensi paling penting dari revolusi ini.

Pada awal sejarah, manusia bertukar informasi melalui bahasa. Maka bahasa adalah teknologi. Bahasa memungkinkan seseorang memahami informasi yang disampaikan oleh orang lain. Tetapi bahasa yang disampaikan dari mulut ke mulut hanya bertahan sebentar saja, yaitu hanya pada saat si pengirim menyampaikan informasi melalui ucapannya itu saja. Setelah ucapan itu selesai, maka informasi yang berada di tangan si penerima itu akan dilupakan dan tidak bisa disimpan lama. Selain itu jangkauan suara juga terbatas. Untuk jarak tertentu, meskipun masih terdengar, informasi yang disampaikan lewat bahasa suara akan terdegradasi bahkan hilang sama sekali.[90]

Penemuan teknologi elektronik seperti radio, tv, komputer mengakibatkan informasi menjadi lebih cepat tersebar di area yang lebih luas dan lebih lama tersimpan. Dalam perkembangannya, kolaborasi antara penemuan komputer dan penyebaran informasi melalui komputer melahirkan apa yang dikenal dengan istilah *internet (internconnected network*-jaringan yang saling terhubung).

Pengembangan teknologi informasi terkait dengan jaringan yang terhubung diawali pada tahun 1962, ketika Departemen Pertahanan Amerika Serikat melakukan riset penggunaan teknologi komputer untuk kepentingan pertahanan udara Amerika Serikat. Melalui lembaga

[90] Di akses dari http://www.wikipedia.com pada tanggal 1 September 2008.

risetnya yaitu *Advanced Research Project Agency* (ARPA) menugasi *the New Information Processing Techniques Office* (IPTO), yaitu suatu lembaga yang diberi tugas untuk melanjutkan riset penggunaan teknologi komputer di bidang pertahanan udara.[91] Selanjutnya Pada tahun 1969 *Departement* Pertahanan Amerika Serikat menemukan sebuah teknologi yang esensinya memadukan teknologi telekomunikasi dengan komputer yang dikenal dengaan nama ARPANet (*Advanced Research Projects Agency Network)* yaitu system jaringan melalui hubungan antar komputer di daerah-daerah vital dalam rangka mengatasi masalah jika terjadi serangan nuklir.[92]

Keberhasilan dalam memadukan teknologi tersebut atau yang dikenal dengan istilah teknologi informasi (*information technology*) pada tahun 1970 mulai dimanfaatkan untuk keperluan non-militer oleh berbagai universitas.[93] Pada dekade inilah sebenarnya manusia telah memasuki era baru yaitu melalui perkembangan teknologi informasi telah dimanfaatkan manusia hampir di semua aspek kehidupan.

Istilah teknologi informasi sendiri pada dasarnya merupakan gabungan dua istilah dasar yaitu teknologi dan informasi. Teknologi dapat diartikan sebagai pelaksanaan ilmu, sinonim dengan ilmu terapan. Sedangkan pengertian informasi menurut *Oxford English Dictionary*, adalah *"that of which one is apprised or told: intelligence, news - facts or details about".*[94] Kamus besar Bahasa Indonesia menyatakan bahwa informasi adalah sesuatu yang dapat diketahui.[95] Undang-Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dalam pasal 1 sub-1 mendefinisikan Informasi Elektronik sebagai satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta,

---

[91] Di akses dari http://www.living*internet*.com/i/ii_ipto.htm pada tanggal 15 Agustus 2008.

[92] Hanny Kamarga, *Belajar Sejarah Melalui E-Learning : Alternatif Mengakses Sumber Informasi Kesejarahan*, PT Intimedia, Jakarta, 2002, hal 2.

[93] Hanny Kamarga, *Belajar Sejarah Melalui E-Learning : Alternatif Mengakses Sumber Informasi Kesejarahan Op.Cit.*,hal.4.

[94] Oxford, *Learners Pocket Dictionary Third Edition*, Oxford *University Press*,pg.222.

[95] Anton M.Moelijono, (et.al).Kamus Besar Bahasa Indonesia, Balai Pustaka, Jakarta,1998, hal.523.

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.[96]

UU ITE dalam Pasal 1 sub-3 menegaskan pengertian teknologi informasi di Indonesia sebagai suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memperoses, mengumumkan, menganalisa, dan menyebarkan informasi.[97] Turban mendefinisikan Teknologi Informasi dengan ungkapan: *in its narrow definition, refers to the technological side of an information system. It includes hardware, databases, software networks and other devices.* Sementara mengenai Sistem Informasi didefinisikan sebagai : *a collection of components that collects, processes, stores, analyzes, and disseminates information for a specific purpose.*[98]

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 .[99]

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.

---

[96] Pasal 1sub-1 Undang-Undang No.11 tahun 2008 tentang Informasi dan Transaksi Elektronik, diundangkan pada 28 April 2008, Lembaran Negara No.58.

[97] Pasal 1sub-3 Undang-Undang No.11 tahun 2008 tentang Informasi dan Transaksi Elektronik, diundangkan pada 28 April 2008, Lembaran Negara No.58.

[98] Lihat dalam naskah akademik RUU tindak pidana di bidang Teknologi Informasi disusun oleh Mas Wigantoro Roes Setiyadi , *Op.Cit*,hal.5.

[99] Abdul Ma'in M., Teknologi Informasi Dalam Sistem Jaringan Perpustakaan Perguruan Tinggi. www.yahoo.com. Diakses pada tanggal 1 September 2008.

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.[100] 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*. *Intranet* adalah "*a private network belonging to an organization, usually a corporation, accessible only by the organization's members, employes, or others with authorization*,[101] dan *ekstranet* adalah "*a fancy way of saying that a corporation has opened up portions of its intranet to authorized users outside the corporation*.[102]

Webopaedia mendefinisikan *internet* sebagai "*a global network connecting millions of computers*",[103] *The Federal Networking Council* (FNC) memberikan definisi mengenai *internet* dalam resolusinya tanggal 24 Oktober 1995 sebagai:

> *"Internet refers to the global information system that –*
> *(i) is logically linked together by a globally unique address space based in the Internet Protocol (IP) or its subsequent extensions/follow-ons;*
> *(ii) is able to support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite or its subsequent extension/followons, and/or other Internet Protocol)IP)-compatible protocols; and*
> *(iii) Providers, uses or makes accessible, either publicly or privately, high level services layered on the communications and related infrastructure described herein."* [104]

---

[100] Lihat di www.ristek.go.id, Perlunya Studi Perbandingan dalam Pengembangan Teknologi Informasi di Indonesia.2001di akses pada tanggal 29 Agustus 2008.

[101] Lihat di http://netforbeginners.minings.com diakses pada tanggal 30 Agustus 2008.

[102] *Ibid.*

[103] Lihat di http://webopaedia.*internet*.com diakses pada tanggal 30 Agustus 2008.

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).[105]

Cyberspace untuk pertama kalinya diperkenalkan pada tahun 1984 oleh William Gibson seorang penulis fiksi ilmiah (*science fiction*) dalam novelnya yang berjudul *Neuromancer* dalam novel tersebut *cyberspace* diartikan sebagai *consensual hallucination experienced daily by billions of legitimate operators ... a graphical representation of data abstracted from the banks of every computer in the human system*.[106] Istilah yang sama kemudian diulanginya dalam novelnya yang lain yang berjudul *Virtual Light*. Menurut Gibson, *cyberspace "... was a consensual hallucination that felt and looked like a physical space but actually was a computer-generated construct representing abstract data"*.

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*).' Pada saat ini, *cyberspace* sebagaimana dikemukakan oleh Cavazos dan Morin adalah:"... *represents a fast array of computer systems accessible from remote physical locations"*.[107]

---

[104] Agus Raharjdo, *Cybercrime pemahaman dan upaya pencegahan kejahatan berteknologi*, *Op.Cit.*, hal. 59.

[105] Agus Rahardjo,. *Cybercrime pemahaman dan upaya pencegahan kejahatan berteknologi*, *Op.Cit.*,hal.20.

[106] Diakses dari http://www.total.or.id/info.php?kk=William%20Gibson Pada tanggal 6 Agustus 2008.

[107] Jeff Zalesky, *Spritualitas Cyberspace, Bagaimana Teknologi Komputer Mempengaruhi Kehidupan Keberagaman Manusia,* Mizan, Bandung, 1999,hal.9.

Secara etimologis, istilah *cyberspace* sebagai suatu kata merupakan suatu istilah baru yang hanya dapat ditemukan di dalam kamus mutakhir. *Cambridge Advanced Learner's Dictionary* memberikan definisi *cyberspace* sebagai *"the Internet considered as an imaginary area without limits where you can meet people and discover information about any subject"*.[108] *The American Heritage Dictionary of English Language Fourth Edition* mendefinisikan *cyberspace* sebagai "*the electronic medium of computer networks, in which online communication takes place*".[109]

Pengertian *cyberspace* tidak terbatas pada dunia yang tercipta ketika terjadi hubungan melalui *internet*. Bruce Sterling mendefinisikan *cyberspace* sebagai *the 'place' where a telephone conversation appears to occur.*[110] Aktivitas yang potensial untuk dilakukan di *cyberspace* tidak dapat diperkirakan secara pasti mengingat kemajuan teknologi informasi yang sangat cepat dan mungkin sulit diprediksi. Namun, saat ini ada beberapa aktivitas utama yang sudah dilakukan di *cyberspace* seperti *Commercial On-line Services, Bullelin Board System, Conferencing Systems, Internet Relay Chat, Usenet, EmaiI list,* dan *entertainment.* Sejumlah aktivitas tersebut saat ini dengan mudah dapat dipahami oleh masyarakat kebanyakan sebagai aktivitas yang dilakukan lewat *Internet*. Oleh karena itu dapat disimpulkan bahwa apa yang disebut dengan "*cyberspace*" itu tidak lain. adalah *Internet* yang juga sering disebut sebagai "*a network of net works*". Dengan karakteristik seperti ini kemudian ada juga yang menyebut "*cyberspace*" dengan istilah "*virtual community*" (masyarakat maya) atau "*virtual world*" (dunia maya).

---

[108] Diakses dari http://dictionary.cambridge.org Pada tanggal 23 Agustus 2008.
[109] Diakses dari http://www.bartleby.com. Pada tanggal 23 Agustus 2008.
[110] Bruce Sterling, *The Hacker Crackdown, Law and Disorder on the electronic Frontier*, Massmarket Paperback, electronic version ,1990, available at http://www.lysator.liu.se/etexts/hacker.

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.[111]

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:[112]

a. *E-Commerce*
   Contoh paling umum dari 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*.

---

[111] Onno W Purbo, *Kebangkitan Nasional Ke-2 Berbasis Teknologi Informasi, Computer Network Research Group*,ITB,2007. Lihat dalam yc1dav@garuda.drn.go.id. Pada tanggal 5 Agustus 2008.

[112] Abdul Wahib dan Mohammad Labib, *Kejahatan Mayantara* (*Cybercrime*), *Kejahatan Mayantara* (*Cybercrime*), Refika Aditama, Bandung , 2005, hal. 24-25.

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 dari 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.[113]

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.

B.2 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

[113] Horton, Paul B dan Chester L.Hunt, *Sosiologi*, Erlangga, Jakarta, 1984, hal.237.

munculnya tindakan-tindakan anti sosial yang selama ini dianggap tidak mungkin terjadi atau tidak akan terpikirkan terjadi. Sebuah teori menyatakan bahwa *crime is product of society it self,* yang secara sederhana dapat diartikan bahwa semakin tinggi tingkat intelektualitas suatu masyarakat maka akan semakin canggih dan beraneka-ragam pulalah tingkat kejahatan yang dapat terjadi.[114]

Salah satu contoh terbesar saat ini adalah kejahatan maya atau biasa disebut "*cybercrime*" (tindak pidana mayantara), merupakan bentuk fenomena baru dalam tindak kejahatan sebagai dampak langsung dari perkembangan teknologi informasi. Beberapa sebutan diberikan pada jenis kejahatan baru ini di dalam berbagai tulisan, antara lain: sebagai " kejahatan dunia maya" (*cyber-space/virtual-space offence*), dimensi baru dari "*hi-tech crime*", dimensi baru dari "*transnational crime*", dan dimensi baru dari "*white collar crime*".[115]

White collar crime menurut Jo Ann Miller, umumnya dibagi ke dalam 4 (empat) jenis, yaitu: kejahatan korporasi, kejahatan birokrat, malpraktek, dan kejahatan individu.[116] Sementara itu, *cybercrime* memiliki ciri khas tersendiri yaitu para pelaku umunya orang muda yang menguasai teknologi informasi dan dilakukan secara ekstra hati-hati dan sangat menyakinkan serta membutuhkan keahlian tambahan atau pertolongan orang lain.[117]

Kekhawatiran akan tindak kejahatan ini dirasakan di seluruh aspek bidang kehidupan. ITAC (*Information Technology Assosiation of Canada*) pada "*International Information Industry Congress* (IIIC) 2000 *Millenium Congress*" di Quebec tanggal 19 September 2000 menyatakan bahwa " *Cybercrime is a real and growing threat to economic and social development around*

---

[114] Abdul Wahib dan Mohammad Labib, *Kejahatan Mayantara* (*Cybercrime*), *Op.Cit,* hal. 39.

[115] Barda Nawawi Arief., *Antisipasi Penanggulangan* "*Cybercrime*" *dengan hukum Pidana*.,makalah pada seminar Nasional mengenai "*Cyber*law"., di STHB, Bandung, Hotel Grand Aquila, 9 April 2001

[116] Sutanto, Hermawan Sulistyo, dan Tjuk Sugiarto, *Cybercrime-Motif dan Penindakan*, Pensil 324, Jakarta, hal.13-14.

[117] Sutanto, Hermawan Sulistyo, dan Tjuk Sugiarto, *Cybercrime-Motif dan Penindakan Op.Cit.*,hal.20.

the world. Information technology touches every aspect of human life and so can electronically enable crime".[118]

Istilah *cybercrime* saat ini merujuk pada suatu tindakan kejahatan yang berhubungan dengan dunia maya (*cyberspace*) dan tindakan kejahatan yang menggunakan komputer. Ada ahli yang menyamakan antara tindak kejahatan *cyber* (*cybercrime*) dengan tindak kejahatan komputer, dan ada ahli yang membedakan di antara keduanya. Meskipun belum ada kesepahaman mengenai definisi kejahatan Teknologi Informasi, namun ada kesamaan pengertian universal mengenai kejahatan komputer.[119]

Kejahatan teknologi informasi atau kejahatan komputer memang identik dengan *cybercrime*, banyak literatur baik nasional maupun internasional yang mendefinisikan terhadap istilah tersebut. *The U.S Departement of Justice* memberikan pengertian *"cybercrime is any illegal act requiring knowledge of computer technology for it perpetration, investigation or prosecution"*. [120] *Computer crime* dapat diartikan sebagai kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara ilegal.[121] Abdul Wahib dan Mohammad Labib menyatakan bahwa kejahatan dunia maya adalah kejahatan yang berkaitan dengan pemanfaatan sebuah teknologi informasi tanpa batas serta memiliki karakteristik yang kuat dengan sebuah rekayasa teknologi yang mengandalkan pada tingkat keamanan yang tinggi dan kredebilitas dari sebuah informasi yang disampaikan dan diakses oleh pengguna *internet*.[122]

Barda Nawawi Arief menunjuk pada kerangka (sitematik). *Draft Convention on Cybercrime* dari Dewan Eropa (Draft No.25, Desember 2000) yang mendefinisikan *cybercrime*

---

[118] ITAC,*" IIIC Common Views Paper On: Cybercrime"*, IIIC 2000 Millenium congress, September 19th, 2000, hal.5. Lihat dalam Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*, *Op.Cit*.,hal.240.

[119] M.Arief Mansur dan Alistaris Gultom, , *CyberLaw;Aspek Hukum Teknologi Informasi*, *Op.Cit*,hal.8.

[120] Petrus Reinhard Golose, *Perkembangan Cybercrimedan Upaya Penanganannya di Indonesia Oleh Polri*, *Op.Cit*. hal.7.

[121] Andi Hamzah, *Aspek-Aspek Pidana di Bidang Komputer,* 1998,hal.4.

[122] Abdul Wahib dan Mohammad Labib, *Kejahatan Mayantara* (*Cybercrime*), *Op..Cit,* hal. 40.

sebagai *"crime related to technology, computers, and the internet*" atau secara sederhana berarti kejahatan yang berhubungan dengan teknologi, komputer dan *internet*.[123] Pengertian lainnya diberikan oleh *Organization of European Community Development*, yaitu *"any illegal, unethical or unauthorized behavior relating to the automatic processing and/or the transmission of data*.[124]

Cybercrime pada dasarnya tindak pidana yang berkenaan dengan informasi, sistem informasi (*information system*) itu sendiri, serta sistem komunikasi yang merupakan sarana untuk penyampaian/pertukaran informasi itu kepada pihak lainnya (*transmitter/orginator to recipient*).[125] Menurut Sutanto, secara garis besar *cybercrime* terdiri dari dua jenis, yaitu:[126]

1. Kejahatan yang menggunakan teknologi informasi (TI) sebagai fasilitas.
   Contoh-contoh dari aktivitas *cybercrime* jenis pertama ini adalah pembajakan (*copyright* atau hak cipta intelektual, dan lain-lain); pornografi; pemalsuan dan pencurian kartu kredit (*carding*); penipuan lewat *e-mail*; penipuan dan pembobolan rekening bank; perjudian *on line*; terorisme; situs sesat; materi-materi *internet* yang berkaitan dengan SARA (seperti penyebaran kebencian etnik dan ras atau agama); transaksi dan penyebaran obat terlarang; transaksi seks; dan lain-lain.
2. Kejahatan yang menjadikan sistem dan fasilitas teknologi informasi (TI) sebagai sasaran.
   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 suatu sistem secara ilegal (*hacking*), perusakan situs *internet* dan *server* data (*cracking*), serta *defacting.*

Menurut Freddy Haris, *Cybercrime* merupakan suatu tindak pidana dengan karateristik-karateristik sebagai berikut:

1. *Unauthorized access* (dengan maksud untuk memfasilitasi kejahatan)

2. *Unauthorized alteration or destruction of data,*

---

[123] Barda Nawawi Arief, *Kapita Selekta Hukum Pidana, Op.Cit*,hal.243.

[124] Naskah akademik RUU tindak pidana di bidang Teknologi Informasi disusun oleh Mas Wigantoro Roes Setiyadi , *Cyber*Policy Club dan Indonesia Media Law and Policy Center,2003.hal.25.

[125] *Ibid.*

[126] Sutanto, Hermawan Sulistyo, dan Tjuk Sugiarto, *Cybercrime*-Motif dan Penindakan, Pensil 324, Jakarta, hal.21.

3. Mengganggu/merusak operasi komputer,

4. Mencegah/menghambat akses pada komputer.[127]

Sedangkan kualifikasi kejahatan dunia maya (*cybercrime*), sebagaimana dikutip Barda Nawawi Arief, adalah kualifikasi *Cybercrime* menurut *Convention on Cybercrime* 2001 di Budapest Hongaria, yaitu:[128]

1. *Illegal access*: yaitu sengaja memasuki atau mengakses sistem komputer tanpa hak.

2. *Illegal interception*: yaitu sengaja dan tanpa hak mendengar atau menangkap secara diam-diam pengiriman dan pemancaran data komputer yang tidak bersifat publik ke, dari atau di dalam sistem komputer dengan menggunakan alat bantu teknis.

3. *Data interference*: yaitu sengaja dan tanpa hak melakukan perusakan, penghapusan, perubahan atau penghapusan data komputer.

4. *System interference*: yaitu sengaja melakukan gangguan atau rintangan serius tanpa hak terhadap berfungsinya sistem komputer.

5. *Misuse of Devices*: penyalahgunaan perlengkapan komputer, termasuk program komputer, password komputer, kode masuk (*access code*)

6. *Computer related Forgery*: Pemalsuan (dengan sengaja dan tanpa hak memasukkan mengubah, menghapus data autentik menjadi tidak autentik dengan maksud digunakan sebagai data autentik)
7. *Computer related Fraud*: Penipuan (dengan sengaja dan tanpa hak menyebabkan hilangnya barang/kekayaan orang lain dengan cara memasukkan, mengubah, menghapus data komputer atau dengan mengganggu berfungsinya komputer/sistem komputer, dengan tujuan untuk memperoleh keuntungan ekonomi bagi dirinya sendiri atau orang lain).

8. *Content-Related Offences*
   Delik-delik yang berhubungan dengan pornografi anak *(child pornography)*

9. *Offences related to infringements of copyright and related rights*
   Delik-delik yang terkait dengan pelanggaran hak cipta

[127] Freddy Haris, *Cybercrimedari Persfektif Akademis,* Lembaga Kajian Hukum dan Teknologi Fakultas Hukum Universitas Indonesia,hal.4.

[128] Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan,Op.Cit*.hal.24

Beberapa bentuk kejahatan yang berhubungan erat dengan penggunaan teknologi informasi yang berbasis utama komputer dan jaringan teknologi informasi, dalam beberapa literatur dan praktiknya menurut Mas Wigantoro dikelompokkan dalam beberapa bentuk antara lain:[129]

1. *Unauthorized Access to Computer System and Service*
   Kejahatan yang dilakukan dengan memasuki/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya.

2. *Illegal Contents*
   Merupakan kejahatan dengan memasukkan data atau informasi ke *Internet* tentang sesuatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum.

3. *Data Forgery*
   Merupakan kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai *scriptless document* melalui *internet*.

4. *CyberEspionage*
   Merupakan kejahatan yang memanfaatkan jaringan *internet* untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (*computer network system*) pihak sasaran.

5. *CyberSabotage and Extortion*
   Kejahatan ini dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan *internet*.

6. *Offence Against Intellectual Property*
   Kejahatan ini ditujukan terhadap hak atas kekayaan intelektual yang dimiliki pihak lain di *Internet*. Sebagai contoh adalah peniruan tampilan pada web page suatu situs milik orang lain secara ilegal, penyiaran suatu informasi di *Internet* yang ternyata merupakan rahasia dagang orang lain dan sebagainya.

7. *Infringements of Privacy*
   Kejahatan ini ditujukan terhadap informasi seseorang yang merupkan hal yang sangat pribadi dan rahasia. Kejahatan ini biasanya ditujukan terhadap keterangan seseorang pada formulir data pribadi yang tersimpan secara *computerized*, yang apabila diketahui oleh orang lain akan dapat merugikan korban secara materil maupun

[129] Naskah akademik RUU tindak pidana di bidang Teknologi Informasi disusun oleh Mas Wigantoro Roes Setiyadi , *Op.Cit*,hal.25-26.

immateril, seperti nomor kartu kredit, nomor PIN ATM, cacat atau penyakit tersembunyi dan sebagainya.

Selain kejahatan di atas sebetulnya masih banyak jenis-jenis kejahatan yang masuk dalam kategori *cybercrime* seperti yang diungkapkan oleh Didik M.Arief dan Alistaris Gultom, jenis-jenis *cybercrime* diantaranya:[130]

1. *Cyber-terorism*
   National Police Agency of Japan (NPA) mendefinisikan CyberTerrorism sebagai electronic attack through computer networks againts critical infrastructure that have potential critical effects on social and economic activities of the nation.

2. *Cyber-Pornography*: penyebarluasan *obscene materials* termasuk pornography, indecent exposure, dan *child pornography.*

3. *Cyber-harassment*: pelecehan seksual melalui e-mail,website, atau chat programs.

4. *Cyber-stalking: crimes of stalking* melalui penggunaan komputer dan iternet

5. *Hacking*: penggunaan *programming abilities* dengan maksud yang bertentangan dengan hukum.

6. *Carding ("credit-card fraud"*) melibatkan berbagai macam aktifitas yang melibatkan kartu kredit. *Carding* muncul ketika seseorang yang bukan pemilik kartu kredit menggunakan kartu kredit tersebut secara melawan hukum

Berdasarkan beberapa tindak pidana yang berkaitan dengan teknologi informasi di atas Menurut RM Roy Suryo kasus-kasus *cybercrime* yang banyak terjadi di Indonesia setidaknya ada tiga jenis berdasarkan modusnya, yaitu : [131]

1. Pencurian Nomor Kredit.
   Penyalahgunaan kartu kredit milik orang lain di *internet* merupakan kasus *cybercrime* terbesar yang berkaitan dengan dunia bisnis *internet* di Indonesia. Penyalahgunaan kartu kredit milik orang lain memang tidak rumit dan bisa dilakukan secara fisik atau *on-line* . Nama dan kartu kredit orang lain yang diperoleh di berbagai tempat (restaurant, hotel, atau segala tempat yang melakukan transaksi pembayaran dengan kartu kredit) dimasukkan di aplikasi pembelian barang di *internet.*
2. Memasuki, Memodifikasi, atau merusak Homepage (Hacking)
   Tindakan *hacker* Indonesia belum separah aksi di luar negeri. Perilaku *hacker* Indonesia baru sebatas masuk ke suatu situs komputer orang lain yang ternyata rentan

[130] M.Arief Mansur dan Alistaris Gultom, , *CyberLaw;Aspek Hukum Teknologi Informasi, Op.Cit*,hal.26.
[131] Majalah Warta Ekonomi No. 9, 5 Maret 2001 hal.12

penyusupan dan memberitahukan kepada pemiliknya untuk berhati-hati. Di luar negeri *hacker* sudah memasuki sistem perbankan dan merusak data base bank

3. Penyerangan situs atau *e-mail* melalui virus atau *spamming.* Modus yang paling sering terjadi adalah mengirim virus melalui *e-mail*. Menurut RM Roy M. Suryo, di luar negeri kejahatan seperti ini sudah diberi hukuman yang cukup berat. Berbeda dengan di Indonesia yang sulit diatasi karena peraturan yang ada belum menjangkaunya.

Dengan memperhatikan jenis-jenis kejahatan sebagaimana dikemukakan di atas dapat digambarkan bahwa *cybercrime* memiliki ciri-ciri khusus, yaitu:

1. *Non-Violance* (tanpa kekerasan);
2. Sedikit melibatkan kontak fisik;
3. Menggunakan peralatan dan teknologi;
4. Memanfaatkan jaringan telematika (telekomunikasi, media dan informatika) global.[132]

Apabila memperhatikan ciri ke-3 dan ke-4 yaitu menggunakan peralatan dan teknologi serta memanfaatkan jaringan telematika global, nampak jelas bahwa *cybercrime* dapat dilakukan dimana saja, kapan saja serta berdampak kemana saja, seakan-akan tanpa batas (*borderless*). Keadaan ini mengakibatkan pelaku kejahatan, korban, tempat terjadinya perbuatan pidana (*locus delicti*) serta akibat yang ditimbulkannya dapat terjadi pada beberapa negara. Oleh karena itu dalam memberantas kejahatan dalam dunia maya ini diperlukan penanganan yang serius serta melibatkan kerjasama internasional baik yang bersifat regional maupun multilateral.

B.3 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

[132] Romli Atmasasmita, *Ruang Lingkup Berlakunya Hukum Pidana terhadap Kejahatan Transnasional Terorganisasi,* artikel dalam Padjajaran Jilid XXIV No.2 tahun 1996,hal.90.

pengakuan dan kedaulatan penuh untuk berbagai aturan dan kebijaksanaannya secara penuh. Kekuasaan demikian harus dihormati pula oleh setiap negara lainnya sebagaimana kekuasaan yang dimiliki oleh negara-negara lain.[133]

Menurut Kamus Bahasa Indonesia, jurisdiksi adalah:[134]

a. kekuasaan mengabdi lingkup kuasa kehakiman;peradilan
b. lingkungan hak dan kewajiban serta tanggung jawab di suatu wilayah atau lingkungan tertentu;kekuasaan hukum.

Black's Law Dictionary memberikan definisi tentang jurisdiksi (*jurisdiction*) adalah :[135]

a. The world is a term of large and comprehensive import and embraces ever kind of judicial action;
b. It is the authority by which courts and judicial officers take cognizance of and decide caces;
c. The legal right by which judges exercise their authority;
d. It exists when courts has cognizance of class of cases involved, proper parties are present, and point to be decided is within power of court;
e. Power and authority of court to hear and detemine a judicial proceeding;
f. The right of power of a court to adjudicate concerning the subject matter in a given case.

Jurisdiksi menurut hukum pidana internasional adalah kekuasaan atau kompetensi hukum negara terhadap orang, benda atau peristiwa (hukum). Jurisdiksi ini merupakan refleksi dari prinsip dasar kedaulatan negara, kesamaan derajat negara dan prinsip tidak campur tangan. Jurisdiksi juga merupakan suatu bentuk kedaulatan yang vital dan sentral yang dapat mengubah, menciptakan atau kewajiban suatu hubungan atau kewajiban hukum.[136]

Jurisdiksi suatu negara yang diakui Hukum Internasional dalam pengertian konvensional, didasarkan pada batas-batas geografis, sementara komunikasi multimedia bersifat internasional,

---

[133] Yudha Bhakti Ardhiwisastra, Imunitas Kedaulatan Negara di Forum Pengadilan Asing, Alumni Bandung, 1999,hal.14

[134] Departemen Pendidikan dan Kebudayaan,Kamus Besar Bahasa Indonesia,Cet.II,Balai Pustaka,Jakarta,1997,hal.1134.

[135] Henry Campbell Black,Black's Law Dictionary", third edition,pg.766.

[136] Shaw, *Internatonal law*, London: Butterworths,1986,hal.342, sebagaimana dikutip oleh Didik M.Arife Mansur dan Alistaris Gultom, , *CyberLaw;Aspek Hukum Teknologi Informasi*, Refika Aditama,Bandung,2005,hal.30.

multi jurisdiksi, tanpa batas, sehingga sampai saat ini belum dapat dipastikan bagaimana jurisdiksi suatu negara dapat diberlakukan terhadap komunikasi multimedia sebagai salah satu pemanfaatan teknologi informasi.[137]

Dalam kaitannya dengan penentuan hukum yang berlaku, dikenal beberapa asas yang biasa dilakukan,yaitu:[138]

1. *Subjective territoriality,* yang menekankan bahwa keberlakuan hukum ditentukan berdasarkan tempat perbuatan dilakukan danpenyelesaian tindak pidananya dilakukan di negara lain.
2. *Objective territoriality,* yang menyatakan bahwa hukum yang berlaku adalah hukum dimana akibat utama perbuatan itu terjadi dan memberikan 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 di luar wilayahnya, yang umumnya digunakan apabila korban adalah negara atau pemerintah.

6. *Universality.* Asas *Universality* selayaknya memperoleh perhatian khusus terkait dengan penanganan hukum kasus-kasus cyber. Asas ini disebut juga sebagai *"universal interest jurisdiction"*.

Pada mulanya asas *Universality* menentukan bahwa setiap negara berhak untuk menangkap dan menghukum para pelaku pembajakan. Asas ini kemudian diperluas sehingga mencakup pula kejahatan terhadap kemanusiaan *(crimes against humanity)*, misalnya penyiksaan, genosida, pembajakan udara dan lain-lain. Meskipun di masa mendatang asas jurisdiksi universal ini mungkin dikembangkan untuk *internet piracy*, seperti *computer,*

---

[137] Tien S, Saefulah, *Jurisdiksi sebagai Upaya Penegakan Hukum dalam Kegiatan Cyberspace, artikel dalam Cyberlaw: Suatu Pengantar*, Pusat Studi *Cyberlaw* Fakultas Hukum UNPAD,ELIPS,2002,hal.96.

[138] Ahmad M.Ramli,*Perkembangan CyberLaw Global dan Implikasinya Bagi Indonesia,* Makalah Seminar The Importance of Information System Security in E-Government,Tim koordinasi Telematika Indonesia,Jakarta,28 Juli 2004,hal.5-6.

cracking, carding, hacking and viruses, namun perlu dipertimbangkan bahwa penggunaan asas ini hanya diberlakukan untuk kejahatan sangat serius berdasarkan perkembangan dalam hukum internasional.

Harus diakui bahwa menerapkan jurisdiksi yang tepat dalam kejahatan-kejahatan di dunia maya (*cybercrime*) bukan merupkan pekerjaaan yang mudah, karena jenis kejahatannya bersifat internasional sehingga banyak bersinggung dengan kedaulatan banyak negara (sistem hukum negara lain). Berkenaan dengan jurisdiksi tersebut maka pertanyaan penting yang harus dikemukakan adalah sampai sejauh mana suatu negara memberikan kewenangannya kepada pengadilan untuk mengadili dan menghukum pelaku tindak pidana.

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 prinsip-prinsip jurisdiksi yang berlaku dalam 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.*[139]

Pendapat Menthe ini dapat ditafsirkan bahwa dengan diakuinya prinsip-prinsip jurisdiksi yang berlaku dalam hukum internasional dalam kegiatan *cyberspace* oleh setiap negara, maka akan mudah bagi negara-negara untuk mengadakan kerjasana dalam rangka harmonisasi ketentuan-ketentuan pidana untuk menanggulangi *cybercrime.*

Ada tiga lingkup jurisdiksi di ruang maya (*cyberspace*) menurut Masaki Hamano, sebagai mana dikutip oleh Barda Nawawi Arief yang dimiliki suatu negara berkenaan dengan penetapan

---

[139] Darrel Menthe, *"Jurisdiction in Cyberspace: A Theory of International Sraces"*, http://www.mttlr.org/volfour/menthe.html, hal.2. diakses tanggal 2 September 2008.

dan pelaksanaan pengawasan terhadap setiap peristiwa, setiap orang dan setiap benda. Ketiga katagori jurisdiksi tersebut, yaitu:[140]

1. Jurisdiksi Legislatif (*legislatif jurisdiction atau jurisdiction to prescribe*);
2. Jurisdiksi Yudisial (*judicial jurisdiction atau jurisdiction to adjudicate*); dan
3. Jurisdiksi Eksekutif (*executive jurisdiction atau jurisdiction to enforce*).

Jurisdiksi di atas berkaitan dengan batas-batas kewenangan negara di tiga bidang penegakan hukum, *Pertama*, kewenangan pembutan hukum substantif (oleh karena itu, disebut jurisdiksi legislatif, atau dapat juga disebut ”jurisdiksi formulatif”).*Kedua*, kewenangan mengadili atau menerapkan hukum (oleh karena itu disebut jurisdiksi judisial atau aplikatif). *Ketiga*, kewenangan melaksanakan/memaksakan kepatuhan hukum yang dibuatnya (oleh karena itu, disebut jurisdiksi eksekutif).[141]

Menurut Barda Nawawi Arief, problem jurisdiksi yang menonjol adalah masalah jurisdiksi judisial (kewenangan mengadili atau menerapkan hukum) dan jurisdiksi eksekutif (kewenangan melaksanakan putusan) daripada masalah jurisdiksi legislatif (kewenangan pembuatan hukum) Dikatakan demikian karena masalah jurisdiksi judisial/adjudikasi dan jurisdiksi eksekutif sangat terkait dengan kedaulatan wilayah dan kedaulatan hukum masing-masing Negara.[142]

Menurut Hikmahanto Juwono dalam konteks hukum Internasional, terdapat beberapa prinsip yang digunakan untuk menegaskan siapa yang memiliki kewenangan untuk mengadili, dikatakannya:[143]

---

[140] Masaki Hamano,”*Comparative Study in the Approach to Jurisdiction in Cyberspace” Chapter: The Principle of Jurisdiction*,hal.1. lihat dalam Barda Nawawi Arief, *Tindak Pidana Mayantara, Op.Cit.*,hal.27-28.

[141] Barda Nawawi Arief, *Kapita Selekta Hukum Pidana*, PT.Citra Aditya Bakti, Bandung,2003,hal.247.

[142] Barda Nawawi Arief, *Sari Kuliah: Perbandingan Hukum Pidana*, PT. Raja Grafindo Persada, Jakarta, 2006, hal.280.

[143] Diakses dari http://www.Hukumonline.com:”jurisdiksi”, 1 Agustus 2008.

Ada beberapa prinsip yang diterapkan, antara lain teritorial, personalitas, nasionalitas, dan universal. Masing-masing prinsip memiliki karakter yang berbeda satu sama lain. Misalkan, prinsip teritorial yang mendasarkan pada wilayah dimana tindak pidana itu terjadi. Di samping itu, juga bisa dilihat dari munculnya akibat. Kemudian, prinsip personalitas dan universalitas. Tiap-tiap prinsip memiliki karakter yang berbeda antara satu dengan yang lain. Prinsip teritorial mendasarkan pada wilayah dimana tindak pidana itu terjadi, bisa juga dari tempat munculnya akibat tindak pidana.

Prinsip personalitas menekankan pada kewarganegaraan dari si pelaku. Misalnya jika pelaku adalah warga negara Indonesia, maka si pelaku bisa disidangkan di Pengadilan Indonesia. Pada prinsip nasionalitas yang ditekankan adalah kepentingan dari negara tempat terjadinya tindak pidana. Prinsip terakhir yaitu prinsip universal yang lebih menekankan kejahatan internasional. Setiap negara yang berkepentingan bisa menerapkan dimana saja,kapan saja, dan bagi siapa saja sepanjang kejahatan tersebut tergolong sebagai kejahatan internasional.

Negara-negara yang tergabung dalam Uni Eropa *(Council of Europe)* pada tanggal 23 November 2001 di kota Budapest, Hongaria telah membuat dan menyepakati *Convention on Cybercrime* yang kemudian dimasukkan dalam *European Treaty Series* dengan Nomor 185. Tujuan Konvensi tersebut adalah untuk melindungi masyarakat dari *cybercrime*, baik melalui undang-undang maupun kerjasama internasional. Hal ini dimaksudkan untuk mengatasi kejahatan *cyber*, tanpa mengurangi kesempatan setiap individu untuk tetap dapat mengembangkan kreativitasnya dalam pengembangan teknologi informasi. Pada *Section* 3, *Article* 22 Konvensi tersebut diatur masalah jurisdiksi, dinyatakan:[144]

1. *Each Party shall adopt such legislative and other measures as may be necessary to estabilish jurisdiction over any offence estabilished in accordance with Article 2 through 11 of this convention,when the offence is commited:*

[144] *Council of Europe, European Treaty Series* No.185,Budapest 23.IX.2001,page 13

a. *In its teritorry; or*
b. *On board a ship flying the flag of that party;or*
c. *On board an aircraft registered under the laws of that party;or*
d. *By one its national,if the offence is punishable under criminal law where it was commited outside the territorial jurisdiction of any state.*

2. *Each party may reserve the right not to apply only in specific cases or conditions the jurisdiction rules laid down in paragrphs 1.b through 1.d of this article or any part there of;*

3. *Each party shall adopt such measures as may be necesarry to estabilish jurisdiction over the offences reffered to in Article 24,paragraph 1, of this convention, in cases where an alleged offender is present in its territory and it does not estradite him or her to another party,solely on the basis of his or her natonality,after a request for extradition;*

4. *This convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law;*

5. *when more than one Party claims jurisdiction over an alleged offence estabilished in accordance with this Convention, the Parties involved shall, where apporiate,consult with a view to determining the most apporiate jurisdiction for prosecution.*

Barda Nawawi Arief menerjemahkannya sebagai berikut:[145]

1. Tiap Pihak (Negara) akan mengambil langkah-langkah legislatif dan langkah-langkah lain yang diperlukan untuk menetapkan jurisdiksi terhadap setiap tindak pidana yang ditetapkan sesuai dengan Pasal 2-11 Konvensi ini, apabila tindak pidana itu dilakukan:

   a. di dalam wilayah teritorialnya; atau

   b. di atas kapal yang mengkibarkan bendera negara yang bersangkutan; atau

   c. di atas pesawat yang terdaftar menurut hukum negara yang bersangkutan;atau

   d. oleh seseorang dari warga negaranya, apabila tindak pidana itu dapat dipidana menurut hukum pidana di tempat tindak pidana itu dilakukan atau apabila tindak pidana itu dilakukan di luar jurisdiksi teritorial setiap negara.

[145] Barda Nawawi Arief, *Sari Kuliah: Perbandingan Hukum Pidana, Op.Cit*,hal.280-281

2. Tiap negara berhak untuk tidak menerapkan atau hanya menerapkan aturan jurisdiksi sebagaimana disebut dalam ayat (1)b-ayat(1)d Pasal ini dalam kasus-kasus atau kondisi-kondisi tertentu.
3. Tiap pihak (negara) akan mengambil langkah-langkah yang diperlukan untuk menetapkan jurisdiksi terhadap tindak pidana yang ditunjuk dalam Pasal 24 ayat (1) Konvensi ini dalam hal tersangka berada di wilayahnya dan negara itu tidak mengekstradisi tersangka itu ke negara lain (semata-mata berdasar alasan kewarganegaraan tersangka), setelah adanya permintaan ekstradisi.
4. Konvensi ini tidak meniadakan jurisdiksi kriminal yang dilaksanakan sesuai dengan hukum domestik (hukum negara yang bersangkutan);
5. Apabila lebih dari satu pihak (negara) menyatakan berhak atas jurisdiksi tindak pidana dalam konvensi ini, maka para Pihak yang terlibat akan melakukan kosultasi untuk menetapkan jurisdiksi yang paling tepat untuk penuntutan.

Terhadap ketentuan di atas konvensi memberikan penjelasan antara lain sebagai berikut:[146]

1. Ayat (1) sub a di atas didasarkan pada asas teritorialitas. Jurisdiksi teritorial ini dapat berlaku, baik apabila pelaku/penyerang komputer dan korbannya berada di wilayahnya maupun apabila komputer yang diserang berada di wilayahnya, tetapi si penyerang tidak berada di wilayahnya. Ayat (1) sub b dan sub c didasarkan pada perluasan asas teritorialitas yang telah diimplementasi di banyak negara, dan ayat (1) sub d didasarkan pada asas nasionalitas.
2. Ayat (2) membolehkan negara untuk mengajukan keberatan/persyaratan (reservasi) terhadap ayat (1) sub b, sub c dan sub d, tetapi tidak untuk ayat (1) sub a atau ayat (3) diperlukan untuk menjamin negara yang menolak ekstradisi warga negaranya mempunyai kemampuan hukum untuk melakukan investegasi dan proses menurut hukumnya sendiri.
3. Jurisdiksi dalam ayat (1) tidak bersifat eksekutif. Oleh karena itu, ayat (4) membolehkan para pihak sesuai dengan hukum nasionalnya,untuk menetapkan juga tipe-tipe jurisdiksi yang lain.

[146] Barda Nawawi Arief, *Kapita Selekta Hukum Pidana, Op.Cit*.,hal.252.

4. Konsultasi dalam ayat (5) tidak bersifat absolut, tetapi apabila dipandang tepat. Misalnya suatu negara bisa memandang tidak perlu melakukan konsultasi apabila sudah diketahui bahwa negara lain itu tidak berencana untuk melakukan tindakan atau apabila konsultasi itu dipandang akan mengganggu proses penyelidikan.

Masalah jurisdiksi berkaitan dengan kecakapan dari suatu forum tertentu untuk mengadili kasus (*adjudicate jurisdiction*). Jurisdiksi dalam *cyberspace* dapat menggunakan teori:[147]

a. *The therory of uploader* and downloader.*Uploader* adalah pemberi informasi dan *downloader* adalah penerima transaksi elektronik.

b. *The law of the server*.Jurisdiksi ditentukan dengan menggunakan atau memperlakukan server dimana webpages secara fisik berlokasi,yaitu dimana mereka dicatat sebagai data elektronik.

c. *The theory of internasional spaces*, ada usulan bahwa *internet* dijadikan ruang tersendiri, menjadi ruang ke empat setelah air,darat, dan udara.

Pengaturan mengenai masalah jurisdiksi merupakan hal penting, dan dalam pembentukan undang-undang khusus mengenai *cybercrime* perlu dipikirkan bentuk jurisdiksi yang mampu menjangkau kejahatan di dunia siber mengingat kejahatan ini punya karakter yang khas dan sifatnya lintas negara (*transborder*). Dengan demikian penerapan asas universal (asas ubikuitas) dapat digunakan disamping juga diperlukan kerjasama dengan negara-negara lain.

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 dari 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

[147] Edmon Makarim,*Kompilasi Hukum Telematika*,Raja Grafindo Persada, Jakarta,2003,hal.305.

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.[148]

- 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.[149]

[148] Pasal 2 Undang-Undang No.11 tahun 2008 tentang Informasi dan Transaksi Elektronik, diundangkan pada 28 April 2008, Lembaran Negara No.58.

[149] Penjelasan Pasal 2 Undang-Undang No.11 tahun 2008 tentang Informasi dan Transaksi Elektronik, diundangkan pada 28 April 2008, Lembaran Negara No.58.

BAB III

HASIL PENELITIAN DAN ANALISIS

A. KEBIJAKAN FORMULASI HUKUM PIDANA TERHADAP TINDAK PIDANA TEKNOLOGI INFORMASI SAAT INI

Globalisasi teknologi informasi yang telah mengubah dunia ke era *cyber* dengan sarana internet yang menghadirkan *cyberspace* dengan realitas virtualnya menawarkan kepada manusia berbagai harapan dan kemudahan. Akan tetapi di balik itu, timbul persoalan berupa kejahatan yang dinamakan *cybercrime*, baik sistem jaringan komputernya itu sendiri yang menjadi sasaran maupun komputer itu sendiri yang menjadi sarana untuk melakukan kejahatan. Tentunya jika kita melihat bahwa informasi itu sendiri telah menjadi komoditi maka upaya untuk melindungi aset tersebut sangat diperlukan.

Kebijakan sebagai upaya untuk melindungi informasi membutuhkan suatu pengkajian yang sangat mendalam, menyangkut aspek sosiologis, filosofis, yuridis, dan sebagainya. Teknologi informasi sekarang ini sangat strategis dan berdampak luas terhadap aktifitas kehidupan manusia oleh karena itu dibutuhkan pengaturan secara khusus dengan dibentuk nya suatu undang-undang yang dapat menanggulangi kejahatan terhadap teknologi informasi.

Peraturan terhadap teknologi informasi agar diterima masyarakat harus mempertimbangkan semua aspirasi (suprastruktur, infrastruktur, kepakaran dan aspirasi internasional) dan pelbagai kepentingan harus diselaraskan dan diserasikan. Persoalan komunikasi massa menempati posisi yang strategis dalam kehidupan demokrasi, dan ini akan bersentuhan secara langsung tidak hanya dengan persoalan supremasi hukum yang bersifat "*top down*" misalnya untuk kepentingan keamanan negara, persatuan dan kesatuan nasional – tetapi

juga sebaliknya, "*bottom up*", sebab orang cenderung akan melemparkan banyak pertanyaan kritis.[150]

Kebijakan hukum pidana (tataran aplikatif) sangat dipengaruhi sistem hukum yang berlaku saat ini. Hukum pidana Indonesia yang ada saat ini dan pengembangan ke depan dipengaruhi oleh tradisi hukum *civil law*. Politik hukum yang cenderung mengarah pada tradisi *civil law* mengandung konsekuensi sebagai berikut:

1. Peraturan perundang-undangan harus dirumuskan secara teliti dan lengkap sehingga diharapkan mampu menjangkau semua permasalahan yang timbul.
2. Asas legalitas ditempatkan sebagai landasan yang bersifat fundamental dan dalam pelaksanaannya harus dijunjung tinggi tanpa kecuali.
3. Operasionalisasi peraturan perundang-undangan diupayakan seoptimal mungkin untuk menangani berbagai kasus yang bervariasi dengan pendekatan penafsiran (interpretasi).

Instrumen hukum memberikan landasan atau pedoman bagi para penegak hukum yang akan diterapkan kepada para pelaku *cybercrime*. Sebagai hukum positif, pembuatannya tentu melalui mekanisme pembuatan perundang-undangan dan sekaligus melekat sifat *ius constitutum*, yakni menjadi hukum positif yang memberikan sanksi bagi peristiwa atau perbuatan kriminal yang menggunakan komputer.

Pembentukan peraturan perundang-undangan di dunia *cyber* pun, berpangkal pada keinginan masyarakat untuk mendapatkan jaminan keamanan, keadilan dan kepastian hukum. Sebagai norma hukum *cyber* atau *cyber law* akan bersifat mengikat bagi tiap-tiap individu-individu untuk tunduk dan mengikuti segala kaidah-kaidah yang terkandung didalamnya.

[150] Muladi, Demokratisasi,*Hak Asasi Manusia dan Reformasi Hukum di Indonesia, Op.Cit*., hal.201.

A.1 Kebijakan Formulasi Sebelum Undang-Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Sebelum diundangkannya Undang-Undang No.11 tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang mengatur secara khusus tentang pemanfaatan teknologi informasi, sebenarnya Indonesia dalam persoalan *cybercrime* tidak ada kekosongan hukum, ini terjadi jika digunakan metode penafsiran yang dikenal dalam ilmu hukum dan ini yang mestinya dipegang oleh aparat penegak hukum dalam menghadapi perbuatan-perbuatan yang berdimensi baru yang secara khusus belum diatur dalam undang-undang.[151]

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 *cybercrime* 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 dari kejahatan konvensional/ di dunia biasa. Sebelum disahkannya UU ITE terdapat beberapa peraturan perundang-undangan yang dapat digunakan untuk menanggulangi tindak pidana di dunia maya.

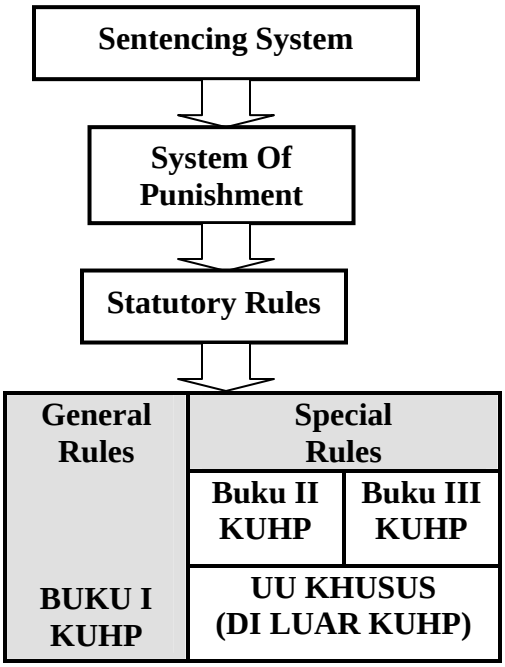
A.1.1 Kitab Undang-Undang Hukum Pidana (KUHP)

[151] Badan Pembinaan Hukum Nasional, Perkembangan Pembangunan Hukum Nasional tentang Hukum Teknologi dan Informasi, BPHN Departemen Kehakiman RI, 1995/1996, hal. 32-34

Kitab Undang-Undang Hukum Pidana (KUHP) yang berlaku sekarang ini berasal dari *Wetboek van Strafrecht voor Nederlandsh Indie* (WvSNI) dengan berbagai perubahan untuk disesuaikan dengan keadaan di Indonesia (Hindia Belanda) saat itu. Sebagai sumber hukum pidana disamping sumber-sumber lainnya, KUHP menduduki posisi yang amat penting, hal ini karena KUHP memuat asas-asas hukum pidana yang dapat dilihat pada Buku Ke-satu mengenai aturan umum. Sistem hukum pidana substantif yang berlaku saat ini dapat digambarkan sebagai berikut:

Gambar 1

Sistem Pemidanaan Substantif



Berdasarkan gambar di atas, sistem peraturan perundang-undangan (*statutory rules*) yang ada di dalam KUHP sebagai induk aturan umum sehingga undang-undang khusus di luar KUHP terikat kepada ketentuan umum yang ada di dalam KUHP (Buku 1). KUHP terbagi atas aturan umum yang terdapat di dalam KUHP (Buku I), dan aturan khusus terdapat di dalam KUHP (Buku II dan III). Namun patut dicatat, bahwa ketentuan umum KUHP yang mengikat (yang berlaku) untuk undang-undang khusus, hanyalah Bab I s/d VIII (Pasal 1 s/d 85) Buku I KUHP,

sepanjang undang-undang khusus tidak membuat ketentuan lain yang menyimpang (Lihat Pasal 103 KUHP). Ketentuan umum dalam Bab IX Buku I KUHP (Pasal 86 s/d 102) hanya berlaku untuk KUHP, tidak untuk undang-undang khusus di luar KUHP.

Sejak diberlakukannya KUHP telah mengalami perubahan dan penambahan. Hal ini dilakukan untuk menghadapi permasalahan-permasalahan yang muncul seiring dengan berkembangnya masyarakat, pengetahuan dan teknologi yang menyertainya. Perubahan-perubahan dalam KUHP antara lain: Pemberatan ancaman pidana untuk Pasal 138, Pasal 359 dan Pasal 360 yang dianggap terlalu ringan (UU No.1 Tahun 1960), perubahan terhadap jumlah denda yang disesuaikan dengan perubahan nilai mata uang (UU No. 18/prp/1960), perubahan tentang penertiban perjudian (UU No.7 Tahun 1974), penambahan ketentuan mengenai kejahatan penerbangan (UU No. 4 Tahun 1976), perubahan yang berkaitan dengan kejahatan terhadap keamanan negara (UU No. 27 tahun 1999).

KUHP sampai saat ini belum melakukan perubahan dan penambahan terhadap tindak pidana yang berhubungan dengan mayantara terutama yang berhubungan dengan penyalahgunaan internet, alat bukti elektronik, yurisdiksi dan sebagainya. Selanjutnya akan dibahas formulasi dalam KUHP yang berhubungan dengan penanggulangan tindak pidana teknologi informasi.

A.1.1.1 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. Adapun pasal-

pasal yang dapat dikenakan dalam KUHP yang mengkriminalisasi terhadap kejahatan dunia maya, sebagaimana dikatakan oleh Petrus Reinhard Golose di antaranya adalah :[152]

a. Pasal 362 KUHP untuk kasus *Carding* dimana pelaku mencuri kartu kredit milik orang lain walaupun tidak secara fisik karena hanya nomor kartunya saja yang diambil dengan menggunakan *software card generator* di internet untuk melakukan transaksi di *E-Commerce*.
b. Pasal 378 KUHP untuk penipuan dengan seolah-olah menawarkan dan menjual suatu produk atau barang dengan memasang iklan di salah satu *website* sehingga orang tertarik untuk membelinya lalu mengirimkan uang kepada pemasang iklan.
c. Pasal 335 KUHP dapat dikenakan untuk kasus pengancaman dan pemerasan yang dilakukan melalui *e-mail*.
d. Pasal 331 KUHP dapat dikenakan untuk kasus pencemaran nama baik dengan menggunakan media internet. Modusnya adalah pelaku menyebarkan *e-mail* kepada teman-teman korban tentang suatu cerita yang tidak benar atau mengirimkan *e-mail* secara berantai melalui *mailling list* (*millis*) tentang berita yang tidak benar.
e. Pasal 303 KUHP dapat dikenakan untuk menjerat permainan judi yang dilakukan secara *on-line* di internet dengan penyelenggara dari Indonesia.
f. Pasal 282 KUHP dapat dikenakan untuk penyebaran pornografi maupun *website* porno yang banyak beredar dan mudah diakses di internet.
g. Pasal 282 dan 311 KUHP dapat dikenakan untuk penyebaran foto atau film pribadi seseorang yang vulgar di internet.

[152] Petrus Reinhard Golose, *Perkembangan Cybercrime dan Upaya Penanggulangannya di Indonesia Oleh Polri*, Buliten Hukum Perbankan dan Kebanksentralan, Volume 4 Nomor 2, Jakarta, Agustus 2006, hal. 38-39.

h. Pasal 378 dan 262 KUHP dapat dikenakan pada kasus *carding*, karena pelaku melakukan penipuan seolah-olah ingin membeli suatu barang dan membayar dengan kartu kredit yang nomor kartu kreditnya merupakan hasil curian.

i. Pasal 406 KUHP dapat dikenakan pada kasus *deface* suatu *website*, karena pelaku setelah berhasil memasuki *website* korban, selanjutnya melakukan pengrusakan dengan cara mengganti tampilan asli dari *website* tersebut.

Terhadap perbuatan dalam ketentuan-ketentuan pasal di atas, masalah yang timbul adalah interpretasi terhadap unsur-unsur pasal karena rumusan pasal-pasal tersebut tidak disebutkan data komputer atau informasi yang dihasilkan komputer. Perkembangan teknologi informasi seiring berkembangannya sistem jaringan komputer telah mengubah pandangan konvensional terhadap unsur barang atau benda sebagai alat bukti menjadi *digital evidence* atau alat bukti elektronik baik sebagai media seperti *disket, tape storage, disk storage*, *compact disk, hard disk, USB, flash disk* dan hasil cetakan bukti elektronis tersebut.

Jaringan komputer yang menghasilkan *cyberspace* dan komunitas virtualnya berkembang seiring dengan berkembangnya kejahatan yang menghasilkan tindak pidana yang dianggap dahulu tidak mungkin pada saat sekarang ini menjadi mungkin bahkan dampaknya dapat dirasakan diluar tempat/wilayah negara. Oleh karena itu penerapan pasal-pasal KUHP sudah tidak relevan dalam penanggulangan tindak pidana teknologi informasi.

A.1.1.2 Subjek, Sanksi Pidana dan Aturan Pemidanaan dalam KUHP

Sesuatu dapat dikatakan sebagai tindak pidana apabila ada subjek (pelaku) dari 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: [153]

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.

Dari 9 (sembilan) bentuk perumusan di atas, dapat diidentifikasikan hal-hal sebagai berikut:[154]

1. KUHP hanya menganut 2 (dua) sistem perumusan, yaitu:
    a. perumusan tunggal yaitu hanya diancam 1 (satu) pidana pokok;

[153] Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana*, *Op.Cit*.hal.165-166.
[154] Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana*, *Op.Cit*.hal.166.

b. perumusan alternatif.

2. Pidana pokok yang diancam/dirumuskan secara tunggal, hanya pidana penjara, kurungan atau denda. Tidak ada pidana mati atau penjara seumur hidup yang diancam secara tunggal.
3. Perumusan alternatif dimulai dari pidana pokok terberat sampai yang paling ringan.

Aturan pemidanaan dalam KUHP berorientasi pada "*strafsoort"* yang ada/ disebut dalam KUHP, baik berupa pidana pokok maupun pidana tambahan. jenis pidana yang dirumuskan/diancamkan dalam perumusan delik hanya pidana pokok dan/atau pidana tambahannya. Pidana kurungan pengganti tidak dirumuskan dalam perumusan delik (aturan khusus), tetapi dimasukkan dalam aturan umum mengenai pelaksanaan pidana ("*strafmodus*"). Dilihat dari sudut "*strafmaat*" (ukuran jumlah/lamanya pidana), aturan pemidanaan dalam KUHP berorientasi pada sistem minimal umum dan maksimal khusus, tidak berorientasi pada sistem minimal khusus. Artinya, di dalam KUHP tidak ada aturan pemidanaan untuk ancaman pidana minimal khusus.

A.1.1.3 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 (*recidive*). Ketiga bentuk tindak pidana ini hanya diatur dalam aturan khusus (Buku II atau Buku III).

Artinya, ketentuan mengenai permufakatan jahat, persiapan, dan pengulangan di dalam KUHP hanya berlaku untuk delik-delik tertentu dalam KUHP, tidak untuk delik di luar KUHP.

A.1.2 Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi

Menurut definisi yang termuat dalam undang-undang telekomunikasi ini, yang dimaksud dengan telekomunikasi (Pasal 1 angka (1)) ialah setiap pemancaran, pengiriman, dan/atau penerimaan dari setiap informasi dalam bentuk tanda-tanda, isyarat, tulisan, gambar, suara, dan bunyi melalui sistem kawat, optik, radio, atau sistem elektromagnetik lainnya. Perangkat telekomunikasi ialah setiap alat-alat perlengkapan yang digunakan dalam bertelekomunikasi. Dan yang dimaksud dengan jaringan telekomunikasi ialah rangkaian perangkat telekomunikasi dan kelengkapannya yang digunakan dalam bertelekomunikasi.

Alasan dikeluarkannya Undang-Undang Telekomunikasi dalam penjelasan umum undang-undang tersebut menyatakan bahwa penyelenggaraan telekomunikasi nasional menjadi bagian yang tidak terpisahkan dari sistem perdagangan global. Pengaruh globalisasi dan perkembangan teknologi komunikasi yang sangat pesat telah mengakibatkan perubahan yang mendasar dalam penyelenggaraan dan cara pandang terhadap telekomunikasi.

A.1.2.1 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 adalah sebagai berikut:

Pasal 21:

- Penyelenggara telekomunikasi dilarang melakukan kegiatan usaha penyelenggaraan telekomunikasi yang bertentangan dengan kepentingan umum, kesusilaan, keamanan, atau ketertiban umum.
- Pasal 21 Undang-Undang Telekomunikasi tersebut tidak mengatur terhadap kejahatan dan tidak diatur dalam ketentuan pidana (Bab VII Ketentuan Pidana Pasal 47 sampai dengan Pasal 57). Ketentuan terhadap Pasal 21 berarti hanya merupakan pelanggaran yang berdasarkan ketentuan Bab VI Pasal 46 sanksinya berupa pencabutan izin. Akibat ringannya sanksi hukum tersebut pornografi dan tindakan pengasutan melalui media telekomunikasi sering terjadi dan dilakukan oleh penyelenggara telekomunikasi.

Pasal 50 juncto Pasal 22:

- Barang siapa yang melanggar ketentuan sebagaimana dimaksud dalam pasal 22 dipidana dengan pidana penjara paling lama 6 (enam) tahun dan / atau denda paling banyak Rp.600.000.000,-(enam ratus juta rupiah).
- Pasal 50 mengkriminalisasi terhadap perbuatan tanpa hak, tidak sah atau memanipulasi akses ke jaringan telekomunikasi khusus (Pasal 22 huruf a,b dan c UU

Telekomunikasi). Unsur-unsur perbuatan tersebut merupakan landasan dalam penyidikan tindak pidana *hacking* website KPU (www.kpu.go.id). Penerapan pasal tersebut terhadap perbuatan *hacking* masih sangat luas dan tidak ditegaskan secara khusus terhadap perbuatan memanipulasi dalam dunia maya.

Pasal 55 juncto Pasal 38:

- Barang siapa yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 38, dipidana dengan pidana penjara paling lama 6 (enam) tahun dan atau denda paling banyak Rp600.000.000,00 (enam ratus juta rupiah).
- Pasal 55 mengkriminalisasi perbuatan yang dapat menimbulkan gangguan fisik elektromagnetik terhadap penyelenggara telekomunikasi (Pasal 38 UU Telekomunikasi). Pasal 55 juncto Pasal 38 berkaitan dengan kerahasiaan, integritas dan keberadaan data dan sistem telekomunikasi, namun pasal ini tidak secara tegas menyebutkan untuk kegiatan di dunia maya (internet).

Pasal 56 juncto Pasal 40:

- Barang siapa yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 40, dipidana dengan pidana penjara paling lama 15 (lima belas) tahun.
- Pasal 56 melarang setiap orang melakukan kegiatan penyadapan atas informasi yang disalurkan melalui jaringan telekomunikasi dalam bentuk apapun (Pasal 40 UU Telekomunikasi). Penjelasan Pasal 40 menyatakan Yang dimaksud dengan penyadapan dalam pasal ini adalah kegiatan memasang alat atau perangkat tambahan pada jaringan telekomunikasi untuk tujuan mendapatkan informasi dengan cara tidak sah. Hal ini tidak relevan dengan tindak pidana *cybercrime* yang dapat melakukan intersepsi atau penyadapan Informasi Elektronik dan/atau Dokumen Elektronik dalam

suatu Komputer dan/atau Sistem Elektronik (*Illegal interception)* melalui internet tanpa harus memasang alat tambahan.

A.1.2.2 Subjek dan Kualifikasi Tindak Pidana dalam UU Telekomunikasi

Subjek tindak pidana dalam UU Telekomunikasi adalah orang dan korporasi dalam hal ini yang dimaksud dengan korporasi adalah penyelenggara jasa telekomunikasi. Hal ini berdasarkan Pasal 1 angka 8 UU Telekomunikasi yang menyebutkan penyelenggara telekomunikasi adalah perseorangan, koperasi, Badan Usaha Milik Daerah (BUMD), Badan Usaha Milik Negara (BUMN), badan usaha swasta, instansi pemerintah, dan instansi pertahanan keamanan negara. Undang-undang tersebut tidak mengatur kapan atau dalam hal bagaimana korporasi dikatakan telah melakukan tindak pidana.

Penegasan terhadap kualifikasi yuridis sebagai kejahatan terhadap pasal-pasal tertentu dalam UU Telekomunikasi, dinyatakan dalam Pasal 59 UU Telekomunikasi yaitu Perbuatan sebagaimana dimaksud dalam Pasal 47, Pasal 48, Pasal 49, Pasal 50, Pasal 51, Pasal 52, Pasal 53, Pasal 54, Pasal 55, Pasal 56, dan Pasal 57 adalah kejahatan. Penegasan terhadap kualifikasi yuridis sebagai kejahatan terhadap pasal-pasal tertentu dalam UU Telekomunikasi sebagaimana tertulis dalam Pasal 59 sangat diperlukan karena terdapat beberapa pasal yang diancam dengan pidana ringan dan tidakan yaitu: Pasal 16 ayat (1), Pasal 18 ayat (2), Pasal 19, Pasal 21, Pasal 25 ayat (2), Pasal 26 ayat (1), Pasal 29 ayat (1), Pasal 29 ayat (2), Pasal 33 ayat (1), Pasal 33 ayat (2), Pasal 34 ayat (1), Pasal 34 ayat (2) , Pasal 47,Pasal 48, Pasal 52 dan Pasal 56.

A.1.2.3 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 dalam 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.

A.1.3 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.

Menurut Pasal 1 angka (8) Undang-Undang No 19 Tahun 2002 tentang Hak Cipta, bahwa program komputer adalah sekumpulan instruksi yang diwujudkan dalam bentuk bahasa, kode, skema ataupun bentuk lain yang apabila digabungkan dengan media yang dapat dibaca dengan komputer akan mampu membuat komputer bekerja untuk melakukan fungsi-fungsi khusus atau untuk mencapai hasil yang khusus, termasuk persiapan dalam merancang instruksi-instruksi tersebut.

A.1.3.1 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

sebagai tempat mengajukan gugatan yang dapat menjatuhkan tindakan administratif dan jalur penal yang terlihat dengan adanya ketentuan pidana dalam Pasal 72 UU Hak Cipta.

Kriminalisasi perbuatan yang berhubungan dengan tindak pidana teknologi informasi dalam UU Hak Cipta berhubungan dengan perbuatan pembajakan dan peredaran program komputer sebagaimana sebagaimana diatur dalam Pasal 72 ayat (1) , (2) dan (3) Undang-Undang Hak Cipta yaitu:

Pasal 72:

(1) Barangsiapa dengan sengaja dan tanpa hak melakukan perbuatan sebagaimana dimaksud dalam Pasal 2 ayat (1) atau Pasal 49 ayat (1) dan ayat (2) dipidana dengan pidana penjara masing-masing paling singkat 1 (satu) bulan dan/atau denda paling sedikit Rp 1.000.000,00 (satu juta rupiah), atau pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp 5.000.000.000,00 (lima miliar rupiah).

(2) Barangsiapa dengan sengaja menyiarkan, memamerkan, mengedarkan, atau menjual kepada umum suatu Ciptaan atau barang hasil pelanggaran Hak Cipta atau Hak Terkait.sebagaimana dimaksud pada ayat (1) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau denda paling banyak Rp 500.000.000,00 (lima ratus juta rupiah).

(3) Barangsiapa dengan sengaja dan tanpa hak memperbanyak penggunaan untuk kepentingan komersial suatu Program Komputer dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau denda paling banyak Rp 500.000.000,00 (lima ratus juta rupiah).

Penjualan *software* bajakan yang sangat murah dibandingkan harga aslinya mengakibatkan semakin berkembangnya produk *software* bajakan dimana-mana. Harga program komputer/*software* yang sangat mahal bagi warga Negara Indonesia merupakan peluang yang

cukup menjanjikan bagi para pelaku bisnis guna menggandakan serta menjual *software* bajakan dengan harga yang sangat murah. Maraknya pembajakan *software* di Indonesia yang terkesan "dimaklumi" tentunya sangat merugikan pemilik Hak Cipta.

Tindak pidana teknologi informasi sebagaimana diatur dalam Pasal 72 di atas belum mencakup perlindungan terhadap objek hak cipta lainnya yang ada dalam aktivitas dunia maya. Pelanggaran hak cipta seperti *download* lagu dan musik dengan pemanfaatan internet dan fasilitas penggunaan *ringtone* sebagai alat komunikasi telepon seluler terus berkembang dilain pihak pembajakan hak cipta melalui *E-book, digital library*, penggunaan *link* dan *hyperlink* di internet juga tidak diatur dalam UU Hak Cipta.

A.1.3.2 Subjek dan Kualifikasi Tindak Pidana dalam UU Hak Cipta

Subjek tindak pidana dalam UU Hak Cipta hanya berorientasi pada "orang" (*natural person*), undang-undang tersebut tidak mengatur terhadap subjek tindak pidana korporasi. Pelanggaran terhadap hak cipta seharusnya mengatur terhadap subjek tindak pidana korporasi karena pelaku tindak pidana Hak Cipta tidak hanya orang perorangan tetapi juga dimungkinkan dilakukan oleh suatu badan hukum/korporasi.

Undang-Undang Hak Cipta tidak menyebutkan kualifikasi delik berupa kejahatan dan Pelanggaran secara tegas. Seyogianya undang-undang di luar KUHP menyebutkan kualifikasi delik tersebut karena sistem pemidanaan di luar KUHP merupakan sub/bagian integral dari keseluruhan sistem pemidanaan, sehingga fungsi dari ditetapkannya kualifikasi yuridis itu adalah untuk menjembatani berlakunya aturan umum KUHP terhadap hal-hal yang tidak diatur dalam UU Hak Cipta.

A.1.3.3 Sanksi Pidana dan Aturan Pemidanaan dalam UU Hak Cipta

Sistem perumusan sanksi pidana dalam Undang-Undang Hak Cipta kebanyakan dilakukan secara alternatif komulatif. Di samping itu UU Hak Cipta juga menggunakan ancaman pindana minimal khusus (Pasal 72 ayat (1)) , penggunaan ancaman pidana minimal khusus tidak disertai dengan aturan atau pedoman pemidanaan untuk menerapkan ancaman pidana minimal khusus tersebut.

Dianutnya sistem minimal khusus dalam Pasal 72 ayat (1) yang menyimpang dari KUHP yang hanya mengenal pidana denda minimal umum sebesar 25 sen (Pasal 30 ayat (1)), maka seharusnya UU Hak Cipta membuat aturan khusus/tersendiri untuk penerapannya. Ini merupakan kosekuensi dari adanya Pasal 103 KUHP, karena KUHP sendiri belum mengatur masalah ini.

Jenis sanksi pidana yang diterapkan dalam UU ini yaitu pidana penjara, pidana denda dan pidana tambahan. Pidana tambahan berupa sanksi administrasi juga perampasan untuk dimusnahkan oleh negara (Pasal 73 ayat (1)), serta tindakan khusus terhadap ciptaan yang bersifat unik dapat dipertimbangkan untuk tidak dimusnahkan.

A.1.4 Undang-Undang No 25 Tahun 2003 tentang Perubahan atas Undang-Undang No. 15 Tahun 2002 tentang Tindak Pidana Pencucian Uang

Money Laundering dikenalkan sebagai hasil kejahatan pada tahun 1920 di Chicago oleh Al-Capone, yang digunakan untuk memperoleh kembali keuntungannya dari perjudian dan minuman keras. Yang dimaksud dengan *money laundering* adalah suatu proses dimana hasil perolehan dari aktivitas kejahatan, dikirim, ditransfer, diubah atau dicampur menjadi hasil

perolehan dari aktivitas yang sah, dengan tujuan untuk menyembunyikan asal kebenaran perolehan keuntungan tersebut atau dari mana sumber memperoleh uang tersebut.[155]

Harta Kekayaan yang berasal dari berbagai kejahatan atau tindak pidana tersebut, pada umumnya tidak langsung dibelanjakan atau digunakan oleh para pelaku kejahatan karena apabila langsung digunakan akan mudah dilacak oleh penegak hukum mengenai sumber diperolehnya Harta Kekayaan tersebut. Biasanya para pelaku kejahatan terlebih dahulu mengupayakan agar Harta Kekayaan yang diperoleh dari kejahatan tersebut masuk ke dalam sistem keuangan (*financial system*), terutama ke dalam sistem perbankan (*banking system*). Dengan cara demikian, asal usul Harta Kekayaan tersebut diharapkan tidak dapat dilacak oleh para penegak hukum.

Perkembangan dan kemajuan ilmu pengetahuan dan teknologi khususnya di bidang komunikasi telah menyebabkan terintegrasinya sistem keuangan termasuk sistem perbankan yang menawarkan mekanisme lalu lintas dana antar negara yang dapat dilakukan dalam waktu yang sangat singkat. Keadaan ini di samping mempunyai dampak positif, juga membawa dampak negatif bagi kehidupan masyarakat yaitu dengan semakin meningkatnya tindak pidana yang berskala nasional maupun internasional, dengan memanfaatkan sistem keuangan termasuk sistem perbankan untuk menyembunyikan atau mengaburkan asal-usul dana hasil tindak pidana (*money laundering*).

Meningkatnya tindak pidana dengan memanfaatkan sistem perbankan tersebut melandasi diamandemennya UU No.15 Tahun 2002 dengan keluarnya UU No.25 tahun 2002 tentang Tindak Pidana Pencucian Uang (TPPU). Ketentuan dalam Undang-Undang No.15 Tahun 2002 tersebut dirasakan oleh pemerintah belum memenuhi standar internasional serta perkembangan

[155] James R. Richards, *Transnational Criminal Organizations, cybercrime and Money Laundering; A Handbook for law Enforcement Officers, Auditors and Financial Investigators*, CRC Press, London New Work Washington, D.C,1999, hal. 123

proses peradilan tindak pidana pencucian uang sehingga perlu diubah, agar upaya pencegahan dan pemberantasan tindak pidana pencucian uang dapat berjalan secara efektif,

A.1.4.1 Kriminalisasi Tindak Pidana Teknologi Informasi dalam UU TPPU

Unsur-unsur *Money Laundering* dalam UU Pencucian Uang terlihat dalam Pasal 1 sub 1 UU No.15/2002 jo.UU No.25/2003 tentang Tindak Pidana Pencucian Uang (TPPU) sebagai perbuatan menempatkan, mentransfer, membayarkan, membelanjakan, menghibahkan, menyumbangkan, menitipkan, membawa ke luar negeri, menukarkan, atau perbuatan lainnya atas Harta Kekayaan yang diketahuinya atau patut diduga merupakan hasil tindak pidana dengan maksud untuk menyembunyikan, atau menyamarkan asal usul Harta Kekayaan sehingga seolah-olah menjadi Harta Kekayaan yang sah.[156]

Asal usul kekayaan (uang) yang dicuci sebagai tindak pidana asal (*predicate crime*) dalam Pasal 2 UU No.25/2003 dirumuskan secara sangat luas sebagaimana tercantum dalam ketentuan Pasal 2 tersebut yaitu 25 tindak pidana juga terhadap tindak pidana yang diancam dengan pidana penjara 4 tahun atau lebih sehingga jumlah nya dapat mencapai ratusan tindak pidana.

Penjelasan UU No.25 Tahun 2003 dinyatakan alasan memperluas cakupan tindak pidana asal (*predicate crime*) yang semula bersifat limitatif yakni hanya terhadap 15 tindak pidana saja, dengan pertimbangan untuk mencegah berkembangnya tindak pidana yang menghasilkan Harta Kekayaan dimana pelaku tindak pidana berupaya menyembunyikan atau menyamarkan asal-usul hasil tindak pidana namun perbuatan tersebut tidak dipidana.[157]

---

[156] Undang-Undang No.25 Tahun 2003 tentang Pencucian Uang dalam Lembaran Negara Republik Indonesia Nomor 108.

[157] Penjelasan Undang-Undang No.25 Tahun 2003 tentang Pencucian Uang dalam Lembaran Negara Republik Indonesia Nomor 108.

Kebijakan kriminalisasi dalam penanggulangan tindak pidana teknologi informasi berdasarkan UU No.15/2002 jo.UU No.25/2003 tentang Tindak Pidana Pencucian Uang sebelum dikeluarkannya UU ITE, hanya terbatas terhadap tindak pidana penipuan (*carding*) dan perjudian melalui Internet (Pasal 2 Ayat (1) Huruf q dan s). Undang-Undang ini merupakan Undang-Undang yang dianggap paling efektif oleh aparat penegak hukum sebelum dikeluarkannya UU ITE karena sudah mengatur terhadap *digital evidence* (Pasal 38 huruf b) dan tidak memerlukan prosedur birokrasi yang panjang dan memakan waktu yang lama dalam proses penyelidikan terhadap pelaku.

Kemajuan teknologi saat ini serta perkembangan jenis tindak pidana *money laundering* ke arah *cyber money laundering* hendaknya didukung pula dengan kebijakan pidana terhadap *cybercrime* tersebut. Setelah disahkannya UU ITE kebijakan kriminalisasi terhadap *cyber money laundering* dapat dilakukan, walaupun tidak dirinci dengan jelas dalam dalam Pasal 2 Ayat (1) huruf y UU No.15/2002 jo.UU No.25/2003 TPPU dapat diterapkan dalam menanggulangi *cyber money laundering* hal ini dilakukan apabila kriteria *pridicate offence* diperluas dengan memasukkan tindak pidana dalam UU ITE yang mengancam dengan pidana 4 (empat) tahun atau lebih.

Upaya untuk menyembunyikan atau menyamarkan asal usul Harta Kekayaan yang diperoleh dari tindak pidana dengan menggunakan sarana *cyber* seperti pelanggaran *E-Commerce, hacking,* Penipuan dengan menggunakan komputer *(Computer related Fraud)* , Pornografi melalui internet *(Content-Related Offences),*Pelanggaran hak cipta melalui internet *(Offences related to infringements of copyright and related rights)* dan tindak pidana lain yang dimuat dalam UU ITE dapat dijadikan *pridicate offence* dalam menanggulangi tindak pidana teknologi informasi.

Kebijakan kriminalisasi terhadap *cybercrime* dengan memperluas cakupan *predicate offence* Pasal 2 Ayat (1) huruf y UU No.25/2003 terhadap UU ITE memang sudah sesuai dengan pertimbangan perluasan kriteria cakupan *pridacate offence* dalam penjelasan UU No.25/2003 yaitu untuk mencegah berkembangnya tindak pidana yang menghasilkan harta kekayaan khususnya tindak pidana berat diluar KUHP. Namun seyogianya, tindak pidana teknologi informasi/*cybercrime* dibuat secara jelas dalam cakupan *predicate offence* UU Pencucian Uang karena *cybercrime* sudah merupakan tindak pidana *organized crime* dan *transnational crime.* Beberapa negara seperti Filipina (*Anti Money Laundering Act of 2001, No.9160 Section 3 Paragraf K*) dan Myanmar (*The Control of Money Laundering Law No.6/2002 Section 5 Paragraf a Art.8*) telah membuat rambu-rambu atau kriteria yang jelas terhadap cakupan *predicate offence* terhadap tindak pidana *cyber money laundering* .

A.1.4.2 Subjek dan Klasifikasi Tindak Pidana dalam UU TPPU

Subjek tindak pidana dalam Undang-undang pencucian uang adalah orang dan korporasi. Menurut ketentuan Pasal 4 ayat (1) UU No.15/2002 jo.UU No.25/2003 TPPU apabila tindak pidana pencucian uang dilakukan oleh pengurus/kuasa pengurus atas nama korporasi, maka yang dapat dipidana adalah pengurus dan/atau kuasa pengurus maupun korporasinya. Perumusan Pasal 4 TPPU terkesan korporasi baru dapat dipidana apabila tindak pidana dilakukan oleh pengurus dan/atau kuasa pengurus. Jadi, kalau dilakukan oleh karyawan/pegawai/buruh/orang lain bukan pengurus atau bukan kuasa pengurus, maka korporasi tidak dapat dipertanggungjawabkan.

Pasal 12 UU No.15/2002 jo.UU No.25/2003 TPPU memberikan kualifikasi terhadap tindak pidana dalam Bab II dan Bab III dalam TPPU sebagai kejahatan. Kualifikasi yuridis ini mutlak diperlukan untuk menjembatani ketentuan umum dalam KUHP sebagai sub/bagian integral dari seluruh sistem pemidanaan.

A.1.4.3 Sanksi Pidana dan Aturan Pemidanaan dalam UU TPPU

Semua delik dalam Pasal 37 sampai dengan 39 UU TPPU diancam dengan pidana minimal khusus dan ancaman pidananya dirumuskan secara komulatif (penjara dan denda). Untuk subjek TPPU berupa orang UU TPPU merumuskan jenis tindak pidana pokok penjara dan denda dengan sistem pidana minimal khusus secara komulatif (tidak ada pidana tambahan atau sanksi tindakan, sedangkan untuk korporasi diatur dalam Pasal 5 yang menjatuhkan pidana pokok berupa pidana denda, dengan ketentuan maksimum pidana denda ditambah 1/3 (satu pertiga). Selain pidana denda korporasi juga dijatuhkan pidana tambahan berupa pencabutan izin usaha dan/atau pembubaran korporasi yang diikuti dengan likuidasi.

Sistem perumusan komulatif dalam UU TPPU bersifat kaku dan imperatif. Oleh karena itu, dapat menjadi masalah apabila yang dipidana korporasi. Apakah juga terhadap korporasi harus dijatuhi pidana penjara dan denda?, seyogianya dalam UU TPPU ada penegasan korporasi hanya dikenakan pidana pokok denda yang diperberat. Ketentuan pemidanaan terhadap korporasi dalam UU TPPU seyogianya memberikan aturan pelaksanaan pidana denda yang tidak dibayar oleh korporasi

Pencantuman pidana minimal khusus dalam perumusan delik merupakan suatu penyimpangan dari sistem pemidaaan induk dalam KUHP. Penyimpangan ini dapat dibenarkan, namun seharusnya disertai dengan aturan/pedoman pemidaan secara khusus, tanpa adanya pedoman tersebut dapat menimbulkan masalah yuridis dan kesulitan/kejanggalan dalam praktek penegakan hukumnya.

A.1.5 Perpu No. 1/2002 jo. Undang-Undang No 15 Tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme

Proses globalisasi dan perkembangan budaya, kemajuan teknologi persenjataan, kemajuan teknologi informasi dan telekomunikasi memicu semakin berkembangnya bentuk-bentuk terorisme, khususnya kejahatan *cyber terrorism*. Sebagaimana sebuah teori mengatakan, *crime is product of society itself* yang dapat diartikan bahwa masyarakat itu sendirilah yang melahirkan sebuah kejahatan. Semakin tinggi tingkat intelektualitas suatu masyarakat, maka semakin canggih pula kejahatan yang mungkin terjadi dalam masyarakat tersebut.

Kemajuan teknologi di bidang telekomunikasi dan informasi menjadi sarana penerapan strategi perlawanan kaum teroris secara tidak langsung (*inderect strategy*). Karena sifatnya yang tidak dibatasi ruang dan waktu maka aksi teror dapat dilakukan di mana saja dan kapan saja sebab distribusi geografisnya mencakup seluruh dunia, tidak dapat pusat kontrolnya dan kecepatan beroperasi sesuai waktu sesungguhnya (*real time speed*).

Aksi *cyber terrorism* cenderung lebih murah hanya dengan cukup kemampuan yang memadai maka aksi dapat dilakukan dengan cepat dan memberi hasil yang spektakuler. Para *hacker* dapat membobol komputer milik bank dan memindahkan dana secara melawan hukum atau menggunakan kartu kredit orang lain untuk berbelanja perlengkapan untuk aksi teror, melakukan kejahatan pencucian uang dan mengobrak-abrik sistem komputer. Melalui internet, proses komunikasi antar-anggota, koordinasi dan konsolidasi, rekruitmen dan propaganda dapat dengan lebih mudah dilakukan.

A.1.5.1 Kriminalisasi Tindak Pidana Teknologi Informasi dalam UU Tindak Pidana Pemberantasan Terorisme

Perkembangan infrastruktur vital berbasis komputerisasi seperti sistem perbankan, *e-commerce, e-government* dan lain-lain maka potensi kejahatan terorisme dengan difasilitasi teknologi informasi sangat rentan terjadi di Indonesia. Indikasi ke arah tersebut sudah terjadi.

Sebagai contoh, dari laptop Imam samudera yang disita penyidik, dapat diketahui adanya hubungan yang kuat antara aksi terorisme dengan tindak pidana berbasis teknologi informasi. Internet dijadikan sarana komunikasi, propaganda, serta *carding* untuk memperoleh dana bagi pembiayaan aksi teror.

Perpu No. 1/2002 jo. Undang-Undang No 15 Tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme melalui penafsiran hukum sebenarnya sudah mengatur terhadap *cyber terrorism* walaupun tidak secara tegas. UU Pemberantasan Tindak Pidana Terorisme memberikan pengertian terorisme yang cukup luas, bahkan seseorang dianggap melakukan aksi terorisme dan dapat dijatuhi hukuman walaupun tindak pidana terorisme belum terjadi atau baru hanya sampai pada tahap dengan maksud atau dengan tujuan atau merencanakan tindak pidana terorisme. Kebijakan kriminalisasi yang dapat digunakan untuk menjerat pelaku aksi *cyber terrorism* dalam Perpu No. 1/2002 jo. UU No.15 Tahun 2003 antara lain:

Pasal 6 :

- Setiap orang yang dengan sengaja menggunakan kekerasan atau ancaman kekerasan menimbulkan suasana teror atau rasa takut terhadap orang secara meluas atau menimbulkan korban yang bersifat massal, dengan cara merampas kemerdekaan atau hilangnya nyawa dan harta benda orang lain, atau mengakibatkan kerusakan atau kehancuran terhadap obyek-obyek vital yang strategis atau lingkungan hidup atau fasilitas publik atau fasilitas internasional, dipidana dengan pidana mati atau penjara seumur hidup atau pidana penjara paling singkat 4 (empat) tahun dan paling lama 20 (dua puluh) tahun.

Pasal 7 :

- Setiap orang yang dengan sengaja menggunakan kekerasan atau ancaman kekerasan bermaksud untuk menimbulkan suasana teror atau rasa takut terhadap orang secara meluas atau menimbulkan korban yang bersifat massal dengan cara merampas kemerdekaan atau hilangnya nyawa atau harta benda orang lain, atau untuk menimbulkan kerusakan atau kehancuran terhadap obyek-obyek vital yang strategis, atau lingkungan hidup, atau fasilitas publik, atau fasilitas internasional, dipidana dengan pidana penjara paling lama seumur hidup.

Pasal 9 :

- Setiap orang yang secara melawan hukum memasukkan ke Indonesia, membuat, menerima, mencoba memperoleh, menyerahkan atau mencoba menyerahkan, menguasai, membawa, mempunyai persediaan padanya atau mempunyai dalam miliknya, menyimpan, mengangkut, menyembunyikan, mempergunakan, atau mengeluarkan ke dan/atau dari Indonesia sesuatu senjata api, amunisi, atau sesuatu bahan peledak dan bahan-bahan lainnya yang berbahaya dengan maksud untuk melakukan tindak pidana terorisme, dipidana dengan pidana mati atau penjara seumur hidup atau pidana penjara paling singkat 3 (tiga) tahun dan paling lama 20 (dua puluh) tahun.

Pasal 11 :

- Dipidana dengan pidana penjara paling singkat 3 (tiga) tahun dan paling lama 15 (lima belas) tahun, setiap orang yang dengan sengaja menyediakan atau mengumpulkan dana dengan tujuan akan digunakan atau patut diketahuinya akan digunakan sebagian atau seluruhnya untuk melakukan tindak pidana terorisme sebagaimana dimaksud dalam Pasal 6, Pasal 7, Pasal 8, Pasal 9, dan Pasal 10.

Kebijakan kriminalisasi sebagaimana dinyatakan dalam pasal-pasal di atas belum secara tegas dan jelas mengatur terhadap masalah teror yang menggunakan komputer sebagai objek maupun sebagai subjek serta pemanfaatkan fasilitas internet dalam melakukan tindak pidana teror. Defenisi terorisme yang begitu luas dalam UU tersebut (belum terjadi atau baru hanya sampai tahap dengan maksud atau dengan tujuan) dan menghindari kekosongan hukum pasal-pasal tersebut dapat digunakan menjerat pelaku aksi *cyber terrorism*.

Untuk membuktikan apakah ada maksud dan rencana melakukan aksi *cyber terrorism* maka harus didukung dengan bukti elektronik/*digital evidence.* Pasal 27 Perpu No. 1/2002 jo. UU No. 15 Tahun 2003 menyatakan berbagai macam alat-alat bukti tersebut. Salah satunya adalah alat bukti elektronik sebagai alat bukti yang sejajar dan sah sebagaimana dimaksud dalam hukum acara pidana, tetapi hal tersebut tidak mudah harus didukung dengan alat-alat bukti elektronik sebanyak-banyaknya untuk mendukung pembuktian tindak pidana *cyber terrorism* tersebut. Diharapkan agar setiap aparat mampu menganalisa, menyimpulkan dan menyajikan informasi, khususnya terkait dengan bukti-bukti komunikasi elektronik atau *wire* dari penyalahgunaan komputer dan internet yang bersifat teror.

A.1.5.2 Subjek dan Klasifikasi Tindak Pidana dalam UU Tindak Pidana Pemberantasan Terorisme

Subjek tindak pidana dalam Undang-undang Tindak Pidana Pemberantasan Terorisme adalah orang dan korporasi. Pertanggungjawaban pidana terhadap korporasi adalah kepada korporasi dan/atau pengurusnya, tindak pidana yang dilakukan oleh korporasi berdasarkan hubungan kerja maupun hubungan lain, bertindak dalam lingkungan korporasi tersebut baik sendiri maupun bersama-sama (Pasal 17).

Perpu No. 1/2002 jo. UU No. 15 Tahun 2003 Tindak Pidana Pemberantasan Terorisme tidak menyebutkan/ menentukan kualifikasi tindak pidana sebagai "kejahatan" atau "pelanggaran" sehingga secara juridis dapat menimbulkan masalah untuk memberlakukan aturan umum KUHP yang tidak secara khusus diatur dalam UU Tindak Pidana Pemberantasan Terorisme tersebut.

A.1.5.3 Sanksi Pidana dan Aturan Pemidanaan dalam UU Tindak Pidana Pemberantasan Terorisme

Semua delik dalam Tindak Pidana Pemberantasan Terorisme diancam dengan pidana minimal khusus dan ancaman pidananya dirumuskan secara tunggal yaitu penjara (kecuali untuk korporasi pidana pokok berupa denda). Aturan pemidanaan (penjatuhan pidana) untuk pidana minimal dinyatakan dalam Pasal 19 dan Pasal 24 yang intinya menyatakan, bahwa penjatuhan pidana minimum khusus tidak berlaku untuk pelaku di bawah usia 18 tahun . Perpu No. 1/2002 jo. UU No. 15 Tahun 2003 tidak mengatur terhadap penjatuhan pidana minimal apabila ada alasan peringanan pidana lainnya (seperti percobaan atau pembantuan), atau apabila ada alasan pemberatan pidana (seperti *concursus* atau *recidive*), seperti halnya aturan penjatuhan pidana maksimal.

Perpu No. 1/2002 jo. UU No. 15 Tahun 2003 menetapkan bahwa permufakatan jahat, percobaan, atau pembantuan dipidana sama dengan tindak pidananya (Pasal 15). Permufakatan jahat merupakan suatu istilah juridis, sama halnya dengan istilah juridis lainnya, seperti percobaan, pembantuan, pengulangan dan sebagainya. Namun di dalam UU Tindak Pidana Pemberantasan Terorisme tidak ada ketentuan yang memberikan pe-ngertian/batasan/syarat-syarat kapan dikatakan ada permufakatan jahat seperti halnya dalam KUHP (Psl. 88), padahal Pasal 88 ini tidak berlaku umum untuk UU khusus di luar KUHP, seyogianya Perpu No. 1/2002 jo. UU No. 15 Tahun 2003 memberikan ketentuan umum terhadap maksud permufakatan jahat tersebut.

A.2 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 legislasi 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 dari masyarakat dalam menanggulangi kejahatan.[158] 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. Menurut Barda Nawawi Arief Evaluasi atau kajian ulang ini perlu dilakukan, karena ada keterkaitan erat antara kebijakan formulasi perundang-undangan (*legaslative policy*) dengan kebijakan penegakan hukum (*law enforcement policy*) dan kebijakan pemberantasan/penanggulangan kejahatan (*criminal policy*). Kelemahan kebijakan formulasi hukum pidana, akan berpengaruh pada kebijakan penegakan hukum pidana dan kebijakan penanggulangan kejahatan.[159]

Dilihat dari 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.

---

[158] Sudarto,*Hukum dan Hukum Pidana, Op.Cit*. ,hal.38.

[159] Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan, Op.Cit* ,hal.214-215.

Penanggulangan kejahatan dengan sistem hukum pidana pada tahapan formulasi pada intinya menurut Nils Jareborg mencakup tiga masalah pokok struktur sistem hukum pidana, yaitu masalah:[160]

4. Perumusan tindak pidana/Kriminalisasi dan Pidana yang diancamkan *(criminalization and threatened punishment)*
5. Pemidanaan *(adjudication of punishment sentencing)*
6. Pelaksanaan pidana *(execution of punishment)*

Apabila pengertian pemidanaan diartikan secara luas sebagai suatu proses pemberian atau penjatuhan pidana oleh hakim, maka dapatlah dikatakan bahwa sistem pemidanaan mencakup pengertian:[161]

- Keseluruhan sistem (aturan perundang-undangan) untuk pemidanaan;
- Keseluruhan sistem (aturan perundang-undangan) untuk pemberian/penjatuhan dan pelaksanaan pidana.
- Keseluruhan sistem (aturan perundang-undangan) untuk fungsionalisasi/operasionalisasi/konkretisasi pidana;
- Keseluruhan sistem (perundang-undangan) yang mengatur bagaimana hukum pidana itu ditegakkan atau dioperasionalisasikan secara konkret sehingga seseorang dijatuhi sanksi (hukum pidana).

A.2.1 Kebijakan Kriminalisasi Tindak Pidana Teknologi Informasi

Kebijakan kriminalisasi merupakan suatu kebijakan dalam menetapkan suatu perbuatan yang semula bukan tindak pidana (tidak dipidana) menjadi suatu tindak pidana (perbuatan yang

[160] Nils Jareborg,"*The Coherence of the Penal System", dalam Criminal Law in Action, Arnhem, page*.239, lihat dalam Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*, *Op.Cit* ,hal.215.

[161] Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana*, *Op.Cit*.hal.136.

dapat dipidana). Jadi pada hakekatnya, kebijakan kriminalisasi merupakan bagian dari 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.[162]

Dilihat dari pengertian kriminalisasi, sesungguhnya kriminalisasi tidak harus berupa membuat undang-undang khusus di luar KUHP, dapat pula dilakukan tetap dalam koridor KUHP melalui amandemen. Akan tetapi proses antara membuat amandemen KUHP dengan membuat undang-undang khusus hampir sama, baik dari segi waktu maupun biaya, ditambah dengan ketidaktegasan sistem hukum kita yang tidak menganut sistem kodifikasi secara mutlak, menyebabkan munculnya bermacam-macam undang-undang khusus.

Tindak pidana teknologi informasi di Indonesia telah diatur dalam UU ITE sehingga bersifat khusus (*lex specialist*). Kebijakan hukum terkait dengan masalah kriminalisasi dalam UU ITE tertuang dalam Bab XI tentang Ketentuan Pidana (Pasal 45 sampai dengan Pasal 52) juncto Pasal 27 sampai dengan Pasal 36. Sedangkan isi Pasal 27 sampai dengan Pasal 36 sebagaimana terlihat dibawah ini:

Pasal 27:

(1) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan.
(2) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian.
(3) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik.

[162] Barda Nawawi Arief, *Pembaharuan Hukum Pidana Dalam Perspektif Kajian Perbandingan,* Loc.Cit., hal. 126. Lihat juga dalam Barda Nawawi Arief, *Tindak Pidana Mayantara, Perkembangan Kajian Cybercrime di Indonesia*, RajaGrafindo Persada, Jakarta, 2006, hal. 90. Lihat juga pengertian kriminalisasi dari Sudarto, *Hukum dan Hukum Pidana,Op.Cit.*, hal. 32 dan 151

(4) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman.

Pasal 28:

(1). Setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik.

(2). Setiap Orang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan (SARA).

Pasal 29:

- Setiap Orang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi.

Pasal 30

(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun.

(2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.

(3) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

Pasal 31:

(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain.

(2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan.

(3) Kecuali intersepsi sebagaimana dimaksud pada ayat (1) dan ayat (2), intersepsi yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi penegak hukum lainnya yang ditetapkan berdasarkan undang undang.

(4) Ketentuan lebih lanjut mengenai tata cara intersepsi sebagaimana dimaksud pada ayat (3) diatur dengan Peraturan Pemerintah.

Pasal 32:

(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak,

menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik.

(2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak.

(3) Terhadap perbuatan sebagaimana dimaksud pada ayat (1) yang mengakibatkan terbukanya suatu Informasi Elektronik dan/atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya.

Pasal 33

- Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya.

Pasal 34

(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki:

a. perangkat keras atau perangkat lunak Komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33;
b. sandi lewat Komputer, Kode Akses, atau hal yang sejenis dengan itu yang ditujukan agar Sistem Elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33.

(3). Tindakan sebagaimana dimaksud pada ayat (1) bukan tindak pidana jika ditujukan untuk melakukan kegiatan penelitian, pengujian Sistem Elektronik, untuk perlindungan Sistem Elektronik itu sendiri secara sah dan tidak melawan hukum.

Pasal 35:

- Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah olah data yang otentik.

Pasal 36:

- Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 34 yang mengakibatkan kerugian bagi Orang lain.

Perbuatan-perbuatan di atas sangat berhubungan dengan pemanfaatan teknologi informasi dan yang berkenaan dengan informasi dan sistem informasi (*information system*) itu sendiri, serta sistem komunikasi yang merupakan sarana untuk penyampaian/pertukaran informasi itu

kepada pihak lainnya (*transmitter/orginator to recipient*).[163] Secara garis besar tindak pidana teknologi informasi terdiri dari dua jenis, yaitu:[164]

3. Kejahatan yang menggunakan teknologi informasi (TI) sebagai fasilitas.
4. Kejahatan yang menjadikan sistem dan fasilitas teknologi informasi (TI) sebagai sasaran.

Pendapat tersebut sejalan dengan *Tenth United Nations congress on the Prevention of Crime and the Traitment of Offender* di Vienna pada 10-17 April 2000, membagi 2 (dua) sub-kategori *cybercrime*, yaitu:[165]

a. *Cybercrime in a narrow sense* (dalam arti sempit) disebut *computer crime: any illegal behavior directed by means of electronic operation that target the security of computer system and the data processed by them.*
b. *Cybercrime in a broader sense* (dalam arti luas) disebut *computer related crime: any illegal behavior committed by means on relation to, a computer system offering or system or network, including such crime as illegal possession in, offering or distributing information by means of computer system or network.*

Dari beberapa pengertian di atas, *cybercrime* dirumuskan sebagai perbuatan melawan 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. Berkaitan dengan kebijakan kriminalisasi dalam UU ITE sebagaimana yang tercantum dalam Bab XI tentang Ketentuan Pidana (Pasal 45 sampai dengan Pasal 52) juncto Pasal 27 sampai dengan Pasal 36, dapat terlihat dalam tabel.1 dibawah ini:

---

[163] Naskah akademik RUU tindak pidana di bidang Teknologi Informasi disusun oleh Mas Wigantoro Roes Setiyadi , *CyberPolicy Club* dan Indonesia Media Law and Policy Center,2003.hal.25.

[164] Sutanto, Hermawan Sulistyo, dan Tjuk Sugiarto, *Cybercrime -Motif dan Penindakan*, Pensil 324, Jakarta, hal.21.

[165] *Tenth United Nations congress on the Prevention of Crime and the Traitment of Offender*, sebagaimana dikutip dalam Raharjo, Agus Raharjo, *Cybercrime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, PT. Citra Aditya Bakti, Bandung, 2002, hal. 229.

Tabel.1

Pembagian kriminalisasi dalam UU ITE

Teknologi Informasi sebagai Fasilitas		**Teknologi Informasi sebagai Objek**	
Pasal	**Muatan**	**Pasal**	**Muatan**
Pasal 45 jo.Pasal 27:	Pelanggaran susila, Perjudian, Penghinaan atau pencemaran nama baik	Pasal 46 jo. Pasal 30	Mengakses Sistem Orang lain (*illegal access*)
Pasal 45 ayat (2) jo.Pasal 28	Penipuan, Menyebarkan informasi yang menyesatkan	Pasal 47 jo Pasal 31	Melakukan intersepsi atau penyadapan (*Illegal interception)*
Pasal 45 ayat (3) jo. Pasal 29	Pengancaman Kekerasan	Pasal 48 jo. Pasal 32	Perbuatan melawan hukum terhadap sistem/dokumen elektronik (*Data interference)*
Pasal 51 ayat (1) jo. Pasal 35	Pemalsuan informasi/dokumen elektronik *(Offences related to infringements of copyright and related rights)*	Pasal 49 jo. Pasal 33	Terganggunya sistem komputer (*System interference*)
		Pasal 50 jo. Pasal 34	Penyalahgunaan komputer *(Misuse of Devices)*

Kebijakan kriminalisasi dalam UU ITE sebagaimana terlihat dalam tabel.1 di atas perlu diperhatikan hal-hal yang intinya sebagai berikut :[166]

e. Penggunaan 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 kesejahteraan dan pengayoman masyarakat.

[166] Sudarto, *Hukum dan Hukum Pidana*, *Op.Cit.*, hal.23.

f. Perbuatan yang diusahakan untuk dicegah atau ditanggulangi dengan hukum pidana harus merupakan ”perbuatan yang tidak dikehendaki” yaitu perbuatan yang mendatangkan kerugian (materil dan spirituil) atas warga masyarakat.

g. Penggunaan hukum pidana harus pula memperhitungkan prinsip biaya dan hasil (*cost dan benefit principle*)

h. Penggunaan hukum pidana harus pula memperhatikan kapasitas atau kemampuan daya kerja dari badan-badan penegak hukum yaitu jaringan sampai ada kelampauan beban tugas (*overblasting*).

Berdasarkan hal di atas lokakarya yang diorganisir oleh UNAFEI selama kongres PBB X/2000 berlangsung telah memberikan pedoman dalam melakukan kriminalisasi terhadap kejahatan yang berhubungan dengan jaringan komputer,yaitu:[167]

e. *Computer Related Crime* (CRC) harus dikriminalisasikan;

f. Diperlukan hukum acara yang tepat untuk melakukan penyidikan dan penuntutan terhadap penjahat cyber (*cyber criminals*);

g. Harus ada kerja sama antara pemerintah dan industri terhadap tujuan umum pencegahan dan penanggulangan kejahatan komputer agar internet menjadi tempat yang aman;

h. Diperlukan kerja sama internasional untuk menelusuri/mencari penjahat di internet;

i. PBB harus mengambil langkah/tindak lanjut yang berhubungan dengan bantuan kerja sama teknis dalam penanggulangan CRC.

---

[167] Dokumen A/CONF.187/15, *Report of the Tenth UN Congress*, *“Report of CommitteeII” mengenai “Workswhop on crimes related to the computer network”* ,yang kemudian dimasukan dalam *“Report of the Tenth United nations Congress on the preventation of crime and the Treatment of Offenders” ,paragraf* 161-174, hal.25-27.Lihat dalam Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*, *Op.Cit* ,hal.241-242.

Kebijakan kriminalisasi bukan sekedar kebijakan menetapkan/ merumuskan/ memformulasikan perbuatan apa yang dapat dipidana (termasuk sanksi pidananya), melainkan juga mencakup masalah bagaimana kebijakan formulasi/legislasi itu disusun dalam satu kesatuan sistem hukum pidana (kebijakan legislatif) yang harmonis dan terpadu. Untuk menyusun kebijakan kriminalisasi yang harmonis maka dibutuhkan harmonisasi materi/substansi tindak pidana baik yang bersifat eksternal (internasional/global), tetapi juga kajian harmonisasi internal/nasional.[168]

A.2.1.1 Harmonisasi Materi/Substansi Tindak Pidana Eksternal

Harmonisasi eksternal (internasional/global) dalam perumusan krimininalisasi perbuatan di mayantara terutama dengan instrumen hukum internasional terkait, bersifat *hard law*, seperti perjanjian-perjanjian internasional, maupun *soft law* yang tersebar dalam berbagai dokumen seperti *Guidelines*, *Code of Conduct*, *Model Law*, *Principles* dan lain-lain.

Instrumen Internasional yang berkaitan dengan kejahatan *cybercrime* adalah *Draft Convention on Cybercrime* oleh 41 (empat puluh satu) negara-negara yang tergabung dalam Uni Eropa *(Council of Europe)* pada tanggal 23 November 2001 di kota Budapest, Hongaria. Konvensi tersebut kemudian dimasukkan dalam *European Treaty Series* dengan nomor 185.[169]

Draf tersebut sampai dengan tanggal 2 September 2006 sudah ditandatangani oleh sebanyak 43 (empat puluh tiga) negara termasuk 4 (empat) negara diluar Dewan Eropa (Canada, Jepang, Afrika Selatan, dan Amerika Serikat). Dari 43 (empat puluh tiga) negara yang sudah menandatangani Draf Konvensi tersebut terdapat 15 (lima belas) negara yang sudah meratifikasinya, yaitu: Albania, Bosnia and Herzegovina, Bulgaria, Kroasia, Cyprus, Denmark,

---

[168] Barda Nawawi Arief, *Kapita Selekta Hukum Pidana*, *Op.Cit*,hal.259-260.

[169] Ahmad M.Ramli, *Cyber Law dan HAKI Dalam Sistem Hukum Indonesia*, PT Refika Aditama, Bandung,2006, hal. 23

Estonia, Prancis, Hongaria, Lithuania, Norwegia, Romania, Slovenia, Macedonia, dan Ukraina.[170]

Draft Konvensi Cybercrime ini terdiri dari 4 bab yaitu: (I) mengenai peristilahan, (II) mengenai tindakan-tindakan yang diambil di tingkat nasional domestik (negara anggota) di bidang Hukum Pidana Materiil dan Hukum Acara, (III) mengenai kerja sama Internasional, dan (IV) Ketentuan Penutup. Draf konvensi tersebut dipersiapkan terlebih dahulu oleh Tim Ahli/Pakar di bidang *cybercrime* dan disosialisasiskan menjadi bahan diskusi publik serta dengan berusaha melakukan harmonisasi kebijakan penal melalui suatu konvensi untuk ditindaklanjuti/dituangkan dalam kebijakan legislasi masing-masing negara anggota. [171]

Draft Konvensi Cybercrime membuat kebijakan kriminalisasi yang limitatif, yaitu hanya merumuskan delik-delik tertentu di bidang *cybercrime* , ruang lingkupnya mencakup: *Pertama*, delik-delik terhadap kerahasiaan, integritas, dan ketersediaan data dan sistem komputer; *Kedua*, delik-delik yang berhubungan dengan komputer, yaitu melakukan pemalsuan dan penipuan dengan komputer; *Ketiga*, delik-delik yang bermuatan pornografi anak, dan; *Keempat*, delik-delik yang berhubungan dengan pelanggaran hak cipta.

Kajian harmonisasi eksternal dalam kriminalisasi UU ITE telah dilakukan terhadap konvensi *cybercrime* , terutama yang berkaitan dengan tindak pidana yang berhubungan dengan penyalahgunaan teknologi informasi, sebagaimana terlihat dalam tabel di bawah.

Tabel.2
Keterkaitan Kriminalisasi *Draft Convention on Cybercrime* dan UU ITE

No	*Draft Convention on Cybercrime*	UU ITE
1	*Illegal access*: yaitu sengaja memasuki atau mengakses sistem komputer tanpa hak.(Art.2)	- Pasal 46 juncto Pasal 30 UU ITE

[170] Lihat dalam *Treaty Office on* http://conventions.coe.int di akses pada tanggal 2 Oktober 2008.
[171] Barda Nawawi Arief, *Kapita Selekta Hukum Pidana, Op.Cit*,hal.244.

2	*Illegal interception*: yaitu sengaja dan tanpa hak mendengar atau menangkap secara diam-diam pengiriman dan pemancaran data komputer yang tidak bersifat publik ke, dari atau di dalam sistem komputer dengan menggunakan alat bantu teknis.(Art.3)	- Pasal 47 juncto Pasal 31 UU ITE
3	*Data interference*: yaitu sengaja dan tanpa hak melakukan perusakan, penghapusan, perubahan atau penghapusan data komputer.(Art.4)	- Pasal 48 ayat (1) juncto Pasal 32 ayat (1) UU ITE
4	*System interference*: yaitu sengaja melakukan gangguan atau rintangan serius tanpa hak terhadap berfungsinya sistem komputer.(Art.5)	- Pasal 49 juncto Pasal 33 UU ITE
5	*Misuse of Devices:* penyalahgunaan perlengkapan komputer, termasuk program komputer, password komputer, kode masuk (*access code*).(Art.6)	- Pasal 50 juncto Pasal 34 UU ITE
6	*Computer related Forgery:* Pemalsuan (dengan sengaja dan tanpa hak memasukkan mengubah, menghapus data autentik menjadi tidak autentik dengan maksud digunakan sebagai data autentik). (Art.7)	- Pasal 51 ayat (1) juncto Pasal 35 UU ITE
7	*Computer related Fraud:* Penipuan (dengan sengaja dan tanpa hak menyebabkan hilangnya barang/kekayaan orang lain dengan cara memasukkan, mengubah, menghapus data komputer atau dengan mengganggu berfungsinya komputer/sistem komputer, dengan tujuan untuk memperoleh keuntungan ekonomi bagi dirinya sendiri atau orang lain). (Art.8)	- Pasal 45 ayat (2) juncto Pasal 28 UU ITE
8	*Content-Related Offences:* Delik-delik yang berhubungan dengan pornografi anak *(child pornography)*.(Art.9)	- Ada dalam ketentuan pidana pasal 52 (1)
9	*Offences related to infringements of copyright and related rights:* Delik-delik yang terkait dengan pelanggaran hak cipta. (Art.10)	- Pasal 48 ayat (2) juncto Pasal 32 ayat (2) UU ITE - Pasal 51 ayat (1) juncto Pasal 35 UU ITE

Convention on Cybercrime 2001 dibentuk dengan pertimbangan kriminalisasi terhadap perbuatan-perbuatan dalam dunia maya ,yaitu:[172]

1. *Recognising the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies*;

[172] *Council of Europe, European Treaty Series* No.185,Budapest 23.IX.2001,page 1-2.

(bahwa masyarakat internasional menyadari perlunya kerja sama antarnegara dan industri di dalam memerangi kejahatan siber dan adanya kebutuhan untuk melindungi kepentingan yang sah di dalam penggunaan dan pengembangan teknologi informasi).

2. *Convinced that the present Convention is necessary to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalization of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation;* (Konvensi saat ini diperlukan untuk meredam penyalahgunaan sistem, jaringan dan data komputer untuk melakukan perbuatan kriminal. Dan perlunya kepastian dalam proses penyelidikan dan penuntutan pada tingkat internasional dan domestik melalui suatu mekanisme kerjasama internasional yang dapat dipercaya dan cepat.
3. *Mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy;*
   (saat ini sudah semakin nyata adanya kebutuhan untuk memastikan suatu kesesuaian antara pelaksanaan penegakan hukum dan hak azasi manusia sejalan dengan Konvensi Dewan Eropa untuk Perlindungan Hak Asasi Manusia dan Kovenan Perserikatan Bangsa-Bangsa 1966 tentang Hak Politik dan Sipil yang memberikan perlindungan kebebasan berpendapat seperti hak berekspresi, yang mencakup kebebasan untuk mencari, menerima, dan menyebarkan informasi dan pendapat).

Pertimbangan pembuatan *Convention on Cybercrime* sangat menekankan dalam hal kerjasama Internasional dalam penegakan hukum dalam upaya penanggulangan tindak pidana teknologi informasi, hal ini tidak ada diatur didalam UU ITE padahal hal ini sangat krusial mengingat tindak pidana teknologi informasi cenderung bersifat lintas negara maka langkah kebijakan kriminal, memerlukan kerjasama internasional; apakah berupa "*mutual assistance"*, ekstradisi, maupun bentuk-bentuk kerjasama lainnya. Karena itu dibutuhkan langkah-langkah harmonisasi hukum antar bangsa sebagai bagian dari kerjasama internasional dalam kaitannya *"double criminality principle"*.

Kerjasama Internasional dalam penanggulangan tindak pidana teknologi informasi juga dinyatakan dalam Kongres PBB X/2000 di Wina. Dalam laporan *Workshop*/kongres tersebut dinyatakan, ada "*general agreement*" bahwa "*State should seek harmanization of the relevant provisions on criminalization, evidence, and procedure*" (negara-negara anggota harus berusaha melakukan harmonisasi ketentuan-ketentuan yang berhubungan dengan kriminalisasi, pembuktian, dan prosedur).[173]

Kongres PBB juga mengemukakan bahwa ada dugaan keras bahwa kejahatan komputer telah banyak ditutupi oleh para korban, khususnya korporasi-korporasi tidak berniat untuk mengungkap kerentanan mereka terhadap "*cyberhackers*". Tipe-tipe kejahatan komputer utama yang terjadi adalah "*fraud, computer forgery, damage to or modifications of computer data or programs, unauthorized access to computer systems and service, and unauthorized reproduction of legally protected computer programs*".[174]

Sebelumnya pada tahun 1983 *The Organization for Economic Co-operation and Development* (OECD) telah mengkaji harmonisasi hukum pidana dalam dunia maya dan pada tahun 1986 mempublikasikan laporan tentang "*Computer Related Crime: Analysis of Legal Policy*" yang mengkaji hukum tentang internet dan merekomendasikan kepada anggota-anggotanya agar mengatur hal-hal tertentu secara minimal. Laporan ini berisi hasil survei terhadap peraturan perundang-undangan negara-negara anggota beserta rekomendasi perubahannya dalam menanggulangi *computer related crime* tersebut, yang mana diakui bahwa sistem telekomunikasi juga memiliki peran penting didalam kejahatan tersebut.

A.2.1.2 Harmonisasi Materi/ Substansi Tindak Pidana Internal

[173] Dokumen A/CONF.187/15, Report of the Tenth UN Congress, 19-7 2000,hal.27.Lihat dalam Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan, Op.Cit* ,hal.245.

[174] Muladi, *Demokratisasi,Hak Asasi Manusia dan Reformasi Hukum di Indonesia*, *Op.Cit*, hal.214.

Harmonisasi materi/ substansi tindak pidana tidak hanya terkait dengan masalah kajian harmonisasi eksternal, tetapi juga kajian harmonisasi internal/ nasional. Kajian harmonisasi internal adalah kajian harmonisasi/ sinkronisasi dengan materi/ substansi tindak pidana yang telah ada atau telah diatur dalam hukum positif selama ini. Harmonisasi terhadap hukum pidana materiil dinyatakan dalam Kongres PBB X/2000 di Wina yang menyebutkan:[175] *Cybercrime* atau *computer related crime* mencakup keseluruhan bentuk-bentuk baru dari kejahatan yang ditujukan kepada komputer, jaringan komputer dan para penggunanya, dan bentuk-bentuk kejahatan tradisional yang sekarang dilakukan dengan menggunakan atau bantuan peralatan komputer.

Kriminalisasi dalam UU ITE apabila dinterplasikan sudah mencakup terhadap beberapa undang-undang positif yang ada di Indonesia sebelum diundangkannya UU ITE tersebut. Perumusan kriminalisasi dalam UU ITE dengan bentuk-bentuk kriminalisasi terhadap perbuatan yang menggunakan atau bantuan peralatan komputer baik secara tradisional atau yang sudah ada dalam KUHP maupun yang sudah memanfaatkan kecanggihan teknologi, sebagaimana terlihat di tabel 3 di bawah:

Tabel.3

Harmonisasi Kriminalisasi UU ITE dan Undang-Undang Positif

UU ITE		**UU Positif**
Pasal 45 ayat (1) juncto Pasal 27	Ayat (1): Pelanggaran susila	Pasal 282, 283, 311,506 KUHP
	Ayat (2): Perjudian	Pasal 303 KUHP
	Ayat (3): Penghinaan atau pencemaran nama baik	Pasal 310 Pasal 311, Pasal 207 KUHP
	Ayat (4): Pemerasan atau Pengancaman	Pasal 335 dan Pasal 369 KUHP
Pasal 45 ayat (2) juncto Pasal 28	Ayat (1): Penipuan	Pasal 372, Pasal 378, Pasal 379, Pasal Pasal 386 dan Pasal 392 KUHP
	Ayat (2): Menyebarkan informasi yang menyesatkan.	Pasal 160 dan Pasal 161 KUHP

[175] Dokumen Kongres PBB X, A/CONF.187/L.10, tgl. 16 april 2000, tgl 19 Juli 2000, paragraf 161-174, p.25-27. Dikutip dari Barda Nawawi Arief , Kapita Selekta Hukum Pidana,*OpCit*. Hal.259.

Pasal 45 ayat (3) juncto Pasal 29: Pengancaman kekerasan	Pasal 368 KUHP
Pasal 46 juncto Pasal 30: Mengakses sistem orang lain	Pasal 167 dan Pasal 551 KUHP
Pasal 47 juncto Pasal 31: Melakukan intersepsi atau penyadapan	- Pasal 112, Pasal113, Pasal114, Pasal 322, Pasal 323 dan Pasal 431 KUHP - Pasal 40 jo.Pasal 56 UU No. 36 tahun 1999 tentang Telekomunikasi
Pasal 48 juncto Pasal 32: Perbuatan melawan hukum terhadap sistem/dokumen elektronik	Pasal 362 Pasal 406, Pasal 407 dan Pasal 412 KUHP
Pasal 49 juncto Pasal 33: Terganggunya sistem komputer	- Pasal 408 KUHP, - Pasal 22 Undang-Undang Telekomunikasi
Pasal 50 juncto Pasal 34: Penyalah gunaan komputer	Pasal 72 ayat (3) UU RI.No.19 tahun 2002 tentang Hak Cipta
Pasal 51 ayat (1) juncto Pasal 35: Pemalsuan informasi/dokumen elektronik	- Pasal 263, 264, 266 dan 271 KUHP - Pasal 22 jo. Pasal 50 UU Telekomunikasi

Harmonisasi kriminalisasi UU ITE sebagaimana dapat dilihat dalam tabel di atas, sudah mencakup delik-delik tradisional dalam KUHP dan hukum positif yang sudah ada. Meskipun demikian undang-undang positif tersebut belum dapat dikatakan sudah memenuhi unsur subjektif maupun objektif dalam penanggulangan tindak pidana teknologi informasi, sehingga penanggulangan kejahatan dengan hukum yang terkait dengan pemanfaatan teknologi informasi dan komunikasi memang sudah selayaknya menggunakan hukum khusus untuk mengantisipasi berkembangnya kejahatan yang berdampak terhadap ekonomi dan sosial seluruh masyarakat.

Delik-delik pidana yang diterapkan dalam KUHP dan undang-undang positif yang lain yang semula bersifat konvensional seperti pengancaman, pencurian, pencemaran nama baik, pornografi, perjudian, penipuan hingga tindak pidana terorisme kini melalui media *internet* beberapa jenis tindak pidana tersebut mengalami perkembangan karena dapat dilakukan secara *on line* oleh individu maupun kelompok serta tidak mengenal batas wilayah (*borderless*) serta waktu kejadian karena korban dan pelaku sering berada di negara yang berbeda.

ITAC (*Information Technology Association of Canada*) pada "*International Information Industry Congress* (IIIC) 2000 *Millennium Congress*" di Quebec tanggal 19 September 2000 menyatakan bahwa " *Cybercrime is a real and growing threat to economic and social development around the world. Information technology touches every aspect of human life and so can electronically enable crime*".[176]

Mencermati hal tersebut kejahatan IT/ *Cybercrime* memiliki karakter yang berbeda dengan tindak pidana umum baik dari segi pelaku, korban, modus operandi dan tempat kejadian perkara sehingga butuh penanganan dan pengaturan khusus di luar KUHP. Kriminalisasi di dunia maya dengan pengaturan khusus diluar KUHP 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 (*over-criminalization*), yang justru mengurangi wibawa hukum.[177]

Forum diskusi *cyberspace* baik melalui milis, blog, maupun di seminar sosialisasi Undang-Undang Informasi dan Transaksi Elektronik Pasal yang disebut krusial dan sering dikritik adalah Pasal 27 ayat 3 tentang muatan pencemaran nama baik dan Pasal 28 ayat 2 tentang muatan penyebaran rasa kebencian atau permusuhan.

Harus diakui agak sulit merumuskan dengan batasan-batasan yang jelas tentang penyebaran kebencian ini dan ini sangat berpotensi menimbulkan diskriminasi hukum dan juga ketidakpastian hukum karena sangat tergantung pada tafsiran sepihak. Tetapi itu dikembalikan kepada sifat toleransi bangsa kita yang berlandaskan Pancasila serta menghormati norma-norma

---

[176] ITAC,*" IIIC Common Views Paper On: Cybercrime "*, IIIC 2000 Millenium congress, September 19th, 2000, hal.5. Lihat dalam Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*, *Op.Cit*.,hal.240.

[177] Muladi, *Kebijakan Kriminal terhadap Cybercrime* , Majalah Media Hukum, Vol.1 No.3 tanggal 22 Agustus 2003,hal.1

agama dan rasa kesusilaan masyarakat untuk menghindari penyebaran informasi yang akan mengakibatkan permusuhan.

Pasal 27 ayat 3 ini dipermasalahkan juga oleh Dewan Pers bahkan akan mengajukan *judicial review* ke Mahkamah Konstitusi. Pasal 27 ayat 3 UU ITE sangat terkait dengan Pasal 310 dan 311 KUHP, Bersihar Lubis dan Risang Bima Wijaya telah mengajukan *judicial review* terhadap kedua pasal KUHP tersebut ke Mahkamah Konstitusi dengan nomor perkara No.14/PUU-VI/2008, permohonan yang diajukan oleh ke dua orang wartawan senior tersebut ditolak oleh MK.

Harjono sebagai ketua hakim majelis Konstitusi dalam kesimpulan sidang MK tersebut menyebutkan;[178] *"Nama baik, martabat, atau kehormatan seseorang adalah salah satu kepentingan hukum yang dilindungi oleh hukum pidana karena merupakan bagian dari hak konstitusional warga negara yang dijamin UUD 1945. Karenanya apabila hukum pidana memberikan ancaman sanksi pidana tertentu terhadap perbuatan yang menyerang nama baik, martabat, atau kehormatan seseorang, hal itu tidaklah bertentangan dengan UUD 1945*".

Hasil keputusan sidang Mahkamah Konstitusi tersebut hendaknya menghilangkan perbedaan pendapat terutama terhadap Pasal 27 ayat 3 dan Pasal 28 ayat 2 UU ITE karena Masyarakat Indonesia memiliki lingkungan sosial yang kental dengan kultur ketimuran yaitu masyarakat agamis. Tidak ada satu pun agama yang membolehkan seseorang untuk melakukan perbuatan mencemarkan nama baik, menyebarkan informasi yang bermuatan rasa kebencian atau permusuhan individu dan/ atau kelompok masyarakat tertentu berdasarkan SARA, tidak dapat dapat dipungkiri hak setiap individu untuk untuk memperoleh dan menyebarkan informasi. Tetapi akses informasi yang disebarkan dan diperoleh hendaknya yang berkualitas mengarah

[178] Lihat dalam www.hukumonline.com , *"Sanksi Penjara masih Relevan untuk Pencemaran Nama Baik*", 19 Agustus 2008.

pada pengembangan pribadi, lingkungan sosial dan pencapaian tujuan Negara Republik Indonesia.

A.2.2 Subjek Tindak Pidana

Pada awalnya dalam hukum pidana, yang dianggap sebagai subjek tindak pidana hanyalah manusia sebagai *natuurlijke-persoonen*, sedangkan badan hukum atau *rechts-persoonen* tidak dianggap sebagai subjek.[179] Meskipun demikian, pada perkembangannya terjadi perluasan terhadap subjek tindak pidana. Korporasi (badan hukum) merupakan suatu ciptaan hukum yakni pemberian status subjek hukum kepada suatu badan, disamping subjek hukum yang berwujud manusia alamiah. Dengan demikian badan hukum dianggap dapat menjalankan atau melakukan suatu tindakan hukum.[180]

Perumusan tindak pidana dalam UU ITE selalu diawali dengan kata-kata ”setiap orang” yang menunjukkan kepada pengertian orang. Namun dalam Pasal 1 sub 21 UU ITE ditegaskan, bahwa yang dimaksud dengan ”orang” adalah orang, perseorangan, baik warga negara Indonesia, warga negara asing, maupun badan hukum. Penegasan dalam pertanggungjawaban pidana terhadap badan hukum juga terdapat dalam penjelasan Pasal 2 UU ITE yang menyatakan badan hukum Indonesia maupun badan hukum asing yang memiliki akibat hukum di Indonesia merupakan subjek tindak pidana U ITE. Demikian pula dalam Bab XI tentang ketentuan pidana, dalam Pasal 52 ayat (4) yang mengatur tentang pertanggungjawaban korporasi. Dengan demikian subjek tindak pidana (yang dapat dipidana) menurut UU ITE dapat berupa orang perorangan maupun korporasi.

---

[179] S.R Sianturi, *Asas-asas Hukum Pidana di Indonesia dan Penerapannya*, Alumni Ahaem – Petehaem, Jakarta,1989, hal. 219.

[180] Teguh Prasetya dan Abdul Hakim Barkatullah, *Politik Hukum Pidana Kajian Kriminalisasi dan Dekriminalisasi*, Pustaka Pelajar, Yogyakarta, 2005,hal.46.

Pertanggungjawaban pidana terhadap korporasi mengenai ketentuan terhadap kapan korporasi dikatakan telah melakukan tindak pidana dan siapa yang dapat dipertanggungjawabkan tidak diatur secara jelas dan khusus dalam UU ITE, tetapi Penjelasan Pasal 52 ayat (4) memberikan persyaratan terhadap subjek pertanggungjawaban korporasi untuk dikenakan sanksi pidana adalah yang dilakukan oleh korporasi *(corporate crime)* dan/ atau oleh pengurus dan/ atau staf korporasi.

Dapat dikenakannya sanksi pidana/ tindakan kepada pengurus korporasi dalam perkara tindak pidana teknologi informasi cukup beralasan dan sesuai dengan rekomendasi Uni Eropa *(Council of Europe)* mengenai *Convention on Cybercrime* , dalam *Title 5. Ancillary liability and sanctions , Article 12 – Corporate liability* antara lain:

1. Dalam rekomendasi Uni Eropa yang kemudian dimasukkan dalam *European Treaty Series* dengan Nomor 185 ditegaskan agar ada tindakan terhadap pengurus perusahaan baik sebagai individu maupun perusahaan itu sendiri yang terlibat dalam *cybercrime (that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person)*
2. Kapasitas pengurus yang dapat dikenakan sanksi pidana dalam *Convention on Cybercrime ,* berdasarkan:
    a. *Power of representation of the legal person* (mewakili korporasi)*;*
    b. *Authority to take decisions on behalf of the legal person* (mengambil keputusan dalam korporasi);
    c. *Authority to exercise control within the legal person* (melakukan pengawasan dan pengendalian dalam korporasi) .

A.2.3 Kualifikasi Tindak Pidana

Penegasan terhadap kualifikasi delik baik 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 dari pembedaan antara ”kejahatan” dan ”pelanggaran”. Penetapan kualifikasi yuridis ini mutlak diperlukan karena sistem pemidanaan di luar KUHP merupakan sub/bagian integral dari keseluruhan sistem pemidanaan.

Aturan umum KUHP membedakan antara aturan umum untuk kejahatan (Buku II) dan aturan umum untuk pelanggaran (Buku III), dalam Pasal 103 KUHP menyatakan ketentuan umum (Buku Kesatu Bab I sampai dengan Bab VIII) KUHP berlaku bagi perbuatan-perbuatan yang oleh ketentuan perundang-undangan lainnya diancam dengan pidana, kecuali jika oleh undang-undang ditentukan lain. Maka apabila aturan umum KUHP itu akan juga diberlakukan, seharusnya UU ITE menyebutkan kualifikasi yang jelas dari tindak pidana yang diaturnya, apakah merupakan ”kejahatan” atau ”pelanggaran”.

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. Oleh karena itu, setiap tindak pidana yang dirumuskan dalam UU ITE harus disebut kualifikasi juridisnya.

Fungsi dari ditetapkannya kualifikasi yuridis ini adalah untuk menjembatani berlakunya aturan umum KUHP terhadap hal-hal yang tidak diatur dalam UU di luar KUHP. Tidak adanya penetapan kualifikasi yuridis dalam UU ITE dapat menimbulkan masalah yuridis dalam praktek, baik dalam arti konsekuensi yuridis materiil (aturan umum dalam KUHP) maupun konsekuensi

yuridis formal (dalam KUHAP). Hal ini berarti dapat mempegaruhi efektivitas penegakan hukum.

A.2.4 Perumusan Sanksi Pidana

Sanksi pidana dalam UU ITE dirumuskan secara kumulatif, dimana pidana penjara dikumulasikan dengan pidana denda. Ketentuan pidana dalam UU ITE tertulis dalam Bab XI Pasal 45 sampai dengan Pasal 52, dengan rumusan sebagai berikut:

Pasal 45:

(1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 27 ayat (1), ayat (2), ayat (3), atau ayat (4) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).
(2) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 28 ayat (1) atau ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).
(3) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 29 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp2.000.000.000,00 (dua miliar rupiah).

Pasal 46 :

(1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp600.000.000,00 (enam ratus juta rupiah).
(2) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp700.000.000,00 (tujuh ratus juta rupiah).
(3) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah).

Pasal 47:

- Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 31 ayat (1) atau ayat (2) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah).

Pasal 48:

(1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (1) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp2.000.000.000,00 (dua miliar rupiah).
(2) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (2) dipidana dengan pidana penjara paling lama 9 (sembilan) tahun dan/atau denda paling banyak Rp3.000.000.000,00 (tiga miliar rupiah).

(3) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (3) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah).

Pasal 49:

- Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 33, dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp10.000.000.000,00 (sepuluh miliar rupiah).

Pasal 50:

- Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 34 ayat (1) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp10.000.000.000,00 (sepuluh miliar rupiah).

Pasal 51:

(1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp12.000.000.000,00 (dua belas miliar rupiah).

(2) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 36 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp12.000.000.000,00 (dua belas miliar rupiah).

Pasal 52:

(1) Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 ayat (1) menyangkut kesusilaan atau eksploitasi seksual terhadap anak dikenakan pemberatan sepertiga dari pidana pokok.

(2) Dalam hal perbuatan sebagaimana dimaksud dalam Pasa 30 sampai dengan Pasal 37 ditujukan terhadap Kompute dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau yang digunakan untuk layanan publik dipidana dengan pidana pokok ditambah sepertiga.

(3) Dalam hal perbuatan sebagaimana dimaksud dalam Pasal 30 sampai dengan Pasal 37 ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau badan strategis termasuk dan tidak terbatas pada lembaga pertahanan, bank sentral, perbankan, keuangan, lembaga internasional, otoritas penerbangan diancam dengan pidana maksimal ancaman pidana pokok masing-masing Pasal ditambah dua pertiga.

(4) Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 37 dilakukan oleh korporasi dipidana dengan pidana pokok ditambah dua pertiga.

Perumusan tindak pidana kedua subjek hukum yang diatur dalam satu pasal yang sama dengan satu ancaman pidana yang sama dalam UU ITE hendaknya dipisahkan karena pada hakikatnya subjek hukum ”orang” dan ”korporasi” berbeda baik dalam hal pertanggungjawaban pidana maupun terhadap ancaman pidana yang dikenakan.

Perumusan secara kumulatif dapat menimbulkan masalah karena dengan perumusan kumulatif bersifat imperatif dan kaku. Sanksi pidana dalam UU ITE adalah antara pidana penjara

dan denda yang cukup besar, tetapi tidak ada dalam redaksi pasal-pasal dalam UU ITE yang mengatur apabila denda tidak dibayar. Ini berarti, berlaku ketentuan umum dalam KUHP (Pasal 30), bahwa maksimum pidana kurungan pengganti adalah 6 (enam) bulan atau dapat menjadi maksimum 8 (delapan) bulan apabila ada pemberatan (*recidive/concursus*).

Apabila mengacu kepada Pasal 30 KUHP maka adanya ancaman pidana denda yang sangat besar dalam UU ITE yaitu antara Rp.600.000.000,00- (enam ratus juta rupiah) hingga Rp.12.000.000.000,00- (dua belas miliar rupiah), tidak akan efektif, karena kalau tidak dibayar hanya terkena pidana kurungan maksimal 8 (delapan) bulan. Bagi terdakwa, ancaman pidana kurungan pengganti denda itu mungkin tidak mempunyai pengaruh apa-apa, karena apabila denda itu dibayar, ia pun akan tetap terkena pidana penjara (karena diancamkan secara kumulatif). Oleh karena itu, kemungkinan besar ia tidak akan membayar dendanya.

A.2.5 Aturan Pemidanaan

Aturan pemidanaan terhadap penyertaan, percobaan, permufakatan jahat, perbarengan (*con-cursus*), pengulangan (*residive*) dan alasan peringanan tidak diatur dalam UU ITE , sebagai perbandingan *Convention on Cybercrime* mengatur terhadap penyertaan dan percobaan dalam *Article 11 Paragraph 2*:[181]

> *Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.*

Karena tidak diaturnya penyertaan, percobaan dan peringanan tindak pidana berarti dalam hal ini berlaku ketentuan umum yakni Bab.I sampai dengan Bab.VIII dalam KUHP. Sebagaimana dimaklumi, aturan pemidanaan dalam KUHP (WvS) tidak hanya ditujukan pada orang yang melakukan tindak pidana, tetapi juga terhadap mereka yang melakukan perbuatan

[181] *Article 11 Paragraph 2 Council of Europe, European Treaty Series* No.185,Budapest 23.IX.2001.

dalam bentuk “percobaan”, “permufakatan jahat”, “penyertaan”, “perbarengan” (*con-cursus*), dan “pengulangan” (*recidive*). Hanya saja di dalam KUHP, “permufakatan jahat” dan “recidive” tidak diatur dalam Aturan Umum Buku I, tetapi di dalam Aturan Khusus (Buku II atau Buku III).

Pasal 52 UU ITE membuat aturan dimungkinkannya pidana tambahan dijatuhkan sebagai sanksi yang berdiri sendiri , yaitu:

Pasal 52:

(1) Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 ayat (1) menyangkut kesusilaan atau eksploitasi seksual terhadap anak dikenakan pemberatan sepertiga dari pidana pokok.
(2) Dalam hal perbuatan sebagaimana dimaksud dalam Pasal 30 sampai dengan Pasal 37 ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau yang digunakan untuk layanan publik dipidana dengan pidana pokok ditambah sepertiga.
(3) Dalam hal perbuatan sebagaimana dimaksud dalam Pasal 30 sampai dengan Pasal 37 ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau badan strategis termasuk dan tidak terbatas pada lembaga pertahanan, bank sentral, perbankan, keuangan, lembaga internasional, otoritas penerbangan diancam dengan pidana maksimal ancaman pidana pokok masing masing Pasal ditambah dua pertiga.
(4) Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 37 dilakukan oleh korporasi dipidana dengan pidana pokok ditambah dua pertiga.

Perumusan Pasal 52 UU ITE hanya mengatur pemberatan pidana yang khusus terhadap delik-delik tertentu dalam UU ITE tersebut, tetapi tidak mengatur pemberatan apabila terjadi pengulangan (*residive*). Mengacu kepada KUHP Bab.II Pasal 12 ayat (3) dalam aturan umum menyatakan: Pidana penjara selama waktu tertentu boleh dijatuhkan untuk dua puluh tahun berturut-turut dalam hal kejahatan yang pidananya hakim boleh memilih antara pidana mati, pidana seumur hidup, dan pidana penjara selama waktu tertentu, atau antara pidana penjara seumur hidup dan pidana penjara selama waktu tertentu; begitu juga dalam hal batas lima belas tahun dilampaui sebab tambahanan pidana karena perbarengan, pengulangan atau karena ditentukan pasal 52.

Aturan umum terhadap pemberatan pidana terhadap pengulangan sebagaimana Pasal 12 ayat (3) KUHP tersebut hendaknya dirumusan juga di dalam pasal UU ITE untuk menghindari terjadinya rasa ketidakadilan terhadap perbuatan *cybercrime* yang berulang tetapi pemidaannya sama dengan tindak pidana yang tidak dilakukan secara pengulangan.

Adanya pemberatan terhadap beberapa perbuatan dalam Pasal 52; ayat (1) menyangkut kesusilaan atau eksploitasi seksual terhadap anak, ayat (2) milik Pemerintah dan/atau yang digunakan untuk layanan publik, ayat (3) milik Pemerintah dan/atau badan strategis termasuk dan tidak terbatas pada lembaga pertahanan, bank sentral, perbankan, keuangan, lembaga internasional, otoritas penerbangan, dan ayat (4) terhadap korporasi Pemberatan-pemberatan tersebut tidak diatur dalam KUHP, maka seharusnya UU khusus di luar KUHP membuat aturan khusus/tersendiri berupa aturan atau pedoman pemidanaan untuk pemberatan tersebut. Ini merupakan konsekuensi dari adanya Pasal 103 KUHP, karena KUHP sendiri belum mengatur masalah ini.

Kejanggalan yang paling menonjol dari ketentuan Pasal 52 ayat (2), ayat (3) dan ayat (4) adalah adanya pemberatan terhadap Pasal 37:"*Setiap Orang dengan sengaja melakukan perbuatan yang dilarang sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 36 di luar wilayah Indonesia terhadap Sistem Elektronik yang berada di wilayah yurisdiksi Indonesia"*[182], redaksi Pasal 37 tersebut tidak mengatur terhadap sanksi tindak pidana, sehingga cenderung ada kelalaian dalam pembuatan undang-undang tersebut.

Permasalahan lain yang menjadi rancu terhadap Pasal 52 UU ITE adalah adanya pemberatan pidana terhadap Pasal 27 sampai dengan Pasal 36, sebab Pasal 27 sampai dengan Pasal 36 tidak mengatur tindak pidana dan sanksi pidana, sehingga tidak bisa menambah 1/3 atau

[182] Pasal 37 Undang-Undang No.11 tahun 2008 tentang Informasi dan Transaksi Elektronik, diundangkan pada 28 April 2008, Lembaran Negara No.58.

2/3 terhadap ancaman pidananya, sementara yang mengatur adanya suatu tindak pidana dan sanksi nya terdapat dalam Pasal 45 sampai dengan Pasal 51 UU ITE. Seharusnya yang disebut Pasal 45 sampai dengan Pasal 51 dijunctokan terhadap pasal yang dikenakan. Apabila tidak demikian dalam sistem pemidanaannya akan mempersulit aparat penegakan hukum terutama dalam operasionalisasi pidana.

A.2.6 Pertanggungjawaban Korporasi

Dijadikannya korporasi sebagai subjek tindak pidana UU ITE, maka sistem pidana dan pemidanaannya juga seharusnya berorientasi pada korporasi. Menurut Barda Nawai Arief apabila korporasi sebagai subjek tindak pidana dalam suatu undang-undang ini berarti, harus ada ketentuan khusus mengenai:[183]

a. Kapan dikatakan korporasi melakukan tindak pidana;

b. Siapa yang dapat dipertanggungjawabkan;

c. Dalam hal bagaimana korporasi dapat dipertanggungjawabkan;

d. Jenis-jenis sanksi apa yang dapat dijatuhkan untuk korporasi.

Redaksi pasal-pasal dalam UU ITE (Pasal 1 sampai dengan Pasal 54) tidak mengatur kapan, siapa dan bagaimana korporasi dapat dipertanggungjawabkan melakukan tindak pidana, tetapi dalam penjelasan Pasal 52 (4) memberikan persyaratan/ kapasitas terhadap korporasi dan/atau oleh pengurus dan/atau staf melakukan tindak pidana, yaitu:

a. mewakili korporasi;

b. mengambil keputusan dalam korporasi;

c. melakukan pengawasan dan pengendalian dalam korporasi;

---

[183] Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan, Op.Cit*.,hal.151.

d. melakukan kegiatan demi keuntungan korporasi.[184]

Penjelasan Pasal 52 ayat (4) di atas merupakan norma 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.

Jenis-jenis sanksi yang dapat dijatuhkan untuk korporasi menurut UU ITE adalah pidana pokok berupa penjara dan denda yang dirumuskan secara komulatif serta ada pemberatan ancaman pidana sebagaimana diatur dalam Pasal 52 ayat (4)[185] yang isinya “*dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 37 dilakukan oleh korporasi dipidana dengan pidana pokok ditambah dua pertiga*”.

Pemberatan pidana terhadap korporasi dalam UU ITE yakni penjatuhan denda ditambah dua pertiga tidak memiliki aturan yang khusus, terutama mengenai pidana pengganti untuk denda yang tidak dibayar. Ini berarti dikenakan ketentuan umum KUHP (Pasal 30), yaitu denda kurungan pengganti denda (maksimal 6 bulan, yang dapat menjadi 8 bulan apabila ada pemberatan pidana). Hal ini menjadi masalah, apabila diterapkan terhadap korporasi, karena tidak mungkin korporasi menjalani pidana penjara/kurungan pengganti. Hal yang lebih pokok dalam KUHP kita sekarang belum mengatur pertanggungjawaban korporasi, hendaknya dibuat suatu aturan khusus dalam UU ITE yang mengatur pertanggungjawaban korporasi terutama mengenai aturan terhadap korporasi yang tidak dapat membayar denda.

Penerapan sanksi pidana pokok berupa penjara dan denda terhadap korporasi dalam UU ITE hendaknya ditambahkan jenis pidana tambahan atau tindakan yang ”khas” untuk korporasi,

---

[184] Penjelasan Pasal 52 (4) Undang-Undang No.11 tahun 2008 tentang Informasi dan Transaksi Elektronik, diundangkan pada 28 April 2008, Lembaran Negara No.58.

[185] Pasal 52 (4) Undang-Undang No.11 tahun 2008 tentang Informasi dan Transaksi Elektronik, diundangkan pada 28 April 2008, Lembaran Negara No.58.

seyogianya terhadap korporasi dapat dijatuhi pidana tambahan misalnya pencabutan izin usaha, penutupan/pembubaran korporasi dan sebagainya .

B. 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 dari 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 dari Sistem Peradilan Pidana inilah yang nantinya akan melaksanakan kebijakan penegakan hukum berupa pencegahan dan penanggulangan terjadinya suatu kejahatan dimana peran-peran dari sub-sistem ini akan menjadi lebih *acceptable* bersama-sama dengan peran masyarakatnya. Tanpa peran masyarakat, kebijakan penegakan hukum akan menjadi tidak optimalistis sifatnya.[186]

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, di dalam suatu negara maupaun dalam hubungan dengan pergaulan di kawasan regional dan internasioanal.

Masalah pokok penegakan hukum sebenarnya terletak pada faktor-faktor yang mungkin mempengaruhinya. Menurut Soerjono Soekanto faktor-faktor yang mempengaruhi penegakan

[186] Indriyanto Seno Adji, *Korupsi Sistematik dan Kendala Penegak Hukum di Indonesia*, Jurnal Studi Kepolisian Perguruan Tinggi Ilmu Kepolisian, CV.Restu Agung, 2005,hal.9.

hukum tersebut mempunyai arti yang netral, sehingga dampak positif atau negatifnya terletak pada isi faktor-faktor tersebut. Faktor-faktor tersebut, adalah:[187]

6. Faktor hukumnya sendiri (undang-undang)
7. Faktor penegak hukum yakni pihak yang membentuk maupun menerapkan hukum.
8. Faktor sarana atau fasilitas yang mendukung penegakan hukum.
9. Faktor masyarakat, yakni lingkungan dimana hukum tersebut berlaku atau diterapkan.
10. 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 hukum (*law enforcement*) di dunia *cyber* dapat terlaksana dengan baik maka harus dipenuhi 4 (empat) syarat yaitu:[188]

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 dari masyarakat yang terkena peraturan.

Selain ke 4 (empat) syarat tersebut penegakan hukum di dunia maya juga sangat tergantung dari pembuktian dan yuridiksi yang ditentukan oleh undang-undang. Uraian selanjutnya akan diuraikan tentang kebijakan penegakan hukum (kebijakan aplikatif) yang dilakukan oleh aparat penegak hukum dalam upaya penanggulangan tindak pidana teknologi informasi .

---

[187] Soerjono Soekanto, *Faktor-faktor yang Mempengaruhi Penegakan Hukum, Op.Cit*., hal.8.

[188] Sutarman, *Cybercrime* : *Modus Operandi dan Penanggulangannya*, Laksbang Pressindo, Jogjakarta, 2007, hal.108-109.

B.1 Aspek Perundang-undangan yang Berhubungan dengan Tindak Pidana Teknologi Informasi

Saat ini Indonesia telah memiliki *cyber law* untuk mengatur dunia maya berikut sanksi bila terjadi *cybercrime* baik di wilayah Indonesia maupun di luar wilayah hukum Indonesia yang akibatnya dirasakan di Indonesia. *Cybercrime* terus berkembang seiring dengan revolusi teknologi informasi yang membalikkan paradigma lama terhadap kejahatan konvensional kearah kejahatan virtual dengan memanfaatkan instrumen elektronik tetapi akibatnya dapat dirasakan secara nyata.

Penanggulangan *cybercrime* oleh aparat penegak hukum sangat dipengaruhi oleh adanya peraturan perundang-undangan, sebagaimana telah diuraikan dalam Sub A.1 di atas terdapat beberapa perundang-undangan yang berkaitan dengan teknologi informasi khususnya kejahatan yang berkaitan dengan internet sebelum disahkannya UU ITE, hal tersebut dapat dilihat dari tabel.4 dibawah:

Tabel.4

Kasus *Cybercrime* yang Ditangani Mabes Polri Tahun 2007

No	Laporan Polisi	Tindak Pidana	Tersangka	Pasal	Ket
1	LP-A/03/I/2007/ *Cybercrime* , 24 Januari 2007	Perjudian bola secara on-line melalui media internet.	Slamet T als Pingan,dkk	Pasal 303 KUHP	Vonis 2 Bulan
2	LP/192/V/2007/Siaga-1, tanggal 15 Mei 2007	Pencemaran nama baik	Lidik	Pasal 311 ayat (1) KUHP dan Pasal 335 KUHP	Dicabut atas permintaan pelapor
3	LP/87/III/2007/Siaga-III tgl 20 Maret 2007	Memperbanyak program komputer secara komersial	Lee Wei Chiang	Pasal 72 ayat (3) UU RI.No.19 tahun 2002 tentang Hak Cipta	Vonis 6 Bulan
4	LP/03/VIII/cyber crime , tgl 3	Penipuan dengan cara menang	-	Pasal 378 KUHP	Proses Penyidi

	Agustus 2008	undian melalui SMS/telepon selular			kan
5	LP/431/IX/2007/ Siaga-II Tgl 24 September 2007	Pencemaran nama baik melalui email di Internet	-	Pasal 331 ayat 1 jo Pasal 335 ayat ke 1 ke 2 (e) KUHP	Proses Penyidikan
6	LP/484/X/2007/Siaga-II tgl 30 Oktober 2007	Penipuan melalui media internet	Ferriyono Lim	Pasal 378 KUHP dan atau Pasal 372 KUHP	Proses penyidikan
7	LP/499/XI/2007/ Siaga-I tanggal 7 Nopember 2007	Penipuan dan Penggelapan melalui internet	Delma Davis,dkk	Pasal 372 dan Pasal 378 KUHP	Dilimpahkan ke Polda Bali

Penegakkan hukum *cybercrime* sebagaimana telah dilakukan Mabes Polri pada tahun 2007 di atas dilakukan dengan menafsirkan *cybercrime* ke dalam perundang-undangan KUHP dan khususnya undang-undang yang terkait dengan perkembangan teknologi informasi seperti:

1. Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi
2. Undang-Undang No.19 tahun 2002 tentang Hak Cipta
3. Undang-Undang No 25 Tahun 2003 tentang Perubahan atas Undang-Undang No. 15 Tahun 2002 tentang Tindak Pidana Pencucian Uang
4. Undang-Undang No 15 Tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme

Penafsiran tersebut dapat dilakukan oleh aparat penegak hukum melalui metode penafsiran ekstensif bukan analogi. Moeljatno memberikan batasan pengertian terhadap penafsiran ekstensif dan analogi. Penafsiran ekstensif adalah perkataan yang diberi arti menurut makna yang hidup dalam masyarakat sekarang dan tetap berpegang pada aturan yang ada.

Sedangkan dalam penafsiran analogi, perbuatan yang menjadi soal itu tidak bisa dimasukkan dalam aturan yang ada, berpegang pada *ratio*.[189]

Penafsiran hukum melalui analogi menurut Sudarto artinya memperluas berlakunya suatu peraturan dengan mengabstrasikannya menjadi aturan hukum yang menjadi dasar dari peraturan itu (*ratio legis*) dan kemudian menerapkan aturan yang bersifat umum ini kepada perbuatan konkrit yang tidak diatur dalam undang-undang.[190]

Penerapan hukum positif tersebut tidaklah sederhana mengingat karakteristik *cybercrime* yang bersifat khas. Metode penafsiran secara analogi bagaimanapun juga tidak diperbolehkan. Namun penafsiran ekstensif diperbolehkan. Agar tidak terjadi penafsiran analogi, maka kebijakan penanggulangan tindak pidana teknologi informasi melalui UU ITE dapat menjadi solusi dalam melindungi internet dan penggunanya.

Instrumen hukum *cyber* dengan keluarnya UU ITE memberikan landasan atau pedoman bagi para penegak hukum yang akan diterapkan pada para pelaku *cybercrime*. UU ITE diharapkan sebagai kekuatan pengendali dan penegak ketertiban bagi kegiatan pemanfaatan teknologi informasi tidak hanya terbatas pada kegiatan internet, tetapi semua kegiatan yang memanfaatkan perangkat komputer, dan instrumen elektronik lainnya.

B.2 Aspek Aparatur Penegak Hukum

Penegak hukum di Indonesia mengalami kesulitan dalam menghadapi merebaknya *cybercrime*. Hal ini dilatarbelakangi masih sedikitnya aparat penegak hukum yang memahami seluk-beluk teknologi informasi (internet), disamping itu aparat penegak hukum di daerah pun belum siap dalam mengantisipasi maraknya kejahatan ini karena masih banyak aparat penegak

[189] Moeljatno, *Asas-Asas Hukum Pidana*, Cetakan.VI, Rineka Cipta, Jakarta, 2000,hal.28-29.
[190] Sudarto, *Hukum Pidana I*,Yayasan Sudarto, Semarang, 1990, hal.23.

hukum yang gagap teknologi ”gaptek” hal ini disebabkan oleh masih banyaknya institusi-institusi penegak hukum di daerah yang belum didukung dengan jaringan internet.

Berdasarkan data Polri, kasus kejahatan dunia maya yang terjadi selama kurun waktu 4 (empat) tahun dari tahun 2002 sampai dengan tahun 2005 tercatat 48 (empat puluh delapan) kasus. Dari 48 (empat puluh delapan) kasus yang dilaporkan tersebut, 25 (dua puluh lima) kasus telah dinyatakan P-21 oleh Jaksa Penuntut Umum.[191]

Data tahun 2006 sampai dengan Juni tahun 2008 yang diperoleh Penulis dari Direktorat II Ekonomi dan Khusus Unit V IT & *Cybercrime* Bareskrim Mabes Polri, kasus kejahatan dunia maya selama kurun waktu 3 (tiga) tahun yang dilaporkan sebanyak 37 (tiga puluh tujuh) kasus dan 14 (empat belas) kasus telah dinyatakan P-21 oleh Jaksa Penuntut Umum dan beberapa kasus telah mendapatkan vonis serta beberapa kasus dihentikan penyidikannya. Alasan dihentikannya penyidikan (SP-3) oleh penyidik dikarenakan tidak cukup bukti, di cabutnya pengaduan atas permintaan pelapor (kasus pencemaran nama baik), dan deportasi ke luar negeri (*handing over*). Data kasus *cybercrime* Polri tahun 2006-2008 serta proses penyidikannya dapat dilihat dalam tabel.5 di bawah ini.

Tabel.5

Data Kasus *Cybercrime* Polri Tahun 2006-2008[192]

NO	TAHUN	JUMLAH	HASIL PENYELIDIKAN			KET
			P-21	Proses Penyidikan	Dihentikan	
1	2006	23	10	10	3	6 (enam) kasus sudah vonis pengadilan
2	2007	7	2	4	1	2 (dua) kasus telah vonis

[191] Petrus Reinhard Golose, *Penegakan Hukum Cybercrime dalam Sistem Hukum Indonesia* dalam *Handout* Seminar Pembuktian dan Penanganan Cybercrime di Indonesia,*Op.Cit*.,hal.6

[192] Sumber dari Direktorat II Ekonomi dan Khusus Unit V IT & *Cybercrime* Bareskrim Mabes Polri, pada tanggal 28 Juli 2008.

3	2008	7	2	4	1	2 (dua) kasus telah vonis
TOTAL		**37**	**13**	**18**	**5**	10 kasus sudah vonis pengadilan

Data dari tabel di atas terlihat masih sedikitnya kasus-kasus *cybercrime* yang sampai ke pengadilan (10 kasus) dan masih rendahnya Vonis pengadilan terhadap kasus-kasus *cybercrime* (8 kasus) yakni antara 2 (dua) sampai dengan 6 (enam) bulan, tetapi terhadap 2 (dua) kasus di vonis lebih dari 1 (satu) tahun yaitu:

1. Tindak pidana *deface* dan perusakan terhadap website Partai Golkar (www.golkar.or.id), Vonis 1 (satu) tahun 2 (dua) bulan.
2. Tindak pidana teroris dengan cara mendaftarkan hosting dan domain website www.anshar.net, terhadap 3 (tiga) orang tersangka,yaitu :
   - Mohammad Agung Prabowo alias Max Fiderman : Vonis 3 Tahun.
   - Agung Setiadi : Vonis 6 Tahun
   - Benny : Vonis 5 Tahun

Agar suatu perkara pidana dapat sampai pada tingkat penuntutan dan pemeriksaan di sidang pengadilan, maka sebelumnya harus melewati beberapa tindakan-tindakan pada tingkat penyidik. Apabila ada unsur-unsur pidana (bukti awal telah terjadinya tindak pidana) maka barulah dari proses tersebut dilakukan penyelidikan, dalam Pasal 1 sub-13 Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia penyelidikan didefinisikan sebagai:" *serangkaian tindakan penyidik dalam hal dan menurut cara yang diatur dalam undang-undang ini untuk mencari serta mengumpulkan bukti yang dengan bukti itu membuat terang tentang tindak pidana yang terjadi dan guna menemukan tersangkanya"*. [193]

[193] Pasal 1 Sub 13 Undang-Undang Nomor 2 tahun 2002 tentang Kepolisian Negara Republik Indonesia.

Penyidikan terhadap tindak pidana teknologi informasi sebagaimana dimaksud dalam UU ITE Pasal 42, dilakukan berdasarkan ketentuan dalam Hukum Acara Pidana dan ketentuan dalam UU ITE. Pasal 43 UU ITE menjabarkan bahwa selain Penyidik Pejabat Polisi Negara Republik Indonesia, Pejabat Pegawai Negeri Sipil tertentu di lingkungan Pemerintahan yang lingkup tugas dan tanggungjawabnya di bidang Teknologi Informasi dan Transaksi Elektronik diberi wewenang khusus sebagai penyidik.

Penyelidik yang dimaksud menurut Pasal 1 KUHAP adalah pejabat polisi negara Republik Indonesia yang diberi wewenang oleh undang-undang ini untuk melakukan penyelidikan. Sedangkan penyidik yang dimaksud dalam Pasal 1 butir 1 ialah pejabat polisi negara Republik Indonesia atau pejabat pegawai negeri sipil tertentu yang diberi kewenangan khusus oleh undang-undang untuk melakukan penyidikan. Penyidik pembantu yang diatur oleh Pasal 1 butir 3 KUHAP ialah pejabat kepolisian negara Republik Indonesia yang karena diberi wewenang tertentu dapat melakukan tugas penyidikan yang diatur dalam undang-undang tentang hukum acara pidana.

Untuk menangani kejahatan dunia maya (*cybercrime*) di Indonesia, Polri telah melakukan tindakan-tindakan penegakan hukum, pendekatan, dan telah menyusun strategi penanggulangan dan penanganan kejahatan dunia maya tersebut, yakni melaksanakan penyelidikan dan penyidikan tindak pidana mayantara (*cybercrime*) terutama kegiatan yang berhubungan dengan teknologi informasi : teknologi komputer, teknologi komunikasi, teknologi elektronika, dan teknologi penyiaran dan menyelenggarakan fungsi laboratorium komputer forensik dalam rangka memberikan dukungan teknis proses penyidikan kejahatan dunia maya.

Upaya penanggulangan tindak pidana teknologi informasi oleh Polri ditangani oleh satu unit khusus di Badan Reserse Kriminal (Bareskrim) Mabes Polri yaitu Direktor II Ekonomi dan

Khusus Unit V IT dan *Cybercrime* . Dalam melakukan penyidikan suatu kasus kejahatan dunia maya, Unit V IT dan *Cybercrime* Bareskrim Polri menggunakan alat-alat investigasi standar (*standart investigative tools*), antara lain" :[194]

1. Informasi : Sebagai dasar bagi suatu kasus Informasi dapat diperoleh dari observasi, pengujian bukti elektronik yang tersimpan dalam *hard disk* atau bahkan masih dalam memori. Bagi penyidik, sangat penting untuk memperoleh informasi melalui *crime scene search* (penyidikan di tempat kejadian perkara) yang bertumpu pada komputer.
2. *Interview* dan Interogasi: Alat ini dipergunakan untuk memperoleh informasi dari pihak-pihak yang terlibat dalam kejahatan dunia maya. Wawancara ini meliputi perolehan informasi dengan memberikan pertanyaan kepada saksi-saksi, korban, dan pihak lain yang mungkin memiliki informasi relevan untuk memecahkan kasus tersebut. Sedangkan interogasi meliputi perolehan informasi dengan memberikan pertanyaan kepada tersangka dan saksi. Adapun tekniknya dilakukan dengan pendekatan simpatik yang meliputi :
    a. Pendekatan logis: Menggunakan alasan-alasan untuk meyakinkan tersangka untuk mengakui perbuatannya;
    b. *Indifference* :Dengan berpura-pura tidak memerlukan pengakuan karena penyidik telah memiliki cukup bukti walaupun tanpa pengakuan. Hal tersebut efektif untuk kasus dengan banyak tersangka, dimana keterangan yang bersangkutan saling dikonfrontir;

[194] Petrus Reinhard Golose, *Penegakan Hukum Cybercrime dalam Sistem Hukum Indonesia* dalam *Handout* Seminar Pembuktian dan Penanganan Cybercrime di Indonesia, FHUI, Jakarta, 12 April 2007,hal.16.

c. *Facing-saving approach*: Dengan membiarkan tersangka memberikan alasan-alasan atas tindakannya dan menunjukkan pengertian mengapa yang bersangkutan melakukan tindakan tersebut.

3. Instrumen kegunaan teknologi dalam memperoleh bukti-bukti: Dalam kasus kejahatan dunia maya, penggunaan data teknik *recovery* untuk menemukan informasi yang "*deleted*" dan "*erased*" dalam *disk* merupakan salah satu tipe instrumennya. Selain itu, contoh-contoh tradisional lainnya meliputi teknik forensik untuk mengumpulkan dan menganalisis bukti-bukti dan analisis DNA.
4. Menyusun laporan kasus: Setelah semua bukti fisik telah dikumpulkan dan didokumentasikan serta interogasi telah dilaksanakan, langkah yang harus dilakukan ialah penyusunan laporan kasus yang memuat :
   a. Laporan penyelidikan;
   b. Laporan penyidikan kasus pidana yang ditindaklanjuti dari laporan penyelidikan;
   c. Dokumentasi bukti-bukti elektronik;
   d. Laporan laboratorium dari ahli forensik komputer;
   e. Pernyataan-pernyataan tertulis dari saksi-saksi, tersangka, dan ahli;
   f. Laporan TKP, foto-foto dan rekaman video;
   g. *Print out* dari bukti-bukti digital yang berkaitan.
5. Pemeriksaan berkas perkara oleh Jaksa Penuntut Umum: Penuntut umum memberikan arahan kepada penyidik atas kelemahan-kelemahan berkas perkara dan tambahan informasi atau bukti tambahan yang perlu diperoleh atau klarifikasi fakta-fakta dalam rangka memperkuat tuntutan serta menyiapkan saksi-saksi untuk proses persidangan jika kasus tersebut dilimpahkan ke pengadilan.

6. Membuat keputusan untuk menuntut: Jika berkas perkara dinyatakan lengkap, penuntut umum melakukan penuntutan hukum kepada tersangka dalam suatu persidangan yang sangat tergantung dari yuridiksi dan prosedur yang ditentukan oleh undang-undang.

Dalam memulai penyidikan tindak pidana Polri menggunakan parameter alat bukti yang sah sesuai dengan Pasal 184 KUHAP yang dikaitkan dengan segi tiga pembuktian/*evidence triangle* untuk memenuhi aspek legalitas dan aspek legitimasi untuk membuktikan tindak pidana yang terjadi. Adapun rangkaian kegiatan penyidik dalam melakukan penyidikan adalah dimulai dari Penyelidikan, Penindakan, pemeriksaan dan penyelesaian berkas perkara.

B.2.1 Penyelidikan

Tahap penyelidikan merupakan tahap pertama yang dilakukan oleh penyidik dalam melakukan penyelidikan tindak pidana serta tahap tersulit dalam proses penyidikan, hal ini disebabkan karena dalam tahap ini penyidik harus dapat membuktikan tindak pidana yang terjadi serta bagaimana dan sebab-sebab tindak pidana tersebut untuk dapat menentukan bentuk laporan polisi yang akan dibuat. Informasi biasanya didapat dari NCB/Interpol yang menerima surat pemberitahuan atau laporan dari negara lain yang kemudian diteruskan ke unit *cybercrime/* satuan yang ditunjuk.

Dalam penyelidikan kasus-kasus *cybercrime* yang modusnya seperti kasus *carding* metode yang digunakan hampir sama dengan penyelidikan dalam menangani kejahatan narkotika terutama dalam *undercover* dan *control delivery*. Petugas setelah menerima informasi atau laporan dari Interpol atau *merchant* yang dirugikan melakukan koordinasi dengan pihak *shipping* untuk melakukan pengiriman barang.

Untuk kasus *hacking* atau memasuki jaringan komputer orang lain secara ilegal dan melakukan modifikasi (*deface*), penyidikannya dihadapkan problematika yang rumit, terutama dalam hal pembuktian. Banyak saksi maupun tersangka yang berada di luar yurisdiksi hukum Indonesia, sehingga untuk melakukan pemeriksaan maupun penindakan amatlah sulit, belum lagi kendala masalah bukti-bukti yang amat rumit terkait dengan teknologi informasi dan kode-kode digital yang membutuhkan SDM serta peralatan komputer forensik yang baik.

Hasil temuan peneliti di Unit V IT & *Cybercrime* Bareskrim Mabes Polri dalam kasus penyerangan situs golkar (*deface*), ada beberapa langkah-langkah yang dilakukan oleh Polri dalam menangani kasus *hacking* atau kasus-kasus perusakan terhadap komputer melalui jaringan, adalah sebagai berikut:

1. Pembuatan Laporan Polisi, yang diikuti dengan pemanggilan Saksi dari pemilik ISP (*Internet Service Provider*) yang telah diketahui bahwa ISP tersebut digunakan oleh si pelaku (*hacker*);
2. Pemeriksaan di Tempat Kejadian Perkara (TKP) dan warnet atau café net yang digunakan pelaku, sekaligus untuk mengumpulkan, melacak dan/atau melakukan penyitaan terhadap bukti elektronik (*digital evidence*) yang ada di TKP, seperti *hard disk*;
3. Melakukan pemeriksaan terhadap para saksi dan ahli yang memiliki keahlian dibidang teknologi informasi.
4. Pemeriksaan terhadap tersangka, setelah didahului dengan upaya paksa penangkapan dan/atau penahanan, berdasarkan bukti permulaan dan/atau alat bukti yang cukup;
5. Pemberkasan dan penerapan pasal-pasal pidana yang dapat disangkakan terhadap tersangka.

B.2.2 Penindakan

Penindakan kasus *cybercrime* sering mengalami hambatan terutama dalam penangkapan tersangka dan penyitaan barang bukti. Dalam penangkapan tersangka sering kali kita tidak dapat menentukan secara pasti siapa pelakunya karena mereka melakukannya cukup melalui komputer yang dapat dilakukan dimana saja tanpa ada yang mengetahuinya sehingga tidak ada saksi yang mengetahui secara langsung.

Hasil pelacakan paling jauh hanya dapat menemukan IP *Address* dari pelaku dan komputer yang digunakan. Hal itu akan semakin sulit apabila menggunakan warnet sebab saat ini masih jarang sekali warnet yang melakukan registrasi terhadap pengguna jasa mereka sehingga kita tidak dapat mengetahui siapa yang menggunakan komputer tersebut pada saat terjadi tindak pidana.

Penyitaan barang bukti banyak menemui permasalahan karena biasanya pelapor sangat lambat dalam melakukan pelaporan, hal tersebut membuat data serangan di *log server* sudah dihapus biasanya terjadi pada kasus *deface*, sehingga penyidik menemui kesulitan dalam mencari *log* statistik yang terdapat di dalam *server* sebab biasanya secara otomatis *server* menghapus *log* yang ada untuk mengurangi beban *server*. Hal ini membuat penyidik tidak menemukan data yang dibutuhkan untuk dijadikan barang bukti sedangkan data *log* statistik merupakan salah satu bukti vital dalam kasus *hacking* untuk menentukan arah datangnya serangan.

B.2.3 Pemeriksaan

Pemeriksaan terhadap saksi dan korban banyak mengalami hambatan, hal ini disebabkan karena pada saat kejahatan berlangsung atau dilakukan tidak ada satupun saksi yang melihat (*testimonium de auditu*). Mereka hanya mengetahui setelah kejadian berlangsung karena

menerima dampak dari serangan yang dilancarkan tersebut seperti tampilan yang berubah maupun tidak berfungsinya program yang ada, hal ini terjadi untuk kasus-kasus *hacking.*

Untuk kasus *carding*, permasalahan yang ada adalah saksi korban kebanyakan berada di luar negri sehingga sangat menyulitkan dalam melakukan pelaporan dan pemeriksaan untuk dimintai keterangan dalam berita acara pemeriksaan saksi korban. Dengan perkembangan disahkannya tanda tangan digital (*digital signature*) diharapkan adanya perkembangan proses pemeriksaan ke arah digital yang menggunakan *cyberspace* sehingga pemeriksaan dapat dilakukan dengan jarak jauih dan menggunakan *e-mail* ataupun *messanger* sebagai sarana dalam melakukan pemeriksaan serta menggunakan *digital signature* sebagai identitas sah terperiksa.

Peranan saksi ahli sangatlah besar sekali dalam memberikan keterangan pada kasus *cybercrime*, sebab apa yang terjadi didunia maya membutuhkan ketrampilan dan keahlian yang spesifik. Saksi ahli dalam kasus *cybercrime* dapat melibatkan lebih dari satu orang saksi ahli sesuai dengan permasalahan yang dihadapi, misalnya dalam kasus *deface*, disamping saksi ahli yang menguasai desain grafis juga dibutuhkan saksi ahli yang memahami masalah jaringan serta saksi ahli yang menguasai program.

B.2.4 Penyelesaian Berkas Perkara

Setelah penyidikan lengkap dan dituangkan dalam bentuk berkas perkara, sebelum disahkannya UU ITE ada perbedaan persepsi diantara aparat penegak hukum terhadap barang bukti digital dalam kasus *cybercrime* sehingga timbul permasalahan dalam proses pelimpahannya di Kejaksaan maupun penuntutannya di pengadilan.

Diterimanya bukti digital sebagai alat bukti penyidikan, penuntutan dan pemeriksaan di sidang pengadilan berdasarkan Pasal 5 ayat (1), ayat (2), dan ayat (3) UU ITE, diharapkan dapat

menyamakan persepsi aparat penegak hukum dalam melakukan interpretasi informasi elektronik dan dokumen elektronik sebagai alat bukti digital (*digital evidence*) dalam sidang pengadilan.

B.3 Sarana dan Fasilitas dalam Penanggulangan *Cybercrime*

Tanpa adanya sarana atau fasilitas tertentu, maka tidak mungkin penegakan hukum akan berlangsung dengan lancar. Sarana atau fasilitas tersebut antara lain, mencakup tenaga manusia yang berpendidikan dan trampil, organisasi yang baik, peralatan yang memadai, keuangan yang cukup, dan seterusnya. Kalau hal-hal itu tidak terpenuhi, maka mustahil penegakan hukum akan mencapai tujuannya.

Untuk meningkatkan upaya penanggulangan kejahatan *cyber* yang semakin meningkat Polri dalam hal ini Bareskrim Mabes Polri telah berupaya melakukan sosialisasi mengenai kejahatan *cyber* dan cara penanganannya kepada satuan di kewilayahan (Polda). Sosialisasi tersebut dilakukan dengan cara melakukan pelatihan (pendidikan kejuruan) dan peningkatan kemampuan penyidikan anggota Polri dengan mengirimkan personel-nya ke berbagai macam kursus yang berkaitan dengan *cybercrime.*

Pengiriman personel Polri tidak hanya terbatas dilakukan dalam lingkup nasional tetapi juga dikirim untuk mengikuti kursus di negara-negara maju agar dapat diterapkan dan diaplikasikan di Indonesia. Data yang diperoleh penulis dari Unit V IT dan *Cybercrime* Bareskrim Mabes Polri sebanyak 16 (enam belas) personel Polri di Unit tersebut sudah pernah melakukan pelatihan sebanyak 2 (dua) hingga 7 (tujuh) kali di luar negeri. Pelatihan atau kursus tersebut antara lain: CETS (Canada), *Internet Investigator* (Hongkong), *Computer Forensic* (Jepang), *Task Force FBI Innocent Images National Initiative* (Washington,USA), *Seminar on Cyber Terrorism* (Busan,Korea), dan negara-negara lainnya.

Pelatihan, kursus dan ceramah kepada aparat penegak hukum lain (jaksa dan hakim) mengenai *cybercrime* juga hendaknya dilaksanakan, dikarenakan jaksa dan hakim belum memiliki satuan unit khusus yang menangani kejahatan dunia maya sehingga diperlukan sosialisasi terutama setelah disyahkannya UU ITE agar memiliki kesamaan persepsi dan pengertian yang sama dalam melakukan penanganan terhadap kejahatan *cyber*.

Jaksa dan Hakim *cyber* sangat dibutuhkan seiring dengan perkembangan tindak pidana teknologi yang semakin banyak terjadi di masyarakat yang akibatnya dapat dirasakan di satu daerah, di luar daerah perbuatan yang dilakukan bahkan di luar negeri. Negara-negara yang tergabung dalam G-8 sudah menyarankan terhadap peningkatan kemampuan aparat penegak hukum dalam penanggulangan *cybercrime* dalam suatu "*Communique*" tertanggal 9-10 Desember 1997, dalam rangka "*the Meeting of Justice and Interior Ministers of the Eight*", menyampaikan 10 butir rencana tentang asas-asas dan aksi sebagai berikut:[195]

1. Tidak akan ada tempat perlindungan yang aman bagi mereka yang menyalahgunakan teknologi informasi;
2. Penyidikan dan penuntutan terhadap *high-tech crimes* internasional harus dikoordinasikan di antara negara-negara yang menaruh perhatian, tanpa melihat di mana akibat yang merugikan terjadi;
3. Aparat penegak hukum harus dilatih dan dilengkapi dalam menghadapi *high-tech crimes*;
4. Sistem hukum harus melindungi kerahasiaan, integritas dan keberadaan data dan sistem dari perbuatan yang tidak sah dan menjamin bahwa penyalahgunaan yang serius harus dipidana;

[195] Muladi, Demokratisasi,*Hak Asasi Manusia dan Reformasi Hukum di Indonesia, Op.Cit.*, hal.211.

5. Sistem hukum harus mengijinkan perlindungan dan akses cepat terhadap data elektronik, yang seringkali kritis bagi suksesnya penyidikan kejahatan;
6. Pengaturan "*mutual assistance"* harus dapat menjamin pengumpulan dan pertukaran alat bukti tepat pada waktunya, dalam kasus-kasus yang berkaitan dengan *high-tech crime;*
7. Akses elektronik lintas batas oleh penegak hukum terhadap keberadaan informasi yang bersifat umum tidak memerlukan pengesahan dari negara di mana data tersebut berada;
8. Standar forensik untuk mendapatkan dan membuktikan keaslian data elektronik dalam rangka penyidikan tindak pidana dan penuntutan harus dikembangkan dan digunakan;
9. Untuk kepentingan praktis, sistem informasi dan telekomunikasi harus didesain untuk membantu mencegah dan mendeteksi penyalahgunaan jaringan, dan harus juga memfasilitasi pencarian penjahat dan pengumpulan alat bukti;
10. Bekerja di lingkungan ini harus berkoordinasi dengan pekerjaan lain di era informasi yang relevan untuk menghindari duplikasi kebijakan.

Rencana aksi dalam pertemuan tersebut telah merumuskan langkah-langkah yang seharusnya dilakukan aparat penegak hukum dalam menanggulangi *cybercrime* , hal ini dirumuskan dalam angka 1,2,3 dan 10 pertemuan G-8 tersebut, yaitu:[196]

- Penggunaan jaringan personil yang berpengetahuan tinggi untuk menjamin ketepatan waktu, reaksi efektif terhadap kasus-kasus *high-tech* transnasional dan mendesain *point of contact* yang siap selama 24 jam;

[196] Muladi, Demokratisasi,*Hak Asasi Manusia dan Reformasi Hukum di Indonesia,* Op.Cit., hal.211-212.

- Mengambil langkah-langkah yang tepat untuk menjamin bahwa personil penegak hukum yang terlatih dan dilengkapi cukup jumlahnya untuk menjalankan tugas memerangi *high-tech crime* dan membantu badan penegak hukum di negara lain;
- Meninjau sistem hukum yang ada untuk menjamin bahwa telah terjadi kriminalisasi yang memadai terhadap penyalahgunaan sistem telekomunikasi dan komputer serta mempromosikan penyidikan terhadap *high-tech crimes*;
- Mengembangkan dan menggunakan standar forensik yang cocok guna mendapatkan dan membuktikan keaslian data elektronik yang digunakan untuk penyidikan dan penuntutan.

Sarana atau fasilitas komputer hampir dimiliki oleh semua kesatuan aparat penegak hukum, namun masih sebatas untuk keperluan mengetik. Alat ini akan sangat membantu manakala dilengkapi dengan akses internet. Kurangnya sarana dan prasarana dalam penegakan hukum *cybercrime* , sangat berpengaruh terhadap kinerja aparat penegak hukum dalam menghadapi *high-tech crimes*. Aparat penegak hukum perlu informasi yang dapat diakses melalui jaringan internet.

B.4 Kesadaran Hukum Masyarakat

Dalam konsep keamanan masyarakat modern, sistem keamanan bukan lagi tanggung jawab penegak hukum semata, namun menjadi tanggung jawab bersama seluruh elemen masyarakat. Dalam pandangan konsep ini, masyarakat di samping sebagai objek juga sebagai subjek. Sebagai subjek, masyarakat adalah pelaku aktivitas komunikasi antara yang satu dengan yang lain, serta pengguna jasa kegiatan internet dan media lainnya. Sebagai objek, masyarakat dijadikan sasaran dan korban kejahatan bagi segenap aktivitas kriminalisasi internet.

Tanggung jawab bersama atas keamanan dan ketertiban di tengah masyarakat dalam konsep modern disebut *Community Policing*. Salah satu model pengamanan dan penegakan hukum yang profesional di negara-negara maju. Semua elemen masyarakat dengan kesadaran penuh terpanggil dan bertanggung jawab atas keamanan dan ketertiban.

Dilibatkannya masyarakat dalam strategi pencegahan kejahatan mempunyai 2 (dua) tujuan pokok, menurut Mohammad Kemal Dermawan, adalah untuk:[197]

1. Mengeliminir faktor-faktor kriminogen yang ada dalam masyarakat.
2. Menggerakkan potensi masyarakat dalam hal mencegah dan mengurangi kejahatan.

Sampai saat ini, kesadaran hukum masyarakat untuk melakukan pengamanan dan merespon aktivitas *cybercrime* masih dirasakan kurang. Hal ini disebabkan antara lain oleh kurangnya pemahaman dan pengetahuan (*lack of information*) masyarakat terhadap jenis kejahatan *cybercrime* . *Lack of information* ini menyebabkan upaya penanggulangan *cybercrime* mengalami kendala, dalam hal ini kendala yang berkenaan dengan penataan hukum dan proses pengawasan (*controlling*) masyarakat terhadap setiap aktivitas yang diduga berkaitan dengan *cybercrime* .

Melalui pemahaman yang komprehensif mengenai *cybercrime* , peran masyarakat menjadi sangat penting dalam upaya pengawasan, ketika masyarakat mengalami *lack of information*, peran mereka akan menjadi mandul. Sebaliknya ketika masyarakat memahami bahwa *cybercrime* merupakan tindak pidana yang harus ditanggulangi, masyarakat akan mengantisipasinya atau melaporkannya kepada aparat kepolisian setempat.

Resolusi Kongres PBB VIII/1990 mengenai "*Computer-related crimes*" dalam point a.3 dan a.5 menghimbau negara anggota untuk:[198]

---

[197] Mohammed Kemal Dermawan, *Strategi Pencegahan Kejahatan*, Citra Aditya Bhakti, Bandung, 1994,hal.10.

a.3 melakukan langkah-langkah untuk membuat peka (sensitif) warga masyarakat, aparat pengadilan dan penegak hukum, terhadap pentingnya pencegahan kejahatan yang berhubungan dengan komputer.

a.5 Memperluas "*rules of ethics"* dalam penggunaan komputer dan mengajarkannya melalui kurikulum informatika.

Tugas masyarakat tidak hanya sebatas mengurangi angka kejahatan semata, melainkan juga harus ikut serta dalam proses menganalisa, mengenal dan memahami ancaman kejahatan tersebut dengan cara melakukan pengamanan terhadap jaringan komputer, *hardware*, dan masing-masing pribadi masyarakat.

B.4.1 Pengamanan *Software* Jaringan Komputer

Tindakan preventif yang dapat dilakukan dalam rangka pengamanan *software* jaringan komputer adalah sebagai berikut:

1. Mengatur akses (*access control*), melalui mekanisme *authentication* dengan menggunakan *password.*
2. *Firewall*, program yang merupakan sebuah perangkat yang diletakkan antara internet dengan jaringan internal, tujuannya adalah untuk menjaga agar akses kedalam maupun keluar dari orang yang tidak berwenang *(unauthorized acces)* tidak dapat dilakukan.
3. *Intruder Detection System* (IDS), diantaranya adalah mendeteksi *probing* dengan *monitor log file (Autobuse)*

---

[198] United Nations, *Eighth UN Congress on the Prevention of Crime and the Treatment of Offenders, Report*, 1991, hal.141, lihat dalam Barda Nawawi Arief, *Sari Kuliah: Perbandingan Hukum Pidana*,PT. Raja Grafindo Persada, Jakarta, 2002,hal.253.

4. *Back-up* rutin, untuk cadangan manakala sistem kita berhasil dimasuki pihak lain (*intruder*)

B.4.2 Pengamanan *Hardware*

Langkah-langkah dalam pengamanan *hardware* yang dapat dilakukan adalah sebagai berikut:

1. Penguncian komputer, untuk komputer baru memang tidak dilengkapi dengan kunci seperti tipe komputer lama, padahal ini merupakan salah satu cara yang paling efektif untuk mencegah penggunaan oleh orang-orang yang tidak dikehendaki.
2. Penggunaan *dial back*, adalah penggunaan telepon *double*, antara telepon kirim dengan telepon terima, dengan cara bergantian dalam pemakaian saluran telepon.

B.4.3 Pengamanan Personalia

Faktor ini sangat penting, dan tidak bisa diabaikan. Seseorang yang ditugaskan sebagai administrator, dan operator harus menguasai segala isi yang ada di dalam komputer. Manajemen administrator perlu dilakukan dengan baik untuk menjamin keamanan jaringan. Pengamanan tersebut meliputi:

1. Seleksi operator dari sisi intelektual dan moral, hal itu harus berjalan secara seimbang karena menyangkut perbuatan yang bersifat subyektif.
2. Membuat perjanjian atau MoU antara operator dengan manajemen yang berkaitan dengan:
    a. Operator yang lebih dari satu;
    b. *Password* dan perubahan *password;*
    c. Cuti operator;
    d. Mutasi operator;

e. Hubungan antara operator dengan pimpinan manajemen;

f. Mutasi operator yang diketahui pimpinan yang memuat segala kegiatan operator secara lengkap;

g. Melaksanakan test psikologi terhadap personel yang mengawaki komputer secara priodik

B.5 Pembuktian dalam Penegakan Hukum Tindak Pidana Teknologi Informasi

Pada hakekatnya, pembuktian dimulai sejak adanya suatu peristiwa hukum. Apabila ada unsur-unsur pidana (bukti awal telah terjadinya tindak pidana) maka barulah dari proses tersebut dilakukan penyelidikan (serangkaian tindakan penyelidik untuk mencari dan menemukan suatu peristiwa yang diduga sebagai tindak pidana guna menentukan dapat atau tidaknya dilakukan penyelidikan menurut cara yang diatur dalam undang-undang ini), yang diatur dalam Undang-undang Nomor 2 Tahun 2002 tentang Kepolisian dalam pasal 1 angka 13.

Menurut M.Yahya Harahap, pembuktian adalah ketentuan-ketentuan yang berisi penggarisan dan pedoman tentang cara-cara yang dibenarkan undang-undang membuktikan kesalahan yang didakwakan kepada terdakwa.[199] Menurut Pitlo, "pembuktian adalah suatu cara yang dilakukan oleh suatu pihak atas fakta dan hak yang berhubungan dengan kepentingannya".[200] Menurut Subekti, yang dimaksudkan dengan "membuktikan" adalah meyakinkan hakim tentang kebenaran dalil ataupun dalil-dalil yang dikemukakan oleh para pihak dalam suatu persengketaan.[201] "Pembuktian tentang benar tidaknya terdakwa melakukan perbuatan yang didakwakan, merupakan bagian yang terpenting dalam hukum acara pidana".[202]

---

[199] M.Yahya Harahap, *Pembahasan Permasalahan Dan Penerapan KUHAP: Pemeriksaan Sidang Pengadilan, Banding, Kasasi, dan Peninjauan Kembali*,*Op.Cit*.,hal.273.

[200] Edmon Makarim, *Kompilasi Hukum Telematika*, Rajagrafindo Persada, Jakarta, 2003,hal. 417.

[201] Subekti, *Hukum Pembuktian*, Pradnya Paramita, Jakarta, 1995, hal. 1.

[202] Andi Hamzah, *Hukum Acara Pidana Indonesia*, Sinar Grafika, Jakarta, 2005, hal. 245.

Dalam hukum pembuktian dikenal istilah *notoire feiten notorious* (*generally known*) yang berarti setiap hal yang "sudah umum diketahui" tidak lagi perlu dibuktikan dalam pemeriksaan sidang pengadilan".[203] Hal ini tercantum dalam Pasal 184 ayat (2) KUHAP yang berbunyi, "hal yang secara umum diketahui tidak perlu dibuktikan". "Menurut Yahya Harahap, mengenai pengertian "hal yang secara umum sudah diketahui" ditinjau dari segi hukum, tiada lain daripada "perihal" atau "keadaan tertentu" atau *omstandigheiden* atau *circumstances*, yang sudah sedemikian mestinya atau kesimpulan atau resultan yang menimbulkan akibat yang pasti demikian".[204]

Berkaitan dengan membuktikan sebagaimana diuraikan di atas, dalam hukum acara pidana (KUHAP) secara tegas disebutkan beberapa alat-alat bukti yang dapat diajukan oleh para pihak yang berperkara di muka persidangan. Berdasarkan Pasal 184 KUHAP,[205] alat-alat bukti ialah : Keterangan saksi, keterangan ahli, surat, petunjuk, dan keterangan terdakwa. Dalam perkembangannya, keberadaan informasi dan data elektronik diakui sebagai "alat bukti lain" selain yang diatur dalam Pasal 184 KUHAP, Pasal 164 *Herzien Inlands Reglements* (HIR) dan 1903 Kitab Undang-Undang Hukum Perdata (bukti tulisan, bukti dengan saksi, persangkaan-persangkaan, pengakuan dan sumpah).

B.5.1 Alat Bukti Informasi dan Data Elektronik

Undang-Undang No.8 Tahun 1997 Tentang Dokumen Perusahaan telah mulai mengatur ke arah pembuktian data elektronik.[206] Melalui undang-undang ini pemerintah berusaha mengatur pengakuan atas *microfilm* dan media lainnya seperti alat penyimpan informasi yang

---

[203] M.Yahya Harahap, *Pembahasan Permasalahan Dan Penerapan KUHAP: Pemeriksaan Sidang Pengadilan, Banding, Kasasi, dan Peninjauan Kembali,Op.Cit*.,hal.276

[204] M.Yahya Harahap, *Pembahasan Permasalahan Dan Penerapan KUHAP: Pemeriksaan Sidang Pengadilan, Banding, Kasasi, dan Peninjauan Kembali,Op.Cit*.,hal.276

[205] M.Yahya Harahap, *Pembahasan Permasalahan Dan Penerapan KUHAP: Pemeriksaan Sidang Pengadilan, Banding, Kasasi, dan Peninjauan Kembali,Op.Cit*., hal.107

[206] Isis Ikhwansyah, *Prinsip-Prinsip Universal Bagi Kontak Melalui E-Commerce dan Sistem Hukum Pembuktian Perdata dalam Teknologi Informasi, dalam Cyberlaw: Suatu Pengantar*, ELIPS, Bandung,2002,hal.36

bukan kertas dan mempunyai tingkat pengamanan yang dapat menjamin keaslian dokumen yang dialihkan atau ditransformasikan, misalnya *Compact Disk-Read Only Memory* (CD-ROM) dan *Write-One-Read-Many* (WORM) sebagai alat bukti yang sah, diatur dalam Pasal 12 Undang-Undang Dokumen Perusahaan.

Pengaturan informasi dan data elektronik tercantum didalam beberapa undang-undang khusus yang lain yaitu Pasal 38 UU No. 15/2002 tentang Tindak Pidana Pencucian Uang, Pasal 27 UU No. 16/2003 jo UU No. 15/2003 tentang Pemberantasan Tindak Pidana Terorisme, dan Pasal 26 (a) UU No. 20/2001 tentang Perubahan atas UU No. 31/1999 tentang Pemberantasan Tindak Pidana Korupsi . Pengaturan terhadap alat bukti dalam perundang-undangan di Indonesia dapat dilihat dalam tabel di bawah ini:

Tabel.6

Alat Bukti Informasi dan Data Elektronik dalam Undang-Undang

No	Undang-Undang	Pasal	Keterangan
1	UU No.8 tahun 1997 ttg Dokumen Perusahaan	Pasal 12	Pengakuan atas Mikrofilm dan media penyimpan yang lain seperti *Compact Disk – Read Only Memory* (CD-ROM), dan *Write-Once–Read–Many* (WORM),
2	UU No. 20/2001 tentang Perubahan atas UU No. 31/1999 ttg Pemberantasan Tindak Pidana Korupsi	Pasal 26 huruf (a)	Pengakuan bukti petunjuk sebagai alat bukti yang sah. Bukti petunjuk juga dapat diperoleh dari alat bukti lain yang berupa informasi yang diucapkan, dikirim, diterima, atau disimpan secara elektronik
3	UU No. 15/2002 tentang Tindak Pidana Pencucian Uang	Pasal 38 huruf (b)	alat bukti elektronik atau *digital evidence* adalah alat bukti lain berupa informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu.
4	UU No. 16/2003 jo UU No. 15/2003 ttg Pemberantasan Tindak Pidana Terorisme,	Pasal 27 huruf (b) dan (c)	Alat bukti berupa informasi yang disimpan secara elektronik dengan alat optik. Data, rekaman atau informasi yang terekam secara elektronik
5	UU No.11 tahun	Pasal 5	Informasi Elektronik dan/atau Dokumen

	2008 ttg Informasi dan Transaksi Elektronik		Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah.Serta merupakan perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia.

Dalam UU No. 15/2002 tentang Tindak Pidana Pencucian Uang, Pasal 27 UU No. 16/2003 jo UU No. 15/2003 tentang Pemberantasan Tindak Pidana Terorisme, dan Pasal 26 (a) UU No. 20/2001 tentang Perubahan atas UU No. 31/1999 tentang Pemberantasan Tindak Pidana Korupsi menyatakan informasi dan bukti elektronik dikatakan sebagai alat bukti baru yang merupakan pelengkap dari alat-alat bukti yang telah dikenal dalam Pasal 184 KUHAP.

Penerapan alat bukti informasi dan data elektronik dalam perundang-undangan sering mengakibatkan multitafsir diantara aparat penegak hukum terutama pada saat pemeriksaan pengadilan. Hal tersebut dikarenakan belum adanya rambu yang jelas terhadap pengakuan alat bukti tersebut.

Konsep Rancangan Undang-Undang KUHP 2000, dimana konsep ini mengalami perubahan sampai dengan 2008 telah mengatur alat bukti elektronik yaitu:[207] Dalam Buku I (Ketentuan Umum) Dibuat Ketentuan mengenai alat bukti:

1. Pengertian “barang” (Pasal 174/178) yang di dalamnya termasuk benda tidak berwujud berupa data dan program komputer, jasa telepon atau telekomunikasi atau jasa komputer.
2. Pengertian “anak kunci” (Pasal 178/182) yang di dalamnya termasuk kode rahasia, kunci masuk komputer, kartu *magnetic*, sinyal yang telah deprogram untuk membuka

[207] Barda Nawawi Arief, *Pembaharuan Hukum Pidana Dalam Perspektif Kajian Perbandingan*, PT. Citra Aditya Bakti, Bandung,2005, hal.131-133.

sesuatu. Menurut Agus Raharjo, [208] maksud dari anak kunci ini kemungkinannya adalah *password* atau kode-kode tertentu seperti privat atau *public key infrastructure*.

3. Pengertian "surat" (Pasal 188/192) termasuk data tertulis atau tersimpan dalam disket, pita *magnetic*, media penyimpanan komputer atau penyimpanan data elektronik lainnya.
4. Pengertian "ruang" (Pasal 189/193) termasuk bentangan atau terminal komputer yang dapat diakses dengan cara-cara tertentu. Maksud dari ruang ini kemungkinan termasuk pula dunia maya atau mayantara atau *cyberspace* atau *virtual reality*.
5. Pengertian "masuk" (Pasal 190/194) termasuk mengakses komputer atau masuk ke dalam sistem komputer. Pengertian masuk menurut Agus Raharjo di sini adalah masuk ke dalam sistem jaringan informasi global yang disebut internet dan kemudian baru masuk ke sebuah situs atau *website* yang di dalamnya berupa *server* dan komputer yang termasuk dalam pengelolaan situs. Jadi ada 2 pengertian masuk, yaitu masuk ke internet dan masuk ke situs.
6. Pengertian "jaringan telepon" (Pasal 191/195) termasuk jaringan komputer atau sistem komunikasi komputer.

Dengan meningkatnya aktivitas elektronik, maka alat pembuktian yang dapat digunakan secara hukum harus juga meliputi informasi atau dokumen elektronik untuk memudahkan pelaksanaan hukumnya. Selain itu hasil cetak dari dokumen atau informasi tersebut juga harus dapat dijadikan bukti yang sah secara hukum. Untuk memudahkan pelaksanaan penggunaan bukti elektronik (baik dalam bentuk elektronik atau hasil cetak), maka bukti elektronik dapat

[208] Agus Raharjo, *CyberCrime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, PTCitra Aditya Bakti, Bandung,2002, hal. 236

disebut sebagai perluasan alat bukti yang sah, sesuai dengan hukum acara yang berlaku di Indonesia, sebagaimana tertulis dalam Pasal 5 UU ITE:

1. Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah.
2. Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya sebagaimana dimaksud pada ayat (1) merupakan perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia.
3. Informasi Elektronik dan/atau Dokumen Elektronik dinyatakan sah apabila menggunakan Sistem Elektronik sesuai dengan ketentuan yang diatur dalam Undang Undang ini.[209]

Namun bukti elektronik tidak dapat digunakan dalam hal-hal spesifik sebagaimana yang tertulis dalam Pasal 5 ayat (4) UU ITE menyatakan: Ketentuan mengenai Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud pada ayat (1) tidak berlaku untuk:

a. surat yang menurut Undang Undang harus dibuat dalam bentuk tertulis; dan
b. surat beserta dokumennya yang menurut Undang Undang harus dibuat dalam bentuk akta notaril atau akta yang dibuat oleh pejabat pembuat akta.[210]

Surat yang menurut undang-undang harus dibuat tertulis seperti dalam pembuatan dan pelaksanaan surat-surat terjadinya perkawinan dan putusnya perkawinan, surat-surat yang menurut undang-undang harus dibuat dalam bentuk tertulis, perjanjian yang berkaitan dengan transaksi barang tidak bergerak, dokumen yang berkaitan dengan hak kepemilikan dan juga dokumen lainnya yang menurut peraturan perundang-undangan mengharuskan adanya pengesahan notaris atau pejabat yang berwenang.

Bukti elektronik baru dapat dinyatakan sah apabila menggunakan sistem elektronik yang sesuai dengan peraturan yang berlaku di Indonesia. Suatu bukti elektronik dapat memiliki kekuatan hukum apabila informasinya dapat dijamin keutuhannya, dapat

[209] Pasal 5 ayat (1),(2) dan (3) Undang-Undang No.11 tahun 2008 tentang Informasi dan Transaksi Elektronik, diundangkan pada 28 April 2008, Lembaran Negara No.58.

[210] Pasal 5 ayat (4) Undang-Undang No.11 tahun 2008 tentang Informasi dan Transaksi Elektronik, diundangkan pada 28 April 2008, Lembaran Negara No.58.

dipertanggungjawabkan, dapat diakses dan dapat ditampilkan, sehingga menerangkan suatu keadaan. Orang yang mengajukan suatu bukti elektronik harus dapat menunjukan bahwa informasi yang dimilikinya berasal dari sistem elektronik yang terpercaya.

Berdasarkan Pasal 5 ayat (1) UU ITE, informasi elektronik memiliki kekuatan hukum sebagai alat bukti yang sah, bila informasi elektronik ini dibuat dengan menggunakan sistem elektronik yang dapat dipertanggungjawabkan sesuai dengan perkembangan teknologi informasi. Bahkan secara tegas, Pasal 6 UU ITE menentukan bahwa "Terhadap semua ketentuan hukum yang mensyaratkan bahwa suatu informasi harus berbentuk tertulis atau asli selain yang diatur dalam Pasal 5 ayat (4), persyaratan tersebut telah terpenuhi berdasarkan undang-undang ini jika informasi elektronik tersebut dapat terjamin keutuhannya dan dapat dipertanggungjawabkan, dapat diakses, dapat ditampilkan sehingga menerangkan suatu keadaan".

Penegasan terhadap informasi elektronik dan dokumen elektronik dapat dijadikan menjadi alat bukti penyidikan, penuntutan dan pemeriksaan di sidang pengadilan tertulis didalam Pasal 44 UU ITE yang isinya sebagai berikut:[211]

a. alat bukti sebagaimana dimaksud dalam ketentuan Perundang-undangan; dan
b. alat bukti lain berupa Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud dalam Pasal 1 angka 1 dan angka 4 serta Pasal 5 ayat (1), ayat (2), dan ayat (3).

Sesungguhnya pandangan yang mengatakan alat bukti elektronik tidak dapat menjadi alat bukti tertulis tidaklah mutlak, karena sangat tidak relevan di jaman teknologi tetap memandang alat bukti tertulis hanya yang berbentuk konvensional. Disinilah Hakim dituntut untuk berani melakukan terobosan hukum, karena dia yang paling berkuasa dalam memutuskan suatu perkara

[211] Pasal 44 ayat (4) Undang-Undang No.11 tahun 2008 tentang Informasi dan Transaksi Elektronik, diundangkan pada 28 April 2008, Lembaran Negara No.58.

dan karena dia juga yang dapat memberi suatu *vonnis van de rechter* (keputusan hakim) yang tidak langsung dapat didasarkan atas suatu peraturan hukum tertulis atau tidak tertulis. Dalam hal ini, Hakim harus membuat suatu peraturan sendiri (*eigen regeling*).[212] Tindakan seperti ini, menurut Pasal 14 Undang-Undang Nomor 14 Tahun 1970 tentang kekuasaan kehakiman, dibenarkan karena seorang Hakim tidak boleh menolak untuk memeriksa, mengadili dan memutuskan suatu perkara dengan alasan peraturan perundang-undangan yang tidak menyebutkan, tidak jelas, atau tidak lengkap (asas *ius curia novit*). Bila keputusan Hakim yang memuat *eigen regeling* ini dianggap tepat dan dipakai berulang-ulang oleh Hakim-hakim lainnya, maka keputusan ini akan menjadi sebuah sumber hukum bagi peradilan (*rechtspraak*).[213]

Dengan dasar-dasar di atas, seorang Hakim diberikan keleluasan untuk menemukan hukum (*rechtsvinding*), baik dengan cara melakukan interpretasi hukum (*wetinterpretatie*) , maupun dengan menggali, mengikuti dan memahami nilai-nilai hukum yang hidup dalam masyarakat. Metoda interpretasi yang dapat digunakan dalam pencarian kekuatan hukum dari akta elektronik dan tanda tangan elektronik khususnya adalah interpretasi analogi, interpretasi ekstensif dan interpretasi sosiologis.[214]

Metoda interpretasi analogis dilakukan dengan memberi ibarat terhadap suatu kata-kata sesuai dengan asas hukumnya, sehingga suatu peristiwa yang pada awalnya tidak dapat dimasukkan, lalu dianggap sesuai dengan ketentuan peraturan tersebut, misalnya menyambung aliran listrik dianggap mencuri/mengambil aliran lisrik sebagaimana yang ditegaskan dalam yurisprudensi tetap *Hoge Raad der Nederlanden* (pengadilan tertinggi di Belanda). Berdasarkan

---

[212] E. Utrecht dan Moh. Saleh Djindang, *Pengantar dalam hukum Indonesia*, cetakan kesebelas, penerbit P.T. Ichtiar Baru dan Penerbit Sinar Harapan, Jakarta, 1989, hal.121.

[213] *Ibid*

[214] E. Utrecht dan Moh. Saleh Djindang, *Pengantar dalam hukum Indonesia*, Op.Cit., hal.203.

asas konkordansi, pengadilan Indonesia menggunakan yurisprudensi ini untuk menjawab kebingungan Hakim dalam menyelesaikan kasus penyalahgunaan/pencurian listrik.[215]

Di Indonesia sendiri terdapat putusan pengadilan yaitu putusan MARI.Nomor.9/KN/1999, yang dalam putusannya hakim menerima hasil *print out* sebagai alat bukti surat. Kemudian kasus pidana yang diputus di Pengadilan Negeri Jakarta Timur mengetengahkan bukti *e-mail* (*elektronic mail*) sebagai salah satu alat bukti. Setelah mendengar keterangan ahli bahwa dalam transfer data melalui *e-mail* tersebut tidak terjadi tindakan manipulatif, hakim memvonis terdakwa dengan hukuman satu tahun penjara karena terbukti telah melakukan tindakan cabul berupa penyebaran tulisan dan gambar.[216]

B.5.2 Tanda Tangan Elektronik

Salah satu alat yang dapat digunakan untuk menentukan keaslian atau keabsahan suatu bukti elektronik adalah tanda tanggan elektronik. Tanda tangan elektronik harus dapat diakui secara hukum karena penggunaan tanda tangan elektronik lebih cocok untuk suatu dokumen elektronik.

Agar suatu tanda tangan elektronik dapat diakui kekuatan hukumnya, maka syarat-syarat yang harus dipenuhi sesuai Pasal 11 ayat (1) UU ITE adalah:[217]

a. Data pembuatan tanda tangan elektronik hanya terkait kepada penanda tangan saja;
b. Data pembuatan tanda tangan elektronik hanya berada dalam kuasa penandatangan pada saat penandatanganan;
c. Perubahan terhadap tanda tangan elektronik yang terjadi setelah waktu penandatanganan dapat diketahui;
d. Perubahan terhadap informasi elektronik yang berhubungan dengan tanda tangan elektronik dapat diketahui setelah waktu penandatanganan;
e. Terdapat cara tertentu yang dipakai untuk mengidentifikasi siapa penandatangannya;

---

[215] E. Utrecht dan Moh. Saleh Djindang, *Pengantar dalam hukum Indonesia*, Op.Cit.,hal.127.

[216] Di akses dari http://www.hukumonline.com/artikel_detail dengan judul ”Data Elektronik sebagai Alat Bukti Masih Dipertanyakan” pada tanggal 30 Agustus 2008.

[217] Pasal 11 Undang-Undang No.11 tahun 2008 tentang Informasi dan Transaksi Elektronik, diundangkan pada 28 April 2008, Lembaran Negara No.58.

f. Terdapat cara tertentu untuk menunjukkan bahwa penandatangan telah memberikan persetujuan terhadap informasi elektronik yang ditandatangani.

Orang yang mengunakan tanda tangan elektronik atau terlibat dalamnya mempunyai kewajiban untuk mengamankan tanda tangan agar tanda tersebut tidak dapat dapat disalahgunakan oleh orang yang tidak berhak. Pengamanan tanda tangan elektronik sesuai Pasal 12 (2) UU ITE meliputi syarat :[218]

a. Sistem tidak dapat diakses oleh orang lain yang tidak berhak;
b. Penandatangan harus waspada terhadap penggunaan tidak sah dari data pembuatan tanda tangan oleh orang lain;
c. Penandatangan harus menggunakan cara atau instruksi yang dianjurkan oleh penyelenggara tanda tangan elektronik. Penandatangan harus memberitahukan kepada orang yang mempercayai tanda tangan tersebut atau kepada pihak pendukung layanan tanda tangan elektronik apabila ia percaya bahwa:
   1. Data pembuatan tanda tangan telah dibobol; atau
   2. Tanda tangan dapat menimbulkan risiko, sehingga ada kemungkinan bobolnya data pembuatan tanda tangan elektronik tersebut.
d Dalam hal sertifikat Elektronik digunakan untuk mendukung tanda tangan Elektronik, penanda tangan harus memastikan kebenaran dan keutuhan semua informasi yang terkait dengan sertifikat elektronik tersebut.

Menurut Penulis, penggunaan kata “data pembuatan tanda tangan elektronik” hendaklah disederhanakan menjadi “tanda tangan elektronik”, agar lebih jelas dan mudah dimengerti karena tidak ada tanda tangan elektronik tanpa data. Tanda tangan elektronik yang diatur di Peraturan Pemerintah sesuai dengan wewenang yang akan diberikan Pasal 11 ayat (2) UU ITE harus memberikan perbedaan antara tanda tangan elektronik *simple* (sederhana) dan tanda tangan elektronik *securisée* (diamankan/terkualifikasi).[219]

Ketentuan-ketentuan Pasal 11 merupakan syarat-syarat minimal (yang harus diintegrasikan dengan pasal 12) untuk dipenuhi agar sebuah tanda tangan elektronik menikmati “asas praduga kehandalan” (*présomption de fiabilité*) yang memberikan kekuatan hukum dan

[218] Pasal 12 Undang-Undang No.11 tahun 2008 tentang Informasi dan Transaksi Elektronik, diundangkan pada 28 April 2008, Lembaran Negara No.58 .

[219] Julius Singara, *Memoire : la cryptologie et la preuve électronique de la France à l’Indonésie*, D.E.A. *Informatique et Droit, Université Montpellier I, année universitaire,* Montpellier, 2003-2004, hal.80

akibat hukum yang sama dengan tanda tangan manuskrip. Tanda tangan elektronik *securisée* (diamankan/terkualifikasi) seharusnya yang diatur dalam Peraturan Pemerintah nantinya dan berhak untuk menikmati *presomption de fiabilité.* Kecuali dibuktikan lain, keuntungan dari asas ini adalah jaminan praduga kehandalan identitas dari pengguna dan integritasnya dengan akta yang dilekatinya. Ketidakmampuan pengguna untuk menikmati asas ini, menciptakan kesulitan kepada mereka dalam membuktikan kehandalan prosedur yang digunakannya. Dari sudut kekuatan hukum dan akibat hukum, jelaslah tipe *securisée* yang akan mendapatkan nilai pembuktian lebih unggul daripada tanda tangan elektronik sederhana.

Selain itu, menurut Penulis, butir (f) pada Pasal 11 ayat (1) sebaiknya dihapus karena dari sudut pandang teknis, butir (e) sudah cukup untuk membuktikan bahwa Penandatangan telah memberikan persetujuannya dengan menandatangani akta elektronik tersebut dengan tanda tangan elektronik miliknya. Namun, untuk membuktikan apakah persetujuan Penandatangan tersebut datang tanpa unsur paksaan, digunakanlah fakta-fakta hukum dalam proses peradilanlah, bukan piranti lunak yang digunakan.

Berkaitan dengan pembuktian R. Subekti. mengatakan bahwa, “beban pembuktian harus dilakukan dengan adil dan tidak berat sebelah, karena suatu pembagian beban pembuktian yang berat sebelah berarti *a priori* menjerumuskan pihak yang mendapat beban terlalu berat kedalam jurang kekalahan”.[220] Berkaitan dengan beban pembuktian terhadap tanda tangan elektronik, hendaknya dibebankan kepada pihak yang mempunyai alat-alat yang memadai untuk membuktikan bahwa tanda tangan elektronik tersebut dibuat dengan prosedur yang handal dan dapat dipertanggungjawabkan.

Sistem beban pembuktian terhadap tanda tangan elektronik hendaknya diserahkan kepada penyelenggara sertifikasi tanda tangan elektronik. Dengan demikian, kesulitan hakim dalam hal

[220] R. Soesilo , *RIB/HIR dengan penjelasan,* Politeia, Bogor, 1995, hal. 113.

membuktikan unsur-unsur tersebut terutama dengan menggunakan alat bukti elektronik dapat diringankan oleh saksi ahli karena penyelenggara sertifikasi tanda tangan elektroniklah yang mempunyai kemampuan teknis dan peralatan teknik untuk membuktikan kehandalan dan keamanan prosedur yang mereka gunakan.

Pengaturan data elektronik sebagai alat bukti walau bagaimanapun telah melakukan pembaharuan mengenai substansi hukum, yang ada dalam hukum acara pidana (KUHAP) Indonesia, HIR dan KUH Perdata. Tetapi perluasan alat bukti tersebut akan terasa sia-sia jika aparat penegak hukumnya belum siap atau belum mampu untuk itu dibutuhkan pengetahuan dan kemampuan aparat penegak hukum dalam teknologi informasi serta keyakinan dan pandangan yang luas hakim dalam menafsirkan hukum sebagai upaya penegakan hukum dunia mayantara di Indonesia.

B.6 Yurisdiksi Hukum Pidana dalam Penanggulangan *Cybercrime*

Pengaturan teknologi informasi yang diterapkan oleh suatu negara berlaku untuk setiap orang yang melakukan perbuatannya baik yang berada di wilayah negara tersebut maupun di luar negara apabila perbuatan tersebut memiliki akibat di Indonesia. Butuhnya pengaturan yurisdiksi ekstrateritorial dikarenakan suatu tindakan yang merugikan kepentingan orang atau negara dapat dilakukan diwilayah negara lain. Oleh karena itu, peraturan mengenai *cyberlaw* harus dapat mencakup perbuatan yang dilakukan diluar wilayah Indonesia tapi merugikan kepentingan orang atau negara dalam wilayah Indonesia.

Undang-Undang No.11 tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) telah mengatur masalah yurisdiksi yang didalamnya sudah menerapkan asas universal. Hal ini dapat dilihat dari 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.[221]

Undang-Undang ini memiliki jangkauan yurisdiksi tidak semata-mata untuk perbuatan hukum yang berlaku di Indonesia dan/atau dilakukan oleh warga negara Indonesia, tetapi juga berlaku untuk perbuatan hukum yang dilakukan di luar wilayah hukum (yurisdiksi) Indonesia baik oleh warga negara Indonesia maupun warga negara asing atau badan hukum Indonesia maupun badan hukum asing yang memiliki akibat hukum di Indonesia, mengingat pemanfaatan Teknologi Informasi untuk Informasi Elektronik dan Transaksi Elektronik dapat bersifat lintas teritorial atau universal. Yang dimaksud dengan ”merugikan kepentingan Indonesia” 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.[222]

Perluasan pengaturan yurisdiksi ekstrateritorial dalam tindak pidana teknologi informasi dimaksudkan untuk melindungi jaringan komunikasi/informasi yang saat ini telah menjadi kepentingan internasional/global. Pengaturan yurisdiksi ekstrateritorial sama dengan prinsip atau azas *ubikuitas* sehingga sangat beralasan dalam menghadapi tindak pidana mayantara. Sebagaimana ditulis oleh Barda Nawawi Arief,[223] mengusulkan untuk memberlakukan prinsip *ubikuitas* (*the principle of ubiquity*) atas tindak pidana mayantara. Alasannya saat ini semakin marak terjadi *cybercrime* seiring dengan pertumbuhan penggunaan internet. Yang dimaksud dengan prinsip atau azas *ubikuitas* adalah prinsip yang mengatakan bahwa delik-delik yang

[221] Pasal 2 Undang-Undang No.11 tahun 2008 tentang Informasi dan Transaksi Elektronik, diundangkan pada 28 April 2008, Lembaran Negara No.58.

[222] Penjelasan Pasal 2 Undang-Undang No.11 tahun 2008 tentang Informasi dan Transaksi Elektronik, diundangkan pada 28 April 2008, Lembaran Negara No.58.

[223] Barda Nawawi Arief, *Kapita Selekta Hukum Pidana, Op,Cit,*hal.253.

dilakukan atau terjadi di sebagian wilayah teritorial negara sebagian di luar wilayah teritorial suatu negara (ekstrateritorial) harus dapat dibawa ke dalam yurisdiksi setiap negara yang terkait.

Berdasarkan Pasal 2 dan penjelasan UUITE pada dasarnya tetap dianut asas-asas ruang berlakunya hukum pidana dalam KUHP yaitu didasarkan pada asas teritorial (pasal 2-5 KUHP), asas personal/nasional aktif (pasal 7 KUHP), dan asas universal (pasal 8 KUHP), hanya ada perubahan dan perkembangan formulasinya yaitu:

- Memuat ketentuan tentang lingkup yurisdiksi yang bersifat transnasional dan internasional serta memuat ketentuan khusus terhadap tindak pidana teknologi informasi.
- Subjek hukum tidak hanya terhadap perorangan baik warga negara Indonesia ataupun warga negara asing yang memiliki akibat hukum di Indonesia tetapi juga terhadap badan hukum asing (koorporasi)

Berlakunya asas-asas ruang hukum pidana dalam KUHP sebenarnya tidak perlu lagi diatur didalam UU ITE, maka lebih aman dan lebih luas jangkauannya apabila UU ITE menegaskan berlakunya asas-asas ruang berlakunya hukum pidana menurut KUHP dengan menambah/memperluas hal-hal yang belum ditegaskan dalam KUHP. Sebagaimana yang tertulis dalam *Section* 3, *Article* 22 *Convention on Cybercrime*, dinyatakan:[224]

6. *Each Party shall adopt such legislative and other measures as may be necessary to estabilish jurisdiction over any offence estabilished in accordance with Article 2 through 11 of this convention,when the offence is commited:*
    a. *In its teritorry; or*
    b. *On board a ship flying the flag of that party;or*
    c. *On board an aircraft registered under the laws of that party;or*
    d. *By one its national,if the offence is punishable under criminal law where it was commited outside the territorial jurisdiction of any state.*
7. *Each party may reserve the right not to apply only in specific cases or conditions the jurisdiction rules laid down in paragrphs 1.b through 1.d of this article or any part there of;*

[224] *Council of Europe, European Treaty Series* No.185,Budapest 23.IX.2001,page 13

8. *Each party shall adopt such measures as may be necesarry to estabilish jurisdiction over the offences reffered to in Article 24,paragraph 1, of this convention, in cases where an alleged offender is present in its territory and it does not estradite him or her to another party,solely on the basis of his or her natonality,after a request for extradition;*
9. *This convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.*
10. *when more than one Party claims jurisdiction over an alleged offence estabilished in accordance with this Convention, the Parties involved shall, where apporiate,consult with a view to determining the most apporiate jurisdiction for prosecution.*

Problema dalam penerapan pengaturan yurisdiksi ekstrateritorial adalah dalam hal penegakan hukumnya. Beberapa komplain sering dilakukan oleh beberapa kedutaan besar, yang disalurkan melalui interpol ke Mabes Polri atau yang disalurkan ke Kepolisian Daerah mengalami jalan buntu. Hal tersebut dapat terlihat dari data korespondensi kasus *cybercrime* Interpol Indonesia dari tahun 2006 sampai dengan tahun 2008 di bawah ini:

Tabel.7

Data Korespondensi Kasus *Cybercrime* Interpol 2006-2008[225]

NO	TAHUN	JUMLAH KASUS	HASIL PENYELIDIKAN	
			Selesai	Proses Penyidikan
1	2006	28	7	21
2	2007	31	-	31
3	2008	38	-	38
TOTAL			**7**	**90**

Penyelidikan dan penyidikan atas komplain yang tidak tuntas tersebut dikarenakan berbagai faktor seperti faktor keterbatasan sumber daya manusia yang dimiliki aparat penegak hukum, faktor biaya, sarana atau fasilitas, sulitnya menghadirkan korban juga dikarekan faktor prinsip kedaulatan wilayah dan kedaulatan hukum masing-masing Negara. Menurut Masaki

[225] Sumber dari situs Interpol Indonesia http://www.interpol.go.id di akses pada tanggal 28 September 2008.

Hamano sebagaimana dikutip oleh Barda Nawawi Arief Ada tiga lingkup yurisdiksi di ruang maya (*cyberspace*), yang dimiliki suatu negara berkenaan dengan penetapan dan pelaksanaan pengawasan terhadap setiap peristiwa, setiap orang dan setiap benda. Ketiga katagori yurisdiksi tersebut, yaitu:[226]

4. Yurisdiksi Legislatif (*legislatif jurisdiction atau jurisdiction to prescribe*);
5. Yurisdiksi Yudisial (*judicial jurisdiction atau jurisdiction to adjudicate*);dan
6. Yurisdiksi Eksekutif (*executive jurisdiction atau jurisdiction to enforce*).

Berdasarkan ketiga katagori yurisdiksi menurut Masaki Hamano di atas perbuatan yang dapat menimbulkan masalah dalam UU ITE ketika warga negara Indonesia melakukan tindak pidana diluar Indonesia (asas personal/nasional aktif) tanpa akibatnya dirasakan di Indonesia. Hal tersebut sangat terkait dengan masalah yurisdiksi judisial (kewenangan mengadili atau menerapkan hukum) dan yurisdiksi eksekutif (kewenangan melaksanakan putusan) karena masalah yurisdiksi judisial/adjudikasi dan yurisdiksi eksekutif sangat terkait dengan kedaulatan wilayah dan kedaulatan hukum masing-masing Negara, karena konstitusi suatu negara tidak dapat dipaksakan kepada negara lain karena dapat bertentangan dengan kedaulatan dan konstitusi negara lain, oleh karena itu hanya berlaku di negara yang bersangkutan saja, sehingga dibutuhkan kesepakatan Internasional dan kerjasama dengan negara-negara lain dalam menanggulangi tindak pidana teknologi informasi.

C. KEBIJAKAN FORMULASI DAN KEBIJAKAN APLIKATIF HUKUM PIDANA DALAM PENANGGULANGAN TINDAK PIDANA TEKNOLOGI INFORMASI DI MASA YANG AKAN DATANG

[226] Masaki Hamano,"*Comparative Study in the Approach to Jurisdiction in Cyberspace" Chapter: The Principle of Jurisdiction*,hal.1. lihat dalam Barda Nawawi Arief, *Tindak Pidana Mayantara, Op.Cit.*,hal.27-28.

Menjawab tuntutan dan tantangan komunikasi global lewat Internet, Undang-Undang yang diharapkan (*ius constituendum*) adalah perangkat hukum yang akomodatif terhadap perkembangan serta antisipatif terhadap permasalahan, termasuk dampak negatif penyalahgunaan internet dengan berbagai motivasi yang dapat menimbulkan korban-korban seperti kerugian materi dan non-materi.

Penanggulangan terhadap tindak pidana teknologi informasi perlu diimbangi dengan pembenahan dan pembangunan sistem hukum pidana secara menyeluruh, yakni meliputi pembangunan kultur, struktur dan subtansi hukum pidana. Dalam hal ini kebijakan hukum pidana menduduki posisi yang strategis dalam pengembangan hukum pidana modern.

Barda Nawawi Arief menyatakan bahwa upaya melakukan pembaharuan hukum pidana pada hakikat nya termasuk bidang " *penal policy*" yang merupakan bagian dan terkait dengan "*Law enforcement policy*" , "*Criminal policy*" dan " *Sosial Policy*". Ini berarti pembaharuan hukum pidana pada hakikatnya :

a. Merupakan bagian dari kebijakan (upaya rasional) untuk memperbaharui substansi hukum (legal substansi) dalam rangka lebih mengefektifkan penegakan hukum ;
b. Merupakan bagian dari kebijakan (upaya rasional) untuk memberantas/menanggulangi kejahatan dalam rangka perlindungan masyarakat ;
c. Merupakan bagian dari kebijakan (upaya rasional) untuk mengatasi masalah sosial dan masalah kemanusiaan dalam rangka mencapai/menunjang tujuan nasional (yaitu "*Social defennce*" dan "*social welfare*") ;
d. Merupakan upaya peninjauan dan penilaian kembali ("reorientasi dan re - evaluasi") pokok-pokok pemikiran, ide-ide dasar atau nilai sosio-filosofik, sosio-politik dan sosio kultural yang melandasi kebijakan kriminal dan kebijakan (penegakan) hukum

pidana selama ini. Bukanlah pembaharuan (*reformasi*) hukum pidana, apabila orientasi nilai dari hukum pidana yang dicita-citakan sama saja dengan orientasi nilai dari hukum pidana lama warisan penjajah (KUHP lama atau WvS). [227]

Pengertian kebijakan atau politik hukum pidana *(penal policy/Strafrechtspolitiek)* menurut A.Mulder adalah kebijakan untuk menentukan :[228]

1. Seberapa jauh ketentuan-ketentuan pidana yang berlaku perlu diubah atau diperbaharui
   (*in welk opzicht de bestaande straf bepalingen herzien dienen te worden*);
2. Apa yang dapat diperbuat untuk mencegah terjadinya tindak pidana
   (*wat gedaan kan worden om strafrechtelijk gedrad verkomen*);
3. Cara bagaimana penyidikan, penuntutan, peradilan dan pelaksanaan pidana harus dilaksanakan
   (*hoe de opsporing, vervolging, berechting en tenuitvoerlegging van straffen dient te verloppen*).

Bertolak dari kebijakan tersebut di atas, usaha dan kebijakan untuk membuat peraturan hukum pidana yang pada pada hakikatnya tidak dapat dilepaskan dari tujuan penanggulangan kejahatan. Dengan demikian penentuan kebijakan hukum pidana menanggulangi *cybercrime* harus dilakukan dengan pendekatan kebijakan dan di dalam setiap kebijakan (*policy*) terkandung pula pertimbangan nilai. Oleh karena itu, pembaharuan hukum pidana dalam penanggulangan tindak pidana teknologi informasi harus pula berorientasi pada pendekatan nilai.

C.1 Kebijakan Formulasi Tindak Pidana

---

[227] Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana*, *Op.Cit*.hal.28.
[228] Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana*, *Op.Cit.* ,hal.25-26

Hukum pidana merupakan salah satu sarana kebijakan kriminal untuk menanggulangi *cybercrime* . Dalam kebijakan hukum pidana maka akan bersentuhan dengan persoalan kriminalisasi (*criminalization*) baik itu perbuatan yang melawan hukum (*actus reus*), pertanggungjawaban pidana (*mens rea*), maupun sanksi yang dijatuhkan berupa pidana (*punishment*) maupun tindakan (*treatment*)

C.1.1 Kebijakan Kriminalisasi

Kriminalisasi harus memenuhi pelbagai syarat antara lain bahwa perbuatan tersebut benar-benar menampakkan korban (*victimizing*) baik aktual maupun pontensial, kemudian konsistensi penerapan asas *ultimum remedium*, dukungan publik yang kuat, bersifat komprehensif dan tidak bersifat *ad-hoc*.[229]

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 merupakan bagian dari 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.[230]

Sebagaimana ditulis oleh Barda Nawawi Arief, [231] kebijakan formulasi merupakan tahapan yang paling strategis dari "*penal policy*" . Pada tahap formulasi inilah disusun semua perencanaan penanggulangan kejahatan dengan sistem hukum pidana, yang mencakup tiga masalah pokok yaitu masalah perumusan tindak pidana (kriminalisasi), pertanggung jawaban

---

[229] Muladi, *Kebijakan Kriminal terhadap Cybercrime* , Majalah Media Hukum Volume I No.3 tanggal 23 Agustus 2003,hal.2.

[230] Barda Nawawi Arief, *Pembaharuan Hukum Pidana Dalam Perspektif Kajian Perbandingan*, Loc.Cit., hal. 126. Lihat juga dalam Barda Nawawi Arief, *Tindak Pidana Mayantara, Perkembangan Kajian Cybercrime di Indonesia*, RajaGrafindo Persada, Jakarta, 2006, hal. 90. Lihat juga pengertian kriminalisasi dari Sudarto, *Hukum dan Hukum Pidana*, Loc.Cit., hal. 32 dan 151

[231] Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*, *Op.Cit* , hal.78-79 dan 215.

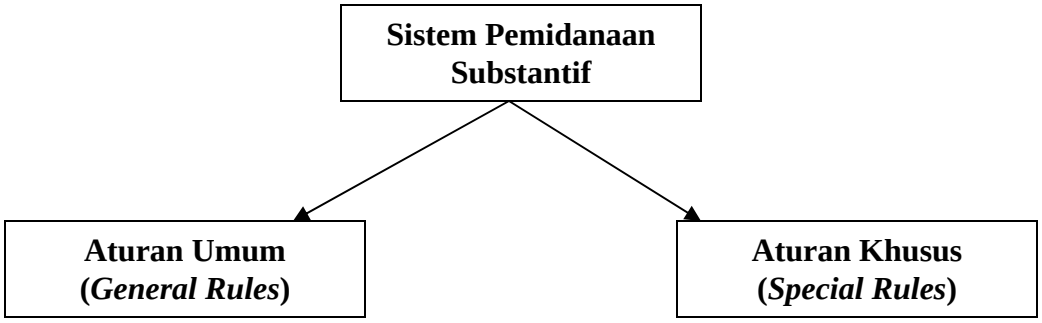
pidana, dan aturan pidana dan pemidanaan. Oleh karena itu upaya penanggulangan kejahatan bukan hanya tugas aparat penegak hukum tetapi juga tugas aparat pembuat undang-undang (aparat legislatif).

Kebijakan formulasi tindak pidana teknologi informasi (UU ITE) harus memperhatikan harmonisasi internal dengan sistem hukum pidana atau aturan pemidanaan umum yang berlaku saat ini. Tidaklah dapat dikatakan harmonisasi/sinkronisasi apabila kebijakan formulasi berada diluar sistem. Oleh karena itu kebijakan formulasi hukum pidana tindak pidana teknologi informasi harus berada dalam sistem hukum pidana yang berlaku saat ini.

Dengan pengertian demikian, maka keseluruhan peraturan perundang-undangan *(statutory rules)* yang ada di dalam KUHP maupun UU khusus di luar KUHP, pada hakikatnya merupakan satu kesatuan sistem pemidanaan, yang terdiri dari "aturan umum" *(general rules)* dan "aturan khusus" *(special rules).* Aturan umum terdapat di dalam Buku I KUHP, dan aturan khusus terdapat di dalam Buku II dan III KUHP maupun dalam UU Khusus di luar KUHP. Dengan demikian, sistem hukum pidana substantif (sistem pemidanaan substantif) secara sederhana dapat digambarkan sebagai berikut:

Gambar.2

Sistem Hukum Pidana Substantif



Bertolak dari gambar di atas dalam upaya penanggulangan tindak pidana teknologi informasi di masa yang akan datang serta agar perumusan delik dalam UU ITE dapat

operasional, seyogianya formulasi kebijakan kriminalisasi UU Teknologi Informasi sebagai berikut.

a) 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. Oleh karena itu, setiap tindak pidana yang dirumuskan dalam UU ITE harus disebut kualifikasi juridisnya. Apabila tidak disebutkan, akan menimbulkan masalah juridis dalam menerapkan aturan umum KUHP terhadap UU ITE.

b) Dalam upaya penanggulangan tindak pidana teknologi informasi seyogianya diperluas bentuk-bentuk tindak pidana berupa “permufakatan jahat”, “persiapan”, ”pembantuan” dan “pengulangan” *(recidive).*[232] *Council of Europe* dalam *Title.*5 *Ancillary liability and sanction* , telah merekomendasikan agar dalam ketentuan hukum pidana substantif memuat terhadap percobaan dan pembantuan (*Article* 11). Amandemen CMA 1998 Singapura Pasal 3 mengatur terhadap pengulangan untuk pelanggaran pertama kali dan dua kali lipat untuk pelanggaran kedua atau penghukuman berulang-ulang; ada juga waktu hukuman penjara baru untuk tindak pidana yang berulang-ulang yaitu penjara selama 3 tahun. Begitu juga ketentuan Pasal 5 ayat 1 telah ditingkatkan menjadi denda 10.000 dollar dan/atau 3 tahun penjara untuk pelanggaran pertama kali, dan penghukuman kedua kali atau berulang ditambah 20.000 dolar atau penjara 5 tahun.

[232] Apabila UU ITE memperluas bentuk-bentuk tindak pidana tersebut hendaknya harus mem-buat aturan khusus/tersendiri mengenai hal itu. Karena KUHP KUHP tidak membuat aturan umum untuk bentuk-bentuk tindak pidana (“*forms of criminal offence*”) yang berupa “permufakatan jahat”, “persiapan”, dan “pengulangan” (recidive).Apabila tidak, akan dapat menimbulkan masalah juridis.

Barda Nawawi Arief menyatakan ada dua masalah sentral dalam kebijakan kriminal dengan menggunakan sarana penal (hukum pidana). Masalah yang harus diperhatikan dalam penganalisasian hukum pidana itu adalah: [233]

1. Perbuatan apa yang seharusnya dijadikan tindak pidana;
2. Sanksi apa yang sebaiknya digunakan atau dikenakan kepada si pelanggar.

Kebijakan kriminalisasi adalah kebijakan menetapkan/merumuskan/ memformulasikan perbuatan apa yang dapat dipidana dan selanjutnya diberikan sanksi pidana yang dapat dikenakan kepada si pelanggar. Perbuatan pidana adalah perbuatan yang bertentangan dengan tata tertib atau ketertiban yang dikehendaki hukum.

Gambaran umum perbuatan pidana adalah suatu perbuatan manusia yang memenuhi rumusan delik, melawan hukum dan membuat bersalah pelaku perbuatan tersebut. Asas legalitas mewajibkan kepada pembuat undang-undang untuk menentukan terlebih dahulu apa yang dimaksud dengan tindak pidana, harus dirumuskan lebih jelas. Rumusan tersebut mempunyai peranan dalam menentukan apa yang dilarang atau apa yang harus dilakukan seseorang.[234]

Tentang penentuan perbuatan mana yang dipandang sebagai perbuatan pidana, kita menganut asas yang dinamakan asas legalitas (*principle of legality*), yakni suatu perbuatan hanya merupakan tindak pidana, jika ditentukan terlebih dahulu dalam suatu ketentuan perundang-undangan (pasal 1 ayat 1 KUHP). Dalam bahasa latin, ada pepatah yang maknanya sama dan berbunyi : *Nullum delictum nulla poena sine preavia legi poenali* (tiada kejahatan, tiada hukuman pidana tanpa undang-undang hukum pidana terlebih dahulu).[235]

---

[233] Barda Nawawi Arief ,*Bunga Rampai Kebijakan Hukum Pidana*, *Op.Cit*.hal.29.

[234] Komariah Emong Supardjaja, *Ajaran Sifat Melawan Hukum Materiel dalam Hukum Pidana Indonesia,* Alumni, Bandung, 2002, hal.22-23.

[235] Wirjono Prodjodikoro, *Asas-asas Hukum Pidana di Indonesia*, Refika Aditama, Bandung, ,2003,hal. 42

Barangsiapa yang melakukan perbuatan pidana diancam dengan pidana tertentu yang telah ditentukan dalam ketentuan perundang-undangan. Akan tetapi, dalam memidana seseorang yang telah disangka melakukan perbuatan pidana tersebut, dikenal asas yang berbunyi : "*Tidak dipidana tanpa kesalahan*"(Bahasa Belanda : "*Geen straf zonder schuld*"). Penentuan mengenai dengan cara bagaimana pengenaan pidana itu dapat dilaksanakan apabila ada orang yang disangka melakukan perbuatan pidana diatur didalam hukum pidana formal atau Hukum Acara Pidana. "Van Bemmelen mengatakan : Ilmu Hukum Acara Pidana mempelajari peraturan-peraturan yang diciptakan oleh negara, karena adanya dugaan terjadi pelanggaran undang-undang pidana".[236]

Dalam merumuskan perbuatan pidana dapat ditempuh dengan berbagai cara, antara lain menyebutkan unsur-unsurnya saja, atau menyebutkan unsur dan kualifikasinya saja. Sesuai dengan prinsip subsidaritas maka dalam menentukan perbutan pidana, harus selektif dalam memproses perkara dan selektif pula dalam memilih ancaman pidana.

Pendapat Mudzakir sebagaimana dikutip oleh Teguh Prasetyo, yang terpenting dalam merumuskan suatu perbuatan adalah :[237]

1. Ditentukan rumusan perbuatan pidana (satu pasal) yang mengatur mengenai aspek tertentu yang hendak dilindungi oleh hukum pidana dalam bab tertentu dengan menyebutkan unsur-unsur dan kualifikasinya. Rumusan perbuatan pidana ini menjadi dasar atau patokan yang berfungsi sebagai pedoman perumusan pasal-pasal lain dalam bab tersebut. Delik genus tersebut menjadi standar (dalam keadaaan normal) dalam pengancaman pidana.

[236] Mohammad Taufik Makarao, Suhasril, *Hukum Acara Pidana dalam Teori dan Praktek*, Penerbit Ghalia Indonesia, Jakarta, 2004,hal.2.

[237] Teguh Prasetyo dan Abdul Halim Barkatullah, *Politik Hukum Pidana: Kajian Kebijakan Kriminalisasi dan Dekriminalisasi*, *Op.Cit.*,hal.45.

2. Delik genus tersebut menjadi pedoman dalam membuat perumusan perbuatan lainnya yang bersifat memberatkan atau meringankan ancaman pidana cukup dengan kualifikasinya saja tanpa mengulangi penyebutan unsur-unsurnya.

Cara perumusan demikian akan memudahkan pemahaman masyarakat terhadap peraturan hukum pidana atau perbuatan yang dilarang. Sedangkan faktor-faktor yang dapat dijadikan pertimbangan-pertimbangan memberatkan dan meringankan ancaman pidana dari delik genus antara lain:[238]

a) Sikap batin pelaku (kesengajaan atau kealpaan);
b) Faktor akibat dari perbuatan pelaku terhadap masyarakat dan korban;
c) Objek/sasaran dilindungi oleh hukum;
d) Nilai yang hendak ditegakkan oleh hukum;
e) Alat yang dipakai untuk melakukan kejahatan;
f) Cara melakukan kejahatan;
g) Situasi dan kondisi pada saat perbuatan dilakukan.

Persoalan kriminalisasi timbul karena dihadapan kita terdapat perbuatan yang berdimensi baru, sehingga muncul pertanyaan adakah hukumnya untuk perbuatan tersebut. Kesan yang muncul kemudian adalah terjadinya kekosongan hukum yang akhirnya mendorong kriminalisasi terhadap perbuatan tersebut.[239] Adapun sumber bahan dalam kebijakan melakukan perubahan dan penyusunan delik-delik baru diambil antara lain dari:[240]

1. masukan berbagai pertemuan ilmiah (simposium/seminar/lokakarya) yang berarti juga dari berbagai kalangan masyarakat luas;

---

[238] Teguh Prasetyo dan Abdul Halim Barkatullah, *Politik Hukum Pidana: Kajian Kebijakan Kriminalisasi dan Dekriminalisasi*, *Op.Cit*.,hal.45.

[239] Tb. Ronny R. Nitibaskara, *Problem Yuridis Cybercrime* , Makalah pada Seminar tentang Cyber Law, diselenggarakan oleh Yayasan Cipta Bangsa, Bandung, 29 Juli 2000, hal. 2 dan 5.

[240] Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana*, *Op.Cit*.hal.245

2. masukan dari beberapa hasil penelitian dan pengkajian mengenai perkembangan delik-delik khusus dalam masyarakat dan perkembangan iptek;
3. masukan dari pengkajian dan pengamatan bentuk-bentuk serta dimensi baru kejahatan dalam pertemuan-pertemuan/kongres internasional;
4. masukan dari berbagai konvensi internasional (baik yang telah diratifikasi maupun yang belum diratifikasi);
5. masukan dari hasil pengkajian perbandingan berbagai KUHP asing.

Kriminalisasi di dunia maya dengan pengaturan khusus diluar KUHP 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 (*over-criminalization*), yang justru mengurangi wibawa hukum. Kajian yang bersifat yuridis komparatif sangat berperan dalam melakukan kebijakan penanggulangan tindak pidana teknologi informasi di masa yang akan datang.

Perkembangan kejahatan teknologi informasi mengakibatkan setiap negara memiliki kebijakan kriminalisasi yang berbeda-beda. Sifatnya yang lintas negara telah menjadikan kejahatan di internet tidak saja merupakan persoalan nasional, namun sudah menjadi persoalan Internasional. Hal ini terlihat dari rekomendasi yang dikeluarkan oleh PBB melalui kongresnya atau juga *Council of Europe*.

Penanggulangan tindak pidana teknologi informasi menjadi persoalan negara-negara di dunia. Pengaturannya juga berbeda-beda di setiap negara. Oleh karena itu dibutuhkan kajian perbandingan hukum (yuridis komparatif) untuk mengetahui bagaimana baiknya pengaturan hukum ke depan dalam masalah tindak pidana teknologi informasi terutama berkaitan dengan kriminalisasi dan model pengaturannya.

A. Amerika Serikat

Meluasnya penggunaan internet yang tak tertandingi di Amerika Serikat telah memunculkan, dan terus menyebabkan berbagai kajian, kebijakan, usulan dan draft perundang-undangan yang mengatur terhadap penyalah gunaan penggunaan teknologi informasi. Amerika Serikat telah memberlakukan berbagai undang-undang yang melakukan kriminalisasi terhadap perbuatan yang berkaitan dengan tindak pidana teknologi informasi.

Pengaturan *cybercrime* di Amerika Serikat antara lain *Computer Fraud and Abuse Act* (*Title 18 Part I Chapter 47 Section 1030* dengan judul *"Fraud and related activity in connection with computers"*), dalam *United States Congress* 1986 yang bertujuan untuk menanggulangi *hacking* terhadap komputer. Pengaturan terhadap *Computer Fraud and Abuse Act* di amandemen pada tahun 1994, 1996 dan 2001. Bentuk-bentuk tindak pidana teknologi informasi yang diatur dalam ketentuan *Section* 1030 tersebut adalah sebagai berikut:[241]

"Whoever –

1. *having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it (authorization in order to obtain national security data) ;*
2. *intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains –*

[241] lihat http://blog.washingtonpost.com/securityfix/2008/07/senate_approves_bill_to_fight.html diakses pada tanggal 2 Oktober 2008.

a. *information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602 (n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);*
b. *information from any department or agency of the United States; or*
c. *information from any protected computer if the conduct involved an interstate or foreign communication;*

3. *intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;*
4. *knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;*
5. a. *knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;*
   b. *intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or*
   c. *intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage;*
6. *knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if –*
   a. *such trafficking affects interstate or foreign commerce; or*
   b. *such computer is used by or for the Government of the United States; "or".*
7. *with intent to extort from any person, firm, association, educational institution, financial institution, government entity, or other legal entity, any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer;"*

Selain *Computer Fraud and Abuse Act* yang tercantum dalam *Title 18 Part I Chapter 47 Section 1030 , United States Congress* juga mengatur tindak pidana teknologi informasi yang kaitannya dengan internet, seperti:

1. *Access Device Fraud Act of 1984 (18 USC Section 1029);*
2. *Wire Fraud Statute of 1952 (18 USC Section 1343);*
3. *Criminal Infringement of a Copyright (the Copyright Act of 1976) (18 USC Section 506 (a));*
4. *Counterfeit Trademarks (the Trademark Counterfeit Act of 1984) (USC Section 2320);*

5. *Mail Fraud (18 USC Section 1341);*
6. *Conspiracy to Defraud the US Government (18 USC 371);*
7. *False Statements (18 USC Section 1001);*
8. *Identity Theft and Assumption Deterrence Act of 1998 (18 USC Section 1028);*
9. *The Racketeer Influenced and Corrupt Organizations Act (RICO) (18 USC Section 2511);*
10. *Wire and Electronic Communications Interception of Oral Communications (18 USC Section 2511);*
11. *Unlawful Access to Stored Communications (18 USC 2701);*
12. *Transportation of Stolen Goods, Securities, Moneys (18 USC Section 2314);*
13. *Trafficking in Counterfeit Goods and Services (18 USC Section 2320);*
14. *Extortion and Threats (18 USC Section 875).*

Amerika Serikat sudah mengatur Mengenai perjudian melalui internet, melalui Pemerintah Federal yang menerapkan *The Wire Act*, *The Travel Act*, *The Professional and Amateur Sports Protection Act* dan *the Interstate Transportation of Wagering Paraphernalia Act***,** Perhatian juga banyak ditujukan pada persoalan perbuatan cabul (*obscenity*) dan *adult entertainment and cyberporn*, khususnya pornografi anak. Dalam hal ini bisa disebutkan adanya ketentuan tentang *Federal Obscenity Law*, berupa **"***Transportation of Obscene Matters for Sale or Distribution"* (18 USC Section 1465) dan **"***Communications Decency Act of 1996"*.

Undang-Undang di Amerika Serikat yang mengatur kriminalisasi perbuatan yang berhubungan dengan teknologi informasi selain yang tercantum *United States Congress* juga tercantum dalam beberapa peraturan khusus antara lain:

a. Undang-Undang Pelarangan Pencurian Elektronis 1997

   Diperkenalkan untuk menutup celah dalam undang-undang hak cipta AS sebelumnya yang tidak mengakui adanya pelanggaran hak cipta bila si terdakwa tidak memperoleh keuntungan.

b. *National Stolen Property Act* 1934 (Undang-Undang barang curian nasional 1934) dan *Economic Espionage Act* 1996 (Undang-Undang Spionase Ekonomi 1996) melarang penyalahgunaan rahasia perdagangan.

c. *Identity Theft and Assumption Deterrence Act of* 1998 (Undang-Undang Pencurian Identitas dan Pengingkaran Asumsi 1998)

Dimaksudkan untuk menciptakan serangan baru bagi siapa pun yang mentransfer atau menggunakan, tanpa izin, sarana identifikasi orang lain dengan maksud untuk melakukan atau membantu, persekongkolan, dalam segala aktivitas yang melanggar hukum. Pelanggaran itu mencakup penggunaan data biometrik unik dan sarana identifikasi elektronis.

B. Singapura

Di Singapura, terdapat perkembangan yang menarik terhadap kebijakan penanggulangan kejahatan teknologi informasi. Atas dasar *The Computer Misuse Act (CMA)* 1993. Undang-Undang penyalahgunaan Komputer (*Computer Misuse Act*,CMA) Singapura tahun 1993 dimodelkan berdasarkan undang-undang Inggris tahun 1990, yang menggatur terhadap 4 (empat) hal yaitu:

a. Akses tidak sah;

Pasal 3 UU CMA yang berisikan melarang '*hacking*' yang menyebabkan sebuah komputer memainkan fungsinya untuk tujuan mengamankan akses tanpa ijin pada program atau data apapun yang tersimpan pada komputer.
Pasal 3 ayat 1 sasarannya hanya pada akses yang tidak sah.
Pasal 3 ayat 2 akses apa saja yang mengakibatkan kerugian yang melebihi nilai 10.000 dolar akan dikenai hukuman berat.

b. Akses dengan maksud tersembunyi;

Pasal 4 UU CMA mempidanakan akses yang tidak sah dimana terdapat tujuan untuk melakukan atau memfasilitasi perbuatan pelanggaran yang melibatkan properti, penipuan, tindakan tidak jujur, atau perbuatan yang mengakibatkan luka badan.

c. Modifikasi isi komputer ;dan

Pasal 5 UU CMA berkaitan dengan modifikasi isi komputer yang tidak sah dan disengaja seperti data, program perangkat lunak komputer dan *database* contohnya dengan memasukkan virus ke dalam sistem komputer.

d. Mencegat suatu layanan komputer.

   Pasal 6 UU CMA memperkenalkan suatu konsep baru tentang penggunaan atau pencegatan layanan komputer tanpa ijin, hal ini mungkin lebih menyerupai pencurian layanan atau waktu penggunaan komputer.

Pada tahun 1998 CMA mengalami amandemen, yang melalui pemberatan pidana dan penciptaan tindak pidana baru berusaha untuk memperkuat perlindungan terhadap sistem komputer yang diatur CMA 1993. Perkembangan bentuk-bentuk baru dari penyalahgunaan jaringan internet mengakibatkan Undang-Undang CMA memerlukan perluasan cakupan sehingga pada tanggal 24 Juli 1998 disahkannya Amandemen Undang-Undang Penyalahgunaan Komputer.

Amandemen CMA 1998 yang bertujuan memperkuat tingkatan dan sifat perlindungan sistem komputer yang telah ditetapkan oleh undang-undang sebelumnya. Amandemen memperbaharui CMA dengan 5 (lima) cara yaitu:

a. Mengajukan definisi tentang kerusakan sebagai perusakan pada sebuah komputer atau integritas atau ketersediaan data, program atau sistem atau informasi. Amandemen menghubungkan tindak pidana dengan tingkat kerusakan yang disebabkannya, sehingga membantu tujuan keseluruhan untuk menghukum pelanggar yang sepadan dengan kerusakan yang mereka timbulkan atau ancaman yang diberikan.
b. Hukuman terhadap berbagai jenis pelanggaran telah ditingkatkan dan berlaku bagi semua orang. Dengan demikian, denda untuk pelanggaran awal menurut Pasal 3 sekarang berlaku maksimal 5.000 dolar untuk pelanggaran pertama kali dan dua kali lipat untuk pelanggaran kedua atau penghukuman berulang-ulang; ada juga waktu hukuman penjara baru untuk tindak pidana yang berulang-ulang yaitu penjara selama 3 tahun. Begitu juga ketentuan Pasal 5 ayat 1 telah ditingkatkan menjadi denda

10.000 dollar dan/atau 3 tahun penjara untuk pelanggaran pertama kali, dan penghukuman kedua kali atau berulang ditambah 20.000 dolar atau penjara 5 tahun.

c. Pengaturan terhadap pelanggaran dengan maksud tersembunyi menurut Pasal 4 dan pencantumannya, berdasarkan Sub Pasal 4(a) yang baru mengenai acuan bagi seseorang yang mempunyai kewenangan mengakses komputer tetapi melebihkan kewenangannya tersebut untuk melakukan pelanggaran yang sama. Selain itu, hukuman maksimal untuk semua pelanggaran tersembunyi dan hukuman minimal bagi pelanggaran yang melibatkan properti, penipuan, ketidakjujuran dan luka badan tetap tidak berubah, meskipun ada reorganisasi keseluruhan pasal.

Kriminalisasi terhadap perbuatan yang baru tertulis dalam *Part II Offences art 3* sampai dengan *art* 10 *The Computer Misuse Act* 1998 Singapura, yang intinya sebagai berikut:[242]

1. *Unauthorised access to computer material (Art.3)*

   Dengan maksud untuk melakukan atau memudahkan pelaksanaan suatu kejahatan yang berkaitan dengan harta kekayaan, penipuan, ketidakjujuran atau perbuatan yang mengakibatkan kerugian/kerusakan jasmaniah. Perubahan dari Pasal 3 ini adalah tidak hanya membatasi perbutan yang menyebabkan kerugian lebih dari 10.000 dolar tetapi terhadap semua perbuatan yang menyebabkan kerugian apapun;

2. *Access with intent to commit or facilitate commission of offence (Art.4)*

   Mengakibatkan suatu komputer menghasilkan suatu fungsi dengan maksud untuk menjamin akses tanpa hak terhadap suatu program atau data yang disimpan oleh di suatu komputer. Perubahan Pasal 4 yaitu mengenai acuan bagi seseorang yang mempunyai kewenangan mengakses komputer tetapi melebihi kewenangannya tersebut dikategorikan telah melakukan tindak pidana;

3. *Unauthorised modification of computer material (Art.5)*

   Modifikasi secara sengaja dan tidak sah muatan/kandungan/isi suatu komputer (data, program perangkat lunak komputer, dan *databases* dengan cara memasukkan virus ke dalam sistem komputer;

[242] *Computer Misuse Act of* Singapore 1998.

4. *Unauthorised use or interception of computer service (Art.6)*

   Membuka/mengungkap *password*, kode akses atau dengan cara lain memperoleh akses terhadap program atau data yang disimpan di suatu komputer. Dalam hal ini pemikiran sampai pada "*confidentiality law*";

5. *Unauthorised obstruction of use of computer (Art.7)*

   Menggunakan atau memintas *(intercepting)* suatu pelayanan komputer tanpa hak; ini semacam mencuri pelayanan komputer atau waktu *(thieft of a computer service or time)*;

6. *Unauthorised disclosure of access code (Art.8)*

   Mengganggu atau menggunakan komputer atau secara tidak sah mangungkap *access codes* atau dengan sarana lain guna memperoleh keuntungan atau tujuan yang tidak sah;

7. *Enhanced punishment for offences involving protected computers (Art.9)*

   Tindak pidana yang melanggar **"***protected computers*" untuk kepentingan pertahanan, keamanan, hubungan internasional, eksistensi dan identitas rahasia tentang sumber informasi dalam rangka penegakan hukum pidana, pengaturan tentang infrastruktur komunikasi, perbankan dan pelayanan keuangan dan keamanan publik.
8. *Abetments and attempts punishable as offences (Art.10)*

   Membantu atau mencoba melakukan perbuatan sebagaimana tertulis di atas;

C. Belanda

Negara Belanda membentuk suatu komisi yang disebut komisi Franken yang bertugas memberi masukan mengenai pengaturan kejahatan mayantara. Komisi tersebut menganggap kejahatan mayantara sebagai kejahatan biasa (*ordinary crime*) yang dilakukan dengan komputer teknologi tinggi (*high-tech*) sehingga hanya menyempurnakan *Wetboek van Strafrecht* (KUHP Belanda) pada tahun 1993 agar dapat dipergunakan untuk menanggulangi tindak pidana mayantara (tentu dengan penambahan) dengan memasukkan pada ketentuan pidana tertentu.

Commissie Franken merumuskan beberapa tindak pidana mayantara dalam perumusan *Wetboek van Strafrecht*, rumusan sembilan bentuk penyalahgunaan (*misbruikvormen*) tersebut adalah :

1. tanpa hak memasuki sistem komputer ;

2. tanpa hak mengambil (*onderscheppen*) data komputer ;

3. tanpa hak mengetahui (*kennisnemen*) ;

4. tanpa hak menyalin/mengkopi ;

5. tanpa hak mengubah ;

6. mengambil data ;

7. tanpa hak mempergunakan peralatan ;

8. sabotase sistem komputer;

9. mengganggu telekomunikasi

D. Australia

Australia telah mengamandemen perundang-undangannya pada tahun 2001 untuk menanggulangi *cybercrime*, amandemen tersebut adalah *Cybercrime Act* 2001, *an act to amend the law relating to computer offences, and for other puposes.* Turut pula di amandemen peraturan dan organisasi yang berkaitan dengan kejahatan komputer atau *cybercrime* seperti amandemen terhadap Australia *Security Intelligence Organization Act* 1979. The Telecomunications Act 1997. Dalam undang-undang ini diberikan definisi-definisi yang berkaitan dengan kegiatan di internet dan juga berbagai istilah dalam komputer.

Undang-undang ini membedakan secara garis besar dua bentuk kejahatan komputer yaitu *serious computer offences* dan bentuk lain kejahatan komputer. *Serious computer offences* diatur pada Division 477 dam terbagi lagi dalam 3 (tiga) bentuk. Berikut diuraikan kejahatan dimaksud:

- *Division 477 -- Serious computer offences*

477.1 Unauthorised access, modification or impairment with intent to commit a serious offence Intention to commit a serious Commonwealth, State or Territory offence

477.2 Unauthorised modification of data to cause impairment

477.3 Unauthorised impairment of electronic communication

- *Division 478 -- Other computer offences*

478.1 Unauthorised access to, or modification of, restricted data

478.2 Unauthorised impairment of data held on a computer disk etc

478.3 Possession or control of data with intent to commit a computer offence

478.4 Producing, supplying or obtaining data with intent to commit a computer offence

Pengaturan terhadap perlindungan komputer dari *spamming* juga di atur adalam *section* 76 E *Crimes Code* 1995 Australia yang berisikan:" *an offence intentionally and without authority interfere with, interrupt or obstruct the lawful use of a computer or to impair the usefulness or effectiveness of data stored in a computer by means of a carrier, such as email. This case related to the relay of a spam through a third party computer system" The maximum penalty is 10 years imprisonment.*

E. Cina

Perlindungan terhadap komputer di Cina dikeluarkan pada tanggal 18 Januari 1994 *Decree No. 147 of the State Council of the Peoples Republic of China* menyatakan tujuan dari pengawasan jaringan oleh Kementrian Keamanan Publik adalah perlindungan pada area-area tertentu semisal urusan nasional,ekonomi, pengembangan pertahanan serta teknologi dan ilmu pengetahuan yang maju. Pengaturan terhadap *cybercrime* dinyatakan dalam *System: Chapter 4 - Legal Responsibilities.*

Article 23 - The public security organisations shall give warnings or may impose maximum fines of 5.000 Yuan on individuals and 15.000 Yuan on organisations in cases

when they deliberately input a computer virus or other harmful data endangering a computer information system, or in a case when they sell special safety protection products for computer information systems without permission. Their illegal income will be confiscated and a fine shall be imposed in the amount of one to three times as much as the illegal income (if any).

Cina telah mengamandemen Hukum Pidana pada tanggal 11 Desember 1997 dengan memasukkan ketentuan baru terhadap kejahatan komputer. UU Pidana ini memberikan sanksi terhadap *hacking* ke dalam sistem komputer pada Bab 285 sampai 287. Bab 285 berisikan memberikan daftar *database* yang dimiliki agen pemerintah dan agen-agen lain, akan mengarahkan pada hukuman penjara tanpa memperhatikan ada atau tidaknya kerusakan apa pun yang diakibatkan dari tindakan tersebut.

Kebijakan terhadap penggunaan internet di Cina membuat siapa pun yang menempatkan materi di internet menjadi subjek regulasi, hal ini akan menakutkan bagi siapapun yang mengirim pesan serta menukar informasi melalui email atau informasi yang berbasis web.

Memasukkan kejahatan komputer ke dalam Amandemen Hukum Pidana di Cina diikuti dengan Ketetapan Perlindungan Keamanan Jaringan Komputer Domestik yang berhubungan dengan Internet (*Circular of the Public Security Bureau*) pada tanggal 30 Desember 1997. Ketetapan tersebut melarang materi-materi yang memunculkan praktik-praktik kecurangan, pornografi, perjudian, kekejaman juga kejahatan lainnya dan pencemaran nama baik melalui internet.

F. Myanmar

Myanmar membuat kebijakan terhadap teknologi informasi sejak 20 September 1996 tentang Pengembangan Ilmu Komputer (*Computer Development Law*), yang mensyaratkan bahwa pengguna-pengguna komputer dalam mengimpor,memiliki atau menggunakan komputer harus memiliki ijin dari Kementrian Komunikasi, Pos dan *Telegraf*. Hukum ini secara khusus

ditujukan pada komputer-komputer yang melakukan pengiriman dan penerimaan data (yang memanfaatkan jaringan internet).

Pasal 34 UU tersebut secara khusus memperlihatkan sanksi-sanksi yang diberikan kepada orang-orang yang melakukan suatu pekerjaan memiliki atau mengirimkan dan mendirstribusikan informasi apapun yang dianggap rahasia oleh negara yang menyalahi secara politis, hukum dan juga ketertiban ekonomi serta budaya nasional. Ancaman terhadap ketentuan pasal 34 ini adalah hukuman 7-15 tahun dan denda bagi mereka yang melanggar.

G. Filipina

Pada awalnya Filipina mengabaikan proteksi terhadap perkembangan teknologi dan informasi, tetapi perkembangan dengan adanya virus *"I Love You*" yang diakui dikeluarkan oleh mahasiswa di Filipina yang mengarah pada penyebarluasan kerusakan pada jaringan di seluruh dunia, yang tidak hanya menyita perhatian global tetapi juga mendesak dilakukannya tindakan darurat oleh seluruh negara.

Kasus virus *"I Love You*" mendorong pemerintah Filipina mengeluarkan kebijakan pada tanggal 12 Juni 2000 dengan mengesahkan *E-Commerce*. Undang-Undang tersebut sebagian berisikan pengakuan hukum dan keaslian pesan serta dokumen elektronik, kebanyakan sejalan dengan kecenderungan internasional.

Tindakan *hacking* dan *cracking* sudah dimuat dalam Bab 33 (1) UU tersebut, yang mengidentifikasikan *hacking* dan *cracking* yang mengacu pada akses tidak sah atau melakukan penyerobotan ke dalam sebuah *server*/sistem komputer atau ke sistem informasi dan komunikasi; atau akses apapun untuk mengurangi, mengubah, mencuri, atau merusak menggunakan sebuah komputer atau peralatan informasi dan komunikasi yang serupa, tanpa sepengetahuan dan izin dari pemilik komputer atau sistem informasi dan komunikasi, termasuk memasukkan virus

komputer dan sejenisnya, yang mengakibatkan pengurangan, pengerusakan, perubahan, pencurian atau penghilangan dokumen elektronik akan di ancam dengan hukuman tahanan dan denda.

H. Malaysia

Dalam penanggulangan tindak pidana teknologi informasi Malaysia memiliki 2 (dua) undang-undang yang berhubungan langsung, yaitu UU Kejahatan di Bidang Komputer tahun 1997 dan UU Komunikasi dan Multimedia 1998 (CMA).

1. UU Kejahatan di Bidang Komputer tahun 1997

Undang-undang ini sebagaimana negara yang memiliki sistem hukum *common law* mengikuti kepada hukum induknya yaitu Inggris, tetapi dengan berbagai tambahan sebagaimana yang dilakukan oleh Negara Singapura. *Computer Crime Act* 1997 (CCA) Negara Malaysia tersebut dibagi atas 3 (tiga) bagian yaitu:

I. *PART. I - PRELIMINARY*

Section 1. Short title and commencement.

Section 2. Interpretation.

II. *PART. II - OFFENCES*

Section 3. Unauthorized access to computer material.

Section 4. Unauthorized access with intent to commit or facilitate commission of further offence.

Section 5. Unauthorized modification of the contents of any computer.

Section 6. Wrongful communication.

Section 7. Abetments and attempts punishable as offences.

Section 8. Presumption.

III. *PART. III - ANCILLARY AND GENERAL PROVISIONS*

Section 9. Territorial scope of offences under this Act.

Section 10. Powers of search, seizure and arrest.

Section 11. Obstruction of search.

Section 12. Prosecution.

Kriminalisasi dalam CCA Malaysia terdapat dalam Part.II yang mengatur tentang beberapa hal yang berhubungan dengan perlindungan komputer, yaitu:

- Pasal 3 ayat 1 dan 2; Akses secara tidak sah pada komputer atau data yang disimpan dalam sebuah komputer dengan segala maksudnya. Unsur yang disebutkan terakhir ini ditetapkan tanpa pertimbangan apakah tindakan tersebut diarahkan pada program atau data tertentu manapun.
- Pasal 5 ayat 1 dan 2; Modifikasi isi dalam komputer manapun secara tidak sah, sekali lagi dengan tanpa mempertimbangkan apakah tindakan ini diarahkan pada suatu program atau data tertentu manapun: atau apakah modifikasi itu bersifat permanen atau temporer.
- Pasal 6 ayat 1 Komunikasi tidak sah, langsung atau tidak langsung dari sebuah nomer, kode, *password* atau cara akses lain ke sebuah komputer atau siapa pun.
- Pasal 7; Persekongkolan, perencanaan untuk melaksanakan atau melanjutkan apa saja dari hal-hal tersebut di atas.

2. Undang-Undang Komunikasi dan Multimedia 1998

Perluasan terhadap pelanggaran dan hukuman dalam pengamanan jaringan dan komunikasi terdapat dalam Pasal 231 sampai 241 undang-undang CMA di Malaysia, yaitu:

- Menurut Pasal 231 ayat 1, penggunaan perangkat atau peralatan apa pun dengan maksud mendapatkan informasi tanpa hak tentang isi,pengiriman atau alamatnya dari komunikasi apa pun;
- Pasal 232 ayat 2, kepemilikan atau pembuatan sebuah sistem untuk mendapatkan akses secara tidak sah pada fasilitas atau layanan jaringan;
- Pasal 234 ayat 1, penyadapan tidak sah dari komunikasi apa pun, dan pengungkapan atau penggunaan komunikasi yang diperoleh dengan cara demikian;
- Melakukan pengerusakan dengan jalan mengubah,memindah, menghancurkan,atau merusak fasilitas jaringan manapun, yang sesuai dengan Pasal 235. Pasal 236 ayat 1 Pembuatan, penerimaan atau penyediaan peralatan akses palsu atau perkakas pembuat peralatan; kepemilikan peralatan akses apa pun yang palsu atau tidak sah; atau mengubah alat itu untuk tujuan yang sama, termasuk perangkat keras atau perangkat lunak yang digunakan untuk tujuan modifikasi seperti itu.

Dengan mengundangkan 2 (dua) hukum terpisah yang bertujuan untuk mencegah penyalahgunaan komputer dan jaringan, badan pembuat undang-undang terlihat ada tumpang tindih diantara ke dua undang-undang tersebut. Baik Undang-Undang Kejahatan di bidang komputer maupun Undang-Undang Komunikasi dan Multimedia melindungi jaringan dari penyalahgunaan, sekalipun yang pertama disebut sebagai sekelompok komputer dan yang kedua yang bersifat langsung. Selain ke 2 (dua) undang-undang di atas Malaysia memiliki beberapa undang-undang khusus lainnya yang berhubungan dengan pemanfaatan teknologi informasi.

- *Copyright (Amendment) Bill 1997*

- *Digital Signature Act 1997*

- *Telemedicine Bill 1997*

- *Digital Signature Regulations 1998*

I. Kanada

Sebagai salah satu negara yang menandatangani konvensi cybercrime Kanada sampai dengan tanggal 25 Juli 2008 belum meratifikasi Draft konvensi tersebut. Tetapi dalam KUHP Kanada ada beberapa pasal yang berhubungan dengan penyalahgunaan komputer, yaitu:[243]

1. 342.01 (1) *Making, having or dealing in instruments for forging or falsifying credit cards.*
2. 342.1 (1) *Unauthorized use of computer*
3. 342.2(1) *Possession of device to obtain computer service*
4. 430(1.1) *Mischief in relation to data*
5. Bill C-27 *Proposes some changes to Canadian laws, in order to fight identity theft.*
6. Section 184 *deals with privacy.*
7. Section 403 *deals with pesonation.*

J. FBI dan National Collar Crime Center

FBI dan *National Collar Crime Center* menguraikan beberapa jenis *Cybercrime* berdasarkan issu yang menjadi bahan studi atau penyelidikan yang selama ini pernah mereka tangani dalam "*Crime on The Internet*", sebagai berikut: [244]

a. Computer network break-ins;
b. Industrial espionage;
c. Software piracy;
d. Child pornography;
e. E-mail bombings;
f. Password sniffers;
g. Spoofing;
h. Credit card fraud.

K. Menurut Rancangan Undang-Undang KUHP Buku II Tahun 2006[245]

---

[243] Di akses dari http://www.canlii.org/ca/sta/c-46/sec342.html pada tanggal 3 Oktober 2008.

[244] Jones International and Jones Digital Century, "*Crime on The Internet*", Jones Telecommunications & Multimedia Encyclopedia, Natalie D Voss, Copyright © 1994-99 hal. 1-2, lihat dalam http://www.digitalcentury.com/encyclo/*update/articles.html*. Diakses pada tanggal 21 September 2008.

1) Bagian Kelima Tindak Pidana terhadap Informatika dan Telematika, Paragraf 1 tentang Penggunaan dan Perusakan Informasi Elektronik dan Domain.

   a) Dipidana dengan pidana penjara paling lama 4 (empat) tahun dan pidana denda paling banyak Kategori IV, setiap orang yang menggunakan dan/atau mengakses komputer dan/atau sistem elektronik dengan cara apapun tanpa hak, dengan maksud untuk memperoleh, mengubah, merusak, atau menghilangkan informasi dalam komputer dan/atau sistem elektronik. (Pasal 374)

   b) Dipidana dengan pidana penjara paling lama 1 (satu) dan pidana denda paling banyak Kategori II penyelenggara agen elektronik yang tidak menyediakan fitur pada agen elektronik yang dioperasikannya yang memungkinkan penggunanya melakukan perubahan informasi yang masih dalam proses transaksi. (Pasal 375)

   c) Dipidana dengan pidana penjara paling lama 6 (enam) tahun dan pidana denda paling banyak Kategori IV setiap orang yang memiliki dan menggunakan nama domain berdasarkan itikad tidak baik melanggar persaingan usaha tidak sehat dan melanggar hak orang lain. (Pasal 376)

      Tindak pidana sebagaimana dimaksud pada Pasal 376 ayat (1) diatas hanya dapat dituntut atas pengaduan dari orang yang terkena tindak pidana.

2) Paragraf 2 tentang Tanpa Hak Mengakses Komputer dan Sistem Elektronik

   a) Dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan pidana denda paling banyak Kategori IV setiap orang yang :

      (1). menggunakan, mengakses komputer, dan/atau sistem elektronik dengan cara apapun tanpa hak, dengan maksud memperoleh, mengubah, merusak, atau

---

[245] Lihat dalam www.legalitas.org/database/rancangan/2006/BUKU%20KEDUA%20KUHP, 2006, RUU KUHP Buku II Tindak Pidana, diakses pada tanggal 27 September 2008

menghilangkan informasi pertahanan nasional atau hubungan internasional yang dapat menyebabkan gangguan atau bahaya terhadap negara dan/atau hubungan dengan subjek hukum internasional;

(2). melakukan tindakan yang secara tanpa hak yang menyebabkan transmisi dari program, informasi, kode atau perintah komputer dan/atau sistem elektronik yang dilindungi Negara menjadi rusak;

(3). menggunakan dan/atau mengakses komputer dan/atau sistem elektronik secara tanpa hak atau melampaui wewenangnya, baik dari dalam maupun luar negeri untuk memperoleh informasi dari komputer dan/atau sistem elektronik yang dilindungi oleh negara;

(4). menggunakan dan/atau mengakses komputer dan/atau sistem elektronik milik pemerintah yang dilindungi secara tanpa hak;

(5). menggunakan dan/atau mengakses tanpa hak atau melampaui wewenangnya, komputer dan/atau sistem elektronik yang dilindungi oleh negara, yang mengakibatkan komputer dan/atau sistem elektronik tersebut menjadi rusak;

(6). menggunakan dan/atau mengakses tanpa hak atau melampaui wewenangnya, komputer dan/atau sistem elektronik yang dilindungi oleh masyarakat, yang mengakibatkan komputer dan/atau sistem elektronik tersebut menjadi rusak;

(7). mempengaruhi atau mengakibatkan terganggunya komputer dan/atau sistem elektronik yang digunakan oleh pemerintah;

(8). menyebarkan, memperdagangkan, dan/atau memanfaatkan kode akses (*password*) atau informasi yang serupa dengan hal tersebut, yang dapat digunakan menerobos

komputer dan/atau sistem elektronik dengan tujuan menyalahgunakan komputer dan/atau sistem elektronik yang digunakan atau dilindungi oleh pemerintah;

(9). melakukan perbuatan dalam rangka hubungan internasional dengan maksud merusak komputer atau sistem elektronik lainnya yang dilindungi negara dan berada di wilayah yurisdiksi Indonesia dan ditujukan kepada siapa pun; atau

(10). melakukan perbuatan dalam rangka hubungan internasional dengan maksud merusak komputer atau sistem elektronik lainnya yang dilindungi negara dan berada di wilayah yurisdiksi Indonesia dan ditujukan kepada siapa pun. (Pasal 377)

b) Dipidana dengan pidana penjara paling singkat 3 (tiga) tahun dan paling lama 15 (lima belas) tahun dan pidana denda paling sedikit Kategori IV dan paling banyak Kategori VI, setiap orang yang menggunakan dan/atau mengakses komputer dan/atau sistem elektronik dengan cara apapun tanpa hak, dengan maksud memperoleh, mengubah, merusak, atau menghilangkan informasi milik pemerintah yang karena statusnya harus dirahasiakan atau dilindungi. (Pasal 378)

c) Dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan pidana denda paling banyak Kategori VI, setiap orang yang :

(1). menggunakan dan/atau mengakses komputer dan/atau sistem elektronik secara tanpa hak atau melampaui wewenangnya dengan maksud memperoleh keuntungan atau memperoleh informasi keuangan dari Bank Sentral, lembaga perbankan atau lembaga keuangan, penerbit kartu kredit, atau kartu pembayaran atau yang mengandung data laporan nasabahnya;

(2). menggunakan data atau mengakses dengan cara apapun kartu kredit atau kartu pembayaran milik orang lain secara tanpa hak dalam transaksi elektronik untuk memperoleh keuntungan;

(3). menggunakan dan/atau mengakses komputer dan/atau sistem elektronik Bank Sentral, lembaga perbankan dan/atau lembaga keuangan yang dilindungi secara tanpa hak atau melampaui wewenangnya, dengan maksud menyalahgunakan, dan/atau untuk mendapatkan keuntungan daripadanya; atau

(4). menyebarkan, memperdagangkan, dan/atau memanfaatkan kode akses atau informasi yang serupa dengan hal tersebut yang dapat digunakan menerobos komputer dan/atau sistem elektronik dengan tujuan menyalahgunakan yang akibatnya dapat mempengaruhi sistem elektronik Bank Sentral, lembaga perbankan dan/atau lembaga keuangan, serta perniagaan di dalam dan luar negeri.

3) Paragraf 3 tentang Pornografi Anak melalui Komputer

a) Dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan pidana denda Kategori IV setiap orang yang tanpa hak melakukan tindak pidana yang berkaitan dengan pornografi anak berupa :

1. memproduksi pornografi anak dengan tujuan untuk didistribusikan melalui sistem komputer;
2. menyediakan pornografi anak melalui suatu sistem komputer;
3. mendistribusikan atau mengirimkan pornografi anak melalui sistem komputer;
4. membeli pornografi anak melalui suatu sistem komputer untuk diri sendiri atau orang lain; atau

5. memiliki pornografi anak di dalam suatu sistem komputer atau dalam suatu media penyimpanan data komputer. (Pasal 380)

L. Masukan dari Penelitian dan Pakar

Kajian harmonisasi dan sinkronisasi dengan materi/substansi kriminalisasi perbuatan dalam dunia maya tidak hanya dapat dilakukan terhadap konvensi atau perundang-undangan negara lain, tetapi juga diperlukan masukan dari pakar-pakar dibidang *cyber*, karena mereka lebih mengetahui perbuatan apa dan bagaimana yang dipandang sangat merugikan atau membahayakan sehingga patut dikriminalisasikan. Roy Suryo seorang ahli/pakar teknologi informasi memberikan landasan kriminalisasi dunia maya sehubungan dengan kasus-kasus *cybercrime* yang banyak terjadi terutama di Indonesia, setidaknya ada tiga jenis *cybercrime* berdasarkan modusnya, yaitu : [246]

1. Pencurian Nomor Kredit.
   Menurut Rommy Alkatiry (Wakil Kabid Informatika KADIN), penyalahgunaan kartu kredit milik orang lain di *internet* merupakan kasus *cybercrime* terbesar yang berkaitan dengan dunia bisnis *internet* di Indonesia. Penyalahgunaan kartu kredit milik orang lain memang tidak rumit dan bisa dilakukan secara fisik atau *on-line* . Nama dan kartu kredit orang lain yang diperoleh di berbagai tempat (restaurant, hotel, atau segala tempat yang melakukan transaksi pembayaran dengan kartu kredit) dimasukkan di aplikasi pembelian barang di *internet.*
2. Memasuki, Memodifikasi, atau merusak Homepage (Hacking)
   Menurut John. S. Tumiwa pada umumnya tindakan *hacker* Indonesia belum separah aksi di luar negeri. Perilaku *hacker* Indonesia baru sebatas masuk ke suatu situs komputer orang lain yang ternyata rentan penyusupan dan memberitahukan kepada pemiliknya untuk berhati-hati. Di luar negeri *hacker* sudah memasuki sistem perbankan dan merusak data base bank
3. Penyerangan situs atau *e-mail* melalui virus atau *spamming.*
   Modus yang paling sering terjadi adalah mengirim virus melalui *e-mail*. Menurut RM Roy M. Suryo, di luar negeri kejahatan seperti ini sudah diberi hukuman yang cukup berat. Berbeda dengan di Indonesia yang sulit diatasi karena peraturan yang ada belum menjangkaunya.

[246] Majalah Warta Ekonomi No. 9, 5 Maret 2001 hal.12

Dikdik M. Areif Mansur dan Elisatris Gultom menjelaskan jenis kejahatan yang termasuk dalam kategory *cybercime*, diantaranya sebagai berikut: [247]

1. *Cyber-terorisme.*
   National Police Agency of Japan (NPA) mendefinisikan Cyber terrorism sebagai electronic attack through computer networks againts critical infrastructure that have potential critical effects on social and economic activities of the nation;

2. *Cyber-pornography*. Penyebaran *obscene* materials termasuk *pornography, indencent exposure*, dan *child pornograpy*;

3. *Cyber-harassment.* Pelecehan seksual melalui *e-mail, websites,* atau *chat programs;*

4. *Cyber-stalking. Crimes of stalking* melalui penggunaan komputer dan Internet;

5. *Hacking.* Penggunaan *programming abilities* dengan maksud yang bertentangan dengan hukum;

6. *Carding* (*credit-card fraud*). Melibatkan berbagai macam aktivitas yang melibatkan kartu kredit. *Carding* muncul ketika seseorang yang bukan pemilik kartu kredit menggunakan kartu kredit tersebut secara melawan hukum.

Melalui kajian perbandingan hukum (yuridis komparatif) tindak pidana terhadap sistem jaringan komputer (*against a computer system or network*) disesuaikan dengan negara-negara di dunia terdiri dari: *Illegal access, Illegal interception ,Data interference, System interference*. Aturan tersebut berbeda di masing-masing negara ada yang mengaturnya dalam KUHP negaranya dan ada juga yang mengaturnya dalam undang-undang tersendiri. Apabila diharmonisasikan terhadap perbuatan-perbuatan yang dilarang dalam UU ITE Indonesia dapat dilihat dalam tabel.8 di bawah ini:

Tabel.8

UU ITE dibandingkan dengan Negara-Negara di Dunia

No	Ketentuan dalam UU ITE	UU Negara Lain[248]
1	*Illegal access*: Mengakses sistem orang lain (Pasal 30 ayat (1),(2)	1. Section 478.1 KUHP Australia. 2. Section 342.1 KUHP Kanada

[247] M.Arief Mansur dan Alistaris Gultom, , *CyberLaw;Aspek Hukum Teknologi Informasi, Op.Cit*,hal.26.
[248] Lihat dalam http://www.mosstingrett.no/info/legal.html di akses pada tanggal 5 Oktober 2008.

	dan (3))	3. Article 2 *Automated Data Processing Crimes* no. 19. Chile. 4. Article 550(b) point 1 KUHP Belgia. 5. Section 1030 Point 1 KUHP Amerika Serikat.
2	*Illegal interception:* Melakukan intersepsi atau penyadapan (Pasal 31 ayat (1) dan ayat (2))	1. Section 272 KUHP Estonia 2. Section 303a point 1 KUHP Jerman. 3. Article 370C point 2 KUHP Yunani. 4. Article 550(b) point 2 KUHP Belgia.
3	*Data interference* :Perbuatan melawan hukum terhadap sistem/dokumen elektronik (Pasal 32 ayat (1), (2) dan ayat (3))	1. Section 33 KUHP Filipina 2. Section 86 point 2 *The Electronic Communications And Transactions Act,* Afrika Selatan. 3. Chapter 50 A Section 4 CMA, Singapura. 4. Section 151 b Polandia.
4	*System interference:* Terganggunya sistem komputer (Pasal 33)	1. Article 550(b) point 3 KUHP Belgia. 2. Section 1030 point 2 KUHP Amerika Serikat. 3. Chapter 18 Point 2 CMA Inggris 4. Article 151 b KUHP Norwegia

Berdasarkan kajian harmonisasi materi/substansi kriminalisasi dengan melakukan perbandingan hukum (yuridis komparatif) terhadap perbuatan dalam dunia maya Kriminalisasi delik-delik dalam UU ITE belum dapat dikatakan mencakup semua aspek kehidupan manusia dalam kehidupan yang modern. ITAC (*Information Technology Assosiation of Canada*) pada "*International Information Industry Congress* (IIIC) 2000 Millenium Congress" di Quebec tanggal 19 September 2000 menyatakan bahwa:[249] "*Cybercrime is a real and growing threat to economic and social development around the world. Information technology touches every aspect of human life and so can electronically enable crime*".

Berkaitan dengan hasil kongres ITAC tersebut ada beberapa tanggapan dan evaluasi kebijakan dalam melakukan perubahan dan penyusunan delik-delik baru terhadap kebijakan

[249] ITAC,*" IIIC Common Views Paper On: Cybercrime "*, IIIC 2000 Millenium congress, September 19th, 2000, hal.5. Lihat dalam Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan, Op.Cit*.,hal.240.

kriminalisasi sebagai upaya menanggulangi tindak pidana teknologi informasi pada masa yang akan datang, yaitu:

C.1.1.1 Perlindungan terhadap anak

Kriminalisasi kesusilaan atau eksploitasi seksual terhadap anak tidak diatur dalam Bab VII Pasal 27 sampai dengan Pasal 37 (Perbuatan yang dilarang) UU ITE, tetapi dinyatakan di dalam Pasal 52 ayat (1) yang berisikan ketentuan pemidanaan menyangkut *child pornography*. Tidak adanya delik-delik dan penjelasan secara khusus terhadap pengertian atau defenisi *child pornography* dalam UU ITE akan mengakibatkan lemahnya penegakan hukum.

Dalam Konvensi *Cybercrime* menyebutkan pornografi anak-anak (*child pornography*) merupakan bentuk kejahatan yang harus diperangi, yang menyatakan secara luas kriminalisasi *child pornography* dalam *Title 3 Art 9 Paragraph 2 & Paragraph 3* :[250]

> 2. *For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:*
>   a. *a minor engaged in sexually explicit conduct;*
>   b. *a person appearing to be a minor engaged in sexually explicit conduct;*
>   c. *realistic images representing a minor engaged in sexually explicit conduct.*
> 3. *For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.*

Amerika melakukan kebijakan khusus yang memberikan perlindungan bagi anak-anak terhadap pengaruh pornografi yaitu undang-undang tentang *child online protection* yang mengharuskan para penyedia jasa dan pemilik situs untuk membatasi akses ke situs yang berisi muatan porno bagi anak-anak yang belum dewasa.

Konsep KUHP tahun 2006 sudah mengatur Pornografi Anak melalui Komputer secara lebih khusus dalam Buku II Paragraf 3 Pasal 380 yang menyatakan setiap orang yang tanpa hak melakukan tindak pidana yang berkaitan dengan pornografi anak berupa :

---

[250] *Council of Europe, European Treaty Series* No.185,Budapest 23.IX.2001,page 3.

1. memproduksi pornografi anak dengan tujuan untuk didistribusikan melalui sistem komputer;
2. menyediakan pornografi anak melalui suatu sistem komputer;
3. mendistribusikan atau mengirimkan pornografi anak melalui sistem komputer;
4. membeli pornografi anak melalui suatu sistem komputer untuk diri sendiri atau orang lain; atau
5. memiliki pornografi anak di dalam suatu sistem komputer atau dalam suatu media penyimpanan data komputer. (Pasal 380)

Child pornography telah memberikan dampak yang luar biasa pada tingkat individu, keluarga, komunitas, masyarakat-bangsa, bahkan umat manusia secara keseluruhan. Khususnya memberikan dampak yang besar pada dunia kebudayaan dan keberagamaan pada umumnya. Oleh karena itu diharapkan adanya pengaturan *Child pornography* dalam *cyberspace* yang dibuat secara tegas dan jelas sebagai upaya perlindungan terhadap anak.

C.1.1.2 Pengaturan terhadap Virus Komputer

Pengaturan virus komputer tidak diatur secara jelas dalam UU ITE. Virus terus berkembang menyerang komputer tanpa terkendali selama tidak ada ketentuan yang mengaturnya. Sebenarnya UU ITE sudah mengatur kriminalisasi terhadap penyebaran virus dan worm, hal tersebut secara implisit terlihat dalam Pasal 33 UU ITE ;*"Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya"*.

Pasal 33 UU ITE tidak mengatur definisi akibat terganggunya sistem elektronik secara jelas. Singapura secara tegas mengatur kriminalisasi terhadap penyebaran virus dalam *The*

Computer Misuse Act (CMA) Singapura tahun 1998 Part 2 art 5 *Unauthorised modification of computer material:*[251]

> *(1) Subject to subsection (2), any person who does any act which he knows will cause an unauthorised modification of the contents of any computer shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both.*
>
> *(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 7 years or to both.*
>
> *(3) For the purposes of this section, it is immaterial that the act in question is not directed at --*
> *(a) any particular program or data;*
> *(b) a program or data of any kind; or*
> *(c) a program or data held in any particular computer.*
>
> *(4) For the purposes of this section, it is immaterial whether an unauthorised modification is, or is intended to be, permanent or merely temporary.*

The Computer Misuse Act (CMA) 1998 di atas sudah memberikan penjelasan secara luas terhadap yang dapat dijadikan masukan terhadap Modifikasi (data, program perangkat lunak komputer, dan *databases* dengan cara misalnya, memasukkan virus ke dalam sistem komputer) secara sengaja dan tidak sah muatan/kandungan/isi suatu komputer baik yang mengakibatkan kerusakan atau tidak dan bahkan pengembangan dan penyebaran yang mengakibatkan kerusakan sementara atau permanent juga diatur dalam CMA tersebut.

C.1.1.3 Pengaturan terhadap *Spamming*

Spamming adalah pengiriman email komersial yang tidak diinginkan (*unsolicited*) kepada orang yang tidak secara khusus memintanya.[252] Kata *spammer* didunia Internet memiliki hubungan dengan email, tetapi memiliki dampak negatif bagi pemakai internet. *Spammer*

---

[251] *Computer Misuse Act of* Singapore 1998.
[252] Sumber http://www.solusihukum.com/artikel/artikel30.php di akses pada tanggal 1 September 2008.

diartikan seseorang yang mengirimkan *e-mail* tetapi tidak mengenal siapa yang akan menerima. Sifat *Spammer* adalah mengirim informasi yang menurut mereka perlu diberikan tetapi tidak diperlukan dan sebanyak mungkin diterima oleh pemilik email. Perkembangan *spamming* tidak terhenti hanya mengirim *e-mail* sampah, tetapi sudah menjurus ke arah penipuan dan lainnya.

Kriminalisasi terhadap perbuatan *spammer* tidak ada dalam UU ITE maupun di undang-undang positif yang lain di Indonesia. Australia telah berupaya membuat kebijakan kriminalisasi berkaitan dengan spamming semenjak tahun 1998 dengan adanya kesepakatan dari *Internet Service Providers* (ISPs) dalam *the Internet Industry Association code of practice contained opt-out spamming provisions (IIA)* tahun 1998 yang mengeluarkan aturan yang mengikat setiap providers dalam spamming, terutama yang berkaitan dengan bisnis :[253]

(1) IIA members and code subscribers must not spam, and must not encourage spam, with exceptions in the case of pre-existing relationships (that is, it does not prevent acquaintance spam).
(2) IIA members and code subscribers who do use acquaintance spam must provide recipients with the capability to opt-out, and must include opt-out instructions in the spam.
(3) IIA members and code subscribers must not send even acquaintance spam containing prohibited content.
(4) IIA member and code subscriber Internet Service Providers should have an Acceptable Use Policy that prohibits spam, and further prohibits services that depend on spam.
(5) ISPs should have a working contact address for spam complaints - that is, an "abuse@" email address.
(6) ISPs should install relay protection on their mail servers, to prevent spammers from using the relay to evade detection or penalty.

Pada bulan Nopember 2000 pemerintah Australia mengkriminalisasikan perbuatan *spammer* kedalam *section* 76 E *Crimes Code* 1995 yang berisikan:" *an offence intentionally and without authority interfere with, interrupt or obstruct the lawful use of a computer or to impair the usefulness or effectiveness of data stored in a computer by means of a carrier, such as email.*

[253] Alan Davidson, "*Spamming in Cyberspace*" ,Journal of the Queensland Law Society, 2002, di akses dari http://www.uq.edu.au/davidson/cyberlaw/april2002.html tanggal 2 September 2008.

This case related to the relay of a spam through a third party computer system" The maximum penalty is 10 years imprisonment. [254]

Upaya pengaturan *spamming* sangat berguna terutama berkaitan dengan keamanan dalam *cyberspace*, untuk itu dibutuhkan suatu kebijakan baik yang bersifat peraturan pemerintah maupun kebijakan khusus lainnya yang mengatur dalam perbuatan spammer sebagai upaya memberikan kenyamanan penggunaan internet dan menghindari perbuatan-perbuatan yang mengarah ke penipuan.

C.1.1.4 Pengaturan *Cyber Terrorism*

Beberapa lembaga dan ahli memberikan definisi terkait *cyber terrorism*. Definisi pertama didapat dari *Black's Law Dictionary*, yang menjelaskan sebagai berikut. *"Cyber terrorism. Terrorism committed by using a computer to make unlawful attacks and threats of attack againts computer, networks, and electronically stored information, and actually causing the target to fear or experience harm".*[255]

Secara bebas dapat diartikan, terorisme yang dilakukan dengan menggunakan komputer untuk melakukan penyerangan terhadap komputer, jaringan komputer, dan data elektronik sehingga menyebabkan rasa takut pada korban. Dari definisi ini terlihat unsur utama dari *cyber terrorism*, yaitu:

a. penggunaan komputer,
b. tujuannya untuk melakukan penyerangan, serangan tersebut ditujukan kepada sistem komputer dan data,
c. serta adanya akibat rasa takut pada korban.

---

[254] Lihat dalam http://www.qscl.org.au/ di akses tanggal 3 September 2008.
[255] Bryan A. Graner, *Black's Law Dictionary Eighth Edition*. St. Paul: West Thomson, 2004.

Definisi selanjutnya dikeluarkan oleh Federal Bureau of Investigation (FBI) yang menyatakan sebagai berikut; "*cyber terrorism is the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against noncombatant targets by sub national groups or clandestine agents*".[256]

Dalam beberapa kasus, penguasaan terhadap teknologi sering kali disalahgunakan untuk melakukan suatu kejahatan. Diantara ragam kejahatan menggunakan teknologi, terdapat didalamnya suatu bentuk kejahatan terorisme baru, yaitu *cyber terrorism*.

Akar perkembangan dari *cyber terrorism* dapat ditelusuri sejak awal 1990, ketika pertumbuhan Internet semakin pesat dan kemunculan komunitas informasi. Di Amerika serikat sejak saat itu diadakan kajian mengenai potensi resiko yang akan dihadapi Amerika Serikat atas ketergantungannya yang begitu erat dengan jaringan (*networks*) dan teknologi tinggi.[257] Dikhawatirkan, karena ketergantungan Amerika Serikat yang begitu tinggi terhadap jaringan dan teknologi suatu saat nanti Amerika akan menghadapi apa yang disebut "*Electronic Pearl Harbor*".[258]

Ketakutan tersebut cukup beralasan, karena telah terjadi beberapa insiden yang dikategorikan sebagai *cyber terrorism*e, antara lain pada April dan Maret 2002, di Amerika Serikat, tepatnya negara bagian California, terjadi kehilangan pasokan listrik secara total yang disebabkan oleh ulah *cracker* dari Cina yang menyusup kedalam jaringan *power generator* di wilayah tersebut.[259]

---

[256] Federal Bureau of Investigation (FBI), *citation* Adam Savino, *CyberTerrorisme*,lihat dalam http://www.cybercrimes.net/Terrorism/ct.html , diakses 15 Oktober 2008.

[257] Gabriel Weimann (a), "*Cyberterrorism: How Real Is the Threat?," USIP Special Report No. 119* ,December 2004 , diakses dari http://www.usip.org/pubs/specialreports/sr119.html, pada tanggal 2 Oktober 2008.

[258] *Ibid.*

[259] Wikipedia, http://en.wikipedia.org/wiki/Cyber-terrorism, diakses 10 Oktober 2008.

Contoh lainnya adalah aksi 40 *cracker* dari 23 negara bergabung dalam perang *cyber (cyber war)* konflik Israel-Palestina sepanjang bulan Oktober 2000 sampai Januari 2001. Kelompok yang menamakan dirinya UNITY dan memiliki hubungan dengan organisasi Hezbollah merencanakan akan menyerang situs resmi pemerintah Israel, sistem keuangan dan perbankan, ISPs Israel dan menyerang situs *e-commerce* kaum zionis Israel.[260]

Pergeseran wilayah terorisme konvensional ke *cyber terrorism*e disebabkan beberapa faktor. Weimann dalam tulisannya *www.terror.net: How Modern Terrorism Uses the Internet* menuturkan delapan alasan mengapa terjadi pergeseran wilayah aktifitas terorisme dari konvensional ke *cyber terrorism*e yaitu sebagai berikut.[261]

a. Kemudahan untuk mengakses. *Cyber terrorism* dapat dilakukan secara *remote*. Artinya tindakan *cyber terrorism* dapat dilakukan dimana saja melalui pengontrolan jarak jauh.
b. Sedikitnya peraturan, penyensoran, dan segala bentuk kontrol dari pemerintah.
c. Potensi penyebaran informasi yang mengglobal.
d. Anonimitas dalam berkomunikasi. Hal ini merupakan hal yang biasa dalam dunia Internet. Kebanyakan orang berinteraksi di Internet menggunakan nama palsu atau biasa disebut *nickname*.
e. Arus informasi yang cepat.
f. Biaya yang rendah untuk mengembangkan dan merawat website, selain itu dalam melaksanakan cyber terrorism yang diperlukan umumnya hanya perangkat komputer yang tersambung ke jaringan Internet.
g. Lingkungan multimedia yang mempermudah penyampaian maksud dan tujuan teror.
h. Kemampuan yang lebih baik dari media massa yang tradisional dalam menyajikan informasi.

Berdasarkan karakteristik dari *cyber terrorism* yang telah dijelaskan sebelumnya, kita dapat melihat bentuk dan macam dari *cyber terrorism*. Bentuk atau karakter pertama *cyber terrorism* adalah sebagai tindakan teror terhadap sistem komputer, jaringan, dan/atau basis data dan informasi yang tersimpan didalam komputer, dan beberapa contoh dari bentuk ini adalah.

---

[260] M.Arief Mansur dan Alistaris Gultom, , *CyberLaw;Aspek Hukum Teknologi Informasi, Op.Cit*,hal.58.

[261] Gabriel Weimann (b), "www.terror.net: *How Modern Terrorism Uses the Internet*,, http://www.usip.org/pubs/specialreports/sr116.pdf, di akses pada tanggal 3 Oktober 2008.

1. *Unauthorized Access to Computer System dan Service*. Merupakan kajahatan yang dilakukan dengan memasuki/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer.[262]
2. *Denial of Service Attacks (DOS)*. Penyerangan terhadap salah satu servis yang dijalankan oleh jaringan dengan cara membanjiri server dengan jutanan permintaan layanan data dalam hitungan detik yang menyebabkan server bekerja terlalu keras dan berakibat dari matinya jaringan atau melambatnya kinerja server.[263]
3. *Cyber Sabotage and Extortion*. Kejahatan ini dilakukan dengan membuat gangguan, pengrusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet.
4. *Viruses*. Virus adalah perangkat lunak yang telah berupa program, script, atau macro yang telah didesain untuk menginfeksi, menghancurkan, memodifikasi dan menimbulkan masalah pada komputer atau program komputer lainnya.
5. *Physical Attacks*. Penyerangan secara fisik terhadap sistem komputer atau jaringan. Cara ini dilakukan dengan merusak secara fisik, seperti pembakaran, pencabutan salah satu *devices* komputer atau jaringan menyebabkan lumpuhnya sistem komputer.

Selanjutnya, beberapa contoh implementasi *cyber terrorism*e berkarakter untuk pemanfaatan Internet untuk keperluan organisasi dan juga berfungsi sebagai media teror kepada pemerintah dan masyarakat, adalah sebagai berikut:

1. *Propaganda*. "*The lack of censorship and regulations of the internet gives terrorists perfect opportunities to shape their image through the websites.*"126 Propaganda

[262] M.Arief Mansur dan Alistaris Gultom, , *CyberLaw;Aspek Hukum Teknologi Informasi, Op.Cit,*hal.67.
[263] Michael Gregg, *Certified Ethical Hacker Exam Prep,* United States of America: Que Publishing, 2006, Ch. 7.

dilakukan melalui website yang dibuat oleh kelompok teroris. Biasanya website tersebut berisi struktur organisasi dan sejarah perjuangan, informasi detail mengenai aktifitas perjuangan dan aktifitas sosial, profil panutan dan orang yang menjadi pahlwan bagi kelompok tersebut, informasi terkait ideologi dan kritik terhadap musuh mereka, dan berita terbaru terkait aktifitas mereka.[264]

2. *Carding* atau yang disebut *credit card fraud. Carding* atau *credit card fraud* dalam *cyber terrorisme* lebih banyak dilakukan dalam bentuk pencarian dana. Selain itu *carding* juga dilakukan untuk mengancam perusahaan yang bergerak di bidang penyedian jasa *e-commerce* untuk menyediakan dana agar para *carder* tidak melepaskan data kartu kredit ke internet.[265]
3. *E-mail.* Teroris dapat menggunakan *e-mail* untuk menteror, mengancam dan menipu, *spamming* dan menyebarkan virus ganas yang fatal, menyampaikan pesan diantara sesama anggota kelompok dan antara kelompok.

Dimasa mendatang dimana kehidupan manusia sangat bergantung pada teknologi telah menimbulkan suatu potensi kejahatan model baru yang disebut *cyber terrorism*. Untuk itu diperlukan sebuah perangkat hukum yang dapat mengakomodir upaya hukum terhadap tindak pidana *cyber terrorism*. Payung hukum dalam pemberantasan tindak pidana terorisme tidak hanya Undang-Undang No 15 Tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme tetapi perlu didukung oleh berbagai undang-undang lainnya terutama yang bersifat *cyber law* dengan mengatur berbagai aspek kejahatan *cyber terrorism* sehingga pengaturannya lebih bersifat komprehensif.

C.1.2 Pertanggungjawaban Pidana

[264] Zhang, lihat dalam http://www.slais.ubc.ca/courses/libr500/04-05-wt1/www/X_Zhang/5ways.htm , diakses pada tanggal 15 Oktober 2008.

[265] M.Arief Mansur dan Alistaris Gultom, , *CyberLaw;Aspek Hukum Teknologi Informasi*, *Op.Cit*,hal.68.

Dalam hukum pidana, ada dua hal penting yang perlu mendapat perhatian, yaitu mengenai hal melakukan perbuatan pidana (*actus reus*) yang berkaitan dengan subjek atau pelaku perbuatan pidana, dan mengenai kesalahan (*mens rea*) yang berkaitan dengan masalah pertanggungjawaban pidana. Berkaitan dalam asas hukum pidana yaitu "*Geen straf zonder schuld, actus non facit reum nisi mens sir rea*", bahwa "tidak dipidana jika tidak ada kesalahan", maka pengertian "tindak pidana" itu terpisah dengan yang dimaksud "pertanggungjawaban tindak pidana".

Tindak pidana hanyalah menunjuk kepada dilarang dan diancamnya perbuatan itu dengan suatu pidana, kemudian apakah orang yang melakukan perbuatan itu juga dijatuhi pidana sebagaimana telah diancamkan akan sangat tergantung pada soal apakah dalam melakukan perbuatannya itu si pelaku juga mempunyai kesalahan. Sedangkan sebagai dasar pertanggungjawaban adalah kesalahan yang terdapat pada jiwa pelaku dalam hubungannya dengan kelakuannya yang dapat dipidana serta berdasarkan kejiwaannya itu pelaku dapat dicela karena kelakuanya itu. Dengan kata lain, hanya dengan hubungan batin inilah maka perbuatan yang dilarang itu dapat dipertanggungjawabkan pada si pelaku.

Batin yang salah (*guilty mind,mens rea*) ini adalah kesalahan yang merupakan sifat subjektif dari tindak pidana karena berada didalam diri pelaku oleh karena itu kesalahan memiliki dua segi, yaitu segi psikologi dan segi normatif. Segi psikologi kesalahan harus dicari didalam batin pelaku yaitu adanya hubungan batin dengan perbuatan yang dilakukan sehingga ia dapat mempertanggungjawabkan perbuatannya. Segi normatif yaitu menurut ukuran yang biasa dipakai masyarakat sebagai ukuran untuk menetapkan ada tidaknya hubungan batin antara pelaku dengan perbuatannya.

Berkaitan dengan kesalahan yang bersifat psikologis dan normatif, serta unsur-unsur tindak pidana maka kesalahan memiliki beberap unsur:[266]

a) Melakukan perbuatan pidana (sifat melawan hukum)
b) Adanya kemampuan bertanggung jawab pada si pelaku (di atas umur dan pelaku dalam keadaan sehat dan normal);
c) Adanya hubungan antara si pelaku dengan perbuatannya baik yang disengaja (*dolus)* maupun karena kealpaan (*culpa*);
d) Tidak adanya alasan pelaku yang dapat menghapus kesalahan.

Telah dikemukakan di atas bahwa untuk adanya pertanggungjawaban pidana pertama-tama harus dipenuhi persyaratan objektif, yaitu perbuatannya harus telah merupakan tindak pidana menurut hukum yang berlaku. Dengan kata lain, untuk adanya pertanggungjawaban pidana pertama-tama harus dipenuhi asas legalitas, yaitu harus ada dasar/sumber hukum (sumber legitimasi) yang jelas, baik dibidang hukum pidana material/substantif maupun hukum pidana formal. Disamping itu harus dipenuhi pula persayaratan subyektif, yaitu adanya sikap batin dalam diri si pelaku/asas culpabilitas.

Berkaitan dengan asas culpabilitas tersebut moeljatno berpendapat meskipun melakukan tindak pidana, tidak selalu pembuatnya dapat dipidana (dapat dipertanggungjawabkan).[267] Lebih jauh lagi hal ini lebih ditegaskan oleh Barda Nawawi Arief dan Muladi, yang mengatakan bahwa pada umumnya yang dapat dipertanggungjawabkan adalah si pembuat tapi tidaklah selalu demikian.[268] Hal ini lebih dipertegas lagi oleh Honderic yang mengatakan:" *punishment is not always of an offender*".[269] Penyimpangan asas kesalahan tersebut dalam kaitannya dengan

[266] Moeljatno, *Asas-Asas Hukum Pidana*, Cetakan.VI, *Op.Cit*.,hal.89.
[267] Moeljatno, *Asas-Asas Hukum Pidana*, Cetakan.VI, *Op.Cit*.,hal.164.
[268] Muladi dan Barda Nawawi Arief, *Teori-Teori dan Kebijakan Pidana*, Alumni, Bandung,1998,hal.97.
[269] Ted Hinderich, Punishment:*The Supposed Justifications*,London: Pegun Books,1976,hal.16.

pertanggungjawaban pidana dalam teori hukum pidana dikenal asas-asas pertanggungjawaban pidana, yaitu:[270]

1. Doktrin pertanggungjawaban pidana langsung (*direct Liability Doctrine*) atau Teori identifikasi (*Identification Theory*)

   dimana mengakui tindakan anggota tertentu dari korporasi, dianggap sebagai tindakan korporasi itu sendiri. Teori ini menyebutkan bahwa tindakan dan kehendak dari direktur juga merupakan tindakan kehendak dari korporasi.

2. Doktrin pertanggungjawaban pidana pengganti (*Vicarious Liability*).

   Doktrin ini merupakan suatu pertanggungjawaban pidana yang dibebankan kepada seseorang atas perbuatan orang lain. Pertanggungjawaban demikian misalnya terjadi dalam hal perbuatan-perbuatan yang dilakukan oleh orang lain yang berkaitan dengan pekerjaan atau jabatannya. Dengan demikian dalam pengertian "*vicarious liability*" ini, walaupun seseorang tidak melakukan sendiri suatu tindak pidana dan tidak mempunyai kesalahan dalam arti biasa, ia masih dapat dipertanggungjawabkan, bahkan dalam hal tertentu, ia dipertanggungjawabkan sebagai pelaku (pembuat).

   Sebagai pertanggungjawaban menurut hukum *vicarious liability* diartikan sebagai seseorang atas perbuatan salah yang dilakukan oleh orang lain merupakan bentuk pertanggungjawaban sebagai pengecualian dari asas kesalahan. Selanjutnya Peter gillies menulis bahwa,[271] "*vicarious liability dalam hukum pidana dapat digambarkan sebagai pengenaan pertanggungjawaban pidana kepada seseorang dalam kapasitas pelaku utama, berdasarkan atas perbuatan pelanggaran yang dilakukan oleh orang lain*".

---

[270] Barda Nawawi Arief, *Kapita Selekta Hukum Pidana, Op.Cit;* hal.233-237.
[271] Peter Gillies, *Criminal Law, Second Edition, The Law Book*, Syney, 1990,hal.23.

3. Doktrin Pertanggungjawaban Pidana (PJP) yang ketat menurut Undang-Undang (*Strict Liability*).

   Doktrin *strict liability*, dimana seseorang sudah dapat dipertanggungjawabkan untuk tindak pidana tertentu walaupun pada diri orang itu tidak ada kesalahan (*mens rea*). Roeslan saleh menyatakan,[272] dalam praktek pertanggungjawaban pidana menjadi lenyap, jika ada salah satu keadaan-keadaan yang memaafkan. Praktek pula melahirkan aneka macam tingkatan keadaan-keadaan mental yang dapat menjadi syarat ditiadakannya pengenaan pidana, sehingga dalam perkembangannya lahir kelompok kejahatan yang untuk pengenaan pidananya cukup dengan *strict liability*.

   Strict liability,sering diidentifikasikan dengan tanggung jawab absolute (*absolute liability*), kendati demikian ada para ahli yang membedakan kedua doktrin tersebut. *Absolute liability*[273] adalah prinsip tanggung jawab tanpa kesalahan dan tidak ada pengecualiannya sehingga walaupun tidak hubungan masih dapat dipertanggungjawabkan sedangkan dalam *strict liability* untuk dipertanggungjawabkan hubungan tersebut wajib ada.

Bertolak dari pengertian diatas perumusan tindak pidana dalam UU ITE, selalu mencantumkan unsur dengan sengaja dan tanpa hak. Dengan tercantumnya unsur sengaja maka dapat dikatakan bahwa pertanggungjawaban pidana dalam UU ITE menganut prinsip *liability based on fault* (pertanggungjawaban berdasarkan kesalahan). Jadi, pada prinsipnya menganut asas kesalahan atau asas culpabilitas. Karena dalam UU ITE semua tindak pidana dalam UU ITE

[272] Roelan Saleh, *Sifat melawan hukum daripada perbuatan pidana* ,Badan Penerbit Gadjah Mada, 1962,hal.23.

[273] Sukarmi, *Cyberlaw:Kontrak Elektronik dalam Bayang-Bayang Pelaku Usaha*,Pustaka Sutra, 2007,hal.23

dianggap sebagai kejahatan. Dengan demikian unsur kesalahan (dalam bentuk kesengajaan dan kealpaan) merupakan unsur yang hakiki (*liability based on fault*);

Asas kesalahan yang diterapkan dalam pertanggungjawaban pidana UU ITE mengindetifikasikan bahwa seolah-olah tidak dimungkinkan adanya pertanggungjawaban mutlak (*strict liability*). Sedangkan dalam tindak pidana teknologi informasi prinsip ajaran *stirct liability* dan *vicarious liabilty* secara teoritis sangat dimungkinkan mengingat tidak mudah membuktikan adanya kesalahan pada delik-delik *cybercrime,* terutama yang berkaitan terhadap kesalahan pada korporasi/badan hukum.

Pemikiran dalam penerapan asas **"***strict liability***",** dan **"***vicarious liability***"** sudah tertulis dalam Konsep KUHP 2004[274] dalam Buku I yang menegaskan, bahwa "*strict liability*" dan "*vicarious liability*" dimungkinkan "untuk tindak pidana tertentu atau dalam hal-hal tertentu. Sehingga dalam kebijakan pertanggungjawaban pidana dalam penanggulangan tindak pidana teknologi informasi yang akan datang memungkinkan untuk menerapkan "*strict liability*" dan "*vicarious liability*".

Pembuat undang-undang dalam merumuskan delik sering memperhitungkan kenyataan manusia melakukan tindakan di dalam atau melalui organisasi yang dalam hukum keperdataan maupun di luarnya muncul sebagai satu kesatuan dan karena dari itu diakui serta mendapat perlakuan sebagai badan hukum/korporasi.[275] Dengan demikian, dalam hukum pidana saat ini subjek hukumnya tidak lagi terbatas pada manusia sebagai pribadi kodrati (*natuurlijke-persoonen*) tetapi juga mencakup manusia sebagai badan hukum (*rechts-persoonen*).

---

[274] Konsep KUHP 2004 juga memberi kemungkinan dalam hal-hal tertentu untuk menerapkan asas **"***strict liability***",** asas **"***vicarious liability***",** dan asas "pemberian maaf/pengampunan oleh hakim" *("rechterlijk pardon***"** atau **"***judicial pardon***").**

[275] Jan Remmelink, *Hukum Pidana: Komentar atas Pasal-Pasal Terpenting dari Kitab Undang-undang Hukum Pidana Belanda dan Padanannya dalam Kitab Undang-undang Hukum Pidana Indonesia,* PT Gramedia Pustaka Umum, Jakarta, 2003, hal. 97.

Perkembangan hukum pidana di Indonesia ada tiga sistem pertanggungjawaban pidana korporasi sebagai subjek tindak pidana yakni:[276]

1. Pengurus korporasi yang berbuat, maka penguruslah yang bertanggungjawab.
2. Korporasi sebagai pembuat, maka penguruslah yang bertanggungjawab.
3. Korporasi sebagai pembuat dan yang bertanggung jawab.

John C.Coffee,Jr sebagaimana di kutip oleh Barda Nawawi Arief menyebutkan alasan penggunaan hukum pidana terhadap korporasi antara lain:[277]

1. Hukum pidana mampu melaksanakan peranan edukatif dalam mendefenisikan/menetapkan dan memperkuat batas-batas perbutan yang dapat diterima (*acceptable conduct*);
2. Hukum pidana bergerak dengan langkah lebih cepat daripada perdata. Dengan pidana restitusi, lebih cepat memperoleh kompensasi bagi korban;
3. Peradilan perdata terhalang untuk mengenakan sanksi pidana;
4. Penuntutan bersama (korporasi dan agennya) memerlukan suatu forum pidana apabila ancaman pengurungan digunakan untuk mencegah individu. Dari sudut penegakan hukum, peradilan bersama itu cukup beralasan karena lebih murah dibandingkan dengan penuntutan terpisah, dan karena mereka mengizinkan penuntut umum mengikuti kasus itu dalam cara yang terpadu.

Adanya ketentuan pertanggungjawaban pidana terhadap korporasi dalam UU ITE merupakan suatu kemajuan dalam hukum pidana indonesia (KUHP) karena KUHP belum mengatur terhadap pertanggungjawaban korporasi. Korporasi sebagai subjek tindak pidana

[276] I.S Susanto, *Tinjauan Kriminologi Terhadap Perilaku Menyimpang dalam Kegiatan Ekonomi Masyarakat dan Penanggulangannya, "Makalah seminar Nasional Peranan Hukum Pidana dalam Menunjang Kebijaksanaan Ekonomi,* Semarang, Fakultas Hukum Universitas Undip, 2007,hal.2.

[277] Barda Nawawi Arief, *Sari Kuliah: Perbandingan Hukum Pidana,Op.Cit*.,,hal.148..

dalam *cybercrime* walaupun tidak diatur secara jelas dan khusus dalam UU ITE, tetapi Penjelasan Pasal 52 ayat (4) memberikan persyaratan terhadap subjek pertanggungjawaban korporasi untuk dikenakan sanksi pidana adalah yang dilakukan oleh korporasi *(corporate crime)* dan/atau oleh pengurus dan/atau staf korporasi.

Seyogianya *adressat* UU ITE tidak hanya mengatur terhadap subjek pertanggungjawaban korporasi sebagai korporasi, pengurus dan/atau staf korporasi saja. Perlunya perhatian pertanggungjawaban *Internet Service Provider* (ISP) sebagai penyedia layanan internet dan Warung Internet (Warnet) yang menyediakan akses internet. Posisi keduanya dalam *cybercrime* cukup penting sebagai penyedia dan jembatan menuju jaringan informasi global, apalagi Warnet telah ditetapkan sebagai ujung tombak untuk mengurangi kesenjangan digital di Indonesia. Bentuk pertanggungjawaban pidana apa yang mesti mereka terima jika terbukti terlibat dalam *cybercrime*. Apakah pertanggungjawabannya dibebankan secara individual atau dianggap sebagai suatu korporasi. Ini akan memiliki konsekuensi tersendiri

Oleh karena korporasi mempunyai sifat yang mandiri dalam hal pertanggungjawaban pidana sehingga ia tidak dapat disamakan dengan subjek tindak pidana yang dilakuan oleh orang . Untuk itu penerapan asas-asas pertanggungjawaban korporasi dengan cara pertanggungjawaban pidana langsung (*direct Liability Doctrine*) atau Teori identifikasi (*Identification Theory*), pidana pengganti (*Vicarious Liability*), Pertanggungjawaban Pidana yang ketat *(Strict Liability),*dan tanggung jawab absolute (*absolute liability*) perlu dipertimbangkan dalam merumuskan pertanggungjawaban pidana korporasi di masa yang akan datang.

Sebagai perbandingan bahwa KUHP Australia menggunakan "*absolute liability*" untuk delik-delik *Computer Crime* tertentu yang diatur dalam KUHP, misalnya terhadap Section 477.1 : "*Unauthorised access, modification or impairment with intent to commit a serious offence*";

477.2 : "*Unauthorised modification of data to cause impairment*"; 477.3 : "*Unauthorised impairment of electronic communication*"; 478.1 : "*Unauthorised access to, or modification of, restricted data";* 478.2 : "*Unauthorised impairment of data held on a computer disk etc*.". Menurut Section 24 KUHP Australia, dalam delik *absolute liability, mistake of fact (error facti*) tidak dapat digunakan sebagai alasan pembelaan (alasan penghapus pidana); dan menurut Section 23, dalam delik *strict liability, mistake of fact* dapat digunakan sebagai alasan pembelaan.

Dengan dijadikannya korporasi sebagai subjek tindak pidana, maka dalam upaya penanggulangan tindak pidana teknologi informasi di masa yang akan datang hendaknya harus ada ketentuan khusus yang mengatur mengenai:

1. Kapan dikatakan korporasi melakukan tindak pidana;
2. Siapa yang dapat dipertanggungjawabkan;
3. dalam hal bagaimana korporasi dapat dipertanggungjawabkan; dan
4. Jenis-jenis sanksi apa yang dapat dijatuhkan untuk korporasi

C.1.3 Pemidanaan

Perkembangan bentuk dan dimensi kejahatan tentulah memerlukan penanganan, yang salah satu cara penanggulangannya adalah dengan sarana penal atau sanksi pidana. Sanksi pidana merupakan salah satu masalah sentral dalam hukum pidana, karena itu menjadi hal yang penting untuk dikaji bagaimana bentuk pidana yang tepat dalam menanggulangi *cybercrime*.

Masalah penalisasi atau pemidanaan sendiri merupakan bagian masalah yang penting dari suatu kebijakan pemidanaan (*sentencing policy*) yang menurut Herbert L.Packer merupakan salah satu masalah kontroversial saat ini dalam hukum pidana.[278] Masalah krimalisasi dan penalisasi atau pidana dan pemidanaan, merupakan masalah yang selalu memerlukan peninjauan

[278] Muladi dan Barda Nawawi Arief, *Teori-Teori dan Kebijakan Pidana, Op.Cit*.,hal.174.

kembali, mengingat sifatnya yang melekat (*inherent*) dengan sifat dan hakekat kejahatan itu sendiri yang selalu mengalami perubahan dan perkembangan. Kemudian berubah dan berkembangnya kejahatan selalu diikuti berubah dan berkembangya pidana itu sendiri.

Pemidanaan dapat diartikan sebagai tahap penetapan sanksi dan pemberian sanksi dalam hukum pidana bila seseorang bersalah melanggar hukum maka ia harus dipidana. Persoalan pemidanaan bukanlah sekedar masalah memidana seseorang dengan menjebloskannya ke penjara, pemidanaan harus mengandung unsur kehilangan atau kesengsaraan yang dilakukan oleh institusi yang berwenang karenanya pemidanaan bukan merupakan balas dendam dari korban terhadap pelanggar hukum yang mengakibatkan penderitaan.

Penetapan jenis pidana oleh pembuat undang-undang antara lain dimaksudkan untuk menyediakan seperangkat sarana bagi penegak hukum dalam rangka menanggulangi kejahatan. Disamping itu dimaksudkan pula untuk membatasi aparat penegak hukum dalam menggunakan sarana berupa pidana yang telah ditetapkan itu. Mereka tidak boleh menggunakan sarana pidana yang tidak lebih dulu ditetapkan oleh pembuat undang-undang. Dengan demikian jenis pidana yang dipilih dan ditetapkan oleh pembuat undang-undang mengikat dan membatasi penegak hukum lainnya.

Oleh karena itu bagian penting dalam sistem pemidanaan adalah menetapkan jenis pidananya/sanksi. Keberadaannya akan memberikan arah dan pertimbangan mengenai apa yang seharusnya dijadikan sanksi dalam suatu tindak pidana untuk menegakkkan berlakunya norma. Disisi lain pemidanaan itu sendiri merupakan proses paling komplek dalam sistem peradilan pidana karena melibatkan banyak orang dan istitusi yang berbeda. Sehingga apabila seperangkat sanksi pidana yang telah ditetapkan merupakan hasil pilihan yang kurang tepat atau sudah tidak

sesuai lagi dengan perkembangan kriminalitas, maka adalah wajar apabila penanggulangan perkembangan kriminalitas terganngu.

Penentuan sanksi pidana, penjatuhan pidana dan pelaksanaan pidana berhubungan erat dengan tujuan pemidanaan, oleh karenanya tujuan pemidanaan harus dijadikan patokan sebelum ditetapkannya sanksi pidana. Muladi dan Barda Nawawi Arief mengatakan,[279] bahwa pidana yang akan ditetapkan adalah pidana yang diharapkan dapat menunjang tercapainya tujuan. Efektifitas pidana harus diukur berdasarkan tujuan atau hasil yang ingin dicapai.

Dari pengertian di atas Barda Nawawi Arief menyatakan perumusan dan tujuan dan pedoman pemidanaan bertolak dari pemikiran,sebagai berikut:[280]

(1). Pada hakikatnya undang-undang merupakan suatu sistem (hukum) yang bertujuan (*"purposive system*"). Dirumuskannya pidana dan aturan pemidanaan dalam undang-undang pada hakikatnya hanya merupakan sarana mencapai tujuan.

(2). Dilihat secara fungsional dan operasional, pemidanaan merupakan suatu rangkaian proses dan kebijakan yang konkretisasinya sengaja direncanakan melalui beberapa tahap (formulasi, aplikasi, eksekusi). Agar ada keterjalinan dan keterpaduan antara ketiga tahap itu sebagai satu kesatuan sistem pemidanaan, diperlukan perumusan tujuan dan pedoman pemidanaan.

(3). Sistem pemidanaan yang bertolak dari paham individualisasi pidana, tidak berarti memberi kebebasan sepenuhnya kepada hakim dan aparat-aparat lainnya tanpa pedoman atau kendali/kontrol. Perumusan tujuan dan pedoman dimaksudkan sebagai "fungsi pengendali/kontrol" dan sekaligus memberikan dasar filosofis, dasar rasionalitas dan motivasi pemidanaan yang jelas dan terarah.

---

[279] Muladi dan Barda Nawawi Arief, *Teori-Teori dan Kebijakan Pidana*, *Op.Cit*.,hal.101.
[280] Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana*, *Op.Cit*.hal.139.

Bertolak dari pengertian sistem pemidanaan L.H.C Hulsman mengemukakan pengertian sistem pemidanaan sebagai;[281] ”aturan perundang-undangan yang berhubungan dengan sanksi pidana dan pemidanaan” (*the stautory rules relating to penal sanctions and punishment*). Oleh karenanya semua hukum pidana materiil/substantif, hukum pidana formal dan hukum pelaksanaan pidana dapat dilihat sebagai satu kesatuan sistem pemidanaan (*the sentencing system*).

Barda Nawawi Arief menyebutkan untuk dapat diterapkan (dioperasionalkan/difungsikan), perumusan sanksi pidana itu masih harus ditunjang oleh sub-sub sistem lainnya, yaitu sub-sistem aturan/pedoman dan asas-asas pemidanaan yang ada di dalam aturan umum KUHP atau aturan khusus dalam UU khusus yang bersangkutan. Oleh karena itu, agar perumusan sanksi pidana dapat operasional, harus memperhatikan aturan umum yang ada di dalam KUHP, antara lain sebagai berikut :[282]

a. Dilihat dari sudut ”*strafsoort*” (jenis-jenis sanksi pidana), semua aturan pemidanaan di dalam KUHP berorientasi pada “*strafsoort”* yang ada/ disebut dalam KUHP, baik berupa pidana pokok maupun pidana tambahan. Oleh karena itu, apabila UU khusus menyebut jenis-jenis pidana/tindakan lain yang tidak ada di dalam KUHP maka UU khusus itu harus membuat aturan pemidanaan khusus untuk jenis-jenis sanksi pidana itu.
b. Menurut pola KUHP, jenis pidana yang dirumuskan/diancamkan dalam perumusan delik hanya pidana pokok dan/atau pidana tam-bahannya. Pidana “kurungan pengganti” tidak dirumuskan dalam perumusan delik (aturan khusus), tetapi

[281] L.H.C Hulsman. *The Dutch Criminal Justice System From A Comparative Legal Perspective*, lihat dalam Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana, Op.Cit*.hal.135.

[282] Barda Nawawi Arief, P*rinsip-Prinsip Dasar atau Pedoman Perumusan/Formulasi Ketentuan Pidana dalam Perundang-undangan*, Makalah Perkuliahan Politik Hukum, Undip, 2007,hal.5-7

dimasukkan dalam aturan umum mengenai pelaksanaan pidana ("*strafmodus*"). Oleh karena itu, UU khusus tidak perlu memasukkan pidana kurungan pengganti se-bagai jenis pidana yang diancamkan dalam perumusan delik, terlebih apabila jumlah lama-nya kurungan pengganti itu tidak menyimpang dari aturan umum KUHP. Kalau pun menyimpang, perumusannya tidak dimasukkan sebagai "*strafsoort*" dalam perumusan delik, tetapi diatur tersendiri dalam aturan tentang pelaksanaan pidana ("*strafmode/strafmodus*").

c. Dilihat dari sudut "*strafmaat*" (ukuran jumlah/lamanya pidana), aturan pemidanaan dalam KUHP berorientasi pada sistem minimal umum dan maksimal khusus, tidak berorientasi pada sistem minimal khusus. Artinya, di dalam KUHP tidak ada aturan pemidanaan untuk ancaman pidana minimal khusus. Oleh karena itu, apabila UU khusus membuat ancaman pidana minimal khusus, maka harus disertai juga dengan aturan/pedoman penerapannya.

d. Aturan pemidanaan umum dalam KUHP berorientasi pada "orang" (*natural person*), tidak ditujukan pada "korporasi". Oleh karena itu, apabila UU khusus menyebutkan adanya sanksi pidana untuk korporasi, maka harus disertai juga dengan aturan khusus pemidanaan untuk korporasi. Misalnya mengenai :

   - aturan pertanggugjawaban korporasi;
   - aturan pelaksanaan pidana denda untuk korporasi.

Bertolak dari hal-hal di atas maka untuk lebih mengefektifkan upaya penanggulangan tindak pidana teknologi informasi seyogianya dilakukan perbaikan kebijakan formulasi sistem pidana dan pemidanaan sebagai berikut:

1. Sanksi pidana sebaiknya tidak dirumuskan secara kumulatif yang bersifat imperatif dan kaku, namun seyogianya perumusan sanksi pidana dengan cara alternatif/ pilihan atau secara kumulatif-alternatif agar memberikan kelonggaran pada tahap aplikasi dengan melihat permasalahan secara kasuistis. Dengan perumusan sanksi pidana secara alternatif akan memberikan pilihan untuk menjatuhkan pidana pokok berupa pidana penjara atau denda berdasarkan motif dan tujuan dilakukannya tindak pidana oleh pelaku yang akan menjadi bahan pertimbangan hakim untuk menjatuhkan vonis.
2. Jenis tindak pidana hanya berupa denda penjara dan/atau denda yang dirumuskan secara komulatif. Jadi tidak ada pidana tambahan atau jenis sanksi tindakan yang diintegrasikan ke dalam sistem pemidanaan. Sebagai upaya penanggulangan tindak pidana teknologi informasi seyogianya diatur jenis pidana tambahan atau tindakan seperti:
    - Pelarangan penggunaan internet selama batas waktu yang ditentukan.
    - Pembayaran ganti kerugian bagi korban
3. Ancaman tindak pidana dalam UU ITE tidak mengenal ancaman pidana minimal. Dalam rangka pembaharuan, cukup layak mencantumkan pidana minimal untuk tindak pidana teknologi informasi. Namun untuk mengoperasionalisasikan ancaman pidana minimal tersebut perlu aturan/pedomannya.
3. Subjek tindak pidana dalam KUHP hanya “orang”, sehingga semua aturan pemidanaan di dalam KUHP diorientasikan pada “orang”, tidak pada korporasi. Oleh karena itu, apabila UU ITE memperluas subjek tindak pidana pada korporasi, seyogianya juga disertai dengan aturan pemidanaan atau pertangjawaban khusus untuk korporasi. Perlu ada ketentuan khusus mengenai pelaksanaan pidana dengan

yang tidak dibayar oleh korporasi. Hal ini penting dikarenakan apabila korporasi diterapakan sebagai subjek tindak pidana tetapi tidak membayar maka tidak mungkin korporasi menjalani pidana kurungan pengganti.

4. Dalam UU ITE tidak ada ketentuan khusus mengenai pengganti denda yang tidak dibayar. Ini berarti berlaku ketentuan umum Pasal 30 KUHP. Untuk mengefektifkan pidana denda, perlu diadakan ketentuan khusus yang menyimpang dari Pasal 30 KUHP (mengenai pelaksanaan pidana denda yang tidak dibayar; atau mengenai pidana pengganti denda).
5. Perlunya penambahan pidana pokok untuk korporasi. *Draft Convention on Cybercrime Title 5.Art.13* menyatakan *Each Party shall ensure that legal persons held liable in accordance with Article 12 (Corporate liability) shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions*. Dari draft tersebut karena pidana pokok yang paling cocok untuk korporasi adalah pidana denda dan perampasan kemerdekaan maka seyogianya penting untuk penambahan sanksi berupa:
   - Penutupan korporasi/badan hukum untuk waktu tertentu: Penutupan Warung Internet (Warnet) sampai batas waktu tertentu.
   - Pencabutan hak/izin usaha : Pencabutan hak *Internet Service Provider* (ISP) sebagai penyedia layanan internet.
   - *Structural Sanctions* atau *Restriction on Enterpreneurial Activities* (pembatasan kegiatan usaha;pembubaran korporasi)

C.2 Penegakkan hukum masa yang akan datang

Proses penegakan hukum pada dasarnya adalah upaya mewujudkan keadilan dan ketertiban di dalam kehidupan bermasyarakat. Melalui sistem peradilan pidana dan sistem pemidanaan. Pada dasarnya hak-hak warga negara yang terganggu akibat perbuatan melawan hukum seseorang akan diseimbangkan kembali. Satjipto Raharjo menyatakan, [283] proses penegakan hukum ini menjangkau pula sampai pada pembuatan hukum. Perumusan pikiran pembuatan undang-undang (hukum) yang dituangkan dalam peraturan hukum akan turut menentukan, bagaimana penegakan hukum dijalankan.

Performance lembaga-lembaga hukum, dengan sendirinya mendapat sorotan yang lumayan tinggi dari rakyat, karena mereka inilah yang mempunyai tugas untuk menterjemahkan aturan-aturan hukum ke dalam praktek, untuk menyelesaikan sengketa dan konflik yang terjadi dalam masyarakat. utamanya adalah keseluruham sistem peradilan pidana (kalaupun dapat disebut sebagai sistem karena nampaknya lebih kental warna non-sistemnya), yakni lembaga kepolisian, kejaksaan, pengadilan dan pemasyarakatan serta kepengacaan, yang kini tengah mendapat sorotan yang luar biasa. Bergandengan dengan sorotan ini, lembaga-lembaga ini juga sekaligus merupakan sumber dan obyek dari pengabaian, ketidak hormatan dan ketidak percayaan masyarakat.

C.3.1 Upaya Penegakan Hukum

Penegakan hukum dalam *cyberspace* membutuhkan sinergi antara masyarakat yang partisipatif dengan aparat penegak hukum yang demokratis, transparan, bertanggung jawab dan berorientasi pada HAM, pada alirannya diharapkan dapat benar-benar mewujudkan masyarakat madani Indonesia yang berkeadilan sosial.

[283] Satjipto Rahardjo, *Masalah Penegakan Hukum, Suatu Tinjauan Sosiologis*, Badan Pembinaan Hukum Nasional Departemen Kehakiman, Jakarta, 1983, hal.54.

Harus diakui bahwa Indonesia belum mengadakan langkah-langkah yang cukup signifikan di bidang penegakan hukum (*law enforcement*) dalam upaya mengantisipasi kejahatan mayantara seperti dilakukan oleh negara-negara maju di Eropa dan Amerika Serikat. Di Inggris dan Jerman membentuk suatu institusi bersama yang ditugaskan untuk dapat menanggulangi masalah *Cybercrime Investigation* dengan nama *National Criminal Intellegence Service* (NCIS) yang bermarkas di London. Pada tahun 2001, Inggris meluncurkan suatu proyek yang diberi nama "*Trawler Project*" bersamaan dibentuknya *National Hi-tech Crime Unit* yang dilengkapi dengan anggaran khusus untuk *cyber cops*. Sementara itu, Amerika Serikat membentuk pula *Computer Emergency Response Team* (CERT) yang bermarkas di Pittsburg pada tahun 1990-an dan *Federal Bureau Investigation* (FBI) memiliki *Computer Crime Squad* di dalam menanggulangi kejahatan mayantara.[284]

Barda Nawawi Arief menyatakan upaya Peningkatan Efektifitas dan Pembaharuan Orientasi (Reformasi/Rekonstruksi) Penegakan Hukum Pidana Menghadapi *Cybercrime* perlu kiranya ditempuh beberapa langkah (upaya) antara lain sebagai berikut :[285]

1. Meningkatkan komitmen strategi/prioritas nasional dalam penanggulangan kejahatan di bidang kesusilaan, yang seyogyanya disejajarkan dengan upaya penanggulangan tindak pidana korupsi, narkoba, terorisme dan sebagainya.
2. Melakukan pembaharuan pemikiran/konstruksi juridis (*juridical construction reform*), antara lain :
    a. rekonstruksi penegakan hukum (pemikiran hukum) dalam konteks kebijakan pembaharuan sistem hukum dan pembangunan nasional;

[284] Buletin Litbang Dephan, Kejahatan Mayantara (*Cybercrime*) *Dampak Perkembangan Teknologi Informasi "Dunia Maya"*, STT No. 2289 Volume VII Nomor 12 Tahun 2004.

[285] Barda Nawawi Arief, "Kajian Kebijakan Hukum Pidana Menghadapi Perkembangan Delik Kesusilaan di Bidang Cyber", Seminar *Cybercrime* dan *Cyber Porn* dalam Perspektif Hukum Teknologi dan Hukum Pidana, Semarang 6-7 Juni 2007, hal.6.

b. melakukan konstruksi hukum yang konseptual/substansial (*substansial legal construction*) dalam menghadapi kendala juridis;

c. meningkatkan budaya/orientasi keilmuan (*scientific culture/scientific approach*) dalam proses pembuatan dan penegakan hukum pidana.

3. Upaya melakukan pembaharuan/rekonstruksi pemikiran yuridis (butir nomor 2 di atas) seyogyanya dilakukan untuk semua bidang penegakan hukum pidana. Namun terutama diperlukan dalam menghadapi masalah *cybercrime* (CC) karena CC tidak dapat disamakan dengan tindak pidana konvensional, sehingga tidak bisa dihadapi dengan penegakan hukum dan pemikiran/konstruksi hukum yang konvensional.

Selain ke 3 (tiga) langkah-langkah diatas, sebagai upaya dalam rangka penanggulangan tindak pidana teknologi informasi di massa yang akan datang terdapat beberapa hal yang dilakukan oleh aparat penegak hukum:

a. Mendidik para aparat penegak hukum

Dalam hal menangani kasus *cybercrime* diperlukan Spesialisasi terhadap aparat penyidik maupun penuntut umum dapat dipertimbangkan sebagai salah satu cara untuk melaksanakan penegakan hukum terhadap *cybercrime*. Spesialisasi tersebut dimulai dari adanya pendidikan yang diarahkan untuk menguasai teknis serta dasar-dasar pengetahuan di bidang komputer dan profil *hacker*.

Saat ini Indonesia sangat membutuhkan Polisi *Cyber*, Jaksa *Cyber*, Hakim *Cyber* dalam rangka penegakan hukum *cybercrime* di Indonesia tanpa adanya penegak hukum yang mempuni di bidang teknologi informasi, maka akan sulit menjerat penjahat-penjahat cyber oleh karena kejahatan *cyber* ini *locos delicti*-nya bisa lintas negara.

Hal yang lebih penting dalam upaya penegakan hukum adalah adanya sosialisasi berupa penataran, kursus atau pun kejuruan bersama antara aparat penegak hukum dalam rangka persamaan presepsi dalam prosedur pembuktian terhadap kasus tindak pidana teknologi informasi.

b. Membangun fasilitas *forensic computing*

Fasilitas *forensic computing* yang akan didirikan Polri diharapkan akan dapat melayani tiga hal penting, yaitu:

a. evidence collection;

b. forensic analysis;

c. expert witness.

Peningkatan sarana atau fasilitas dalam penanggulangan tindak pidana teknologi informasi tidak hanya terbatas dengan berusaha semaksimal mungkin untuk meng -*up date* dan *up grade* sarana dan prasarana yang sudah dimiliki oleh aparat penegak hukum tetapi juga dengan melengkapi sarana atau fasilitas tersebut sesuai dengan perkembangan teknologi dewasa ini. Oleh karenanya diperlukan tenaga yang terampil serta biaya terutama untuk mendukung kemampuan dan keterampilan aparat penegak hukum di bidang komputer.

Fasilitas tersebut juga hendaknya tidak hanya melibatkan Polri saja tetapi pihak Pemerintah melalui departemen komunikasi dan informasi membangun fasilitas sendiri yang berfungsi sebagai pusat informasi atau laboratorium sebagai mana layaknya laboratorium forensik sebagai tempat penelitian bagi kepentingan penyidikan dan pengembangan teknologi informasi.

c. Meningkatkan upaya penyidikan

Karena tindak pidana yang diatur UU ITE adalah tindak pidana khusus, maka diperlukan penyidik yang khusus pula. Pasal 43 UU ITE menyatakan, selain polisi, wewenang penyidikan berada di pundak Pejabat Pegawai Negeri Sipil (PPNS). Meski tak terang-terangan menyebut Depkominfo, UU ini menjabarkan bahwa PPNS itu berasal dari lingkungan pemerintah yang bertugas di bidang TI dan Transaksi Elektronik.

Sebagai sarana untuk menghadapi *cyberterorrism* aparat penegak hukum hendaknya membentuk satuan tugas bersama seperti yang dilakukan oleh Negara Jepang dengan membentuk *Cyber Task Force* pada bulan April 2001. Peran dari *Cyber Task Force* tersebut adalah untuk Mencegah serta merespon keadaan darurat agar kerugian / resiko akibat serangan pada Sistim Informasi terhadap infra struktur kritis seminimal mungkin.

Pembentukan *cyber task force* tersebut tidak hanya melibatkan Polri tetapi juga PPNS, Jaksa dan juga hakim yang ruang lingkupnya mulai dari tingkat pusat hingga ke provinsi dan juga kabupaten-kabupaten Upaya kerjasama tidak hanya dilakukan dengan sesama aparat penegak hukum *cyber* tetapi juga meminta bantuan ahli yang diperlukan dalam penyidikan. “Ahli” yang dimaksud di sini tentu saja adalah seseorang yang memiliki keahlian khusus di bidang TI dan harus bisa dipertanggungjawabkan secara akademis maupun praktis.

d. Kerja sama Internasional

Melakukan kerjasama dalam melakukan penyidikan kasus kejahatan *cyber* karena sifatnya yang *borderless* dan tidak mengenal batas wilayah, sehingga kerjasama dan koordinasi dengan aparat penegak hukum negara lain merupakan hal yang sangat penting untuk dilakukan. Sebagai contoh perlu dibentuknya jaringan investigasi kejahatan di dunia maya, jaringan ini

akan memudahkan polisi di berbagai belahan dunia melakukan identifikasi dan mendapatkan bantuan dari investigator dari negara lain.

Kerjasama internasional juga meliputi perjanjian kerjasama diantara negara-negara baik dalam hal "*mutual assistance*", ekstradisi maupun dalam hal pembantuan dalam upaya menghadirkan korban yang berada diluar teritorial negara. Sebagai upaya lebih efektif dan efesiensi waktu hendaknya dalam upaya pembaharuan hukum pemeriksaan korban dan saksi dalam tindak pidana teknologi informasi dapat dilakukan melalui cara *e-mail* atau *messengger* yang ditandatangani dengan tanda tangan digital sebagai sahnya penyidikan, serta pemeriksaan berupa *teleconfrence* dalam persidangan di pengadilan.

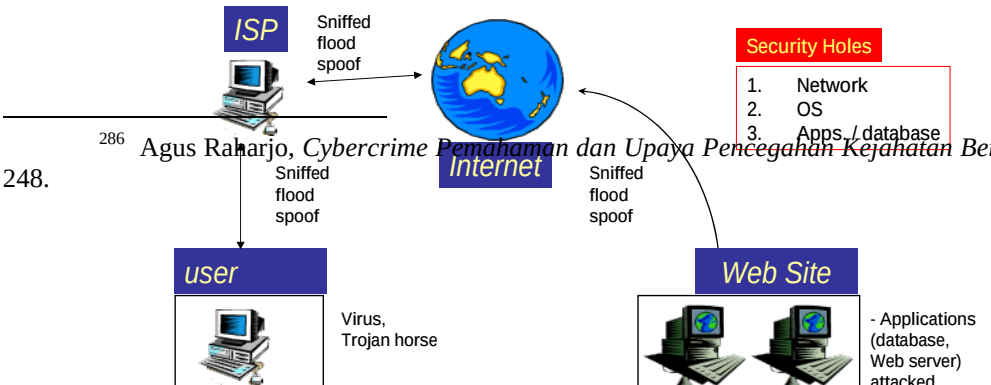
C.3.2 Upaya Pengamanan Sistem Informasi

Salah satu langkah lagi agar penanggulangan *cybercrime* ini dapat dilakukan dengan baik, maka perlu dilakukan kerja sama dengan *Internet Service Provider* (ISP) atau penyedia jasa internet. Meskipun *Internet Service Provider* (ISP) hanya berkaitan dengan layanan sambungan atau akses Internet, tetapi *Internet Service Provider* (ISP) memiliki catatan mengenai ke luar atau masuknya seorang pengakses, sehingga ia sebenarnya dapat mengidentifikasikan siapa yang melakukan kejahatan dengan melihat log file yang ada.[286]

Tipologi terhadap upaya pengamanan sistem informasi meliputi berbagai aspek yang berorientasi terhadap perlindungan jaringan informasi baik yang dilakukan secara personal maupun dilakukan oleh penyedia jasa informasi. Hal tersebut dapat dilihat dari gambar di bawah ini:

Gambar.3

Pengamanan Sistem Informasi



[286] Agus Raharjo, *Cybercrime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, Op.Cit.,, hal. 248.

Bertolak dari gambar.3 di atas, ada beberapa cara yang dapat digunakan untuk mengamankan sistem informasi berbasis internet yang telah dibangun yaitu:[287]

1. Mengatur akses (*access control*).

   Salah cara yang umum digunakan untuk mengamankan informasi adalah dengan mengatur akses ke informasi melalui mekanisme *authentication* dan *access control.* Implementasi dari mekanisme ini antara lain dengan menggunakan *password*. Di sistem UNIX dan Windows NT, untuk masuk dan menggunakan sistem computer,pemakai harus melalui proses *authentication* dengan menuliskan userid (*user identification*) dan *password*. Apabila keduanya valid, maka pemakai diperbolehkan untuk masuk dan menggunakan sistem, tetapi apabila di antara keduanya atau salah satunya tidak valid, maka akses akan ditolak. Penolakan ini tercatat dalam berkas log berupa waktu dan tanggal akses, asal hubungan (*connection*) dan berapa kali koneksi yang gagal itu. Setelah proses *authentication*, pemakai diberikan akses sesuai dengan level yang dimilikinya melalui sebuah *access control*. *Access control* ini biasanya dilakukan dengan mengelompokkan pemakai

[287] Agus Raharjo, *Cybercrime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, Op.Cit.,, hal. 252-260.

dalam sebuah grup, seperti grup yang berstatus pemakai biasa, tamu dan ada pula administrator atau disebut juga superuser yang memiliki

kemampuan lebih dari grup lainnya. Pengelompokan ini disesuaikan dengan kebutuhan dari penggunaan sistem yang ada.

2. Menutup service yang tidak digunakan

   Seringkali dalam sebuah sistem (perangkat keras dan atau perangkat lunak) diberikan beberapa servis yang dijalankan sebagai default, seperti pada sistem UNIX yang sering dipasang dari vendor-nya adalah *finger*, telnet, ftp, smtp, pop, echo dan sebagainya. Sebaiknya servis-servis ini kalau tidak dipakai dimatikan saja. Karena banyak kasus terjadi yang menunjukkan *abuse* dari servis tersebut atau ada lubang keamanan dalam servis tersebut. Akan tetapi administrator sistem tidak menyadari bahwa servis tersebut dijalankan di komputernya.

3. Memasang Proteksi

   Proteksi ini bisa berupa filter (secara umum) dan yang lebih spesifik lagi adalah firewall. Filter ini dapat digunak untuk memfilter e-mail, informasi, akses atau bahkan dalam level packet. Sebagai contoh, di sistem UNIX ada paket program *topwrapper* yang dapat digunakan untuk membatasi akses kepada servis atau aplikasi tertentu. Misalnya, servis untuk telnet dapat dibatasi untuk sistem yang memiliki nomor IP tertentu atau memiliki domain tertentu. Sementara firewall digunakan untuk melakukan filter secara umum. Ada juga program filter internet yang bernama ZeekSafe. Program ini bisa memblokir situs-situs yang tidak diinginkan. Selain itu, ada juga program filter yang lain, yaitu We- Blocker, sama dengan ZeekSafe,

program ini bisa menentukan parameter apa saja yang akan membatasi akses ke website yang dianggap tidak layak dilihat.

4. *Firewall*

   Program ini merupakan perangkat yang diletakkan antara internet dengan jaringan internal. Informasi yang ke luar dan masuk harus melalui *firewall* ini.Tujuan utama dari firewall adalah untuk menjaga (prevent) agar akses (ke dalam maupun ke luar) dari orang tidak berwenang (*unauthorized access*) tidak dapat dilakukan. Firewall bekerja dengan mengamati paket Internet Protocol (IP) yang melewatinya. Berdasarkan konfigurasi dari *firewall*, maka akses dapat diatur berdasarkan *Internet Protocol (IP) address*, port dan arah informasi.

5. Pemantau adanya serangan

   Sistem pemantau (*monitoring system*) digunakan untuk mengetahui adanya tamu tidak diundang (intruder) atau adanya serangan *(attack).* Nama lain dari simtem ini adalah *Intruder Detection System* (IDS). Sistem ini dapat memberi tahu administrator melalui email maupun melalui mekanisme lain seperti pager. Ada beberapa cara untuk memantau adanya intruder, baik yang sifatnya aktif maupun pasif. *Intruder Detection System* (IDS) cara yang pasif misalnya dengan *memonitor log file*. Contoh *Intruder Detection System* (IDS) adalah, Pertama, *Autobuse*, mendeteksi probing dengan memonitor log file. Kedua, *Courtney* dan *portsentry* adalah mendeteksi probing (*port scanning*) dengan memonitor *packet* yang lalu-lalang. *Portsentry* bahkan dapat memasukkan Internet Protocol (IP) penyerang dalam filter *topwrapper*. Ketiga, *Shadow* dari SANS. Keempat, Snort, mendeteksi pola (pattern) pada paket yang lewat dan mengirimkan alert jika pola tersebut terdeteksi. Pola-pola atau rules

disimpan dalam berkas yang disebut library yang dapat dikonfigurasi sesuai dengan kebutuhan.

6. Pemantau integritas sistem

   Sistem ini dijalankan secara berkala untuk menguji integritas sistem. Salah satu contoh program yang umum digunakan di sistem UNIX adalah program *Tripwire*. Program ini dapat digunakan untuk memantau adanya perubahan pada berkas. Pada mulanya program ini dijalankan dan membuat data base mengenai berkas-berkas atau direktori yang ingin kita amati beserta *signature* dari berkas tersebut. *Signature* berisi informasi mengenai besarnya berkas, kapan dibuatnya, pemiliknya, hasil checksum atau hash dan sebagainya. Apabila ada perubahan pada berkas tersebut, maka keluaran dari hash function akan berbeda dengan yang ada di data base sehingga ketahuan adanya perubahan.

7. Audit: Mengamati berkas log

   Segala kegiatan penggunaan sistem dapat dicatat dalam berkas yang biasanya disebut *log file* atu *log* saja. Berkas log ini sangat berguna untuk mengamati penyimpanan yang terjadi. Kegagalan untuk masuk ke sistem (login) misalnya tersimpan dalam berkas log. Untuk itu pada administrator diwajibkan untuk rajin memelihara dan menganalisis berkas log yang dimilikinya.

8. *Back up* secara rutin

   Sering kali intruder masuk dalam sistem dan merusak sistem dengan menghapus berkasberkas yang ditemui. Jika intruder ini berhasil menjebol sistem dan masuk sebagai superuser, maka ada kemungkinan dia dapat menghapus seluruh berkas. Untuk itu, adanya back up yang digunakan secara rutin merupakan hal yang esensial.

9. Penggunaan enkripsi untuk meningkatkan keamanan

   Salah satu mekanisme untuk meningkatkan keamanan adalah dengan menggunakan teknologi enkripsi. Data-data yang dirimkan diubah sedemikian rupa sehingga tidak mudah disadap. Banyak servis di internet yang masih menggunakan plain text untuk authentication seperti penggunaan pasangan userid dan password. Informasi ini dapat dilihat dengan mudah dengan program penyadap atau pengendus (*sniffer*). Untuk meningkatkan keamanan *server world wide web* dapat digunakan enkripsi pada tingkat socket. Dengan menggunakan enkripsi, orang tidak bisa menyadap data-data (transaksi) yang dikirimkan dari /ke server WWW. Salah satu mekanisme yang cukup populer adalah dengan menggunakan Secure Socket Layer (SSL) yang mulanya dikembangkan oleh Netscape. Selain server WWW dari Netscape dapat juga dipakai server WWW dari Apache yang dapat dikonfigurasi agar memiliki fasilitas *Secure Socket layer* (SSL) dengan menambahkan *software* tambahan (SSLeay-*implementasi Secure Socket Layer* (SSL) dari *Eric Young* atau *Open Secure Socket Layer* (SSL). Penggunaan *Secure Socket Layer* (SSL) memiliki permasalahan yang bergantung kepada lokasi dan hukum yang berlaku. Hal ini disebabkan pemerintah melarang ekspor teknologi enkripsi (kriptografi) dan paten *Public Key Partners* atas *Rivest-Shamir-Adleman* (RSA) *public key cryptography* yang digunakan pada *Secure Socket Layer* (SSL). Oleh karena itu, implementasi *SSLeay Eric Young* tidak dapat digunakan di Amerika Utara (Amerika dan Kanada) karena melanggar paten Rivest-Shamir-Adleman (RSA) dan RC4 yang digunakan dalam implementasinya.

10. *Telnet* atau *shell* aman

Telnet atau remote login yang digunakan untuk mengakses sebuah remote site atau computer melalui sebuah jaringan computer. Akses ini dilakukan dengan menggunakan hubungan TCP/IP dengan menggunakan userid dan password. Informasi tentang userid dan password ini dikirimkan melalui jaringan komputer secara terbuka. Akibatnya kemungkinan password bisa kenak sniffing. Untuk menghindari hal ini bisa memakai enkripsi yang dapat melindungi adanya sniffing. Selain itu bisa juga memakai firewall, alat ini untuk melindungi data-data penting. Akan tetapi sistem pengamanan yang telah dipaparkan di atas tadi tidak menjamin aman 100% (seratus persen), oleh karena itu dianjurkan untuk terus memantau perkembangan sistem pengamanan internet.

Upaya pengamanan sistem informasi di atas erat hubungannya dengan teknologi, khususnya teknologi komputer dan telekomunikasi sehingga pencegahan *cybercrime* dapat digunakan melalui saluran teknologi atau disebut juga *techno-prevention*. Langkah ini sesuai dengan apa yang telah diungkapkan oleh *International Information Industri Congress* (IIIC) sebagai berikut:[288]

> *The IIIC recognizes that government action and internasional treaties to harmonize laws and coordinate legal procedures are keying the fight cybercrime, but warns that these should not be relied upon as the only instrument. Cybercrime is enabled by technology and requires as healty reliance on technology for its solution.*

Pendekatan teknologi ini merupakan subsistem dalam sebuah sistem yang lebih besar, yaitu pendekatan budaya, karena teknologi merupakan hasil dari kebudayaan atau merupakan kebudayaan itu sendiri. Pendekatan budaya atau cultural ini perlu dilakukan untuk membangun atau membangkitkan kepekaan warga masyarakat dan aparat penegak hukum terhadap masalah

[288] Barda Nawawi Arief, *Beberapa Aspek Kebijakan Penegakan dan Pengembangan Hukum Pidana*, PT Citra Aditya Bakti, Bandung: 1998, hal. 5.

cybercrime dan menyebarluaskan atau mengajarkan etika penggunaan komputer melalui media pendidikan.

BAB IV

PENUTUP

A. KESIMPULAN

Bertolak dari perumusan masalah dan uraian hasil penelitian dan analisa yang dikemukakan pada bab-bab sebelumnya, maka dalam tesis ini dapat ditarik kesimpulan sebagai berikut:

1. 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 kriminalisasi-nya 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. Perkembangan kejahatan mayantara ini perlu didukung oleh undang-undang *cyber* yang bersifat komprehensif

dengan berbagai undang-undang lainnya sehingga tercipta kepastian hukum dan kejelasan hukum dalam menanggulangi tindak pidana *cyber* tersebut.

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 UU ITE ditemukan hal-hal sebagai berikut:

a) 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.*
b) 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 dari pembedaan antara ”kejahatan” dan ”pelanggaran”. Penetapan kualifikasi yuridis ini mutlak diperlukan karena sistem pemidanaan di luar KUHP merupakan sub/bagian integral dari keseluruhan sistem pemidanaan.
c) Penerapan sanksi pidana secara kumulatif bersifat imperatif dan kaku, karena perumusan tindak pidana kedua subjek hukum 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.

d) 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.

e) 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. Hendaknya dibuat suatu aturan khusus dalam UU ITE yang mengatur pertanggungjawaban korporasi terutama mengenai aturan terhadap korporasi yang tidak dapat membayar denda.

2. Kebijakan kebijakan aplikatif yang dilakukan oleh aparat penegak hukum dalam upaya penanggulangan tindak pidana teknologi informasi

Penegakan hukum dalam *cyberspace* membutuhkan sinergi antara masyarakat yang partisipatif dengan aparat penegak hukum yang demokratis, transparan, bertanggung jawab dan

berorientasi pada HAM, pada alirannya diharapkan dapat benar-benar mewujudkan masyarakat madani Indonesia yang berkeadilan sosial.

Penegak hukum di Indonesia mengalami kesulitan dalam menghadapi merebaknya *cybercrime* . Hal ini dilatarbelakangi masih sedikitnya aparat penegak hukum yang memahami seluk beluk teknologi informasi (internet), terbatasnya sarana dan prasarana, serta kurangnya kesadaran hukum masyarakat dalam dalam upaya penanggulangan tindak pidana teknologi informasi.

Diaturnya alat pembuktian informasi , dokumen elektronik dan tanda tangan elektronik yang dapat digunakan secara hukum diharapkan dapat memudahkan pelaksanaan penegakan hukum terhadap tindak pidana teknologi informasi di Indonesia, tetapi hal tersebut harus didukung dengan pengetahuan dan keterampilan, serta kerja sama antara aparat penegak hukum baik lingkup regional maupun internasional mengingat tindak pidana *cybercrime* yang *borderless.*

Yurisdiksi *cyberspace* sangat berpengaruh dalam penegakan hukum, mengingat jarak, biaya dan kedaulatan masing-masing negara. Oleh karena itu dibutuhkan kerjasama Internasional baik secara *mutual assistance,* perjanjian ekstradisi dan kesepakatan atau kerjasama dengan negara-negara lain terkait kejahatan *cybercrime* dalam upaya penegakan hukum dalam menanggulangi tindak pidana teknologi informasi.

3. Kebijakan formulasi dan kebijakan aplikatif hukum pidana dalam penanggulangan tindak pidana teknologi informasi di masa yang akan datang.

Kebijakan formulasi tindak pidana teknologi informasi harus memperhatikan harmonisasi internal dengan sistem hukum pidana atau aturan pemidanaan umum yang berlaku saat ini. Tidaklah dapat dikatakan harmonisasi/sinkronisasi apabila kebijakan formulasi berada diluar

sistem. Oleh karena itu kebijakan formulasi hukum pidana tindak pidana teknologi informasi pada masa yang akan datang harus berada dalam sistem hukum pidana yang berlaku saat ini.

Berdasarkan kajian perbandingan hukum (yuridis komparatif) pengaturan *cybercrime* dari beberapa negara di dunia dibutuhkan evaluasi kebijakan kriminalisasi berupa perubahan dan penyusunan delik-delik baru terhadap kebijakan kriminalisasi tindak pidana teknologi informasi pada masa yang akan datang, yaitu: Ketentuan khusus terhadap perlindungan anak, Pengaturan lebih jelas terhadap virus komputer, Pengaturan terhadap *spamming,* Pengaturan terhadap *cyberterrorism.*

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.

Pertanggungjawaban 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 hukum pidana, adalah sebagai berikut:

1. Kebijakan kriminalisasi terhadap perbuatan dalam dunia maya harus terus diharmonisasikan seiring maraknya kejahatan di dunia *cyber* yang semakin canggih.

Hal ini disebabkan tindak pidana teknologi informasi yang tidak mengenal batas-batas teritorial dan beroperasi secara maya oleh karena itu menuntut pemerintah harus selalu berupaya mengantisipasi aktivitas-aktivitas baru yang diatur oleh hukum yang berlaku.

2. Perlu Aturan pemidanaan terhadap penyertaan, percobaan, dan pengulangan (*residive*) terhadap tindak pidana teknologi informasi. Pemidanaan yang sama terhadap penyertaan dan pencobaan serta ada pemberatan terhadap perbuatan pengulangan dimaksudkan 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 korporasi.
4. Meningkatkan komitmen strategi/prioritas nasional terutama aparat penegak hukum dalam penanggulangan kejahatan di dunia maya oleh karena itu pembentukan *cyber task force* dari lingkup pusat hingga ke daerah perlu dipertimbangkan agar ada satuan tugas khusus yang menangani kasus-kasus *cybercrime* seperti layaknya kasus korupsi, terorisme, narkoba dan sebagainya.
5. Mengingat yurisdiksi *cybercrime* bersifat *transnational 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

A. BUKU

Adi, Rianto, *Metode Penelitian Sosial dan Hukum*, PT Grafika, Jakarta, 2004

Ardhiwisastra,Yudha Bhakti, *Imunitas Kedaulatan Negara di Forum Pengadilan Asing*, Alumni Bandung, 1999

Badan Pembinaan Hukum Nasional, *Perkembangan Pembangunan Hukum Nasional tentang Hukum Teknologi dan Informasi*, BPHN Departemen Kehakiman RI, 1995/1996

Black ,Henry Campbell,*Black's Law Dictionary*", third edition.

----------,*Black's Law Dictionary, Seventh Edition*, St.Paulmin West Publicing,Co.,1999

Departemen Pendidikan dan Kebudayaan, Kamus Besar Bahasa Indonesia,Cet.II,Balai Pustaka,Jakarta,1997

Didik J.Rachbini,*"Mitos dan Implikasi Globalisasi"* : Catatan Untuk Bidang Ekonomi dan Keuangan, Pengantar edisi Indonesia dalam Hirst, Paul dan Grahame Thompson, Globalisasi adalah Mitos, Jakarta, Yayasan Obor,2001

Didik M.Arif Mansur dan Alistaris Gultom, , *Cyber Law;Aspek Hukum Teknologi Informasi*, Refika Aditama,Bandung,2005

Djindang, Moh. Saleh dan Utrecht, E., *Pengantar dalam hukum Indonesia*, cetakan kesebelas, penerbit P.T. Ichtiar Baru dan Penerbit Sinar Harapan, Jakarta, 1989

Edmon Makarim,*Kompilasi Hukum Telematika*,Raja Grafindo Persada, Jakarta,2003

Emong Supardjaja,Komariah, *Ajaran Sifat Melawan Hukum Materiel dalam Hukum Pidana Indonesia*, Alumni, Bandung, 2002

Farouk Muhammad dan H. Djaali, *Metodologi Penelitian Sosial (Bunga Rampai*), Penerbit PTIK Press, Jakarta, 2003

Gillies, Peter ,*Criminal Law, Second Edition, The Law Book*, Syney, 1990

Graner, Bryan A., *Black's Law Dictionary Eighth Edition*. St. Paul: West Thomson, 2004

Gregg, Michael, *Certified Ethical Hacker Exam Prep,* United States of America: Que Publishing, 2006

Hamzah, Andi, *Aspek-Aspek Pidana di Bidang Komputer*, 1998

----------, *Hukum Acara Pidana Indonesia*, Sinar Grafika, Jakarta, 2005

Harahap, M.Yahya, *Pembahasan Permasalahan Dan Penerapan KUHAP: Pemeriksaan Sidang Pengadilan, Banding, Kasasi, dan Peninjauan Kembali*, Edisi Kedua, Sinar Grafika, Bandung,2000

Hinderich, Ted, Punishment:*The Supposed Justifications*,London: Pegun Books,1976

Horton, Paul B dan Chester L.Hunt, *Sosiologi*, Erlangga, Jakarta, 1984

Ikhwansyah, Isis, *Prinsip-Prinsip Universal Bagi Kontak Melalui E-Commerce dan Sistem Hukum Pembuktian Perdata dalam Teknologi Informasi, dalam Cyberlaw: Suatu Pengantar*, ELIPS, Bandung,2002

Kamarga, Hanny, *Belajar Sejarah Melalui E-Learning : Alternatif Mengakses Sumber Informasi Kesejarahan*, PT Intimedia, Jakarta, 2002

Kemal Dermawan, Mohammed, *Strategi Pencegahan Kejahatan*, Citra Aditya Bhakti, Bandung, 1994

M. Moelijono, Anton, (et.al).Kamus Besar Bahasa Indonesia, Balai Pustaka, Jakarta,1998

M. Ramli, Ahmad, *Cyber Law dan HAKI Dalam Sistem Hukum Indonesia*, PT Refika Aditama, Bandung,2006

Makarim, Edmon, *Kompilasi Hukum Telematika*, Rajagrafindo Persada, Jakarta, 2003

Moeljatno, *Asas-Asas Hukum Pidana*, Cetakan.VI, Rineka Cipta, Jakarta, 2000

Moh.Mahfud,MD, *Pergulatan Politik dan Hukum di Indonesia*, Gama Media, Yogyakarta,1999.

Muladi dan Nawawi Arief, Barda, *Teori-Teori dan Kebijakan Pidana*, Alumni, Bandung, 1998

Muladi, Demokratisasi,*Hak Asasi Manusia dan Reformasi Hukum di Indonesia*, The Habibie Center, Jakarta,2002

---------, Kapita Selekta Sistem Peradilan Pidana, UNDIP,Semarang,1995

Nawawi Arief, Barda, *Beberapa Aspek Kebijakan Penegakan dan Pengembangan Hukum Pidana*, PT Citra Aditya Bakti, Bandung: 1998

----------, *Kapita Selekta Hukum Pidana*, PT.Citra Aditya Bakti, Bandung,2003

----------, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*, Kencana Prenada Media Group, Jakarta, 2007

---------- *Pembaharuan Hukum Pidana Dalam Perspektif Kajian Perbandingan*, PT. Citra Aditya Bakti, Bandung,2005

----------, *Sari Kuliah: Perbandingan Hukum Pidana,* PT. Raja Grafindo Persada, Jakarta, 2006

----------, *Tindak Pidana Mayantara*, Raja Grafindo Persada, Jakarta, 2006

O.S. Hiariej, Eddy dkk, *Bunga Rampai Hukum Pidana Khusus*, Pena Pundi Aksara, Jakarta: 2006

Oxford, *Learners Pocket Dictionary Third Edition*, Oxford *University Press*

Parthina, I Wayan, *Ekstradisi dalam Hukum Internasional dan Hukum Nasional Indonesia*, Mandar Maju, Bandung, 1990

Prasetyo,Teguh dan Barkatullah,Abdul Halim, *Politik Hukum Pidana: Kajian Kebijakan Kriminalisasi dan Dekriminalisasi*, Pustaka Pelajar, Yogyakarta, 2005

Prodjodikoro, Wirjono, *Asas-asas Hukum Pidana di Indonesia*, Refika Aditama, Bandung, ,2003

R. Richards, James, *Transnational Criminal Organizations, cybercrime and Money Laundering; A Handbook for law Enforcement Officers, Auditors and Financial Investigators,* CRC Press, London New Work Washington, D.C,1999

Rahardjo, Agus, *Cybercrime pemahaman dan upaya pencegahan kejahatan berteknologi*, PT.Citra Aditya Bakti, Bandung, 2002

Rahardjo, Satjipto, *Masalah Penegakan Hukum, Suatu Tinjauan Sosiologis,* Badan Pembinaan Hukum Nasional Departemen Kehakiman, Jakarta, 1983

----------, *Hukum dan Masyara*kat,Angkasa, Bandung,1980

----------, Ilmu Hukum, PT.Citra Aditya Sakti, Bandung, 1991

Rahman Nitibaskara, Tubagus Ronny, *Ketika Kejahatan Berdaulat: Sebuah Pendekatan Kriminologi, Hukum dan Sosiologi*,Peradaban, Jakarta,2001

Reksodiputro, Marjono, *Kemajuan Pembangunan Ekonomi dan Kejahatan. Kumpulan karangan buku kesatu*, Pusat Pelayanan Keadilan dan Pengabdian Hukum, Jakarta, 1994

Remmelink, Jan, *Hukum Pidana: Komentar atas Pasal-Pasal Terpenting dari Kitab Undang-undang Hukum Pidana Belanda dan Padanannya dalam Kitab Undang-undang Hukum Pidana Indonesia,* PT Gramedia Pustaka Umum, Jakarta, 2003

Saleh, Roelan, *Sifat melawan hukum daripada perbuatan pidana* ,Badan Penerbit Gadjah Mada, 1962

Seno Adji,Indriyanto, *Korupsi Sistematik dan Kendala Penegak Hukum di Indonesia,* Jurnal Studi Kepolisian Perguruan Tinggi Ilmu Kepolisian, CV.Restu Agung, 2005

Serikat Putra Jaya, Nyoman, *Bahan Kuliah Sistem Peradilan Pidana*, Program Magister Ilmu Hukum, Undip,2006

----------, *Beberapa Pemikiran ke Arah Pengembangan Hukum Pidana*, PT.Citra Aditya Bakti, Bandung, 2008

Sianturi, S.R, *Asas-asas Hukum Pidana di Indonesia dan Penerapannya,* Alumni Ahaem – Petehaem, Jakarta,1989

Singara, Julius , *Memoire : la cryptologie et la preuve électronique de la France à l'Indonésie*, D.E.A. *Informatique et Droit, Université Montpellier I, année universitaire*, Montpellier, 2003-2004

Soekanto, Soerjono dan Mamuji, Sri, *Penelitian Hukum Normatif 'Suatu Tinjauan Singkat*', PT. Raja Grafindo Persada, Jakarta, 2004

Soekanto, Soerjono, *Faktor-faktor yang Mempengaruhi Penegakan Hukum*, PT.Raja Grafindo Persada, Jakarta, 2005

Soesilo R., *RIB/HIR dengan penjelasan*, Politeia, Bogor, 1995

Stephenson, Peter, *Investigating Computer-Related Crime: A Hanbook For Corporate Investigators* CRC Press, London ,New York Washington D.C:2000

Subekti, *Hukum Pembuktian*, Pradnya Paramita, Jakarta, 1995

Subroto, Wisnu, *Kebijakan Hukum Pidana dalam Penanggulangan Penyalahgunaan Komputer* Universitas Atmajaya, Yogyakarta, 1999

Sudarto, *Hukum Pidana I,*Yayasan Sudarto, Semarang, 1990

----------, Kapita Selekta Hukum Pidana, Alumni, Bandung, 1986

----------, Hukum dan Hukum Pidana, Penerbit Alumni, ,Bandung , 1977

Sukarmi, *Cyberlaw:Kontrak Elektronik dalam Bayang-Bayang Pelaku Usaha*,Pustaka Sutra, 2007

Susanto, I.S *,Tinjauan Kriminologi Terhadap Perilaku Menyimpang dalam Kegiatan Ekonomi Masyarakat dan Penanggulangannya, "Makalah seminar Nasional Peranan Hukum Pidana dalam Menunjang Kebijaksanaan Ekonomi,* Semarang, Fakultas Hukum Universitas Undip, 2007

Sutanto, Hermawan Sulistyo, dan *Cybercrime-Motif dan Penindakan*, Pensil 324, Jakarta, 2002

Sutarman, *Cybercrime* : *Modus Operandi dan Penanggulangannya*, Laksbang Pressindo, Jogjakarta, 2007

Taufik Makarao, Mohammad, dan Suhasril, *Hukum Acara Pidana dalam Teori dan Praktek*, Penerbit Ghalia Indonesia, Jakarta, 2000

Tien S, Saefulah, Jurisdiksi sebagai Upaya Penegakan Hukum dalam Kegiatan *Cyberspace*, artikel dalam Cyberlaw: Suatu Pengantar, Pusat Studi Cyber Law Fakultas Hukum UNPAD,ELIPS,2002

Wahib, Abdul dan Labib, Mohammad, *Kejahatan Mayantara* (*Cybercrime*), *Kejahatan Mayantara* (*Cybercrime*), Refika Aditama, Bandung , 2005

Zalesky, Jeff, *Spritualitas Cyberspace, Bagaimana Teknologi Komputer Mempengaruhi Kehidupan Keberagaman Manusia*, Mizan, Bandung, 1999

B. ARTIKEL, MAKALAH

Agus Raharjo, *Cyber crime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, PT. Citra Aditya Bakti, Bandung, 2002

Atmasasmita, Romli , *Ruang Lingkup Berlakunya Hukum Pidana terhadap Kejahatan Transnasional Terorganisasi*, artikel dalam Padjajaran Jilid XXIV No.2 tahun 1996

Bellefroid, *Inleidag tot de Rechtswetenschap in Nederland*, 1953.pg.17.Lihat dalam Moempoeni Martojo, *Politik Hukum dalam Sketsa*, Fakultas Hukum Undip, Semarang, 2000

Buletin Litbang Dephan, Kejahatan Mayantara (*Cybercrime*) *Dampak Perkembangan Teknologi Informasi "Dunia Maya"*, STT No. 2289 Volume VII Nomor 12 Tahun 2004

EU Convention on Cybercrime, lihat dalam Naskah Akademik Undang-Undang Informasi dan Transaksi Elektronik,2006

Golose, Petrus Reinhard, *Perkembangan Cybercrime dan Upaya Penanganannya di Indonesia Oleh Polri*, Makalah pada Seminar Nasional tentang "Penanganan Masalah *Cybercrime* di Indonesia dan Pengembangan Kebijakan Nasional yang Menyeluruh Terpadu", diselenggarakan oleh Deplu,BI, dan DEPKOMINFO, Jakarta, 10 Agustus 2006

Haris, Freddy , *Cybercrimedari Persfektif Akademis*, Lembaga Kajian Hukum dan Teknologi Fakultas Hukum Universitas Indonesia

International Review of law Computers and Technology, 'Insider Cyber-Threat: Problems and Perspectives', Volume 14, 2001

ITAC,*" IIIC Common Views Paper On: Cybercrime"*, IIIC 2000 Millenium congress, September 19th, 2000

Laporan Kongres PBB ke-6,tahun 1981,lihat dalam Nawawi Arief, Barda, *Bunga Rampai Kebijakan Hukum Pidana*, PT. Citra Aditya Bakti, Bandung, 2005

M.Arife Mansur, Didik dan Gultom ,Alistaris, , *CyberLaw;Aspek Hukum Teknologi Informasi*, Refika Aditama,Bandung,2005

M.Ramli, Ahmad , *Perkembangan CyberLaw Global dan Implikasinya Bagi Indonesia*, Makalah Seminar The Importance of Information System Security in E-Government,Tim koordinasi Telematika Indonesia,Jakarta,28 Juli 2004

Majalah Warta Ekonomi No. 9, 5 Maret 2001.

Majalah *CyberTECH* , dengan judul "Steven Haryanto" ,6 November 2002

Majalah Gatra No.23 Tahun XIV17-23 April 2008

Muladi, *Kebijakan Kriminal terhadap Cybercrime* , Majalah Media Hukum, Vol.1 No.3 tanggal 22 Agustus 2003

Naskah Akademik Rancangan Undang-Undang Tentang Informasi dan Transaksi Elektronik, Departemen Komunikasi dan Informatika Republik Indonesia,2006

Naskah akademik RUU tindak pidana di bidang Teknologi Informasi disusun oleh Mas Wigantoro Roes Setiyadi , Cyber Policy Club dan Indonesia Media Law and Policy Center,2003

Nawawi Arief, Barda, *Prinsip-Prinsip Dasar atau Pedoman Perumusan/Formulasi Ketentuan Pidana dalam Perundang-undangan*, Makalah Perkuliahan Politik Hukum, Undip, 2007

----------, *"Kajian Kebijakan Hukum Pidana Menghadapi Perkembangan Delik Kesusilaan di Bidang Cyber*", Seminar *Cybercrime* dan *Cyber Porn* dalam Perspektif Hukum Teknologi dan Hukum Pidana, Semarang 6-7 Juni 2007

----------., *Antisipasi Penanggulangan "Cybercrime" dengan hukum Pidana*.,makalah pada seminar Nasional mengenai "*Cyber*law"., di STHB, Bandung, Hotel Grand Aquila, 9 April 2001

R. Nitibaskara, Tb. Ronny ,*Problem Yuridis Cybercrime* , Makalah pada Seminar tentang Cyber Law, diselenggarakan oleh Yayasan Cipta Bangsa, Bandung, 29 Juli 2000

Reinhard Golose, Petrus, *Penegakan Hukum Cybercrime dalam Sistem Hukum Indonesia* dalam *Handout* Seminar Pembuktian dan Penanganan Cybercrime di Indonesia, FHUI, Jakarta, 12 April 2007

----------, *Perkembangan Cybercrime dan Upaya Penanggulangannya di Indonesia Oleh Polri*, Buliten Hukum Perbankan dan Kebanksentralan, Volume 4 Nomor 2, Jakarta, Agustus 2006

S, Saefulah, Tien, *Jurisdiksi sebagai Upaya Penegakan Hukum dalam Kegiatan Cyberspace, artikel dalam Cyberlaw: Suatu Pengantar*, Pusat Studi *Cyberlaw* Fakultas Hukum UNPAD,ELIPS,2002

Seno Adji, Indriyanto, *Korupsi Sistematik dan Kendala Penegak Hukum di Indonesia*, Jurnal Studi Kepolisian Perguruan Tinggi Ilmu Kepolisian, CV.Restu Agung, 2005

Sutanto, Hermawan Sulistyo, dan Tjuk Sugiarto, *Cybercrime -Motif dan Penindakan*, Pensil 324, Jakarta

United Nations, *Eighth UN Congress on the Prevention of Crime and the Treatment of Offenders, Report*, 1991

C. SUMBER ELEKTRONIK

http//www.gipi.or.id

http://www.detik.com

www.bisnisindonesia.com

http://www.wikipedia.com

http://www.living*internet*.com/i/ii_ipto.htm

www.yahoo.com.

www.ristek.go.id

http://netforbeginners.minings.com

http://webopaedia.*internet*.com

http://www.total.or.id/info.php?kk=William%20Gibson

http://dictionary.cambridge.org

http://www.bartleby.com

http://www.lysator.liu.se/etexts/hacker.

yc1dav@garuda.drn.go.id

http://www.mttlr.org/volfour/menthe.html

http://conventions.coe.int

www.hukumonline.com

http://www.interpol.go.id

http://blog.washingtonpost.com/securityfix/2008/07/senate_approves_bill_to_fight.html

http://www.canlii.org/ca/sta/c-46/sec342.html

http://www.digitalcentury.com/encyclo/*update/articles.html*.

www.legalitas.org/database/rancangan/2005/BUKU%20KEDUA%20KUHP

http://www.mosstingrett.no/info/legal.html

http://www.solusihukum.com/artikel/artikel30.php

http://www.uq.edu.au/davidson/cyberlaw/april2002.html

http://www.qscl.org.au/

http://www.cybercrimes.net/Terrorism/ct.html

http://www.usip.org/pubs/specialreports/sr119.html

http://en.wikipedia.org/wiki/Cyber-terrorism

http://www.usip.org/pubs/specialreports/sr116.pdf

http://www.slais.ubc.ca/courses/libr500/04-05-wt1/www/X_Zhang/5ways.htm

D. PERATURAN

Computer Misuse Act of Singapore 1998

Council of Europe, European Treaty Series No.185,Budapest 23.IX.2001

Konsep KUHP 2006

Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi

Undang-Undang No.19 tahun 2002 tentang Hak Cipta

Undang-Undang No 15 Tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme

Undang-Undang No.11 tahun 2008 tentang Informasi dan Transaksi Elektronik Lembaran Negara No.58.

Undang-Undang No.8 Tahun 1981 tentang Kitab Undang-Undang Hukum Acara Pidana Lembaran Negara Republik Indonesia Nomor 76

Undang-Undang Nomor 2 tahun 2002 tentang Kepolisian Negara Republik Indonesia.

Undang-Undang No.25 Tahun 2003 tentang Pencucian Uang dalam Lembaran Negara Republik Indonesia Nomor 108.