UNIVERSITAS INDONESIA

FUNGSIONALISASI HUKUM PIDANA DALAM RANGKA PENANGGULANGAN KEJAHATAN MAYANTARA DI INDONESIA

TESIS

RISKI BAGUS PURWANTO
0606005542

FAKULTAS HUKUM
PROGRAM PASCA SARJANA
JAKARTA
JULI 2009

UNIVERSITAS INDONESIA

FUNGSIONALISASI HUKUM PIDANA DALAM RANGKA PENANGGULANGAN KEJAHATAN MAYANTARA DI INDONESIA

TESIS

Diajukan Sebagai Salah Satu Syarat Guna Memperoleh Gelar Magister Hukum

RISKI BAGUS PURWANTO
0606005542

FAKULTAS HUKUM
PROGRAM PASCA SARJANA
JAKARTA
JULI 2009

HALAMAN PERNYATAAN ORISINALITAS

Tesis ini adalah hasil karya sendiri dan semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar.

Nama	: Riski Bagus Purwanto
NPM	: 0606005542
Tanda Tangan	:  .....
Tanggal	: 9 Juli 2009

HALAMAN PENGESAHAN

Tesis ini diajukan oleh :
Nama : Riski Bagus Purwanto
NPM : 0606005542
Program Studi : Sistem Peradilan Pidana (Hukum Pidana)
Judul Tesis : FUNGSIONALISASI HUKUM PIDANA DALAM RANGKA PENANGGULANGAN KEJAHATAN MAYANTARA DI INDONESIA

Telah berhasil dipertahankan dihadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Magister Hukum pada Program Studi Sistem Peradilan Pidana, Fakultas Hukum, Universitas Indonesia.

DEWAN PENGUJI

Penguji (Ketua) :

.....
(Prof. H. Mardjono Reksodiputro, S.H.,M.A)

Pembimbing/Penguji :

.....
(Topo Santoso. S.H.,M.H PhD)

Penguji :

.....
(Dr. Surastini Fitriasih S.H., M.H)

Ditetapkan di : Jakarta

Tanggal : 9 Juli 2009

KATA PENGANTAR

بسم الله الرحمن الرحيم

Puji syukur saya panjatkan kepada ALLAH SWT, karena atas berkat dan rahmat-Nya, saya dapat menyelesaikan tesis ini. Penulisan tesis ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Magister Hukum Jurusan Hukum Pidana pada Fakultas Hukum Universitas Indonesia. Saya menyadari bahwa, tanpa bantuan dan bimbingan dari berbagi pihak, dari masa perkuliahaan sampai pada penyusunan tesisi ini, sangatlah sulit bagi saya untuk menyelesaikan tesis ini. Oleh karena itu, saya mengucapkan terima kasih kepada:

(1) Prof. Dr. der Soz. Drs. Gumilar Rusliwa Somantri selaku Rektor Universitas Indonesia;
(2) Prof. Safri Nugraha S.H, LL.M, Ph.D selaku Dekan Fakultas Hukum Universitas Indonesia;
(3) Prof. H Mardjono Resksodiputro S.H, MA selaku Ketua konsentrasi Hukum Pidana Universitas Indonesia;
(4) Topo Santoso S.H. M.H. Ph.D, selaku dosen pembimbing yang telah menyediakan waktu, tenaga, dan pikiran untuk mengarahkan saya dalam penyusunan tesis ini;
(5) Prof. Dr. Muladi yang telah banyak membantu dan memberi dorongan kepada penulis;
(6) Dr. Suharyono AR S.H M.H Departemen Hukum dan Ham yang telah banyak membantu dalam memperoleh data yang saya perlukan;
(7) Brigjend TNI Heru Cahyono SH MH, Oditur Jenderal TNI yang membantu dalam memberikan masukan-masukan yang diperlukan.
(8) Kombes Pol Drs.Petrus Golose M.M Kanit V IT dan Cybercrime Mabes Polri;
(9) Dosen, dan karyawan Progam studi Pidana Pasca sarjana Universitas Indonesia, yang telah memberikan dorongan kesempatan dan berbagai kemudahan kepada penulis selama mengikuti kuliah dan penulisan thesis.
(10) Penulis juga dengan bangga menyampaikan ucapan terimakasih yang mendalam kepada ayahanda tercinta Mayjend TNI H.Hari Krisnomo Sip Msc, Ibunda tercinta Ny. Sri Redjeki Ba, Kedua adinda tersayang drg.Wahyu Retnosari dan Sri Hartati Widyaningrum atas kesetiaan mendampingi penulis sehingga dapat menyelesaikan studi ini.
(11) Rekan dan sahabat yang telah banyak membantu baik moril dan materiil hingga selesainya penulisan thesis ini, semoga budi baiknya mendapat balasan yang setimpal dari ALLAH SWT.

Dengan segala kerendahan hati dan penuh kesadaran, penulis sangat menyadari bahwa karya ilmiah ini masih jauh untuk dikatakan karya ilmiah yang sempurna untuk itu penulis mengharapkan saran dan kritik yang bersifat konstruktif dari berbagai pihak.

Salemba, 9 Juli 2009

Riski Bagus Purwanto

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Universitas Indonesia, saya yang bertanda tangan di bawah ini:

Nama : Riski Bagus Purwanto
NPM : 0606005542
Program Studi : Sistem Peradilan Pidana
Fakultas : Hukum
Jenis Karya : Tesis

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Indonesia **Hak Bebas Royalti Noneksklusif (*Non-exclusive Royalty-Free Right*)** atas karya ilmiah saya yang berjudul :
"FUNGSIONALISASI HUKUM PIDANA DALAM RANGKA PENANGGULANGAN KEJAHATAN MAYANTARA DI INDONESIA."

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini Universitas Indonesia berhak menyimpan, mengalihmedia/ formatkan, mengelola dalam bentuk pangkalan data (database), merawat, dan memublikasikan tugas akhir saya tanpa meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta
Pada tanggal : 9 Juli 2009

Yang menyatakan

(Riski Bagus Purwanto)

ABSTRAK

Nama : Riski Bagus Purwanto (NPM: 0606005542)
Judul : Fungsionalisasi Hukum Pidana dalam Penanggulangan *Kejahatan Mayantara* di Indonesia

Perkembangan Internet dan umumnya dunia *cyber* tidak selamanya menghasilkan hal-hal yang positif. Salah satu hal negatif yang merupakan efek sampingan atau memang menjadi tujuan, antara lain adalah kejahatan di dunia *cyber* atau disebut kejahatan mayantara (*cyber crime)*. Dihadapkan dengan sistem hukum pidana di Indonesia, ada satu pertanyaan penting yang dapat diajukan. Apakah sistem hukum pidana ataupun perundang-undangan yang ada, sudah dapat menjangkau bentuk-bentuk kejahatan *cyber crime*. Untuk menjawab hal tersebut dilakukan dilakukan penelitian bersifat deskriptif, dengan metode penelitian hukum normatif. Berdasarkan penelitian ini disimpulkan penanggulangan kejahatan mayantara/*cyber crime* di Indonesia harus dilakukan dengan upaya penal yaitu dengan menggunakan sarana hukum dan sanksi pidana dan upaya non penal (tanpa menggunakan sanksi pidana). Meskipun secara substansial Indonesia belum memiliki undang-undang khusus tentang kejahatan mayantara/*cyber crime*. berbagai undang-undang yang sudah ada, telah difungsikan untuk menanggulangi bentuk-bentuk kejahatan mayantara/*cyber crime* Terhadap kejahatan *cyber crime* ini, hukum pidana Indonesia, telah difungsionalisasikan dalam menindak para pelaku kejahatan mayantara. Selanjutnya, terkait dengan *Locus delicti* (tempat terjadinya tindak pidana) kaitannya dengan aspek yurisdiksi kejahatan mayantara, masih menimbulkan permasalahan, karena hukum pidana Indonesia belum dapat menjangkau yuridiksi kejahatan mayantara yang dilakukan di luar wilayah Indonesia. Kedepan, sebaiknya penanggulangan dan penegakan hukum terhadap kejahatan mayantara pertama-tama harus dilakukan dengan menggunakan sarana penal. Untuk itu perlu diatur rumusan tindak pidana yang khusus mengatur mengenai bentuk-bentuk kejahatan mayantara/*cyber crime* dengan unsur-unsur tindak pidana yang lebih jelas dengan sanksi yang proporsional. Lebih lanjut, hal ini perlu didukung kesamaan persepsi dari aparat penegak hukum dalam memandang kejahatan mayantara. Selanjutnya, perlu dirumuskan di dalam RUU KUHP, tentang *locus delicti* (tempat terjadinya tindak pidana) dalam kaitannya dengan yurisdiksi yang berkaitan dengan kejahatan mayantara/*cyber crime* khususnya perlu diperluas rumusan mengenai tempat terjadinya tindak pidana.

Kata Kunci: Fungsionalisasi Hukum Pidana, Penanggulangan Kejahatan,Kejahatan Mayantara, Indonesia

ABSTRACT

Name : Riski Bagus Purwanto (NPM: 0606005542)
Title : Enforcement of Criminal Law on Response to Cyber Crime in Indonesia

Although cyber world has grown fast nowadays, we should consider its bad effect, one of the examples is called cyber crime. Related to the penal code in Indonesia, a question can be asked, has the penal code or the regulations in Indonesia reached out the cyber crime. To answer that question, a descriptive study has been done using a norm law method. The result of the study is that penal remedy, using legal facility and penal sanction and non penal remedy (without penal sanction), should be used to cope with the cyber crime in Indonesia. Even though Indonesia has no specific regulations about the cyber crime substantially, there are some regulations which are functioned to cope with the cyber crime and also the criminal. Related to *Locus delicti*, Indonesian law still has some problems about the cyber crime happens outside the Indonesia regional. In the future, it is recommended that the law enforcement use a penal remedy. Therefore, it is necessary to have a formula related to forms of cyber crime with the penal substance and the sanction which is proportional. Moreover, *locus delicti* should be incorporated in RUU KUHP concerning jurisdiction in cyber crime, especially an extended formula about the *Locus delicti* itself.

Keywords : Enforcement of Criminal Law, Response to Cyber Crime, Indonesia

DAFTAR ISI

BAB I
PENDAHULUAN

1.1. Latar Belakang

Perkembangan dan pemanfaatan teknologi informasi, media, dan komunikasi telah mengubah baik perilaku masyarakat maupun peradaban manusia secara global. Perkembangan teknologi informasi dan komunikasi telah pula menyebabkan hubungan dunia menjadi tanpa batas (*borderless*) dan menyebabkan perubahan sosial, ekonomi, dan budaya secara signifikan berlangsung demikian cepat. Pemanfaatan teknologi informasi di bidang ekonomi juga telah mengembangkan perekonomian ke arah *digital economy* yang tidak hanya berarti terselenggaranya sistem elektronik sebagai infrastruktur untuk kelancaran perdagangan, tetapi juga telah merubah perilaku masyarakat, yang semula melakukan pertukaran informasi dengan media kertas (*paper based*) menjadi berbasiskan media elektronik (*electronic based*).

Teknologi Informasi telah memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia. Namun, pada sisi yang lain teknologi informasi menjadi sarana efektif perbuatan melawan hukum. Seiring dengan perkembangan teknologi informasi dan komunikasi tersebut, saat ini tengah berkembang bidang hukum baru yang mengkaji dinamika konvergensi teknologi, yang populer dengan istilah *cyberlaw* atau hukum siber atau hukum telematika. Hukum siber atau *cyberlaw*, secara internasional digunakan untuk istilah hukum yang terkait dengan pemanfaatan teknologi informasi dan komunikasi. Demikian pula, hukum telematika yang merupakan perwujudan dari konvergensi hukum telekomunikasi, hukum media dan hukum informatika. Istilah lain yang juga digunakan adalah hukum teknologi informasi (*law of information technology*), hukum dunia maya (*virtual world law*), dan hukum mayantara.[1]

---

[1]Undang-Undang No 11 Tahun 2008 *Tentang Informasi dan Teknologi Elektronik*, Lembaran Negara 2008 Nomor 58, Penjelasan Umum.

Sejalan dengan perkembangan dan pemanfaatan teknologi informasi dan komunikasi yang telah melahirkan satu sistem hukum baru yang disebut sebagai hukum siber atau *cyberlaw*, sekaligus juga melahirkan satu bentuk kejahatan yang menggunakan atau memanfaatkan sarana teknologi informasi yang kemudian dikenal sebagai *cyber crime*. Menurut Barda Nawawi Arief, *cyber crime* merupakan salah satu bentuk atau dimensi baru dari kejahatan masa kini yang mendapat perhatian luas di dunia internasional.[2] Beberapa sebutan lain dari *cyber crime* adalah kejahatan dunia maya (*cyber space/virtual space offence*), dimensi baru dari *hight tech crime*, dimensi baru dari *transnational crime*, dan dimensi baru dari *white collar crime*.[3]

Sebagai satu bentuk kejahatan teknologi tinggi (*high tech crime)* dan sekaligus kejahatan yang dapat menjangkau dan lintas negara (*transnational/transborder crime*) dan bahkan dapat dilakukan secara terorganisasi (*organized crime*) maka *cyber crime* dapat mencakup bidang, tujuan, dan dampak yang sangat luas. Oleh sebab itu dapat dikatakan bahwa *cyber crime* merupakan salah satu sisi gelap dari kemajuan teknologi yang mempunyai dampak negatif sangat luas bagi seluruh bidang kehidupan modern saat ini.[4]

Pada lingkup internasional, kekhawatiran terhadap *cyber crime* telah sejak lama terungkap, yaitu salah satunya pada *International Information Congres* (IIC) *2000 Millenium Congres* di Quebec pada tanggal 19 September 2000, yang menyatakan bahwa:

> *Cyber crime is a real and growing threat to economic and social development around the word. Information technology touches every aspect of human life and so can electronically enabled crime.*[5] (Cyber crime adalah suatu kenyataan yang mengancam pertumbuhan ekonomi dan pembangunan sosial seputar teknologi informasi dunia menyentuh segenap aspek kehidupan manusia dan juga elektronik).

---

[2] Barda Nawawi Arief, *Tindak Pidana Mayantara, Perkembangan Kajian Cyber Crime di Indonesia*, Jakarta: RajaGrafindo, 2006, hal. 1.
[3] *Ibid.*
[4] Barda Nawawi Arief, *Perbandingan Hukum Pidana,* Jakarta: Raja Grafindo, 2002, hal. 252.
[5] *Ibid.*

Sehubungan dengan kekhawatiran akan ancaman bahaya *cyber crime* karena berkaitan erat dengan kejahatan ekonomi (*economic crime*) dan kejahatan terorganisasi (*organized crime*) terutama untuk *money laundering*, maka kongres PBB mengenai *The Prevention of Crime and the Treatment of offenders* telah pula membahas masalah ini. Sejalan dengan itu, terdapat beberapa konvensi internasional yang telah membahas permasalahan tersebut, antara lain *World Intellectual Property Organization* (WIPO), *United Nation on Commission International Trade Law* (UNCITRAL) yang telah mengeluarkan model hukum *(Model Law)* tentang *Electronic Commerce and Electronic Signature*. Selain itu juga terdapat *Convention Cybercrime* yang mengharapkan semua negara mencegah tindakan-tindakan pidana yang terkait dengan komputer dan *cyber* dalam rangka memberikan kepastian perlindungan hukum untuk pemanfaatan sistem komputer secara global.[6]

Oleh sebab itu, dinamika konvergensi telematika telah disambut oleh banyak negara untuk melakukan revisi peraturan perundang-undangan, bahkan beberapa negara membuat undang-undang baru untuk mengisi kekosongan hukum. Sistem hukum di Indonesia sebenarnya juga tengah mengalami konvergensi, namun jika di beberapa negara mereka melakukannya dengan membuat peraturan mengarah pada pembentukan satu undang-undang.[7]

Berdasarkan kenyataan tersebut, dihadapkan dengan sistem hukum pidana di Indonesia, ada satu pertanyaan penting yang dapat diajukan. Apakah sistem hukum pidana ataupun perundang-undangan yang ada, sudah dapat menjangkau bentuk-bentuk kejahatan *cyber crime*. Pertanyaan ini penting untuk diberikan jawaban, sebab kejahatan-kejahatan *cyber crime* secara faktual sudah terjadi dan potensial untuk terus terjadi di Indonesia. Diharapkan dengan perundang-undangan yang sudah ada mampu menjangkau kejahatan yang tergolong sebagai *cyber crime* baik menggunakan Kitab Undang-Undang Hukum Pidana (KUHP) maupun undang-undang di luar KUHP seperti Undang-Undang Nomor 36 Tahun

---

[6] *Ibid.*

[7] Mohammad Nuh, "Regulasi, Sistem Keamanan Serta Kepastian Penegakan Hukum dalam ITE" Seminar Sehari Menteri Komunikasi dan Informatika, Jakarta: FH Usakti, 6 Agustus 2008, hal. 3.

1999 Tentang Telekomunikasi, maupun Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (ITE).

Kasus menarik yang pernah terjadi di Indonesia yang berkait dengan kejahatan yang dilakukan dengan menggunakan sarana teknologi informasi adalah perkara dengan Terdakwa Dani Firmansyah, pada tanggal 17 April 2004 yang melakukan *deface*[8] dengan mengubah nama-nama partai yang ada dengan nama-nama buah dalam *website*[9] www.kpu.go.id. Tindakan terdakwa Dani Firmansyah merupakan salah satu bukti nyata bagaimana *cyber crime* telah terjadi di Indonesia. Tindakan tersebut telah mengakibatkan berkurangnya kepercayaan masyarakat terhadap pemilu yang sedang berlangsung pada saat itu. Kasus ini menimbulkan kekhawatiran 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.[10]

Kelemahan *admin*[11] dari suatu *website* juga terjadi pada penyerangan terhadap *website* www.golkar.or.id milik partai golkar. Serangan terjadi hingga 1577 kali melalui jalan yang sama tanpa adanya upaya menutup celah tersebut disamping kemampuan *Hacker*[12] yang lebih tinggi, dalam hal ini teknik yang digunakan oleh *Hacker* adalah *PHP Injection*[13] dan mengganti tampilan muka *website* dengan gambar wanita sexy serta gorilla putih sedang tersenyum.[14]

---

[8] *Deface* adalah perubahan pada tampilan ataupun penambahan materi pada suatu website yang dilakukan oleh hacker.

[9] *Website* adalah sebuah kumpulan dari halaman web.

[10] Petrus Reinhard Golose, *Perkembangan Cybercrime Dan Upaya Penanganannya Di Indonesia Oleh POLRI,* Jakarta: Buletin Hukum Perbankan Dan Kebanksentralan, Volume 4, Nomor 2, Agustus 2006, hal. 32.

[11] *Admin* adalah orang yang bertanggung jawab untuk mengatur dan menjalankan satu sistem. Sesuai dengan tugas utamanya, seorang administrator diberi kewenangan penuh untuk memberikan dan mengatur hak akses dengan batas-batas tertentu. Administrator pada server yang bersifat kritikal diwajibkan untuk selalu menjaga kontinuitas operasinal dan realibilitas server tersebut.

[12] *Hacker* adalah seseorang yang memasuki komputer orang lain tanpa izin.

[13] PHP adalah singkatan rekursif dari PHP: Hypertext preprocessor. Bahasa scripting server side (kebalikan dari client side, seperti java script), digunakan sebagai *script* untuk memperoses data melalui GUI dari form HTML. Script PHP bekerja di komputer server untuk memproduksi kode HTML yang dikirimkan kepada *web browser*. Script PHP dapat ditempelkan (*embedded*) di halaman HTML, dan disimpan dengan extension PHP sedangkan *PHP Injection* adalah salah satu teknik *injection* atau serangan ke *web browser* menggunakan script PHP.

[14] Petrus Reinhard Golose, *loc. cit.*

Banyak orang yang beranggapan bahwa jika belum ada *cyberlaw* maka kita menghadapi kevakuman hukum sehingga kejahatan di dunia maya dapat dilakukan. Ini anggapan yang salah, para penegak hukum dapat menggunakan hukum-hukum yang belaku untuk menjerat para pelaku *cyber crime*. Memang landasan hukum konvensional akan mempersulit pekerjaan penegak hukum (Polisi).[15]

Cyber crime telah menjadi satu bentuk kejahatan yang merupakan ancaman faktual dalam sistem teknologi informasi, yang dapat menimbulkan kerugian terhadap individu, kelompok masyakarat, badan usaha, dan bahkan negara. Dalam kaitan ini, masalah penting yang perlu mendapatkan perhatian adalah bagaimana keseluruhan sistem hukum Indonesia mengatur mengenai pengawasan, pengendalian penggunaan teknologi informasi, sekaligus bagaimana mengatur sistem sanksi terhadap pelaku kejahatan yang telah dikualifikasikan sebagai pelaku *cyber crime.*

Berdasarkan uraian di atas, negara Indonesia sebagai bagian dari masyarakat bangsa-bangsa tidak luput dari perkembangan dan munculnya *cyber crime*. penulis tertarik mengkaji permasalahan ini ke daiam sebuah tesis yang berjudul: **"Fungsionalisasi Hukum Pidana dalam Rangka Penanggulangan Kejahatan Mayantara di Indonesia."**

1.2.Identifikasi Masalah

Berdasarkan latar belakang, *cyber crime* selain merupakan ancaman potensial di masa mendatang juga telah merupakan ancaman faktual, karena beberapa kasus telah terjadi di Indonesia. Transaksi maupun komunikasi dengan menggunakan sarana teknologi informasi ternyata dapat menimbulkan kerugian baik terhadap seseorang, masyarakat maupun badan hukum tertentu. Pada satu sisi kerugian akibat penggunaan atau melalui sarana teknologi informasi, masyarakat memandangnya sebagai satu bentuk kejahatan, pada sisi yang lain bentuk-bentuk kejahatan tersebut relatif baru dalam sistem hukum yang berlaku di Indonesia.

---

[15] Budi Rahardjo, *Pernak Pernik Peraturan dan Pengaturan Cyberspace di Indonesia,* http://budi.insan.co.id, diakses tanggal 22 Januari 2008.

Untuk memfokuskan, maka pertanyaan penelitian dalam pokok permasalahan ini adalah sebagai berikut:

1. Apakah upaya penanggulangan kejahatan mayantara di Indonesia harus dilakukan melalui upaya penal dengan menggunakan sanksi pidana?
2. Apakah fungsionalisasi hukum pidana Indonesia dapat memberikan efek pencegahan sekaligus memberikan keadilan kepada para korban kejahatan?
3. Apakah sistem hukum (khususnya hukum pidana) Indonesia telah memadai untuk menjangkau kejahatan mayantara?
4. Bagaimana yurisdiksi kejahatan mayantara, mengingat pelaku dan akibat kejahatan dapat melintasi batas-batas negara?

1.3.Tujuan Penelitian

Adapun yang menjadi tujuan dari penelitian ini adalah:

1. Untuk mengetahui apakah penanggulangan kejahatan mayantara harus dilakukan dengan upaya penal (sanksi pidana) ataukah upaya non penal.
2. Untuk mengetahui apakah fungsionalisasi hukum pidana Indonesia terhadap *kejahatan mayantara* memberikan efek pencegahan dan memberikan rasa keadilan kepada para korban.
3. Untuk mengetahui apakah sistem hukum (khususnya hukum pidana) Indonesia telah memadai untuk menjangkau kejahatan mayantara.
4. Untuk mengetahui yurisdiksi kejahatan mayantara, dalam sistem hukum di Indonesia.

1.4.Kegunaan Penelitian

Dilakukannya penelitian tentang Fungsionalisasi Hukum Pidana dalam Penanggulangan Mayantara di Indonesia diharapkan dapat memberikan sumbangan pemikiran, sebagai berikut:

1. Kegunaan teoritis, memberikan sumbangan ilmu pengetahuan dalam bidang pendidikan ilmu hukum, khususnya hukum pidana.

2. Kegunaan praktis, sebagai pedoman bagi praktisi hukum, mahasiswa hukum dan semua pihak yang tertarik untuk mengetahui penyelesaian kejahatan mayantara dan kejahatan-kejahatan dengan menggunakan sarana komputer pada umumnya dengan memfungsikan hukum pidana.

1.5.Kerangka Teoritis

Pada hakikatnya hukum adalah instrument kontrol, yang akan difungsikan untuk mengontrol perilaku warga dalam kehidupan masyarakat. [16] Sebagai instrumen kontrol, hukum ditengarai oleh sifatnya yang formal, tidak pernah berharap kesediaan warga untuk secara suka dan rela menaatinya, dan pelaksanaannya selalu disertai ancaman sanksi. Berfungsi sebagai sarana kontrol, hukum dan sanksi yang melekat padanya, akan menjadi suatu variabel yang berkorelasi erat dengan variable struktur organisasi negara yang berfungsi sebagai pengada dan penegak hukum. Idealnya, segenap aspek kehidupan masyarakat diatur di dalam tata hukum, sehingga akan memberikan perlindungan terhadap hak-hak, kewajiban dan kepentingan warga masyarakat, dan lebih jauh dari itu, kepada pelanggarnya yang telah menimbulkan kerugian dan terlanggarnya hak orang lain dapat diambil tindakan berupa sanksi tertentu oleh negara. Setiap perkembangan dan dinamika kehidupan masyarakat yang potensial menimbulkan kerugian orang lain ataupun dapat melanggar hak seseorang dapat diikuti dengan tatanan normatif sekaligus disertai dengan sanksi hukum. Sanksi berfungsi sentral sabagai sarana kontrol akan terlaksana dengan baik apabila ditunjang dengan organisasi yang kuat.

Kemajuan teknologi informasi dan telekomunikasi adalah salah satu bentuk perkembangan dinamika kehidupan masyarakat, namun nampaknya belum diimbangi secara memadai oleh tatanan normatif undang-undang. Namun demikian tidak berarti bahwa jika terjadi perbuatan di bidang teknologi informasi dan telekomunikasi yang telah mengarah pada timbulnya kerugian seseorang atau sekelompok orang atau badan hukum, kemudian tidak diambil sanksi. Dengan hukum atau undang-undang yang ada, negara harus mampu memberikan

---

[16] Soetandyo Wignjosoebroto, *Hukum dalam Masyarakat, Perkembangan dan Masalah.* Malang: Bayu Media, 2008, hal. 135.

perlindungan hukum bagi warganya yang telah dirugikan akibat perbuatan seseorang atau sekelompok orang di bidang teknologi menggunakan sarana teknologi informasi dan telekomunikasi, dengan menggunakan sarana sanksi.

Perkembangan Internet dan umumnya dunia *cyber* tidak selamanya menghasilkan hal-hal yang positif. Salah satu hal negatif yang merupakan efek sampingan atau memang menjadi tujuan, antara lain adalah kejahatan di dunia *cyber* atau *cyber crime.* Upaya memasuki dan atau menggunakan fasilitas komputer atau jaringan komputer tanpa ijin dan dengan melawan hukum dengan atau tanpa menyebabkan perubahan dan atau kerusakan pada fasilitas komputer yang dimasuki atau digunakan tersebut. Dengan demikian jelaslah bahwa jika seseorang menggunakan komputer atau bagian dari jaringan komputer tanpa seijin yang berhak, tindakan tersebut sudah tergolong pada kejahatan komputer.

Negara Indonesia yang mewarisi sistem hukum Eropa Kontinental (*Civil Law System*) tidak bisa lepas dari sistem hukum yang bersifat tertulis (legalistik). Teori hukum legalistik, sesungguhnya muncul sejalan dengan pertumbuhan masyarakat modern sebagai akibat adanya industrialisasi yang melahirkan sistem ekonomi kapitalis. Hukum sebagaimana diterima dan di jalankan diberbagai negara-negara di dunia sekarang ini, pada umumnya termasuk ke dalam kategori hukum yang modern. Modernitas ini menurut Satjipto Rahardjo, mempunyai ciri-ciri sebagai berikut:

1. mempunyai bentuk tertulis;
2. hukum itu berlaku untuk seluruh wilayah negara;
3. hukum merupakan instrumen yang dipakai secara sadar untuk mewujudkan keputusan-keputusan politik masyarakatnya.[17]

Sejalan dengan sistem hukum yang beraliran *civil law system* dengan prinsip hukum tertulis maka bentuk kejahatan mayantara dan sanksi hukumnya perlu diatur di dalam undang-undang. Perumusan suatu perbuatan di dalam undang-undang menjadi perbuatan jahat dalam pengetahuan hukum disebut sebagai kriminalisasi.

---

[17] Satjipto Rahardjo, *Membedah Hukum Progresif,* Jakarta: Penerbit Kompas, 2007, hal. 252.

Dalam hal kriminalisasi, Barda Nawawi Arief membedakan antara harmonisasi materi / substansi dan harmonisasi kebijakan formulasi, yang pertama adalah tentang apa yang disebut sebagai tindak pidana di bidang Teknologi Informasi, dan yang kedua apakah pengaturan hukuman pidana bagi kejahatan teknologi informasi tersebut berada di dalam atau di luar KUHP. Tentang kebijakan formulasi dapat dilakukan dengan dua pendekatan yaitu:

1. Menganggapnya sebagai kejahatan biasa, dilakukan dengan komputer teknologi tinggi dan KUHP dapat digunakan untuk menanggulanginya;
2. Menganggapnya sebagai kejahatan kategori baru yang membutuhkan suatu kerangka hukum yang baru dan komprehensif untuk mengatasi sifat khusus teknologi yang sedang berkembang dan tantangan baru yang tidak ada pada kejahatan biasa dan karena itu perlu diatur secara tersendiri di luar KUHP.[18]

Namun disadari bahwa membentuk suatu undang-undang baru (misalnya akan dibentuk undang-undang tentang kejahatan mayantara) memerlukan waktu dan biaya yang besar, dan harus didukung dengan kebijakan legislatif berdasarkan skala prioritas negara untuk perlunya mengatur kejahatan mayantara dalam sebuah undang-undang khusus. Oleh sebab itu, kejahatan mayantara yang secara nyata telah muncul dalam kehidupan masyarakat di Indonesia, harus dapat diatasi dengan undang-undang/hukum yang ada dan pelakunya harus dipertanggungjawabkan pidana berdasarkan undang-undang pidana yang telah ada.

1.6.Kerangka Konseptual

Eksistensi kerangka konsepsional dalam suatu penelitian diperlukan untuk membatasi pengertian yang akan ditemukan dalam penulisan, karena mungkin saja satu kata atau istilah mempunyai pengertian yang jamak. Dengan demikian, antara penulis dan pembaca akan tercipta suatu kerangka pemikiran dan

---

[18] Barda, Nawawi Arief, *Tindak Pidana Mayantara, Perkembangan Kajian Cybercrime di Indonesia,* Jakarta: RajaGrafindo Persada. 2006. hal. 90.

pemahaman yang sama terhadap *terminology* suatu pengertian istilah, agar tidak terjadi *verbal dispute dengan kata lain adalah perdebatan kata-kata.*[19]

Untuk dapat lebih memahami penulisan ini, terlebih dahulu akan dijelaskan mengenai pengertian atau definisi-definisi yang berkaitan dengan topik penelitian ini. Pembatasan definisi bertujuan agar penelitian yang akan dilakukan nantinya tidak terlalu luas dan tetap pada tujuan penelitian yang telah ditetapkan. Adapun beberapa definisi yang akan menjadi bahan pembahasan dalam penelitian ini adalah sebagai berikut :

1. **Kejahatan**

Kejahatan merupakan sebuah istilah yang sudah lazim dan populer di kalangan masyarakat Indonesia atau *crime* bagi orang Inggris. Akan tetapi, jika dipertanyakan, apakah yang dimaksud dengan kejahatan, orang mulai berpikir dan atau bahkan berbalik bertanya. Menurut Hoefnagels kejahatan merupakan suatu pengertian yang relatif. Banyak pengertian yang digunakan dalam ilmu-ilmu sosial yang berasal dari bahasa sehari-hari, tetapi jarang kita mengartikannya. Hal tersebut karena bahasa sehari-hari itu tidak memberikan gambaran yang jelas dari kejahatan, tetapi hanya merupakan suatu ekspresi dalam melihat perbuatan tertentu. Lebih lanjut Hoefnegels menulis bahwa dalam bahasa sehari-hari hanya membedakan antara perbuatan kongkret. Perilaku menyimpang dari seseorang tertentu dipandang sebagai kejahatan, yaitu apabila perbuatan tersebut dirasakan sebagai perbuatan yang serius. Sementara itu, perbuatan yang sama mungkin tidak dianggap sebagai kejahatan apabila terjadinya dalam konteks yang berbeda.[20]

Namun demikian, sebagaimana yang ditulis oleh Hoefnagels, apabila memperhatikan unsur-unsur dari kata kejahatan (*crime)* yang dalam bahasa Belanda disebut *misdaad,* dalam bahasa Jerman disebut *missetat,* dan dalam bahasa Inggris disebut *misdeed,* dalam bahasa sehari-hari dari beberapa negara, sebagai contoh perbuatan yang sangat tercela biasanya perbuatan

---

[19] Soerjono Soekanto, *Ringkasan Metode Penelitian Hukum Empiris.* Cet. I. Jakarta : Ind.Hill.Co, 1990. hal. 83.

[20] M. Arief Amrullah, *Politik Hukum Pidana Dalam Perlindungan Korban Kejahatan Ekonomi Bidang Perbankan,* Malang: Bayumedia Publishing, 2007, hal. 28.

yang dapat dipidana. Hal itu seringkali dipandang sebagai kejahatan dalam beberapa hukum pidana (*penal code*), meskipun tidak selalu begitu. Pencurian ringan, misalnya, dalam hukum pidana Belanda secara hukum ditentukan sebagai kejahatan tetapi tidak selalu dipandang sebagai kejahatan menurut publik.[21]

2. Fungsionalisasi hukum pidana

Fungsionalisasi hukum pidana dapat diartikan sebagai upaya untuk membuat hukum pidana itu dapat berfungsi, beroperasi atau bekerja dan terwujud secara konkret. Jadi istilah fungsionalisasi hukum pidana dapat diidentikkan dengan istilah yang pada hakekatnya sama dengan pengertian penegakan hukum pidana.[22]

3. Informasi Elektronik

Informasi elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, 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.[23]

4. Transaksi Elektronik

Transaksi Elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer, dan/atau media elektronik lainnya.[24]

5. Teknologi Informasi

Teknologi Informasi adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan/atau menyebarkan informasi.[25]

---

[21] *Ibid.* hal. 28.
[22] Muladi dan Barda Nawawi Arief, *Bunga Rampai Hukum Pidana*, Bandung: Alumni, 1992, hal. 157.
[23] Undang-Undang Nomor 11 Tahun 2003 tentang *Informasi dan Transaksi Elektronik*, Lembaran Negara 2008 Nomor 58, Pasal 1 Angka 1.
[24] *Ibid.*, Pasal 1 Angka 2.
[25] *Ibid.*, Pasal 1 Angka 3.

6. Dokumen Elektronik

Dokumen elektronik, adalah setiap Informasi Elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui komputer atau Sistem Elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, kode akses, simbol atau perforasi yang memiliki makan atau arti atau dapat dipahami oleh orang yang mampu memahaminya.[26]

7. Sistem Elektronik

Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik.[27]

8. Penyelenggaraan Sistem Elektronik

Penyelenggaraan Sistem Elektronik adalah pemanfaatan Sistem Elektronik oleh penyelenggara negara, orang, badan usaha, dan/atau masyarakat.[28]

9. Jaringan Sistem Elektronik

Jaringan Sistem Elektronik adalah terhubungnya dua Sistem Elektronik atau lebih, yang bersifat tertutup ataupun terbuka.[29]

10. Tindak Pidana

Tindak pidana adalah terjemahan dari istilah *Het strafbare feit* atau *delict* diterjemahkan dalam Bahasa Indonesia sebagai:[30]

a. perbuatan yang dapat atau boleh dihukum
b. peristiwa pidana
c. perbuaan pidana

---

[26] *Ibid.*, Pasal 1 Angka 4.
[27] *Ibid.*, Pasal 1 Angka 5.
[28] *Ibid.*, Pasal 1 Angka 6.
[29] *Ibid.*, Pasal 1 Angka 7.
[30] S.R. Sianturi, *Asas-asas Hukum Pidana di Indonesia dan Penerapannya,* Jakarta: Alumni Ahaem-Petehaem, 1985, hal. 200.

d. tindak pidana

e. delik

Tindak pidana berarti suatu perbuatan yang pelakunya dapat dikenai hukuman pidana. Pelaku ini dapat dikatakan merupakan "subjek" tindak pidana. Hukum pidana Belanda memakai istilah *strafbaar feit*, kadang-kadang juga delict yang berasal dari bahasa latin delictum. Hukum pidana negara-negara Anglo-Saxon memakai istilah *offense* atau *criminal act* untuk tindak pidana. Oleh karena KUHP Indonesia bersumber pada WvS Belanda, maka istilah aslinya pun sama yaitu *strafbaar feit*. Pengertian dari istilah *strafbaar feit* adalah suatu kelakuan manusia yang diancam pidana oleh peraturan undang-undang, jadi suatu kelakuan yang pada umumnya dilarang dengan ancaman pidana.[31]

Istilah yang sering digunakan penulis dalam penulisan ini adalah kejahatan mayantara (*Cyber crime),* kejahatan siber, CC, banyaknya istilah yang dipakai dikarenakan belum ada pengertian yang lebih tepat untuk penggunaan istilah dalam kejahatan ini dari para ahli dan para sarjana.

1.7.Metode Penelitian

Metode penelitian yang dipergunakan dalam penulisan tesis ini, bersifat deskriptif, dimaksudkan untuk memberikan data yang seteliti mungkin tentang manusia, keadaan atau gejala-gejala lainnya sehingga memperoleh gambaran yang jelas mengenai permasalahan yang diangkat.[32] Metode pendekatan yang digunakan dalam penelitian ini adalah penelitian kepustakaan dimana studi dokumen akan menjadi alat pengumpulan data utama dalam penelitian ini.

Penelitian ini pada dasarnya merupakan penelitian hukum normatif dengan menggunakan data primer sebagai pelengkap. Data primer atau data dasar merupakan data yang diperoleh langsung dari masyarakat.[33] Penelitian hukum normatif adalah penelitian yang dilakukan khusus untuk meneliti hukum sebagai

---

[31] *Ibid.*, hal. 205.

[32] Sutandyo, Wignjosoebroto, *Hukum Paradigma: Metode dan Dinamika Masalahnya*, Jakarta: Lembaga Studi dan Advokasi Masyarakat (ELSAM), 2002, hal. 147.

[33] Soekanto, Soerjono, *Pengantar Penelitian Hukum*, Jakarta: Universitas Indonesia Press, hal. 11.

norma positif (*as it is written in the books*).[34] Dalam penelitian hukum normatif, bahan pustaka merupakan data primer yang dalam ilmu pengetahuan digolongkan sebagai data sekunder.

Analisis kualitatif merupakan alat analisis utama dalam penelitian ini, mengingat data yang akan dikumpulkan adalah data sekunder. Dalam proses perjalanan penelitian ini, dimungkinkan pula melakukan penelitian lapangan untuk menunjang pengumpulan data. Penelitian lapangan dilakukan dengan melakukan wawancara dengan pihak-pihak terkait seperti nara sumber atau informan yang ahli dalam bidang Teknologi dan Informasi.

1.8.Sistematika Penulisan

Penulisan hukum ini terbagi kedalam 4 bab, Bab I berisi pendahuluan yang tersusun kedalam 8 sub-bab yang membahas latar belakang penelitian, rumusan masalah, tujuan penelitian, kegunaan penelitian, kerangka teori, kerangka konsepsional, metode penelitian, serta yang terakhir sistematika penulisan untuk membantu penyusunan penulisan hukum ini.

Dalam Bab II dibahas Gambaran Umum Kejahatan Mayantara, membahas mengenai kejahatan pada umumnya, pengertian kejahatan mayantara (*cybercrime*), karakteristik kejahatan mayantara, dan perkembangan kejahatan mayantara dengan sarana internet.

Bab III Fungsionalisasi Hukum Pidana dalam rangka Penanggulangan Kejahatan Mayantara. Membahasa mengenai hakikat penanggulangan kejahatan, Penanggulangan Kejahatan Mayantara dengan Menggunakan Sanksi Pidana, Fungsionalisasi Hukum dan Sanksi Pidana dalam Penanggulangan Kejahatan mayantara, dan Pertanggungjawaban pidana kejahatan mayantara.

Bab IV yang merupakan bab Penutup akan menguraikan tentang kesimpulan yang dapat ditarik dari penelitian. Pada akhir bab ini disertakan juga saran-saran yang akan disampaikan oleh penulis.

---

[34] Sutandyo, Wignjosoebroto, *Op. Cit.*, hal.146.

BAB II
GAMBARAN UMUM KEJAHATAN MAYANTARA

Dalam bab ini penulis membahas mengenai gambaran umum kejahatan mayantara, pengertian kejahatan pada umumnya, pengertian kejahatan mayantara, karakteristik kejahatan mayantara, perkembangan kejahatan mayantara dengan sarana internet.

2.1. Kejahatan Pada Umumnya

Perkembangan kejahatan mayantara tidak dapat dilepaskan dari perkembangan masyarakatnya. Pada awalnya, hanya kejahatan konvensional yang dianggap sebagai kejahatan yang sesungguhnya, namun dalam perkembangannya seiring dengan pertumbuhan korporasi dan kemajuan teknologi yang semakin pesat dalam bidang kegiatan ekonomi, muncul yang disebut dengan kejahatan cyber (*cyber crime*), yang dalam penelitian ini kemudian diterjemahkan sebagai kejahatan mayantara.

Ahli hukum pidana dan kriminologi telah lama mengungkapkan bahwa kejahatan adalah masalah abadi umat manusia. Kejahatan akan selalu ada sebagaimana adanya masyarakat manusia di dunia ini. Kejahatan merupakan suatu fenomena yang ada dan melekat dalam masyarakat, *crime is eternal –as eternal as- society*, demikian tulis Frank Tannenbaum.[35] Oleh karena itu tidak keliru bila Benedict S. Alper mengatakan kejahatan sebagai *"the oldest social problem."*[36] Kejahatan tidak terjadi dan tidak terdapat dalam kekosongan. Di mana ada manusia lebih dari satu orang, di mana ada masyarakat, di situ ada kejahatan. Kejahatan selalu erat berkaitan dengan nilai-nilai, struktur, dan bentuk masyarakat itu sendiri.[37] Lebih lanjut diuraikan oleh J.E. Sahetapy bahwa secara sosio-

---

[35]J.E. Sahetapy, *Kausa Kejahatan*, Surabaya: Pusat Studi Kriminologi Fakultas Hukum Unair, 1979, hal. 1.

[36]Barda Nawawi Arief, *Kebijakan Legislatif Dalam Penanggulangan Kejahatan Dengan Pidana Penjara*, Semarang: Ananta, 1994, hal. 11.

[37]J.E. Sahetapy, *Suatu Studi Khusus Mengenai Ancaman Pidana Mati Terhadap Pembunuhan Berencana*, Jakarta: Rajawali Press, hal. 183.

kriminologik kejahatan adalah suatu gejala normal dalam setiap masyarakat, bagaimanapun bentuk masyarakat itu, di mana saja dan kapan saja. Membuat suatu definisi yuridis tentang kejahatan, bukanlah hal yang mudah. Sebagaimana halnya dengan membuat definisi tentang hukum, terdapat kesulitan dalam mendefinisikan apa itu kejahatan.[38]

Sutherland menekankan bahwa ciri pokok dari kejahatan adalah perilaku yang dilarang oleh negara karena merupakan perbuatan yang merugikan negara dan terhadap perbuatan itu negara bereaksi dengan hukuman sebagai upaya pamungkas. Dalam pengertian yuridis, kejahatan sebagai perbuatan yang telah ditetapkan oleh negara sebagai kejahatan dalam hukum pidananya dan diancam dengan suatu sanksi.[39]

Namun, tidak semuanya setuju dengan definisi yang diberikan oleh para sarjana yang menganut aliran yuridis, Bonger menyatakan bahwa kejahatan merupakan perbuatan anti sosial yang secara sadar mendapat reaksi dari negara berupa pemberian derita dan kemudian sebagai reaksi terhadap rumusan-rumusan hukum *(legal definitions)* mengenai kejahatan.[40] Golongan kedua ini merupakan para sarjana yang tidak menyetujui pembatasan definisi kejahatan dalam pengertian yuridis tersebut. Meski definisi yuridis telah memberikan kepastian atas batasan perilaku mana yang dimaksud dengan kejahatan dan penjahat, namun definisi tersebut sama sekali tidak memuaskan para sarjana kriminologi karena sifatnya yang statis.

Thorsten Sellin, [41] mengutarakan bahwa pemberian batasan definisi kejahatan secara yuridis itu tidak memenuhi tuntutan-tuntutan keilmuan. Suatu dasar yang lebih baik bagi perkembangan kategori-kategori ilmiah menurutnya

---

[38] "*Noch suchen die Juristen eine Definition zu ihrem Begriffe von Recht*, demikian Kant. Walaupun sejak beberapa ribu tahun orang sibuk mencari sesuatu definisi tentang hukum, namun belum pernah terdapat sesuatu yang memuaskan. Tiap-tiap definisi mengenai hukum memberi kesan yang tidak tepat kepada mereka yang baru belajar, sehingga perkenalan pertama dimulai dengan salah paham, karena tidak mungkin memberi definisi tentang hukum, yang sungguh-sungguh dapat memadai kenyataan. Lihat L.J. van Apeldoorn, *Pengantar ilmu Hukum*, Jakarta: Pradnya Paramita, 1981, hal. 13.

[39] Topo Santoso dan Eva Achjani Zulfa, *Kriminologi*, Jakarta: Raja Grafindo Persada, 2002, hal. 14

[40] *Ibid.*

[41] *Ibid.*, hal. 15.

adalah dengan memberikan dasar yang lebih baik dengan mempelajari norma-norma kelakuan *(conduct norms)*, karena konsep norma-norma perilaku yang mencakup setiap kelompok atau lembaga seperti negara serta merupakan ciptaan kelompok-kelompok normatif manapun, serta tidak terkurung oleh batasan-batasan politik dan tidak selalu harus terkandung dalam hukum.

Secara sosiologis, kejahatan merupakan suatu perilaku manusia yang diciptakan oleh masyarakat. Walaupun masyarakat memiliki berbagai macam perilaku yang berbeda-beda, akan tetapi ada didalamnya bagian-bagian tertentu yang memiliki pola yang sama. Keadaan ini dimungkinkan karena adanya sistem kaidah dalam masyarakat. Gejala yang dinamakan kejahatan pada dasarnya terjadi didalam proses dimana ada interaksi sosial antara bagian-bagian dalam masyarakat yang mempunyai kewenangan untuk melakukan perumusan tentang kejahatan dengan pihak-pihak mana yang memang melakukan kejahatan.

Aliran kriminologi baru lahir dari pemikiran yang bertolak pada anggapan bahwa perilaku menyimpang yang disebut sebagai kejahatan, harus dijelaskan dengan melihat pada kondisi-kondisi struktural yang ada dalam masyarakat dan menempatkan perilaku menyimpang dalam konteks ketidakmerataan kekuasaan, kemakmuran dan otoritas serta kaitannya dengan perubahan-perubahan ekonomi dan politik dalam masyarakat.[42]

Ukuran dari menyimpang atau tidaknya suatu perbuatan bukan ditentukan oleh nilai-nilai dan norma-norma yang dianggap sah oleh mereka yang duduk pada posisi-posisi kekuasaan atau kewibawaan, melainkan oleh besar kecilnya kerugian atau keparahan sosial (*social injuries*) yang ditimbulkan oleh perbuatan tersebut dan dikaji dalam konteks ketidakmerataan kekuasaan dan kemakmuran dalam masyarakat. Perilaku menyimpang sebagai proses sosial dianggap terjadi sebagai reaksi terhadap kehidupan kelas seseorang. Disini yang menjadi nilai-nilai utama adalah keadilan dan hak-hak asasi manusia. Rumusan kejahatan dalam kriminologi semakin diperluas. Sasaran perhatian terutama diarahkan kepada kejahatan-kejahatan yang secara politis, ekonomis dan sosial amat merugikan yang berakibat jatuhnya korban-korban bukan hanya korban individual melainkan

---

[42] *Ibid.*, hal 18.

juga golongan-golongan dalam masyarakat. Pengendalian sosial dalam arti luas dipahami sebagai usaha untuk memperbaiki atau mengubah struktur politik, ekonomi dan sosial sebagai keseluruhan.[43]

Sutherland dan Cressey mengemukakan adanya tujuh syarat untuk perbuatan yang dapat dikategorikan sebagai kejahatan, yaitu:

1. Sebelum suatu perbuatan disebut sebagai kejahatan harus terdapat akibat-akibat tertentu yang nyata, yang berupa kerugian;
2. Kerugian yang ditimbulkan harus merupakan kerugian yang dilarang oleh undang-undang dan secara jelas tercantum dalam hukum pidana;
3. Harus ada perbuatan yang membiarkan terjadinya perbuatan yang menimbulkan kerugian tersebut;
4. Dalam melakukan perbuatan tersebut harus terdapat maksud jahat atau *"mens rea"*;
5. Harus ada hubungan perilaku dan *"mens rea"*;
6. Harus ada hubungan kausal antara kerugian yang dilarang Undang-undang dengan perbuatan yang dilakukan atas kehendak sendiri (tanpa adanya unsur paksaan);
7. Harus ada pidana terhadap perbuatan tersebut yang ditetapkan oleh undang-undang. [44]

Mendasari pada uraian hakikat kejahatan sebagaimana telah dikemukakan di atas, menurut penulis hakikat kejahatan dalam perspektif hukum Indonesia, menekankan bahwa ciri pokok adalah perilaku yang dilarang oleh negara karena merupakan perbuatan yang merugikan negara dan terhadap perbuatan itu negara bereaksi dengan hukuman sebagai upaya pamungkas. Dalam pengertian yuridis, kejahatan sebagai perbuatan yang telah ditetapkan oleh negara sebagai kejahatan dalam hukum pidananya dan diancam dengan suatu sanksi.

---

[43] *Ibid*

[44] Edwin H. Sutherland dan Donald R. Cressey, *Principles of Criminology*, Sixth Edition, New York: Lippincott Company, 1960, hal. 3.

2.2. Pengertian Kejahatan Mayantara

Seiring dengan perkembangan masyarakat, maka kejahatan juga mengalami perkembangan. Perkembangan tidak hanya menyangkut segi kuantitas kejahatan tetapi juga kualitas kejahatan. Berbagai kongres internasional diadakan guna mencegah serta menanggulangi kejahatan.

Meningkatnya kualitas dan kuantitas kejahatan di kebanyakan negara yang kemudian menimbulkan kekhawatiran dan sekaligus menimbulkan keinginan untuk melakukan upaya-upaya pencegahan, sesungguhnya telah dirasakan oleh masyarakat bangsa-bangsa sejak dahulu, pada Tahun 1975 konggres kelima PBB di Jenewa telah membicarakan mengenai:

1. perubahan-perubahan bentuk dan dimensi kejahatan, baik secara trans-nasional maupun nasional; dan
2. akibat-akibat ekonomi dan sosial dari kejahatan.

Beberapa perubahan dari bentuk dan dimensi kejahatan yang dibicarakan dalam kongres kelima tersebut ialah mengenai:

1. *Crime as business* yaitu bentuk kejahatan yang bertujuan mendapatkan keuntungan material melalui kegiatan dalam bidang usaha (bisnis) atau industri, yang pada umumnya dilakukan secara terorganisasi dan dilakukan oleh mereka yang mempunyai kedudukan terpandang didalam masyarakat, termasuk dalam bentuk kejahatan ini antara lain yang berhubungan dengan pencemaran lingkungan, perlindungan konsumen dan dalam bidang perbankan, disamping kejahatan-kejahatan lainnya yang bisa dikenal dengan *organized crime*; *white-collar crime* dan korupsi.
2. Tindak pidana yang berhubungan dengan hasil-hasil pekerjaan seni dan kekayaan budaya, obyek-obyek budaya atau warisan budaya.
3. Kejahatan yang berhubungan dengan alkohol dan penyalahgunaan obat-obatan.
4. Perbuatan kekerasan antar-perorangan.
5. Perbuatan kekerasan antar perorangan (*interpersonal violence*) khususnya perbuatan-perbuatan kekerasan terhadap remaja.
6. Kejahatan yang berhubungan dengan lalu lintas kendaraan bermotor.

7. Kejahatan yang berhubungan dengan perpindahan tempat (migrasi) dan larian pengungsi akibat bencana alam dan peperangan; masalah-masalah yang berhubungan dengan perpindahan tempat misalnya mengenai pelanggaran paspor dan visa, pemalsuan dokumen, mengeksploitir tenaga kerja, pelacuran dan sebagainya.
8. Masalah-masalah yang berhubungan dengan pengungsi antara lain, masalah pengalihan bantuan dan masalah spionase.
9. Kejahatan yang dilakukan oleh wanita.[45]

Meskipun pada waktu itu, kejahatan mayantara belum masuk sebagai bentuk kejahatan yang mengkawatirkan, namun perhatian masyarakat dunia terhadap pesatnya perkembangan kejahatan sangatlah besar. Pada tahun 1990, barulah ada perhatian mengenai kejahatan yang berkaitan dengan komputer, yaitu dalam kongres ke-8 di Havana-Cuba, disoroti dimensi kejahatan antara lain:

1. Masalah *urban crime.*
2. *Crime against the nature and the envorinment.*
3. *Corruption* keterkaitannya dengan *economic crime, organized crime, illicit trafficking narcotic drugs and psicotropic substances* termasuk juga masalah *moneylaundering.*
4. *Crime against movable cultural, property* (*cultural heritage*).
5. *Computer related crime.*
6. *Terorism.*
7. *Domestic violence.*
8. *Instrumental use children in criminal activities.* [46]

Dewasa ini, istilah kejahatan mayantara (*cyber crime*) memang belum mapan. Hal ini dikemukakan oleh T.Ronny Nitibaskara, bahwa sebagai dunia yang masih dalam proses pembentukannya (*to being*), maka nilai-nilai, norma-norma dan konsep-konsep yang menyertainya belum mapan. Istilah-istilah baru

---

[45] Barda Nawawi Arief, 1994, *Op. Cit.* hal. 13.
[46] Barda Nawawi Arief, 1996, *Op. Cit.* hal. 18.

terus bermunculan, yang seringkali belum memenuhi maknanya oleh sebagian besar anggota masyarakat dunia siber itu sendiri.[47]

Munculnya istilah kejahatan mayantara sebagai sebuah bentuk penamaan aktifitas atau perbuatan kriminal dalam dunia maya merupakan salah satu contohnya. Terkait dengan istilah *cyber crime*, agar mendapat gambaran yang komprehensif dan mendalam, penulis mengutip beberapa definisi-definisi *cyber crime* dari berbagai sumber dan pakar-pakar hukum pidana.[48]

Peter Stephenson, dalam bukunya *Investigating Computer-Related Crime*, menjelaskan *Cyber Crime* sebagai :

> *"The easy definition of cyber crime is crimes directed at a computer or a computer system. The nature of cyber crime, however, is far more complex. As we will see later, cyber crime can take the form of simple snooping into a computer system for which we have no authorization. It can be the feeing of a computer virus into the wild. It may be malicious vandalism by a disgruntled employee. Or it may be theft of data, money, or sensitive information using a computer system."*[49] (Definisi yang mudah dari kejahatan siber adalah kejahatan yang ditujukan pada suatu komputer atau suatu sistem komputer. Namun, sifat kejahatan mayantara, jauh lebih kompleks. Sebagaimana akan kita lihat selanjutnya, kejahatan siber dapat berbentuk memasuki tanpa ijin suatu sistem komputer. Ia dapat berupa menyebarkan suatu virus komputer ke dalam ruang bebas. Ia dapat vandalisme penuh kebencian oleh seorang pekerja yang merasa tidak puas. Atau ia dapat berupa pencurian data, uang, atau informasi sensitif dengan menggunakan suatu sistem komputer).

Cyber crime pada hakikatnya adalah kejahatan dengan menggunakan sarana komputer, kemudian diterjemahkan sebagai kejahatan dunia maya. Indra Safitri mengemukakan bahwa kejahatan dunia maya adalah:

> "Jenis kejahatan yang berkaitan dengan pemanfaatan sebuah teknologi informasi tanpa batas serta memiliki karakteristik yang kuat dengan

---

[47] TR.Nitibaskara, *Ketika Kejahatan Berdaulat* (sebuah pendekatan kriminologi, hukum dan sosiologi). Jakarta: Peradaban, 2001, hal. 38.

[48] Istilah *cyber crime* oleh beberapa orang diterjemahkan sebagai kejahatan siber, kejahatan ruang siber (Muladi) dan tindak pidana mayantara. Menurut Barda Nawawi Arief, tindak pidana mayantara identik dengan tindak pidana di ruang siber (cyberspace). Penulis sependapat dengan pemakaian istilah kejahatan mayantara, karena perbuatan pelaku identik dengan kejahatan dalam arti kriminologis yang memanfaatkan kecanggihan sarana teknologi informasi, berupa jaringan internet untuk melakukan perbuatan yang merugikan seseorang atau badan hukum demi mencapai tujuannya, seperti memperoleh keuntungan materiel dan lain-lainnya.

[49] Peter Stephenson, *Investigating Computer-Related Crime*: A Hanbook For Corporate Investigators London, New York, CRC Press: Washington D.C:, 2000, hal. 56.

sebuah rekayasa teknologi yang mengandalkan kepada tingkat keamanan yang tinggi dan kredibilitas dari sebuah informasi yang disampaikan dan diakses oleh pelanggan internet."[50]

Dalam beberapa literatur, *cyber crime* sering diidentikkan sebagai *computer crime*.[51] *The U.S. Department of Justice* memberikan pengertian *computer crime* sebagai:"*...any illegal act requiring knowledge of computer technology for its perpetration, investigation, or prosecution*".[52]

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*"[53]

Canadian law enforcement agencies mendefinisikan *Cybecrime* sebagai berikut : *cyber crime is generally defined as a criminal offence involving a computer as the object of the crime, or the tool used to commit a material component of the offence*[54]. Selanjutnya, berdasarkan definisi tersebut, *Canadian Police College* mengklasifikasikan 2 macam katagori *cyber crime*, yakni :

1. *First, where the computer is the tool of the crime. This category includes crimes that law enforcement has been fighting in the physical world but now is seeing with increasing frequency on the Internet. Some of these crimes include child pornography, criminal harassment, fraud,*

---

[50] Indra Safitri, "Tindak Pidana di Dunia Cyber" dalam Insider, Legal Journal From Indonesian Capital and Investment Market. Sumber: http://business.fortunecity.com/buffett/ 842/ art180199 tindakpidana.html.

[51] Sementara sebagian pendapat yang lain memisahkan secara tegas istilah computer crime dan cyber crime. Nazura Abdul Manap dalam makalahnya yang berjudul Cyber-crimes: Problems and Solutions Under Malaysian Law, memberikan definisi sebagai berikut:"Defined broadly, "computer crime" could reasonably include a wide variety of criminal offences, activities or issues. It also known as a crime committed using a computer as a tool and it involves direct contact between the criminal and the computer. There is no Internet line involved, or only limited networking used such as the Local Area Network (LAN). Whereas, cyber-crimes are crimes committed virtually through Internet online. This means that the crimes committed could extend to other countries.Anyway, it causes no harm to refer computercrimes as cyber-crimes or vise versa, since they have same impact in law. Nazura Abdul Manap, *Cyber-crimes: Problems and Solutions Under Malaysian Law*, makalah pada seminar nasional Money Laundering dan Cybercrime dalam Perspektif Penegakan Hukum di Indonesia, diselenggarakan oleh Laboratorium Hukum Pidana FH Universitas Surabaya, 24 Februari 2001, hal.3.

[52] Petrus Reinhard Golose, "Perkembangan Cyber Crime dan Upaya Penanggulangannya di Indonesia Oleh Polri", Jakarta: *Buletin Hukum Perbankan dan Kebanksentralan*, Volume 4 Nomor 2, Agustus, 2006, hal. 34.

[53] *Ibid*

[54] Cyber-Crime: *Issues, Data Sources, and Feasibility of Collecting Police-Reported Statistics*, Canadian Centre for Justice Statistics. Published by authority of the Minister responsible for Statistics Canada, 2002, hal.6.

intellectual property violations and the sale of illegal substances and goods. (Pertama, menggunakan komputer sebagai alat kejahatan. Kategori ini termasuk kejahatan-kejahatan yang diberantas oleh para penegak hukum di dunia nyata secara fisik tetapi yang sekarang terlihat semakin meningkat di internet. Beberapa dari kejahatan ini termasuk pornografi anak, penistaan, penipuan, pelanggaran hak atas kekayaan intelektual, dan penjualan bahan-bahan atau barang-barang ilegal).

2. *Second, where the computer is the object of the crime. Cyber-crime consists of specific crimes dealing with computers and networks. These are new crimes that are specifically related to computer technology and the Internet. For example, hacking or unauthorized use of computer systems, defacing websites, creation and malicious dissemination of computer viruses.*[55] (Kedua, komputer sebagai obyek kejahatan. Kejahatan maya terdiri atas kejahatan-kejahatan yang spesifik berkaitan dengan komputer dan jaringannya. Ini merupakan kejahatan baru yang secara spesifik berkaitan dengan teknologi komputer dan internet. Misalnya, hacking atau penggunaan sistem komputer tanpa ijin, perubahan materi pada website, pembuatan dan penyebaran jahat virus-virus komputer).

Eoghan Casey merumuskan "*Cyber crime is used throughout this text to refer to any crime that involves computer and networks, including crimes that do not rely heavily on computer*".[56] Selanjutnya Ia mengkategorikan *cyber crime* dalam empat kategori yaitu:

1. *A computer can be the object of crime.*
3. *A computer can be a subject of crime.*
4. *The computer can be used as the tool for conducting or planning a crime.*
5. *The symbol of the computer itself can be used to intimidate or deceive.*

---

[55] *Ibid*

[56] Eoghan Casey, *Digital Evidence and Komputer Crime*, London : A Harcourt Science and Technology Company, 2001. hal. 16.

Selanjutnya, merujuk pada dokumen Kongres PBB tentang *The Prevention of Crime and the Treatment of Offenders* yang dikeluarkan di Havana Cuba pada tahun 1990 dan di Wina, Austria pada tahun 2000, dua istilah yang terkait dengan pengertian *cyber crime*, yaitu *cyber crime* dan *computer related crime*. Dalam *back ground paper* untuk lokakarya Kongres PBB X/2000 di Wina Austria, istilah *cyber crime* dibagi dalam dua kategori. Pertama, *cyber crime* dalam arti sempit (*in a narrow sense*) disebut *computer crime*, dan kedua, *cyber crime* dalam arti luas (*in a broader sense*) disebut *computer related crime*. Lengkapnya sebagai berikut:

1. *Cyber crime in a narrow sense (computer crime): any legal behaviour directed by means of electronic operations that targets the security of computer system and the data processed by them.* (Kejahatan siber dalam arti sempit [kejahatan komputer]: setiap perilaku hukum yang dilakukan dengan menggunakan operasi elektronik dengan sasaran sistem keamanan komputer dan data yang diproses oleh komputer).
2. *Cyber crime in a broader sense (computer related crime): any illegal behaviour committed by means on in relation to, a computer system or network, including such crime as illegal possession, offering or distributing information by means of a computer system or network.*[57] (Kejahatan siber dalam arti luas [kejahatan yang berhubungan dengan komputer]: Setiap perilaku illegal yang dilakukan berkaitan dengan, suatu sistem atau jaringan komputer, termasuk kejahatan seperti pemilikan, penawaran atau penyebaran informasi ilegal dengan menggunakan suatu sistem atau jaringan komputer).

Sementara itu Collin Barry C. menjelaskan istilah *cyber crime* sebagai berikut :

> *"Term "cyber-crime" is young and created by combination of two words: cyber and crime. The term "cyber" means the cyber-space (terms "virtual space", "virtual world" are used more often in literature) and means (according to the definition in "New hacker vocabulary" by Eric S. Raymond) the informational space modeled through computer, in which defined types of objects or symbol images of information exist – the place where computer programs work and*

---

[57] Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*, Jakarta: Kencana Predana Media Group, 2007, hal. 24.

> *data is processed.*"[58] ("Istilah "kejahatan mayantara" masih baru dan diciptakan atas dasar kombinasi dua kata: mayantara dan kejahatan. Istilah 'mayantara' berarti ruang siber [istilah "ruang virtual", "dunia virtual" lebih sering digunakan dalam literatur] dan berarti [menurut definisi dalam "kosa kata baru hacker" oleh Eric S. Raymond] ruang informasi yang di bentuk melalui komputer, dimana jenis-jenis obyek dan simbol-simbol citra informasi tertentu berada – tempat dimana program komputer bekerja dan data di proses).

Kejahatan dunia maya atau *cyber crime* pada dasarnya adalah suatu tindak pidana yang mempunyai hubungan dengan ruang dunia maya, baik yang menyerang fasilitas umum di dalam ruang dunia maya ataupun kepemilikan pribadi.

Encyclopedia of crime and justice mendefinisikan *cyber crime* atau kejahatan dunia maya sebagai setiap perbuatan melawan hukum yang memerlukan pengetahuan tentang teknologi komputer yang bertujuan untuk dapat melakukan kejahatan yang dapat dikategorikan dalam dua bentuk, yaitu: *pertama*, penggunaan komputer sebagai alat untuk melakukan suatu kejahatan, seperti pemilikan uang secara ilegal, pencurian property. *Kedua* penggunaan *computer* untuk merencanakan suatu kejahatan, menggunakan komputer sebagai obyek dari suatu kejahatan, seperti sabotase, pencurian atau perubahan data- data milik pihak lain.[59] Salah satu versi membagi kejahatan dunia maya menjadi tiga bagian yaitu pelanggaran akses, pencurian data, dan penyebaran informasi untuk tujuan kejahatan.

Versi yang lain membagi tipe-tipe kejahatan dunia maya menjadi tujuh, seperti dikemukakan Philip Renata[60] yaitu:

1. *Joy computing*, yaitu pemakaian komputer orang lain tanpa izin. Hal ini termasuk pencurian waktu operasi komputer. Penggunaan waktu operasi komputer lain banyak digunakan untuk mengirimkan *spam e-mail* agar tidak terlacak. Saat ini terdapat sekitar 3 sampai 4 juta *bot* yang aktif di

---

[58]Collin Barry C, "The Future of CyberTerrorism, Proceedings of 11th Annual International Symposium on Criminal Justice Issues", The University of Illinois at Chicago, dikutip dari makalah Vladimir Golubev, *cyber-crime and legal problems of usage network the INTERNET.* 1996.

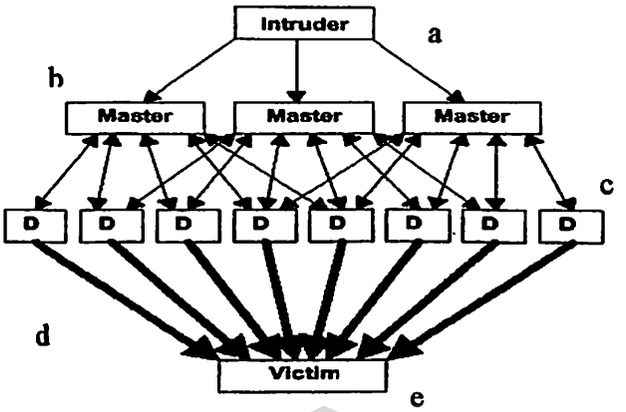
[59]Encyclopedia of crime and justice, volume 4, New York: Free Press, 1983, hal. 218-222.

[60]Philip Renata, "Type of Cyber Crime", *Suplemen BisTek Warta Ekonomi,* No. 24 edisi Juli 2000, hal. 52.

Internet. *Botnet* telah menjadi pasukan penggerak di balik organisasi kejahatan *online* karena mereka memiliki risiko yang rendah dengan potensi keuntungan yang tinggi,

2. *Hacking,* yaitu mengakses secara tidak sah atau tanpa izin dengan alat suatu terminal. Menurut sebuah penelitian di Inggris, *hacker* biasanya melakukan serangan ke sistem komputer rumahan sebanyak 50 kali per malam. Selama satu bulan penelitian, salah satu PC rumahan dibiarkan terkoneksi terus dengan internet. Ternyata para *hacker* berupaya memperoleh data di dalam PC dengan menggunakan virus dan malware untuk menjumput informasi penting pemiliknya.
3. *The Trojan Horse,* yaitu manipulasi data atau program dengan jalan mengubah data atau instruksi pada sebuah program, menghapus, menambah, menjadikan tidak terjangkau dengan tujuan untuk kepentingan pribadi atau orang lain. Salah satu kasus terbaru dengan trojan terjadi pada pengguna *Voice over Internet Protocol* (*VoIP*) *Skype*. Trojan tersebut menyebar melalui *software* komunikasi *VoIP Skype* dan berupaya mencuri *password* aplikasi tersebut. Trojan mengirim sebuah pesan melalui *tool Skype Chat* dan meminta penerimanya untuk menjumput *file* sp.exe. Virus di dalam *file* tersebut akan menyebar jika program dijalankan dan akan men-*download* kode pemprograman *Skype*, menggandakan diri, dan mengambil alih *password*. Situs web yang diserang oleh trojan ini telah ditutup untuk menghindari kerugian lebih lanjut.
4. *Data Leakage,* yaitu menyangkut bocornya data ke luar terutama mengenai data yang harus dirahasiakan. Pembocoran data komputer itu bisa berupa berupa rahasia negara, perusahaan, data yang dipercayakan kepada seseorang dan data dalam situasi tertentu.

Ilustrasi salah satu contoh tindakan kejahatan dunia maya oleh seorang penyusup (*intruder*) melalui komputernya untuk mencuri data yang sedang dipertukarkan antara dua komputer lain dengan cara memperlambat respon server dapat dilihat pada gambar berikut:



Gbr.2.INTRUDER

Keterangan gambar:

a. *Look up* foobar.the-intruder.com untuk dipaksakan masuk ke ISP's cache
b. *Look up* www.the-intruder.com untuk mendapatkan nomor sekuensial selanjutnya dari ISP
c. Permintaan kepada www.theintruder.com (membawa nomor sekuensial selanjutnya dari ISP, sebut saja D
d. Dengan sigap dan cepat look up user2.com (untuk memaksa ISP untuk memasukkan com server ke dalam antrian pada langkah 5)
e. Antrian yang sah untuk user2 dengan sekuensial = n+1

5. *Data Diddling*, yaitu suatu perbuatan yang mengubah data valid atau sah dengan cara tidak sah, mengubah *input* data atau *output* data. Perbuatan penyusup yang memasuki ruang komunikasi antara para pengguna yang sah bisa berlanjut kepada *data didling*.
6. *To frustate data communication* atau penyia-nyiaan data komputer.
7. *Software piracy* yaitu pembajakan perangkat lunak terhadap hak cipta yang dilindungi HAKI.

Salah satu jenis kejahatan lain pada dunia maya yang termasuk baru tetapi telah cukup banyak merugikan konsumen internet adalah "*phishing*". *Phishing* adalah suatu tindak kejahatan yang menggunakan cara sosial. Pelakunya mencoba untuk mendapatkan informasi sensitif seperti *password* dan informasi detil kartu kredit dengan cara yang curang seperti dengan menyamar menjadi seseorang atau

perusahaan pada suatu jaringan komunikasi elektronik, baik melalui surat elektronik, pesan instan, dengan membuat *website* yang seakan-akan dari perusahaan dagang elektronik yang menawarkan berbagai barang, ataupun sejenisnya. *Phishing* sebelumnya telah banyak dilakukan melalui telepon.[61]

Instrumen Hukum Internasional di bidang kejahatan mayantara (*cyber crime*) merupakan sebuah fenomena baru dalam tatanan Hukum Internasional modern mengingat kejahatan siber sebelumnya tidak mendapat perhatian negara-negara sebagai subjek Hukum Internasional. Munculnya bentuk kejahatan baru yang tidak saja bersifat lintas batas (transnasional) tetapi juga berwujud dalam tindakan-tindakan virtual telah menyadarkan masyarakat internasional tentang perlunya perangkat Hukum Internasional baru yang dapat digunakan sebagai kaidah hukum internasional dalam mengatasi kasus-kasus *cyber crime.*[62]

Cyber crime merupakan salah satu bentuk atau dimensi baru dari kejahatan masa kini yang mendapat perhatian luas di dunia internasional. Volodymyr Golubev menyebutnya sebagai *"the new form of antisocial behavior"*. Beberapa julukan/sebutan lainnya yang "cukup keren" diberikan kepada jenis kejahatan baru ini di dalam berbagai tulisan antara lain, sebagai "kejahatan dunia maya" *("cyberspace/virtual space offence")*, dimensi baru dari *"hitech crime"*, dimensi baru dari *"transnational crime"*, dan dimensi baru dari *"white collar crime"*. Bahkan dapat dikatakan sebagai dimensi baru dari *"environmental crime"*.[63]

2.3. Karakteristik Kejahatan Mayantara

Karakteristik kejahatan mayantara (*cyber crime*) yang paling menonjol, bahwa kejahatan tersebut dilakukan dengan sarana komputer atau teknologi informasi. Namun disadari bahwa kejahatan dengan sarana komputer ternyata tidak sederhana, karena banyak persoalan teknis yang berkaitan dengan teknologi komputer yang tidak banyak dipahami oleh masyarakat pada umumnya. Berkaitan

---

[61] *Ibid*

[62] Ahmad M. Ramli, "Instrumen Hukum Internasional tentang Cyber Crime dan Antisipasi Implementasinya dalam Hukum Pidana Nasional, Makalah Seminar Nasional Information Technology Security dan Cyber Crime", Jakarta: *Kementrian Komunikasi dan Informasi RI*, 9 Desember 2003. hal. 2.

[63] Barda Nawawi Arief, *Antisipasi Penanggulangan Cybercrime Dengan Hukum Pidana*. Jakarta: Perdana Kencana Group, 2007, hal. 237.

dengan itu, Prof Mardjono Reksodiputro[64] mengemukakan bahwa kejahatan dengan sarana komputer, apakah dapat menjadi suatu permasalahan dalam penggunaan-penggunaanya sebagaimana dikemukakan bahwa masyarakat modern sekarang dalam masa peralihan dari "masyarakat industri" ke "masyarakat informasi". Dalam masyarakat informasi ini yang merupakan ciri utamanya adalah penggabungan antara pengetahuan informasi dengan pengetahuan telekomunikasi. Jika sebelumnya komputer telah mendobrak cara-cara penyimpanan, pengolahan dan penyampaian data di dalam pusat-pusat otak elektronik (otomatisasi), maka sekarang pusat-pusat tersebut saling dihubungkan pula melalui alat-alat telekomunikasi (antara lain telpon). Pengambilan keputusan, pelaksanaan dan pemantauan (monitoring) dilakukan berdasarkan data yang tersedia dalam pusat-pusat tadi, yang saling berhubungan (juga melampaui batas-batas wilayah negara) melalui alat telekomunikasi. Kegiatan ini menjadi lebih abstrak, rumit (*complex*) dan sukar terlihat. Penggunaan kertas, sebagai media penyampaian data dan informasi, makin berkurang (kertas dapat dilihat dan diraba), sehingga kesalahan-kesalahan (baik karena kelalaian, maupun kesengajaan) tidak begitu cepat dapat diketahui lagi. Lebih jauh lagi, alat canggih komputer ini memerlukan ahli-ahli khusus (ahli komputer) untuk menanganinya, yang jumlahnya terbatas. Manipulasi data komputer sering pula sukar ditelusuri (apalagi oleh 'orang awam') karena relatif mudahnya pula untuk menghapus jejak. Inilah secara sederhana inti permasalahan kita. Pertanyaannya kini menjadi: "seberapa jauh hukum pidana dapat dan harus dipergunakan untuk menghambat penyalahgunaan komputer, tanpa mengurangi arus data dan informasi yang lancar (yang sangat diperlukan dalam masyarakat informasi adalah kecepatan dalam "transfer data").

Penyalahgunaan komputer dapat dibagi dalam kategori sebagai berikut: (a) manipulasi komputer, (b) spionase komputer, (c) sabotase komputer, (d) pemakaian secara tidak sah komputer, dan (e) "memasuki" secara tidak sah komputer. Pada umumnya pembahasan penyalahgunaan "biasa" menyangkut: manipulasi, pemakaian secara tidak sah (*unauthorized acces*). Kerugian yang

---

[64]Mardjono Reksodiputro, *Kemajuan Pembangunan Ekonomi dan Kejahatan*, Jakarta: PPKPH UI, 1994, hal 10-11.

diderita disini umumnya bersifat 'privat', manusia maupun perusahaan). Dalam hal "spionase" hal ini sudah menyangkut data rahasia, seperti rahasia negara tetapi dapat juga menyangkut rahasia perusahaan (seperti "*software piracy*" dan "*high technology theft*"). Kejahatan dalam bentuk "sabotase" akan dapat menimbulkan efek kerugian yang besar pada masyarakat, karena caranya dengan "merusak" atau "menghancurkan" peralatan dan atau sistem jaringan komputer.

Pendekatan yang lain dilakukan oleh Komisi Kejahatan Komputer Belanda dalam laporannya, yaitu dengan membedakan antara perlindungan untuk "sarana"(*middelen*) dan perlindungan untuk "data" (*gegevens*). Dalam hal sarana disarankan agar dijadikan tindak pidana: (a) menghancurkan, merusak, membuat tidak dapat dipakai atau pun menimbulkan gangguan kerja dalam sarana komputer, dan (b) apa yang dinamakan *"computervredebreuk"* (analog dengan "huisvredebreuk", pasal 167 KUHP), yaitu "memasuki" secara melawan hukum sistem komputer atau bagian yang dilindungi oleh sistem pengamanan komputer. Mengenai perlindungan untuk data disarankan agar dijadikan tindak pidana: (a) membuat tidak dapat dipakai atau menghapus atau membuat tidak dapat "dimasuki" data bersangkutan, (b) memanipulasi data, seperti menghilangkan, merubah atau menambah data lain, dan (c) hal-hal yang melanggar perlindungan terhadap data yang harus dirahasiakan atau bersifat eksklusif atau bersifat konfidensial. Dicatat pula bahwa sebagian dari perlindungan ini terletak dalam bidang perlindungan "transfer data" atau telekomunikasi.[65]

Demikian pula menurut Stein Sehjolberg bahwa *cyber crime* merupakan kejahatan komputer yang menggunakan sistem jaringan internet yang sangat luas dan terhubung satu komputer dengan komputer yang lain, namun beberapa aktivis di *cyberspace* membutuhkan ketentuan baru untuk memperkuat ketentuan hukum pidana yang lama.[66]

Mardjono Reksodiputro lebih jauh berpendapat bahwa Indonesia dapat menggunakan kedua pendekatan tersebut bersama-sama, sebagaimana Amerika

---

[65] *Ibid.*

[66] Judge Stenin, Schjolberg dan Amanda M. Hubbard, *Harmonizing National Legal Approaches on Cybercrime,* WSIS Thematic Meeting on Cybersecurity, ITU, Geneva, 28 June-1July 2005, Document: CYB/04, 10 June 2005, dapat dijumpai di http://www.itu. int/osg/cybersecurity //doc/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf

Serikat mempergunakan pendekatan tersebut, contohnya dengan mengamandemen *Securities Act* 1933 (UU pasar modal) dan mengundangkan *Computer Fraud and Abuse Act.* Tumbuh kembangnya tindak pidana *cyber crime* disebabkan oleh banyak macam faktor, tetapi secara garis besar faktor yang menimbulkan tindak pidana *cyber crime* tersebut disebabkan oleh dua hal, yaitu teknis dan sosio ekonomi (kemasyarakatan).[67]

Pertama dari segi teknis, tidak bisa dipungkiri bahwa kemajuan teknologi (teknologi informasi) berdampak negatif bagi perkembangan masyarakat. Berhasilnya teknologi tersebut menghilangkan batas wilayah negara menjadikan dunia ini menjadi begitu sempit. keterhubungan antara jaringan yang satu dengan jaringan yang lain memudahkan bagi si pelaku kejahatan untuk melakukan aksinya. Kemudian, tidak meratanya penyebaran teknologi menjadikan yang satu lebih kuat daripada yang lain. Kelemahan tersebut dimanfaatkan oleh mereka yang tidak bertanggung jawab untuk melakukan kejahatan. [68]

Kedua, faktor sosio ekonomi, *cyber crime* merupakan produk ekonomi. Isu global yang kemudian dihubungkan dengan kejahatan tersebut adalah keamanan jaringan (*security network*). Kemanan jaringan merupakan isu global yang digulirkan berbarengan dengan internet. Sebagai komoditi ekonomi, banyak negara yang tentunya sangat membutuhkan perangkat keamanan jaringan. *Cyber crime* berada dalam skenario besar dari kegiatan ekonomi dunia. Pengalaman kita pada saat memasuki tahun 2000. Isu virus Y2K yang akan menghilangkan (menghapuskan) data dan informasi ternyata tidak pernah terjadi. Hal ini tentu saja mengkhawatirkan dunia perbankan dan pasar modal, para penyediasa jasa lalu memberikan jaminan keamanan bahwa data dan informasi yang ada telah terbebas dari Y2K.[69]

Dalam perspektif hukum, *cyber crime* ini bukan merupakan kejahatan yang baru yang kemudian dikembangkan dengan media oleh para pelaku. Konsep dari

---

[67]Pendekatan Hukum untuk keamanan dunia cyber serta Urgensi Cyber Jenis Berkas: PDF/Adobe Acrobat-Versi HTML prastowo.staff.ugm.ac.id/files/130M-09-final2.0-laws_investigations_and_ethics.pdf

[68]Barda Nawawi Arief, *Op.Cit.*, hal. 90.

[69]Telekomunikasi dan Teknologi Tindak Pidana *Cyber Crime* http: // www. Hukumonline .com/klinik_detail.asp?id=2824

tindak pidana tersebut juga tidak mengalami perkembangan, hanya caranya saja yang sedikit berbeda.

Sejak abad 21, kejahatan telah berkembang tidak hanya bersifat konvensional dan dalam lingkup regional, tetapi telah berkembang mengarah pada lintas negara, dan memiliki dampak yang luas dan mendasar terhadap asas-asas hukum, norma, dan lembaga yang berkaitan dengan penerapan hukum pidana. Dari sinilah kemudian muncul istilah kejahatan transnasional dan kejahatan internasional. [70] *Cyber crime* merupakan suatu kejahatan yang bersifat transnasional sehingga termasuk ke dalam kategori *transnational crime*. Adapun karakteristik dari *transnational crime* adalah:

1. *it is committed in more than one State;*
2. *it is committed in one State but a substanstial part of its preparation, planning, direction or control takes place in another State;*
3. *it is committed in one State but involves an organized criminal group that engages in criminal activities in more than one State; or*
4. *it is committed in one State but has substantial effects in another State.* [71]

Perkembangan kejahatan yang bersifat transnasional ini, memberikan makna baru bahwa kejahatan bukan lagi merupakan hak eksklusif suatu negara melainkan telah menjadi hak relatif dari satu atau lebih negara, yang dapat melakukan penyidikan dan penuntutan atas kejahatan transnasional yang sama.[72] Kondisi yang demikian ini dihadapkan pada hukum pidana nasional yang masih bersifat konvensional, sehingga diperlukan kajian yang mendalam guna memahami dan menata perkembangan hukum pidana, asas-asas, serta norma-norma hukum nasional.

Di samping itu menurut, Howard Abadinsky menulis bahwa kejahatan sering dipandang sebagai *Mala in se* atau *mala prohibita*. *Mala in se* menunjuk

---

[70]Istilah transnasional dalam hukum internasional diperkenalkan oleh Phillip C. Jessup, pada tahun 1968, dan istilah "*transnational crime*" diakui sebagai nomenklatur baru dalam hukum internasional, yaitu dalam *Convention Against Transnational Organized Crime.*

[71]Pasal 3 ayat (2) *Convention Against Transnational Organized Crimes.*

[72]H. Romli Atmasasmita, "Pengaruh Konvensi Internasional terhadap Perkembangan Asas-Asas Hukum Pidana Nasional", Makalah dalam Seminar Tentang Asas-Asas Hukum Pidana Nasional, Semarang 26 –28 April, 2004, hal.2.

kepada perbuatan yang pada hakikatnya adalah kejahatan, contohnya pembunuhan. Sedangkan *Mala prohibita* menunjuk kepada perbuatan yang hanya ditetapkan oleh negara sebagai perbuatan yang dilarang (*unlawful*).[73]

Menurut Mardjono Reksodiputro sebagian masyarakat Indonesia mengartikan kejahatan sebagai pelanggaran atas hukum pidana, baik dalam undang-undang pidana maupun dalam perundang-undangan administrasi yang bersanksi pidana.[74] Dengan persepsi yang demikian, Arief Amrullah mengatakan bahwa kejahatan mendahului hukum. Maksudnya, suatu perbuatan yang dianggap sangat merugikan masyarakat, kemudian muncul hukum pidana yang bertujuan melindungi kepentingan masyarakat.[75] Selain itu, lanjut Reksodiputro, ada pula yang mengartikan suatu perbuatan tertentu sebagai kejahatan karena hukum yang menyatakan demikian. Dengan kata lain, hukum yang mendahului kejahatan. Maksudnya, belum tentu hukum pidana melindungi kepentingan masyarakat secara keseluruhan karena dapat saja hukum pidana hanya melindungi kepentingan sebagian kelompok masyarakat tertentu.

Berdasarkan penjelasan diatas, dikaitkan dengan penyimpangan-penyimpangan dalam dunia maya, dapat identifikasi bahwa penyimpangan-penyimpangan yang terjadi dalam dunia maya, sebagian besar dapat dikatakan sebagai sebuah kejahatan.

Hal ini bukan tanpa dasar, apa yang telah diuraikan diatas memenuhi kriteria sangat merugikan masyarakat. Sebagai gambaran, meski penetrasi teknologi informasi di Indonesia masih rendah, nama Indonesia ternyata begitu populer terkait kejahatan di dunia maya.

Berdasar data *Clear Commerce*, tahun 2002 lalu Indonesia berada di urutan kedua setelah Ukraina sebagai negara asal *carder* terbesar di dunia. Sebelumnya, Survei AC Nielsen 2001 mencatat, Indonesia berada pada posisi keenam terbesar di dunia atau keempat di Asia dalam tindak kejahatan mayantara, karena dicap sebagai sarang teroris dunia maya, banyak alamat IP (*internet protocol*) Indonesia

---

[73] *Ibid.* hal. 29.
[74] Mardjono, Reksodiputro, *Sistem Peradilan Pidana Indonesia* (Melihat Kejahatan dan Penegakan Hukum dalam batas-batas toleransi), Jakarta: Pusat Keadilan dan Pengabdian Hukum, 1994, hal. 10.
[75] H. Romli Atmasasmita, Op. cit., hal. 29.

yang sempat diblokir. Sehingga, orang Indonesia yang ingin berbelanja lewat internet tidak dipercaya lagi oleh pemilik-pemilik situs belanja online di luar negeri. [76] Secara garis besar, kejahatan yang berkaitan dengan teknologi informasi dapat dibagi jadi dua bagian besar. Pertama, kejahatan yang bertujuan merusak atau menyerang sistem atau jaringan komputer. Dan kedua, kejahatan yang menggunakan komputer atau internet sebagai alat bantu dalam melancarkan kejahatan. Namun begitu, mengingat teknologi informasi merupakan hasil konvergensi telekomunikasi, komputer dan media, kejahatan jenis ini berkembang menjadi luas lagi.

Dalam catatan beberapa literatur dan situs-situs yang mengetengahkan *cyber crime*, berpuluh jenis kejahatan yang berkaitan dengan dunia siber. Yang masuk dalam kategori kejahatan umum yang difasilitasi teknologi informasi antara lain penipuan kartu kredit, penipuan bursa efek, penipuan perbankan, pornografi anak, perdagangan narkoba, serta terorisme. Sedang kejahatan yang menjadikan sistem dan fasilitas TI sebagai sasaran diantaranya adalah *denial-of-service attack (DDoS), defacing, cracking* ataupun *phreaking*.

Hingga akhir 2008, Unit V IT/*Cybercrime*, Direktorat II Ekonomi Mabes Polri mencatat sekitar 55 kasus terkait dengan kejahatan teknologi informasi. Modus kejahatan yang dilakukan meliputi penipuan kartu kredit, penipuan perbankan dan terorisme dengan korban berasal dari AS, Inggris, Australia, Jerman, Korea, Singapura serta beberapa daerah di tanah air. Perkembangan ini menarik, terutama yang berkenaan dengan penipuan penggunaan kartu kredit meningkat tajam. Kejahatan dengan menggunakan kartu kredit orang lain, prakteknya sudah berlangsung lama di tanah air. Bahkan telah menjadi barang mainan dengan menukarkan informasi mengenai nomor *account* kartu kredit antara satu *carder* dengan lainnya.

Berdasarkan uraian tersebut, sebagai bahan acuan sekaligus dalam usaha untuk tidak menimbulkan salah tafsir, dapat dikemukakan tulisan Muladi dan Barda Nawawi Arief yang memberi ruang lingkup kejahatan komputer sebagai: [77]

---

[76] Rully Ferdian, "Mengintai Pelaku Cybercrime", http://www.eBizzAsia.html.com, Juli 2003, diakses 20 Nopember 2008.
[77] Muladi dan Barda Nawawi Arief, Op. Cit., hal. 53.

1. Komputer sebagai instrumen untuk melakukan kejahatan tradisional, seperti pencurian, penipuan, penggelapan uang atau deposito kredit, penyalahgunaan *credit card* dan pemalsuan.
2. Komputer dan perangkatnya sebagai objek penyalahgunaan, seperti *computer sabotage* yang dapat mencakup perbuatan-perbuatan *destroys or alter data, renders it mainingless, useless or inefective, interveres with its lawful use, interferes with any person entitled there to,*
3. Penyalahgunaan yang berkaitan dengan komputer atau data yang dapat berkaitan erat dengan *interference with lawful use, interception of communication or functions of computer system, unautorized use of computer computer system* mencakup *unauthorized obtaining of computer service or time* dan *unauthorized use of computer system*, dan
4. *Unauthorized acquisition, disclosure or use of information and data.*

Dari hal-hal tersebut di atas, dikaitkan dengan *cyber crime*, dimana terjadi konvergensi telekomunikasi, komputer dan media, penulis mengidentifikasi tiga bentuk anatomi kejahatan *cyber crime*, sebagai berikut :

1. Tindak pidana yang berkaitan dengan jaringan telekomunikasi internet, umumnya terkait erat dengan persoalan kerahasiaan, integritas dan keberadaan data dan sistem komputer:
   a. *Illegal access* (akses secara tidak sah terhadap sistem komputer), yaitu dengan sengaja dan tanpa hak melakukan akses secara tidak sah terhadap seluruh atau sebagian sistem komputer, dengan maksud untuk mendapatkan data komputer atau maksud-maksud lainnya demi memperoleh manfaat secara melawan hukum, biasanya, berkaitan erat dengan suatu sistem komputer yang terhubung dengan sistem komputer lain. *Hacking* merupakan salah satu dari jenis kejahatan ini yang sangat sering terjadi.
   b. *Data interference* (mengganggu data komputer), yaitu dengan sengaja melakukan perbuatan merusak, menghilangkan sebagian, menghapus, memerosotkan (*deterioration*), mengubah atau menyembunyikan (*suppression*) data komputer tanpa hak. Perbuatan

menyebarkan virus komputer merupakan salah satu dari jenis kejahatan ini yang sering terjadi.

c. *System interference* (mengganggu sistem komputer), yaitu dengan sengaja dan tanpa hak melakukan gangguan terhadap fungsi sistem komputer dengan cara memasukkan, memancarkan, merusak, menghapus, memerosotkan, mengubah, atau menyembunyikan data komputer. Perbuatan menyebarkan program virus komputer dan *e-mail bombings* (surat elektronik berantai) merupakan bagian dari jenis kejahatan ini yang sangat sering terjadi.

d. *Illegal interception in the computers, systems and computer networks operation* (intersepsi secara tidak sah terhadap komputer, sistem, dan jaringan operasional komputer), yaitu dengan sengaja melakukan intersepsi tanpa hak, dengan menggunakan peralatan teknik, terhadap data komputer, sistem komputer, dan atau jaringan operasional komputer yang bukan diperuntukkan bagi kalangan umum, dari atau melalui sistem komputer, termasuk didalamnya gelombang elektromagnetik yang dipancarkan dari suatu sistem komputer yang membawa sejumlah data. Perbuatan dilakukan dengan maksud tidak baik, atau berkaitan dengan suatu sistem komputer yang dihubungkan dengan sistem komputer lainnya.

e. *Data theft* (mencuri data), yaitu kegiatan memperoleh data komputer secara tidak sah, baik untuk digunakan sendiri ataupun untuk diberikan kepada orang lain. *Identity theft* merupakan salah satu dari jenis kejahatan ini yang sering diikuti dengan kejahatan penipuan (*fraud*). Kejahatan ini juga sering diikuti dengan kejahatan *data leakage*.

f. *Data leakage and espionage* (membocorkan data dan memata-matai), yaitu kegiatan memata-matai dan atau membocorkan data rahasia baik berupa rahasia negara, rahasia perusahaan, atau data lainnya yang tidak diperuntukkan bagi umum, kepada orang lain, suatu badan atau perusahaan lain, atau negara asing.

g. *Misuse of devices* (menyalahgunakan peralatan komputer), yaitu dengan sengaja dan tanpa hak, memproduksi, menjual, berusaha memperoleh untuk digunakan, diimpor, diedarkan atau cara lain untuk kepentingan itu, peralatan, termasuk program komputer, password komputer, kode akses, atau data semacam itu, sehingga seluruh atau sebagian sistem komputer dapat diakses dengan tujuan digunakan untuk melakukan akses tidak sah, intersepsi tidak sah, mengganggu data atau sistem komputer, atau melakukan perbuatan-perbuatan melawan hukum lain.

2. Tindak pidana yang menggunakan komputer sebagai alat kejahatan:
   a. *Credit card fraud* (penipuan kartu kredit);
   b. *Bank fraud* (penipuan terhadap bank);
   c. *Service offered fraud* (penipuan melalui penawaran suatu jasa);
   d. *Identity theft and fraud* (pencurian identitas dan penipuan);
   e. *Computer-related fraud* (penipuan melalui komputer);
   f. *Computer-related forgery* (pemalsuan melalui komputer);
   g. *Computer-related betting* (perjudian melalui komputer);
   h. *Computer-related extortion and threats* (pemerasan dan pengancaman melalui komputer).
3. Tindak pidana yang berkaitan dengan Komputer sebagai Media, yakni terkait dengan isi atau muatan data atau sistem komputer:
   a. *Child pornography* (pornografi anak);
   b. *Infringements of copyright and related rights* (pelanggaran terhadap hak cipta dan hak-hak terkait);
   c. *Drug traffickers* (peredaran narkoba), dan lain-lain.

Kejahatan mayantara atau *cyber crime* memang diidentikkan dengan kejahatan dengan sarana komputer. Namun, di dalam literatur, dijumpai adanya istilah *cyber crime* dan *computer related crimes* (CRC). Dalam konteks ini *cyber crime* dapat dibagi dalam dua kategori, yaitu *cyber crime* dalam arti sempit ("*in a narrow sense*") disebut *computer crime* dan *cyber crime* dalam arti luas ("*in a*

broader sense") disebut *computer related crime* (CRC). Dijelaskan dalam dokumen itu, bahwa: [78]

> *Cyber crime (CC) in a narrow sense (computer crime):*
>
> > *Any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them; (*Kejahatan mayantara dalam arti sempit [kejahatan komputer]: setiap perilaku hukum yang dilakukan dengan menggunakan operasi elektronik dengan sasaran sistem keamanan komputer dan data yang diproses oleh komputer).
>
> *Cyber Crime in a broader sense (computer-related crime):*
>
> > *Any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession, offering or distributing information by means of a computer system or network.* (Kejahatan siber dalam arti luas [kejahatan yang berhubungan dengan komputer]: Setiap perilaku illegal yang dilakukan berkaitan dengan, suatu sistem atau jaringan komputer, termasuk kejahatan seperti pemilikan, penawaran atau penyebaran informasi ilegal dengan menggunakan suatu sistem atau jaringan computer).

Istilah *computer related crime* (CRC) mencakup keseluruhan bentuk-bentuk baru dari kejahatan yang ditujukan pada komputer, jaringan komputer dan para penggunanya, dan bentuk-bentuk kejahatan tradisional yang sekarang dilakukan dengan menggunakan atau dengan bantuan peralatan komputer. [79]

Jadi, dalam pemahaman *cyber crime* sebagai kejahatan dengan menggunakan sarana komputer, maka dapat pula dikatakan bahwa *cyber crime* meliputi kejahatan yang dilakukan:

1. Dengan menggunakan sarana-sarana dari sistem/jaringan komputer *("by means of a computer system or network");*
2. Di dalam sistem/ jaringan komputer *("in a computer system or network")* dan ;
3. Terhadap sistem/jaringan komputer *("against a computer system or network").*
4. Dengan memperhatikan kutipan di atas (a dan b), dapatlah disimpulkan, bahwa *Cyber Crime* jenis ke-l dan ke-2 merupakan *Cyber Crime* dalam

---

[78] Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan,* Jakarta: Kencana Perdana Media, 2007, hal. 242.
[79] *Ibid,* hal. 243.

arti luas; sedangkan jenis ke-3 merupakan *Cyber Crime* dalam arti sempit.

2.4. Perkembangan Kejahatan Mayantara dengan Sarana Internet

Pesatnya perkembangan di bidang teknologi informasi saat ini merupakan dampak dari semakin kompleksnya kebutuhan manusia akan informasi itu sendiri. Perkembangan ini telah menjadi realita sehari-hari bahkan menjadi tuntutan masyarakat yang tidak dapat ditawar lagi. Tujuan utama perkembangan ilmu pengetahuan dan teknologi (iptek) adalah kehidupan masa depan umat manusia yang lebih baik, mudah, murah cepat dan aman sebagai bagian filsafat teknologi.[80]

Revolusi teknologi informasi (TI) diawali dengan ditemukannya peralatan yang disebut komputer, dalam prosesnya telah membentuk dunia tersendiri, yaitu yang dikenal dengan sebutan dunia maya *(cyberspace)* atau *alam virtual* (semu). Disebut dunia, karena pada kenyatannya *web-site interconection* atau sistem jaringan komplek dalam TI telah menjadi sub sistem besar tersendiri, yang merupakan miniatur dunia.[81] Lahirnya internet sebagai hasil revolusi teknologi dimulai pada 1969 ketika Departemen Pertahanan Amerika, *U.S. Defense Advanced Research Projects Agency* (DARPA) memutuskan untuk mengadakan riset tentang bagaimana caranya menghubungkan sejumlah komputer sehingga membentuk jaringan organik. Program riset ini dikenal dengan nama ARPANET (*Advanced Research Projects Agency Network).* Pada 1970, sudah lebih dari 10

---

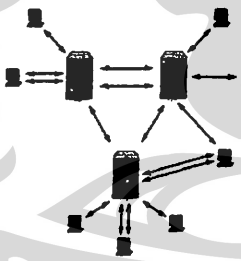
[80]Mario Bunge, http://filsafat-ilmu.blogspot.com/ Hakekat teknologi diakses tanggal 20 Nopember 2008. Filsafat teknologi dapat dipandang sebagai gabungan dari lima cabang filsafat yang masih berkembang yaitu: *technoepistemology, technometaphysic, technoaxiology, technoethics, technopraaxiology*. Technoepistemology adalah telaah filsafat tentang pengetahuan teknis. Persoalan yang dibebaskan, antara lain adalah membedakan pengetahuan teknologi dan pengetahuan biasa dan pengetahuan ilmiah, atau metode teknologi yang sejajar dengan metode ilmiah serta aturan-aturannya. Technometaphysic adalah telaah filsafat tentang sifat dasar sistem-sistem buatan dari mesin-mesin sederhana sampai sistem-sistem bagan manusia yang rumit. Persoalan yang dibahasnya antara lain adalah prasyarat-prasyarat ontologis dari teknologi atau kekhasan dari semua barang teknologi yang membedakannya dari benda-benda alamiah. Technoaxiologi adalah telaah filsafat tentang penilaian yang dilakukan oleh para ahli teknologi dalam pelaksanaan kegiatan-kegiatan teknologi mereka. Persoalan yang dibahasnya, antara lain adalah, nilai-nilai yang dipegang oleh para ahli teknologi kognitif, moral, ekonomi, sosial atau politis dan petunjuk-petunjuk nilai nilai teknologi yang paling dapat dipercaya; perbandingan kemanfaatan atau biaya, pemasaran kebutuhan sosial atau lainnya.

[81]Interconection, http://74.125.153.132/ search?q=cache:mSeFEXF8lV4J: www.interconnection. org/+web-site+interconection&cd= 1&hl=id&ct=clnk&gl=id&client=firefox-a, di akses tanggal 20 Nopember 2008.

komputer yang berhasil dihubungkan satu sama lain sehingga mereka bisa saling berkomunikasi dan membentuk sebuah jaringan.[82]

Tahun 1972, Roy Tomlinson berhasil menyempurnakan program e-mail yang ia ciptakan untuk ARPANET. Program e-mail ini begitu mudah sehingga langsung menjadi populer. Pada tahun yang sama, icon @ juga diperkenalkan sebagai lambang penting yang menunjukkan "at" atau "pada". Tahun 1973, jaringan komputer ARPANET mulai dikembangkan ke luar Amerika Serikat. Computer University College di London merupakan komputer pertama yang ada di luar Amerika yang menjadi anggota jaringan ARPANET. Pada tahun yang sama, dua orang ahli komputer yakni Vinton Cerf dan Bob Kahn mempresentasikan sebuah gagasan yang lebih besar, yang menjadi cikal bakal pemikiran internet. Ide ini dipresentasikan untuk pertama kalinya di Universitas Sussex.[83]

Hari bersejarah berikutnya adalah tanggal 26 Maret 1976, ketika Ratu Inggris berhasil mengirimkan e-mail dari *Royal Signals and Radar Establishment* di Malvern. Setahun kemudian, sudah lebih dari 100 komputer yang bergabung di ARPANET membentuk sebuah jaringan atau *network*. Pada 1979, Tom Truscott, Jim Ellis dan Steve Bellovin, menciptakan *newsgroups* pertama yang diberi nama USENET.[84]



Gbr.1 USENET

Tahun 1981 France Telecom menciptakan gebrakan dengan meluncurkan telpon televisi pertama, dimana orang bisa saling menelpon sambil berhubungan dengan *video link.*[85] Karena komputer yang membentuk jaringan semakin hari semakin banyak, maka dibutuhkan sebuah protokol resmi yang diakui oleh semua

---

[82]Eddy Purwanto dan Tim Sub Bag Jaringan Informasi IPTEK, JIIPP dikutip dari http:// www. litbang. depkes.go.id/tik/media/Pengantar_WWW.doc

[83] *Ibid.*

[84] Gambar skema USENET, http://upload.wikimedia.org/wikipedia /commons/thumb/f/f4/ Usenet_servers_and_clients.svg/ 370px-Usenet_servers_and_clients.svg.png. diakses pada tanggal 20 Nopember 2008.

[85] *Ibid.*

jaringan. Pada tahun 1982 dibentuk *Transmission Control Protocol* atau TCP dan Internet Protokol atau IP. Sementara itu di Eropa muncul jaringan komputer tandingan yang dikenal dengan Eunet, yang menyediakan jasa jaringan komputer di negara-negara Belanda, Inggris, Denmark dan Swedia. Jaringan Eunet menyediakan jasa e-mail dan newsgroup USENET.[86]

Untuk menyeragamkan alamat di jaringan komputer yang ada, maka pada tahun 1984 diperkenalkan sistem nama domain, yang kini kita kenal dengan DNS atau *Domain Name System*. Komputer yang tersambung dengan jaringan yang ada sudah melebihi 1000 komputer lebih. Pada 1987 jumlah komputer yang tersambung ke jaringan melonjak 10 kali lipat menjadi 10.000 lebih. [87]

Tahun 1988, Jarko Oikarinen dari Finland menemukan dan sekaligus memperkenalkan IRC atau *Internet Relay Chat*. Setahun kemudian, jumlah komputer yang saling berhubungan kembali melonjak 10 kali lipat dalam setahun. Tak kurang dari 100.000 komputer kini membentuk sebuah jaringan. Tahun 1990 adalah tahun yang paling bersejarah, ketika Tim Berners Lee menemukan program editor dan browser yang bisa menjelajah antara satu komputer dengan komputer yang lainnya, yang membentuk jaringan itu. Program inilah yang disebut www, atau *World Wide Web*.[88]

Tahun 1992, komputer yang saling tersambung membentuk jaringan sudah melampaui sejuta komputer, dan di tahun yang sama muncul istilah *surfing the internet*. Tahun 1994, situs internet telah tumbuh menjadi 3000 alamat halaman, dan untuk pertama kalinya *virtual-shopping* atau *e-retail* muncul di internet. Dunia langsung berubah. Di tahun yang sama *Yahoo!* didirikan, yang juga sekaligus kelahiran *Netscape Navigator* 1.0.[89]

Dekatnya hubungan antara informasi dan teknologi jaringan komunikasi telah menghasilkan dunia maya yang amat luas yang biasa disebut dengan teknologi *cyberspace*. Teknologi ini berisikan kumpulan informasi yang dapat diakses oleh semua orang dalam bentuk jaringan-jaringan komputer yang disebut jaringan internet. Sebagai media penyedia informasi internet juga merupakan

---

[86] *Ibid.*
[87] *Ibid.*
[88] *Ibid.*
[89] *Ibid.*

sarana kegiatan komunitas komersial terbesar dan terpesat pertumbuhannya. Sistem jaringan memungkinkan setiap orang dapat mengetahui dan mengirimkan informasi secara cepat dan menghilangkan batas-batas teritorial suatu wilayah negara. Kepentingan yang ada bukan lagi sebatas kepentingan suatu bangsa semata, melainkan juga kepentingan regional bahkan internasional.[90]

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. Hal tersebut menunjukan adanya pergeseran paradigma dimana jaringan informasi merupakan infrastruktur bagi perkembangan suatu negara.[91]

Setiap negara harus menghadapi kenyataan bahwa informasi dunia saat ini dibangun berdasarkan suatu jaringan yang ditawarkan oleh kemajuan bidang teknologi. Salah satu cara berpikir yang produktif adalah mendirikan usaha untuk menyediakan suatu infra struktur informasi yang baik di dalam negeri, yang kemudian dihubungkan dengan jaringan informasi global.[92]

Perkembangan teknologi jaringan komputer global atau Internet telah menciptakan dunia baru yang dinamakan *cyberspace*, sebuah dunia komunikasi berbasis komputer yang menawarkan realitas yang baru, yaitu realitas virtual. Istilah *cyberspace* muncul pertama kali dari novel William Gibson berjudul Neuromancer pada tahun 1984.[93] 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".*[94] *The*

---

[90]Teguh Arifiyadi, "Cyber Crime dan Upaya Antisipasinya Secara Yuridis (I)", http://. wordpress. com/2009/04/23/cyber-crime-dan-upaya-antisipasinya-secara-yuridis/+Teguh+Arifiyadi+Cyber +Crime+dan+Upaya+ Antisipasinya+Secara+Yuridis&cd =6&hl=id&ct=clnk&gl=I d&client= firefox-a *cyber crime*/Portal Departemen Komunikasi dan Informatika Republik Indonesia. html.

[91] *Ibid.*

[92] *Ibid.*

[93] Agus Raharjo, *Cyber Crime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, Bandung: PT Citra Aditya Bakti, 2002, hal. 236.

[94] Cyberspace, http://dictionary.cambridge.org/define.asp?key=19297&dict=CALD di akses tanggal 13 September 2008.

American Heritage Dictionary of English Language Fourth Edition mendefinisikan *cyberspace* sebagai "*the electronic medium of computer networks, in which online communication takes place*".[95] 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.*[96] Kecenderungan mengglobalnya karakteristik teknologi informasi yang semakin *user friendly*, Karena teknologi informasi (khususnya dalam dimensi *cyber*) tidak akan mengkotak-kotak dan membentuk signifikasi karakter. Namun selalu ada gejala negatif dari setiap fenomena teknologi, salah satunya adalah aktifitas kejahatan. Bentuk kejahatan (*crime*) secara otomatis akan mengikuti dan kemudian beradaptasi pada tingkat perkembangan teknologi.[97]

Dari berbagai hakekat kejahatan komputer dalam hal kejahatan mayantara seperti *carding, atm fraud, child pornography*, penulis menilai bahwa pemerintah harus mengambil sikap tegas bagi pelaku kejahatan dunia mayantara, mengingat bahaya yang ditimbulkan oleh kejahatan tersebut pada kenyataannya memang begitu luas dan berdampak merata di setiap bidang teknologi modern. Dengan adanya perangkat hukum Internasional yaitu konvensi PBB mengenai penanggulangan *cyber crime* bahwa sarana penal dan non penal sebagai sarana efektif menanggulangi kejahatan mayantara.

Penerapan sanksi dengan sarana penal atau non penal agar kepastian hukum serta perlindungan hukum dapat terpenuhi serta kebijakan untuk penanggulangan kejahatan mayantara di Indonesia dapat kita lihat pada bab III mengenai penanggulangan kejahatan mayantara.

---

[95] Cyberspace, http://www.bartleby.com/59/23/cyberspace.html diakses tanggal 13 September 2008.

[96] Bruce Sterling, "The Hacker Crackdown, Law and Disorder on the electronic Frontier", *Massmarket Paperback*, electronic version available at http://www.lysator.liu.se/etexts/hacker, 1990.

[97] Teguh Afriyadi, *Loc. Cit.*

BAB III
PENANGGULANGAN KEJAHATAN MAYANTARA DENGAN HUKUM PIDANA

Dalam bab ini dibahas mengenai hakikat penanggulangan kejahatan, fungsionalisasi hukum dan sanksi pidana dalam kejahatan mayantara, pertanggungjawaban pidana kejahatan mayantara, pertanggungjawaban pidana kejahatan mayantara menurut KUHP, dan pertanggungjawaban pidana kejahatan mayantara menurut hukum khusus.

3.1. Hakikat Penanggulangan Kejahatan

Kejahatan, apapun bentuknya, sangat mengganggu ketentraman dan kualitas kehidupan manusia. Oleh karena itu kejahatan harus dikurangi, bukan karena kejahatan itu telah menimbulkan penderitaan bagi korban dan masyarakat keseluruhan, tetapi juga karena telah menimbulkan penderitaan bagi diri si pelanggar yang dipidana itu sendiri.[98] Dalam hal inilah, hukum pidana yang memuat perbuatan-perbuatan yang dilarang serta sanksi pidana bagi mereka yang melanggar, sangat diperlukan.

Penanggulangan kejahatan terkait dengan kebijakan penanggulangan kejahatan atau yang biasa dikenal dengan istilah kebijakan kriminal yang dapat meliputi ruang lingkup yang cukup luas. G. Peter Hoefnagels menggambarkan ruang lingkup *criminal policy* sebagai berikut:[99]

1. Penerapan hukum pidana (*criminal law application*);
2. Pencegahan tanpa pidana (*prevention without punishment*), dan
3. Mempengaruhi pandangan masyarakat mengenai kejahatan dan pemidanaan lewat media massa (*influencing views of society on crime and punishment/mass media*).

---

[98] Barda Nawawi Arief, *Kebijakan Legislatif Dalam Penanggulangan Kejahatan Dengan Pidana Penjara*, Semarang : Ananta, 1994, hal. 11,16.
[99] Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana*, Bandung : Citra Aditya Bakti, 1996, hal. 47.

Upaya penanggulangan kejahatan sesungguhnya tidak semata-mata hanya menggunakan sarana hukum pidana, sebab secara garis besar penanggulangan kejahatan dapat dibagi dua, yaitu lewat jalur *penal* (hukum pidana) dan lewat jalur *non penal* (bukan/di luar hukum pidana). Dalam pembagian G.P. Hoefnagels upaya-upaya yang disebut sebagai Pencegahan tanpa pidana (*prevention without punishment*), dan mempengaruhi pandangan masyarakat mengenai kejahatan dan pemidanaan lewat media massa (*influencing views of society on crime and punishment/mass media*) dapat dimasukkan dalam kelompok upaya *non penal*.

Secara umum dapatlah dibedakan, bahwa upaya penanggulangan kejahatan lewat jalur *penal* lebih menitikberatkan pada sifat *repressive*(penindasan /pemberantasan/penumpasan) sesudah kejahatan terjadi. Sedangkan jalur *non penal* lebih menitikberatkan pada sifat *preventive* (pencegahan/ penangkalan/pengendalian) sebelum kejahatan terjadi. Dikatakan sebagai perbedaan secara umum, karena tindakan represif pada hakekatnya juga dapat dilihat sebagai tindakan preventif dalam arti luas.[100]

Mengingat upaya penanggulangan kejahatan lewat jalur *non penal* lebih bersifat tindakan pencegahan untuk terjadinya kejahatan, maka sasaran utamanya adalah menangani faktor-faktor kondusif penyebab terjadinya kejahatan. Faktor-faktor kundusif itu antara lain berpusat pada masalah-masalah atau kondisi-kondisi sosial yang secara langsung atau tidak langsung dapat menimbulkan atau menumbuh suburkan kejahatan. Dengan demikian dilihat dari sudut kebijakan kriminal secara makro dan global, maka upaya-upaya non penal menduduki posisi kunci dan strategis dari keseluruhan upaya kebijakan kriminal. Posisi kunci dan strategis dalam menanggulangi sebab-sebab dan kondisi-kondisi yang menimbulkan kejahatan, ditegaskan pula dalam berbagai kongres PBB mengenai *The prevention of Crime and the Treatment of Offenders,* [101] sebagai berikut:

1. Pada Kongres PBB ke-6 Tahun 1980 di Caracas, Venezuela, antara lain dinyatakan didalam pertimbangan resolusi mengenai *Crime trends and*

---

[100]Komisi Hukum, "Executive Summary", http://www.komisihukum. go.id/index.php? option= com_rubberdoc&view=doc&id=1&format=raw&Itemid=84 〈=in, diakses tanggal 20 Nopember 2008.

[101] *Ibid.*, hal. 50.

Crime prevention strategies, bahwa masalah kejahatan merintangi kemajuan untuk pencapaian kualitas lingkungan hidup yang layak/pantas bagi semua orang; strategi pencegahan kejahatan harus didasarkan pada penghapusan sebab-sebab dan kondisi-kondisi yang menimbulkan kejahatan; selain itu, penyebab utama dari kejahatan di banyak negara adalah ketimpangan sosial, diskriminasi rasial dan diskriminasi nasional, standart hidup yang rendah, pengangguran dan kebutahurufan (kebodohan) diantara golongan besar penduduk. Setelah mempertimbangkan hal-hal tersebut di atas, maka dalam resolusi itu dinyatakan antara lain:

> "menghimbau semua anggota PBB untuk mengambil tindakan dalam kekuasaan mereka untuk menghapus kondisi-kondisi kehidupan yang menurunkan martabat kemanusiaan dan menyebabkan kejahatan, yang meliputi masalah pengangguran, kemiskinan, kebutahurufan (kebodohan), diskriminasi rasial dan nasional serta bermacam-macam bentuk dari ketimpangan sosial."

2. Pada Kongres PBB ke-7 Tahun 1985 di Milan, Italia, antara lain ditegaskan didalam dokumen A/CONF. 121/L/9 mengenai *Crime prevention in the context of development* bahwa upaya penghapusan sebab-sebab dan kondisi yang menimbulkan kejahatan harus merupakan strategi pencegahan kejahatan yang mendasar. Demikian pula di dalam *Guiding principles* yang dihasilkan Kongres ke-7 ditegaskan antara lain bahwa: "kebijakan-kebijakan mengenai pencegahan kejahatan dan peradilan pidana harus mempertimbangkan sebab-sebab ketidakadilan yang bersifat sosio-ekonomi, dimana kejahatan sering hanya merupakan gejala/*symptom.*"
3. Pada Kongres PBB ke-8 Tahun 1990 di Havana, Cuba, antara lain ditegaskan didalam dokumen A/CONF. 144/L. 17 mengenai *social aspects of crime prevention and criminal justice in the context of development.*

Bahwa aspek-aspek sosial dari pembangunan merupakan faktor penting dalam pencapaian sasaran strategi pencegahan kejahatan dan peradilan pidana dalam konteks pembangunan dan harus diberikan prioritas paling utama.

Secara umum, usaha-usaha penaggulangan masalah kejahatan sesungguhnya telah banyak dilakukan, termasuk juga di dalamnya penanggulangan kejahatan mayantara, namun hasilnya belum memuaskan. Menarik sekali apa yang dikemukakan oleh Habib-Ur-Rahman Khan dalam tulisannya yang berjudul *Prevention of Crime-It is Society Which Needs The Treatment' and not The Criminal,* sebagaimana dikutip Barda Nawawi Arief:

> "Dunia modern sepenuhnya menyadari akan problem yang akut ini (maksudnya problem tentang kejahatan). Orang demikian sibuk melakukan penelitian, seminar-seminar, konferensi-konferensi internasional dan menulis buku-buku untuk mencoba memahami masalah kejahatan dan sebab-sebabnya agar dapat mengendalikannya. Tetapi hasil bersih dari semua usaha ini adalah sebaliknya. Kejahatan bergerak terus."[102]

Salah satu usaha penanggulangan kejahatan ialah menggunakan hukum pidana dengan sanksinya berupa pidana. Namun demikian usaha inipun masih sering dipersoalkan. Perbedaan mengenai peranan pidana dalam menghadapi masalah kejahatan ini, menurut Inkeri Antilla, telah berlangsung beratus-ratus tahun.[103] Menurut Herbert L. Packer, usaha pengendalian perbuatan anti sosial dengan mengenakan pidana pada seseorang yang bersalah melanggar peraturan pidana, merupakan suatu problem sosial yang mempunyai dimensi hukum yang penting.[104]

Penggunaan upaya hukum, termasuk hukum pidana, sebagai salah satu upaya untuk mengatasi masalah sosial termasuk dalam bidang kebijakan penegakan hukum. Disamping itu karena tujuannya untuk mencapai kesejahteraan masyarakat pada umumnya, maka kebijakan penegakan hukum ini pun termasuk dalam bidang kebijakan sosial, yaitu segala usaha yang rasional untuk mencapai kesejahteraan masyarakat.

Penanggulangan kejahatan, termasuk penanggulangan kejahatan mayantara, dengan menggunakan sanksi pidana merupakan cara yang paling tua, setua peradaban manusia itu sendiri. Dilihat sebagai suatu masalah kebijakan, maka ada yang mempermasalahkan apakah perlu kejahatan itu ditanggulangi, dicegah atau

---

[103] *Ibid.*, hal. 17.
[104] *Ibid.*

dikendalikan dengan menggunakan sanksi pidana. Ada sebagian berpendapat bahwa terhadap pelaku kejahatan atau para pelanggar hukum pada umumnya tidak perlu dikenakan pidana. Menurut pendapat ini, pidana merupakan *a vestige of our savage past* (peninggalan dari kebiadaban kita masa lalu) yang seharusnya dihindari.[105] Pendapat ini nampaknya didasarkan pada pandangan bahwa pidana merupakan tindakan perlakuan atau pengenaan penderitaan yang kejam. Sejarah hukum pidana menurut M. Cherif Bassiouni, penuh dengan gambaran-gambaran mengenai perlakuan yang oleh ukuran-ukuran sekarang dipandang kejam dan melampaui batas.

Dasar pemikiran lainnya mengenai penanggulangan kejahatan, adalah adanya paham determinisme yang menyatakan bahwa orang tidak mempunyai kehendak bebas dalam melakukan suatu perbuatan karena dipengaruhi oleh watak pribadinya, faktor-faktor biologis dan faktor lingkungan kemasyarakatannya. Dengan demikian kejahatan sebenarnya merupakan manifestasi dari keadaan jiwa seseorang yang abnormal. Oleh karena itu si pelaku kejahatan tidak dapat dipersalahkan atas perbuatannya dan tidak dapat dikenakan pidana. Karena seorang penjahat merupakan jenis manusia khusus yang memiliki ketidaknormalan organic dan mental, maka bukan pidana yang seharusnya dikenakan kepadanya tetapi yang diperlukan adalah tindakan-tindakan perawatan yang bertujuan memperbaiki. [106]

Pandangan determinisme inilah yang menjadi ide dasar dan sangat mempengaruhi aliran positif didalam kriminologi dengan tokohnya antara lain Lombroso, Garofalo dan Ferri. Menurut Alf. Roos, pandangan inilah yang kemudian berlanjut pada gerakan modern mengenai *the campaign against punishment*. Kampanye anti pidana ini masih terdengar di abad XX ini dengan slogan barunya yang terkenal; *the struggle agains punishment atau abolition of punishment*. Misalnya dikemukakan oleh seorang ahli psikiatri forensic dan kriminolog Swedia, Olof Kinberg, yang pada tahun 1946 mengeluarkan tulisan yang berjudul: *punishment and Impunity* dan pada Tahun 1948 berjudul *Le droit de punir*. Menurut Kinberg, kejahatan pada umumnya merupakan perwujudan

---

[105] *Ibit.*, hal. 18.
[106] *Ibid.*

ketidaknormalan atau ketidakmatangan si pelanggar yang lebih memerlukan tindakan perawatan (treatment) daripada pidana. Seorang kriminolog lainnya bernama Karl Menninger menerbitkan pula sebuah buku yang dramatis pada Tahun 1966 dengan judul *the crime of punishment*. Menurut Menninger, "sikap memidana" (*punitive attitude*) harus diganti dengan "sikap mengobati" (*therapeutic attitude*).[107]

Ide penghapusan pidana dikemukakan pula oleh Filippo Gramatica, seorang tokoh ekstrim dari aliran *defense sociale* yang merupakan perkembangan lebih lanjut dari aliran modern. Pada Tahun 1947 tulisan-tulisan dan ceramah-ceramahnya dipublikasikan didalam Rivista di difesa sociale yang salah satu tulisannya berjudul *La lotta contra la pena (the fights against punishment)*. Menurut Gramatica, "hukum perlindungan sosial" harus menggantikan hukum pidana yang ada sekarang. Tujuan utama dari hukum perlindungan social adalah mengintegrasikan individu kedalam tertib sosial dan bukan pemidanaan terhadap perbuatannya. Hukum perlindungan sosial mensyaratkan penghapusan pertanggungjawaban pidana (kesalahan) dan digantikan tempatnya oleh pandangan tentang perbuatan anti sosial. Jadi pada prinsipnya ajaran Gramatica menolak konsepsi-konsepsi mengenai tindak pidana, penjahat dan pidana.[108]

Penanggulangan kejahatan terhadap kejahatan mayantara (*cyber crime*), PBB sudah menghimbau agar dipergunakan sarana penal, karena secara internasional, terhadap kejahatan siber, kongres PBB telah mengeluarkan dua dokumen yang memberi himbauan agar negara anggota menggunakan sarana penal (baik hukum pidana materiil maupun hukum acara pidana) sebagai salah satu upaya untuk menanggulangi *cyber crime* atau CRC (*computer related crime*).

3.2. Penanggulangan Kejahatan Mayantara dengan Menggunakan Sanksi Pidana

Pada pembahasan hakikat penanggulangan kejahatan telah dikemukakan bahwa upaya menanggulangi kejahatan dapat dilakukan secara penal dan non penal. Jika dikehendaki upaya penanggulangan kejahatan mayantara dengan

---

[107] *Ibid.*
[108] *Ibid.*

menggunakan upaya penal yaitu dengan sanksi pidana maka sesungguhnya hal ini merupakan salah satu bagian saja dari upaya yang lain yang bersifat non penal.

Meskipun disadari bahwa penggunaan sanksi pidana untuk menanggulangi kejahatan terlah menimbulkan sikap pro dan kontra. Tetapi, sebagaimana telah dikemukakan pada bagian di atas, bahwa secara internasional PBB telah menghimbau agar terhadap kejahatan mayantara *(cyber crime)* penanggulangannya dilakukan dengan menggunakan sarana penal atau sarana hukum pidana. Maka, Negara Indonesia harus mengupayakan bahwa penanggulangan kejahatan mayantara dilakukan dengan menggunakan sarana penal, meskipun tetap pula harus memperhatikan kemungkinan-kemungkinan penyelesaian penanggulangan dan penegakan hukum dengan sarana hukum yang lainnya, misalnya secara hukum perdata maupun hukum administrasi negara.

Pandangan atau alam pikiran untuk menolak penggunaan pidana menurut Roeslan Saleh adalah keliru.[109] Beliau mengemukakan tiga alasan yang cukup panjang mengenai masih perlunya pidana (sanksi pidana untuk menanggulangi kejahatan). Adapun inti alasannya adalah sebagai berikut:

1. Perlu tidaknya hukum pidana tidak terletak pada persoalan tujuan-tujuan yang hendak dicapai, tetapi terletak pada persoalan seberapa jauh untuk mencapai tujuan itu boleh menggunakan paksaan;
2. Persoalan bukan terletak pada hasil yang akan dicapai, tetapi dalam pertimbangan antara nilai dari hasil itu dan nilai dari batas-batas kebebasan pribadi masing-masing;
3. Ada usaha-usaha perbaikan atau perawatan yang tidak mempunyai arti sama sekali bagi si terhukum; dan disamping itu harus tetap ada suatu reaksi atas pelanggaran-pelanggaran norma yang telah dilakukannya itu dan tidaklah dapat dibiarkan begitu saja;
4. Pengaruh pidana atau hukum pidana bukan semata-mata ditujukan pada si penjahat, tetapi juga untuk mempengaruhi orang yang tidak jahat yaitu warga masyarakat yang mentaati norma-norma masyarakat.

---

[109] Roeslan Saleh, *Mencari Asas-asas umum yang sesuai untuk hukum pidana nasional.* Kumpulan bahan upgrading hukum pidana, jilid 2, 1971, hal. 15-17. dalam Barda Nawawi Arief, Kebijakan Legislatif dalam Penanggulangan Kejahatan Dengan Pidana Penjara. hal. 20.

Permasalahan selanjutnya yang dapat muncul apabila kejahatan mayantara (*cyber crime*) akan ditanggulangi dengan menggunakan sarana penal atau sanksi pidana, adalah:

1. Apakah cukup hanya dengan mengandalkan hukum pidana yang sudah ada, ataukah;
2. Perlu disusun undang-undang baru dengan merumuskan suatu tindak pidana khusus mengenai kejahatan mayantara (*cyber crime*).

Apabila menggunakan hukum pidana yang sudah ada tentu harus mencari ketentuan-ketentuan rumusan tindak pidana yang ada di dalam KUHP ataupun undang-undang tertentu di luar KUHP. Kelemahan apabila menggunakan ketentuan hukum pidana yang sudah ada, tentu harus banyak menggunakan penafsiran hukum ataupun konstruksi hukum agar supaya kasus-kasus kejahatan mayantara dapat dijangkau oleh ketentuan hukum pidana yang sudah ada dimana hukum pidana tersebut memang tidak dipersiapkan untuk bentuk tindak pidana mayantara *(cyber crime)*. Kelemahan kedua, karena hukum pidana umum (KUHP) ketika disusun memang belum terpikirkan adanya bentuk kejahatan mayantara atau kejahatan dengan sarana komputer pada umumnya, dapat menimbulkan berbagai penafsiran atau konstruksi hukum sesuai dengan tingkat pemahaman para penegak hukum yang beragam, sehingga kepastian hukum akan terganggu. Keuntungannya, tidak perlu disusun undang-undang khusus sehingga tidak perlu adanya anggaran keuangan Negara untuk menyusun undang-undang khusus.

Sebaliknya, apabila harus disusun undang-undang khusus mengenai kejahatan mayantara (*cyber crime*) selain perlu dukungan anggaran negara untuk menyusun undang-undang, juga memerlukan waktu yang relatif lama. Apabila setiap bentuk kejahatan baru kemudian diikuti dengan penyusunan undang-undang khusus yang baru, juga dapat menimbulkan tumpang tindihnya beberapa undang-undang yang mengatur aspek hukum yang sejenis, misalnya sudah ada Undang-Undang Penyiaran, Undang-Undang Telekomuniskasi, Undang-Undang Informasi dan Transasksi Elektronik dan masih harus ditambah lagi dengan Undang-Undang tentang Kejahatan Mayantara *(cyber crime)*. Keuntungannya tentu saja akan memberikan kepastian hukum khususnya kepastian dalam

rumusan dan pelaksanaan penegakannya, karena rumusan-rumusan kejahatannya dapat ditentukan secara jelas unsur-unsur tindak pidananya.

Apabila kita akan memilih untuk menyusun undang-undang baru tentang kejahatan mayantara (*cyber crime*) barangkali kita dapat mencontoh di negara-negara Uni Eropa. Sebab, dalam perkembangannya, instrumen hukum internasional publik yang mengatur masalah kejahatan siber yang saat ini paling mendapat perhatian adalah Konvensi tentang Kejahatan Siber (*Convention on cyber crime*) 2001 yang digagas oleh Uni Eropa. Konvensi ini meskipun pada awalnya dibuat oleh organisasi regional Eropa, tetapi dalam perkembangannya dimungkinkan untuk diratifikasi dan diaksesi oleh negara manapun di dunia yang memiliki komitmen dalam upaya mengatasi kejahatan mayantara *(cyber crime)*.

Karena kejahatan mayantara atau *cyber crime* merupakan salah satu sisi gelap dari kemajuan teknologi yang mempunyai dampak negatif sangat luas bagi seluruh bidang kehidupan modern saat ini, sehingga menaruh perhatian sekaligus kekhawatiran keberbahayaannya, dimana kekhawatiran itu kemudian terungkap dalam makalah *cyber crime* yang disampaikan oleh ITAC (*Information Technology Association of Canada*) pada *International Information Industry Congress* (IIIC) *2000 Millenium Congress* di Quebec pada tanggal 19 September 2000, yang menyatakan bahwa "*Cyber crime is a real and growing threat to economic and social develop ment around the world. Information technology touches aspect of human life and so can electronically enabled crime.*"[110]

Sehubungan dengan kekhawatiran akan ancaman/bahaya *cyber crime* ini, karena berkaitan erat dengan *economic crimes* dan *organized crime* (terutama untuk tujuan *money laundering*), maka Kongres PBB mengenai "*The Prevention of Crime and the Treatment of Offenders.*"[111] telah pula membahas masalah ini. Sudah dua kali masalah *cyber crime* ini diagendakan yaitu pada Kongres VIII/1990 di Havana dan pada Kongres X/ 2000 di Wina. Dalam rangka upaya menanggulangi *cyber crime* itu, Resolusi Kongres PBB VIII/1990 mengenai "*computer-related crimes*" mengajukan beberapa kebijakan antara lain sebagai

---

[110] Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*, Jakarta: Kencana Prenada Media, 2007, hal. 238.

[111] www.unodc.org/unodc/en/commissions/crime-congresses.html diakses tanggal 20 Nopember 2008.

berikut:

1. Menghimbau negara anggota untuk mengintensifkan upaya-upaya penanggulangan penyalahgunaan komputer yang lebih efektif dengan mempertimbangkan langkah-langkah sebagai berikut:
   a. Melakukan modernisasi hukum pidana materiil hukum acara pidana;
   b. Mengembangkan tindakan-tindakan pencegahan dan pengamanan komputer;
   c. Melakukan langkah-langkah untuk membuat peka (sensitif) warga masyarakat, aparat pengadilan, dan penegak hukum, terhadap pentingnya pencegahan jahatan yang berhubungan dengan komputer;
   d. Melakukan upaya-upaya pelatihan (*training*) bagi para hakim, pejabat, dan aparat penegak hukum mengenai kejahatan ekonomi dan *cyber crime*;
   e. Memperluas *"rules of ethics"* dalam penggunaan komputer dan mengajarkannya melalui kurikulum informatika;
   f. Mengadopsi kebijakan perlindungan korban *cyber crime* sesuai dengan Deklarasi PBB mengenai korban, dan mengambil langkah-langkah untuk mendorong korban melaporkan adanya *cyber crime*.[112]
2. Menghimbau negara anggota meningkatkan kegiatan internasional dalam upaya penanggulangan *cyber crime*;
3. Merekomendasikan kepada Komite Pengendalian dan Pencegahan Kejahatan *(Committee on Crime Prevention and Control)* PBB untuk:
   a. Menyebarluaskan pedoman dan standar untuk membantu negara anggota menghadapi *cyber crime* di tingkat nasional, regional dan internasional;
   b. Mengembangkan penelitian dan analisis lebih lanjut guna menemukan cara-cara baru menghadapi problem *cyber crime* di masa yang akan datang;

---

[112] Barda Nawawi Arief. *Op. cit.*, hal. 238-239.

c. Mempertimbangkan *cyber crime* sewaktu meninjau implementasi perjanjian ekstradisi dan bantuan kerja sama di bidang penanggulangan kejahatan.[113]

Garis kebijakan penanggulangan kejahatan mayantara (c*yber crime)* yang dikemukakan dalam Resolusi PBB di atas, terlihat cukup komprehensif. Tidak hanya penanggulangan melalui kebijakan "*penal*" (baik hukum pidana materiil maupun hukum pidana formal), tetapi juga kebijakan "*nonpenal*". Hal menarik dari kebijakan nonpenal yang dikemukakan dalam Resolusi PBB itu ialah upaya mengembangkan "pengamanan/perlindungan komputer dan tindakan-tindakan pencegahan" *("computer security and prevention measures";* lihat poin 1.a di atas). Jelas hal ini terkait dengan pendekatan *"techno-prevention"*, yaitu upaya pencegahan/ penanggulangan kejahatan dengan menggunakan teknologi. Sangat disadari tampaknya oleh Kongres PBB, bahwa *cyber crime* yang terkait dengan kemajuan teknologi, tidak dapat semata-mata di tanggulangi dengan pendekatan yuridis, tetapi juga harus ditanggulangi dengan pendekatan teknologi itu sendiri. Menurut Volodymyr Golubev, [114] banyak aspek dari kasus-kasus *cyber crime* lebih merupakan akibat lemahnya perlindungan informasi daripada diakibatkan oleh perbuatan pelaku kejahatan. Oleh karena itu perlu diberikan lebih banyak informasi mengenai kelemahan/kerentanan dari sistem komputer dan sarana perlindungan efektif.

Aspek lain yang menarik dari kebijakan non-penal yang diungkap dari Resolusi PBB di atas, ialah perlunya pendekatan budaya/kultural/etik dalam kebijakan penanggulangan kejahatan mayantara atau *cyber crime* yaitu membangun/ membangkitkan kepekaan warga masyarakat dan aparat penegak hukum terhadap masalah *cyber crime* dan menyebarluaskan/mengajarkan etika penggunaan komputer melalui media pendidikan. Pendekatan budaya ini penting dilakukan, khususnya upaya mengembangkan kode etik dan perilaku "*codes of behaviour and ethics*" supaya ada kesadaran hukum masyarakat untuk tidak melakukan perbuatan yang dapat merugikan kepentingan orang lain ketika

---

[113] *Ibid.*
[114] *Ibid.*, hal. 240.

melakukan transaksi, komunikasi dan sebagainya melalui atau menggunakan sarana teknologi informasi.

Satu hal yang harus mendapatkan perhatian, apabila penanggulangan kejahatan dengan menggunakan sarana penal atau hukum pidana, berarti akan mengkriminalisasikan suatu perbuatan menjadi kejahatan. Oleh sebab itu menarik pula untuk dikemukakan bahwa telah pula dibahas secara khusus dalam suatu lokakarya (yaitu "*Workshop on crimes related to computer networks*") yang diorganisir oleh UNAFEI selama Kongres PBB X/2000 berlangsung.) Lokakarya ini dibagi dalam empat diskusi panel. Pertama, membahas tentang "*the criminology of computer crime*". Kedua, membahas studi kasus mengenai "*the technical and legal issues*" yang timbul dari tindakan penyidikan dan perampasan data komputer. Ketiga, membahas masalah "*the tracing of computer communication in multinational networks*". Keempat, membahas masalah "*the relationship between law enforcement and computer and Internet industries*". Adapun kesimpulan dari lokakarya ini adalah sebagai berikut:[115]

1. CRC (*computer-related crime*) harus dikriminalisasikan;
2. Diperlukan hukum acara yang tepat untuk melakukan penyidikan dan penuntutan terhadap penjahat *cyber* (*cyber criminals*);
3. Harus ada kerja sama antara pemerintah dan industri terhadap tujuan umum pencegahan dan penanggulangan kejahatan komputer agar Internet menjadi tempat yang aman;
4. Diperlukan kerja sama internasional untuk menelusuri / mencari para penjahat di Internet;
5. PBB harus mengambil langkah/tindak lanjut yang berhubungan dengan bantuan dan kerja sama teknis dalam penanggulangan CRC.

Sebagai gambaran, bahwa masyarakat bangsa-bangsa telah menyusun sebuah Konvensi tentang *cyber crime* yang berisi beberapa hal, antara lain (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.

---

[115] *Ibid.*, hal. 241.

Khusus terhadap hukum pidana, konvensi ini melahirkan beberapa ketentuan, antara lain:

1. Title 1: *Offences against the confidentiality, integrit and availability of computer data and systems;*
   a. *Illegal Access:* sengaja memasuki/mengakses sistem komputer tanpa hak;
   b. *Illegal Interception:* sengaja dan tanpa hak mendengar/menangkap secara diam-diam pengiriman (transmisi) dan pemancaran (emisi) data komputer yang tidak bersifat publik ke, dari atau di dalam sistem komputer dengan menggunakan alat bantu teknis;
   c. *Data Interference:* sengaja dan tanpa hak melakukan perusakan, penghapusan, perubahan atau penghapusan data komputer;
   d. *System Interference:* sengaja melakukan gangguan/ rintangan serius tanpa hak terhadap berfungsinya sistem komputer;
   e. *Misuse of Devices:* penyalahgunaan perlengkapan komputer, termasuk program komputer, password komputer, kode masuk (*access code*).
2. Title 2: *Computer related offences;*
   a. *Computer related Forger*: Pemalsuan (dengan sengaja dan tanpa hak memasukkan, mengubah, menghapus data autentik menjadi tidak autentik dengan maksud digunakan sebagai data autentik);
   b. *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).
3. Title 3: *Content related offences;*

   Delik-delik yang berhubungan dengan pornografi anak (*child pornography*); meliputi perbuatan:
   a. Memproduksi dengan tujuan didistribusikan melalui sistem komputer;

b. Menawarkan melalui sistem komputer;
c. Mendistribusi atau mengirim melalui sistem komputer;
d. Memperoleh melalui sistem komputer;
e. Memiliki di dalam sistem komputer atau di dalam media penyimpanan data.

4. Title 4: *"Offences related to infringements of copyright and related rights"*;
5. Title 5: *Ancillary liability and sanctions*:
   a. *Attempt and aiding or abetting*;
   b. *Corporate liability*;
   c. *Sanctions and measures.*[116]

Apabila akan ditempuh kebijakan untuk menyusun undang-undang tentang kejahatan mayantara *(cyber crime)* tersendiri sebagai tindak pidana khusus, maka yang perlu diperhatikan adalah perlunya melakukan sinkronisasi dengan berbagai undang-undang yang telah ada agar tidak terjadi tumpang tindih satu sama lain. Barda Nawawi Arief mengenai hal ini menggunakan istilah harmonisasi kebijakan formulasi. Kebijakan kriminalisasi, dalam hal ini kriminalisasi kejahatan mayantara (*cyber crime*) bukan sekedar kebijakan menetapkan/merumuskan/ memformulasikan perbuatan apa yang dapat dipidana termasuk sanksi pidananya, melainkan juga mencakup masalah bagaimana kebijakan legislasi itu disusun dalam satu kesatuan sistem hukum pidana yang harmonis dan terpadu.[117] Oleh sebab itu, apabila hendak disusun undang-undang khusus mengenai kejahatan mayantara (*cyber crime*) seyogyanya dilakukan kajian terhadap masalah:

1. Harmonisasi materi/substansi tindak pidana (antara tindak pidana mayantara yang akan disusun dengan tindak pidana lainnya), dan
2. Harmonisasi kebijakan formulasi tindak pidana, di bidang kejahatan mayantara/*cyber crime.*

Mengenai harmonisasi materi/substansi tindak pidana (antara tindak pidana mayantara yang akan disusun dengan tindak pidana lainnya), tidak hanya terkait

---

[116] *Ibid.*, hal. 247.
[117] Barda Nawawi Arief, *Kapita Selekta Hukum Pidana,* Bandung: Citra Aditya Bakti, 2003, hal. 259.

dengan masalah kajian harmonisasi eksternal yaitu internasional, tetapi juga kajian harmonisasi internal nasional. Harmonisasi eksternal dimaksudkan adanya kajian harmonisasi dan sinkronisasi dengan materi tindak pidana mayantara/*cyber crime* yang disepakati secara internasional (global maupun regional). Harmonisasi ini perlu dilakukan mengingat sifat hakiki dari kejahatan mayantara sebagai *global crime* yaitu kejahatan yang melampaui batas-batas negara atau kejahatan tanpa batas wilayah. Sedangkan kajian harmonisasi internal merupakan kajian harmonisasi atau sinkronisasi dengan materi tindak pidana yang telah ada atau telah dirumuskan di dalam berbagai undang-undang sebagai hukum positif selama ini.

Harmonisasi kebijakan formulasi tindak pidana, antara lain mencakup masalah apakah formulasi kebijakan penal di bidang kejahatan mayantara/*cyber crime* perlu diatur dalam undang-undang khusus atau diintegrasikan dalam Undang-Undang Hukum Pidana Umum KUHP, atau dituangkan bersama-sama dalam undang-undang umum dan khusus. Mengenai hal ini, Barda Nawawi Arief memberikan pendapat:[118]

1. Harmonisasi kebijakan formulasi hukum pidana materiil/ substansi sangat bergantung dan berkaitan erat dengan sistem hukum pidana materiil yang sedang berlaku di suatu negara atau sistem yang ingin dibangun/dicita-citakan. Tidaklah dapat dikatakan ada harmonisasi atau sinkronisasi apabila kebijakan formulasinya berada di luar sistem. Oleh karena itu, dalam kondisi saat ini kebijakan formulasi hukum pidana di bidang kejahatan mayantara/ *cyber crime* harus tetap berada dalam sistem hukum pidana materiil yang saat ini berlaku.
2. Sistem hukum pidana materiil yang saat ini berlaku di Indonesia terdiri dari keseluruhan sistem peraturan perundang-undangan yang ada di dalam KUHP sebagai induk aturan umum dan undang-undang khusus di luar KUHP. Keseluruhan peraturan perundang-undangan di bidang hukum pidana substantif tersebut terisi dari Aturan Umum (*General Rules*) dan Aturan Khusus (*Special Rules*). Aturan umum terdapat di

[118] *Ibid.*, hal. 261.

dalam Buku I KUHP dan aturan khusus terdapat di dalam Buku II dan Buku III KUHP maupun di dalam undang-undang khusus di luar KUHP.

3. Dilihat dari kerangka sistem hukum pidana substansi, maka kebijakan formulasi hukum pidana yang berkaitan dengan kejahatan mayantara/ *cyber crime* dapat ditempuh dengan berbagai kebijakan:
   a. Untuk menjaring kejahatan mayantara/*cyber crime* dalam kasus-kasus delik biasa/ umum yang sudah ada di dalam KUHP ataupun delik-delik khusus di luar KUHP, dibuat/ditambahkan aturan umum dalam Buku I KUHP yang berkaitan dengan perkembangan teknologi informasi. Aturan Umum dalam Buku I KUHP yang berkaitan dengan teknologi informasi ini, tentunya juga tidak menutup kemungkinan dibuatnya aturan umum yang bersifat/ berlaku khusus untuk delik-delik khusus di luar KUHP.
   b. Untuk menjaring kejahatan mayantara/*cyber crime* dalam bentuk delik baru yang belum terdapat di dalam KUHP, ditambahkan perumusan delik baru di dalam aturan khusus Buku II dan Buku III KUHP. Disamping itu, apabila kejahatan mayantara/*cyber crime* diperkirakan dapat juga terjadi untuk delik-delik khusus di luar KUHP, maka delik khusus kejahatan mayantara/*cyber crime* itu dimasukkan/ diintegrasikan ke masing-masing undang-undang khusus di luar KUHP tersebut. Dengan demikian dimungkinkan adanya formulasi kejahatan mayantara/ *cyber crime* di berbagai undang-undang khusus.
   c. Untuk mengatasi berbagai kelemahan sistem KUHP yang berlaku saat ini (antara lain subyek tindak pidana hanya orang; tidak adanya sistem perumusan ancaman pidana secara kumulasi dan kumulasi alternatif; tidak adanya pidana minimum khusus; tidak adanya jenis sanksi pidana khusus dan aturan pemidanaan umum/khusus untuk korporasi), maka dapat dimaklumi kebijakan formulasi mengenai kejahatan mayantara/*cyber crime* ditempatkan dalam undang-undang khusus. Namun undang-undang khusus ini seyogyanya tidak

hanya merumuskan tindak pidana tindak pidananya saja, tetapi juga membuat aturan umum yang dapat menjadi aturan payung bagi delik-delik yang sudah ada di dalam maupun di luar KUHP.

Maka, sambil menunggu langkah kebijakan yang akan ditempuh oleh pemerintah, apakah nantinya akan menyusun suatu undang-undang khusus ataukah akan memasukkan rumusan tindak pidana ke dalam hukum pidana yang sudah ada dengan rumusan tambahan mengenai kejahatan mayantara, saat sekarang bagi bangsa Indonesia yang harus dilakukan dalam rangka penanggulangan kejahatan mayantara atau *cyber crime* adalah bagaimana memfungsikan hukum pidana yang sudah ada untuk didayagunakan dalam rangka penanggulangan kejahatan tersebut. Dengan adanya berbagai undang-undang nampaknya akan sangat sulit apabila mengharapkan adanya kebijakan negara untuk membuat satu undang-undang khusus tentang kejahatan mayantara (*cyber crime*).

3.3. Fungsionalisasi Hukum dan Sanksi Pidana dalam Kejahatan Mayantara

Fungsionalisasi hukum pidana dapat diartikan sebagai upaya untuk membuat hukum pidana itu dapat berfungsi, beroperasi atau bekerja dan terwujud secara konkret. Jadi istilah fungsionalisasi hukum pidana dapat diidentikkan dengan istilah operasional atau konkritisasi hukum pidana yang pada hakekatnya sama dengan pengertian penegakan hukum pidana.[119] Bertolak dari pengertian yang demikian, maka fungsionalisasi hukum pidana, seperti fungsionalisasi atau proses penegakan hukum pada umumnya, melibatkan minimal tiga faktor yang saling terkait yaitu faktor perundang-undangan, faktor aparat/badan penegak hukum dan faktor kesadaran hukum. Pembagian ketiga faktor ini dapat dikaitkan dengan pembagian tiga komponen sistem hukum, yaitu substansi hukum, struktur hukum dan budaya hukum.[120]

---

[119] Muladi dan Barda Nawawi Arief, *Bunga Rampai Hukum Pidana*, Bandung: Alumni, 1992, hal.157.

[120] Barda Nawawi Arief, *Kebijakan Legislatif dalam Penanggulangan Kejahatan dengan Pidana Penjara*, Semarang: BP Undip,1994, hal. 17.

Pada substansi hukum, penulis memfokuskan pada faktor perundang-undangan yang terkait dengan persoalan *cyber crime*. Hal ini patut dikaji karena faktor perundang-undangan adalah faktor kebijakan legislatif yang berhubungan dengan masalah kejahatan mayantara atau *cyber crime*. Peninjauan masalah ini sangat penting karena kebijakan legislatif pada dasarnya merupakan tahap awal yang paling strategis dari keseluruhan perencanaan proses fungsionalisasi hukum pidana atau proses penegakan hukum pidana. Dengan perkataan lain, tahap kebijakan legislatif merupakan tahap paling strategis bagi upaya penanggulangan kejahatan dengan hukum pidana. Tahap ini merupakan tahap formulasi yang menjadi dasar, landasan dan pedoman bagi tahap-tahap fungsionalisasi berikutnya, yaitu tahap aplikasi dan tahap eksekusi.

Karena fungsionalisasi pada hakikatnya merupakan operasionalisasi hukum pidana, maka berfungsinya hukum pidana tersebut harus diarahkan pada tujuan dari pemidanaan. Secara umum, tujuan pemidanaan adalah untuk pencegahan, baik pencegahan khusus maupun pencegahan secara umum. Namun, pemidanaan juga harus mampu mengarahkan pada perbaikan si pelaku kejahatan. Untuk dapat berfungsinya hukum pidana dengan baik, tentu harus ditetapkan norma hukum berikut sanksinya dengan mempertimbangkan dan memperhitungkan aspek-aspek tujuan pemidanaan. Dalam penetapan inilah kemudian sering menimbulkan perdebatan dan perbedaan pandangan dari para ahli hukum pidana mengenai perlu tidaknya pengancaman sanksi pidana terhadap perbuatan tertentu. Perlu tidaknya memfungsikan hukum dan sanksi pidana terhadap perbuatan tertentu.

Oleh karena itu perlu ada ketentuan atau larangan dan selalu ada pelanggaran-pelanggaran terhadap ketentuan dan larangan tersebut di mana tidak mungkin pemerintah membiarkan perlindungan terhadap pelanggaran itu berada di tengah individu. Alf Ross juga termasuk golongan yang tidak setuju dengan aliran yang bertujuan menghapuskan sanksi pidana. Menurut Alf Ross, paham *abolition of punishment* seperti dikemukakan oleh Karl Menninger merupakan konsepsi yang tidak jelas. Ketidakjelasan itu disebabkan tidak adanya definisi yang jelas mengenai pengertian atau makna pidana. Dikemukakan oleh Alf Ross misalnya, bahwa Karl Menninger dalam bukunya *the Crime of punishment* menyatakan tuntutan untuk *the abolition of punishment* sudah barang tentu tidak

berarti *the omission or curtailment of penalties.* [121] Sehubungan dengan pernyataan Karl Menninger ini, Alf Ross lalu mempertanyakan apakah perbedaan antara *punishment* dan *penalty*. Menninger berusaha untuk menjelaskan perbedaan itu dengan memberikan contoh-contoh, tetapi menurut Alf Ross, ia tidak dapat menganalisa perbedaan itu. Menurut Alf Ross *concept of punishment* bertolak pada dua syarat atau tujuan, yaitu:

1. Pidana ditujukan pada pengenaan penderitaan terhadap orang yang bersangkutan *(punishment is aimed at inflicting suffering upon the person whom it is imposed);* dan
2. Pidana itu merupakan suatu pernyataan pencelaan terhadap perbuatan si pelaku *(the punishment is an expression of disapproval of the action for which it is imposed).*

Berdasar analisa kedua unsur utama tersebut, akhirnya Alf Ross berkesimpulan bahwa sebenarnya menjadi sasaran dari abolisionis adalah "pidana sebagai pencelaan, bukan pidana sebagai penderitaan" (*punishment as disapproval, not punishment as suffering*). Ide-ide dasar dari golongan abolitionis atau gerakan kampanye anti pidana yang demikian itu, dibahas secara panjang lebar oleh Alf Ross di dalam bukunya terutama dalam Bab 4 mengenai *The Compaign against Punishment* dan Bab 5 mengenai *On Determinism and Mortality*. Berdasar uraian tersebut disimpulkan bahwa menurut Alf Ross, aliran abolisionis yang dipelopori oleh penganut aliran positivis bertolak dari dua ide dasar, yaitu: (1) pandangan determinisme; dan (2) tujuan pidana adalah pencegahan (*prevention*).[122]

Menurut Alf Ross, secara singkat dapat dikatakan bahwa pandangan determinisme bertolak pada dua premis, yaitu:

1. postulat atau dalil bahwa determinisme telah terbukti secara ilmiah; dan
2. prinsip inkompatibilitas (ketidaksesuaian), yaitu bahwa pandangan determinisme tidak dapat disesuaikan dengan pandangan mengenai kesalahan dan pertanggungan jawab.

---

[121] *Ibid.*, hal. 21.
[122] *Ibid.*

Dengan premis pertama ini, mereka menolak pandangan bahwa orang mempunyai kehendak bebas (*free will*). Mereka berpendapat, telah terbukti secara ilmiah bahwa kehendak manusia, seperti halnya dengan semua fenomena lainnya, ditentukan oleh hukum kausal.[123]

Premis kedua berkaitan erat dengan premis pertama. Menurut pandangan determinisme, karena moral responsibility didasarkan pada adanya *free will* maka pembicaraan mengenai kesalahan atau pertanggungan jawab moral tidak mempunyai arti (*meaningless*).[124]

Selanjutnya berarti pula pembicaraan mengenai pidana sebagai pencelaan moral *(moral disapproval)* juga tidak mempunyai arti. Kedua premis itu menurut Alf Ross tidak benar. Dengan jawaban yang singkat ini, Ross ingin menegaskan bahwa mereka yang pernah marah, pernah jengkel, pernah mencela orang, pernah memarahi diri sendiri dan pernah merasa bertanggung jawab berarti sebenarnya mengakui adanya *moral disapproval* dan moral *responsibility.*[125]

Ide dasar yang kedua, yaitu tujuan pidana adalah pencegahan, menurut Alf Ross merupakan alasan pragmatis dari golongan positivis untuk menentang konsepsi pidana sebagai pencelaan moral (*moral disapproval*). Salah seorang penganut positivis yang menuntut dihapuskannya kesalahan yang berupa kesengajaan dan kealpaan serta menghapuskan pertanggungjawaban mental (*imputability*) sebagai syarat pemidanaan karena hal itu tidak relevan untuk suatu kebijakan kriminal yang rasional ialah Barbara Wootton. Premis dari ide dasar yang kedua ini menurut Alf Ross dapat diuraikan sebagai berikut:

1. Tujuan dari perundang-undangan pidana adalah pencegahan bukan pembalasan;
2. Undang-undang pidana seharusnya dibuat dengan memperhatikan tujuannya dan hanya dibuat untuk tujuan itu;
3. Oleh karena itu system hukum pidana seharusnya dibuat, dan berfungsi hanya dengan maksud untuk melakukan pencegahan; bukan sebagai perwujudan dari pencelaan moral;

---

[123] *Ibid.*
[124] *Ibid.*
[125] *Ibid.*

4. Syarat pertanggungan jawab mental hanya merupakan syarat untuk adanya pencelaan moral;
5. Oleh karena itu syarat pertanggungan jawab mental harus dinyatakan sebagai tidak beralasan atau tanpa dasar.

Ide dasar kedua yang bertolak dari premis-premis tersebut ditolak pula oleh Alf Ross. Alasan yang dikemukakan oleh Alf Ross pada intinya sebagai berikut:

1. Tidak benar mempertentangkan retribution dengan prevention.

Kekeliruan fundamental menurut Ross terletak pada premis pertama ini. Mempertentangkan *prevention* dengan *retribution* sebagai dua tujuan dari perundang-undangan pidana adalah "tidak berarti" (*meaningless*) karena hal itu didasarkan pada suatu kebingungan mengenai permasalahan yang berlainan dan kesalahpahaman teori-teori *retributive* yang klasik. Sama sekali tidak beralasan untuk mengira bahwa *retribution* merupakan tujuan, yaitu efek yang sengaja dituju, dari perundang-undangan pidana. Pada retributivis seperti Kant dan Binding tidak pernah menyatakan seperti itu. Masalah yang mereka perhatikan adalah masalah ethis yang berhubungan dengan hak moral Negara untuk mengenakan penderitaan pidana pada seseorang yang sering berupa pelanggaran batas terhadap kebebasannya, integritas badannya, bahkan terhadap jiwanya. Jadi yang mereka bicarakan bukanlah pengaruh-pengaruh yang dituju oleh pembuat undang-undang, tetapi dasar moral dari pengenaan pidana atau disebut juga dasar hukum dari pidana *(the Rechtsgrund of punishment).*

Teori mereka bukanlah mengenai kebijaksanaan atau kemanfaatan sosial *(social expediency),* tetapi hanya mengenai fakta bahwa seseorang yang telah melakukan suatu tindak pidana dapat dibenarkan untuk dipidana. Dibenarkannya seseorang untuk dipidana, karena pertama ia telah melakukan tindak pidana dan kedua karena ia bertanggungjawab atas pelanggaran yang dilakukannya berdasar kondisi-kondisi mental yang menyebabkan ia dinyatakan bersalah. Dengan demikian persyaratan adanya kesalahan dalam suatu pelanggaran hukum merupakan suatu pertimbangan moral yang membatasi hak negara dalam menggunakan penderitaan pidana untuk mencapai tujuan sosial berupa *prevention.* Syarat-syarat itu

bermaksud mencegah atau menghalangi pemidanaan terhadap orang yang tidak melakukan tindak pidana (*non-perpetrator*) dan terhadap orang atau pelanggar yang tidak bersalah (*non-guilt perpetrator*), tanpa memandang apakah pidana semacam itu akan menunjang tujuan dari pencegahan.[126]

Berdasar uraian diatas, maka menurut Alf Ross pendirian yang dimulai dengan atau bertitik tolak dari pertentangan antara *prevention* dan *retribution* menempatkan kita pada jalan atau jurusan yang salah. Lebih lanjut berarti kita akan kesasar apabila mengambil kesimpulan dan titik tolak yang salah itu.

2. Tidak benar mempertentangkan *moral disapproval* (pencelaan) dengan *prevention* (pencegahan).

Mengeluarkan pembicaraan mengenai kesalahan dan pertanggung jawaban dari konsepsi "pencegahan", menurut Ross juga merupakan kekeliruan fundamental karena "pencelaan (moral)" pada hakikatnya merupakan suatu bentuk reaksi yang berhubungan dengan tingkah laku (*behavioural reaction*) yang mempunyai fungsi mempengaruhi tingkah laku atau mempunyai fungsi pencegahan.

Pencelaan (*disapproval*) bekerja sebagai faktor yang mempengaruhi perbuatan karena hal itu dialami oleh orang yang bersangkutan sebagai sesuatu yang tidak menyenangkan atau menderitakan. Terlebih karena penilaian yang demikian (yaitu pencelaan) diterima oleh yang bersangkutan, masuk kedalam kesadaran moralnya, dan dengan demikian menjadi faktor yang menentukan tingkah lakunya dimasa yang akan datang. Jadi tidak karena semata-mata takut akan sesuatu yang tidak menyenangkan, sesuatu yang menderitakan atau sebagainya, tetapi juga karena rasa hormatnya pada orang yang dipandangnya benar dan adil.

Selanjutnya dikemukakan oleh Ross bahwa tidak diragukan lagi stigma moral itu sangat penting bagi efek preventif dari suatu system pidana, baik sebagai faktor pencegahan maupun sebagai faktor yang mempengaruhi sikap-sikap moral. Setelah menganalisa premis-premis di atas, akhirnya Alf Ross

---

[126] *Ibid.*, hal. 25.

menyimpulkan bahwa ide-ide dasar dari penganut "kampanye anti pidana" yang bertolak dari aliran positif itu tidak dapat dipertahankan, karena:

1. merupakan asumsi yang tidak benar bahwa pencelaan moral dan pidana yang merupakan perwujudan dari pencelaan moral itu, adalah bertentangan atau tidak cocok dengan pemikiran ilmiah yang didasarkan pada determinisme, hal ini merupakan suatu kekeliruan yang disebabkan oleh pandangan filsafat yang kacau;
2. merupakan asumsi yang tidak benar bahwa pencelaan moral dan pidana yang merupakan perwujudan dari pencelaan moral itu tidak ada hubungannya dengan tujuan system pidana, yaitu pencegahan, hal ini merupakan suatu kekeliruan yang timbul dari kebingungan konseptual bahwa "pencegahan"(*prevention*) dan "pembalasan" (*retribution*) merupakan tujuan-tujuan pidana yang bersifat *alternative*;
3. merupakan asumsi yang tidak benar bahwa tidak mungkin merumuskan dan menerapkan suatu kriteria mengenai pertanggungjawaban mental; hal ini merupakan tuntutan yang berlebih-lebihan terhadap ilmu pengetahuan yang diperlukan untuk membuat penilaian moral dan penilaian yuridis.

Salah seorang sarjana yang juga tidak sependapat dengan dihapuskannya sanksi (hukum) pidana adalah Marc Ancel. Ia termasuk penganut aliran *defence sociale* yang lebih moderat dibandingkan Fillipo Gramatica yang ekstrim. Dikemukakan olehnya bahwa menurut para penulis sekarang kesimpulan yang dilakukan oleh F.Gramatica nampaknya agak terburu-buru dan berlebihan.

Menurut Marc Ancel tiap masyarakat mensyaratkan adanya tertib sosial, yaitu seperangkat peraturan yang tidak hanya sesuai dengan kebutuhan untuk kehidupan bersama tetapi juga sesuai dengan aspirasi warga masyarakat pada umumnya. Oleh karena itu, peranan yang besar dari hukum pidana merupakan kebutuhan yang tak dapat dielakkan bagi suatu sistem hukum. Perlindungan individu maupun masyarakat tergantung pada perumusan yang tepat dari kehidupan masyarakat itu sendiri. Oleh karena itu sistem hukum pidana, tindak pidana, penilaian hakim terhadap si pelanggar dalam hubungannya dengan hukum secara murni dan pidana merupakan lembaga-lembaga yang harus tetap

dipertahankan, hanya saja dalam menggunakan sistem hukum pidana Marc Ancel menolak penggunaan fiksi-fiksi yuridis dan teknis-teknis yuridis yang terlepas dari kenyataan sosial.

Marc Ancel menolak pandangan aliran klasik dan neo klasik yang memperlakukan kejahatan sebagai konsepsi hukum yang murni dan sanksi pidana merupakan konsekuensi yang diperlukan menurut hukum terhadap pelanggaran/ketertiban yang ada, dan juga menolak bahwa tujuan pidana atau sanksi-sanksi lain adalah "pembaharuan kembali tertib hukum tersebut secara abstrak." Kejahatan sebagai *a human and social problem*. Menurut Ancel tidak begitu saja mudah dipaksa untuk dimasukkan kedalam perumusan suatu peraturan undang-undang. Ini tidak berarti bahwa hakim pidana tidak memutus berdasar undang-undang dan harus menolak pidana. Diakuinya, bahwa hal ini, penerapan pidana berdasar undang-undang, merupakan bagian essensial dari tugas seorang hakim, tetapi Marc Ancel menyangkal bahwa problem kemanusiaan dan problem kemasyarakatan yang ditimbulkan oleh suatu tindak pidana dapat diselesaikan atau dipecahkan secara keseluruhan oleh bekerjanya suatu konsepsi keadilan distributif secara abstrak. Herbert L. Packer yang juga membicarakan masalah pidana ini dengan segala keterbatasannya di dalam bukunya *The Limits of Criminal Sanction*, akhirnya menyimpulkan antara lain sebagai berikut:[127]

1. Sanksi pidana sangatlah diperlukan, kita tidak dapat hidup, sekarang maupun dimasa yang akan datang, tanpa pidana.
2. Sanksi pidana merupakan alat atau sarana terbaik yang tersedia, yang kita miliki untuk menghadapi bahaya-bahaya besar dan segera serta untuk menghadapi ancaman-ancaman dari bahaya.
3. Sanksi pidana suatu ketika merupakan "penjamin yang utama atau terbaik" dan suatu ketika merupakan "pengancam yang utama" dari kebebasan manusia. Ia merupakan penjamin apabila digunakan secara hemat-cermat dan secara manusiawi, ia merupakan pengancam apabila digunakan secara sembarangan dan secara paksa.

---

[127] Herbert L Packer, " The Limits of Criminal Sanction", http://my--anne1.blogspot.com /2009/01/analisis-yuridis -penerapan-sistem.html, diakses tanggal 20 Nopember 2008.

Pendapat H.L Parker di atas dapatlah secara singkat dinyatakan dengan meminjam ungkapan John P. Conrad: *Punishment may not always satisfactory, but it is our only means of control.*

Sehubungan dengan pandangan pro dan kontra terhadap masalah *the abolition of punishment*, patut pula dikemukakan pandangan Johannes Andenaes yang menyatakan:

> "masalah penghapusan konsepsi pidana tidak hanya menimbulkan masalah-masalah hukum yang bersifat teknis, tetapi juga masalah-masalah dasar tentang filsafat moral. Dari sudut pandangan praktis murni, harus diakui bahwa konsepsi-konsepsi mengenai kesalahan dan pidana telah berakar secara kuat dalam kesadaran masyarakat umum. Pembuat undang-undang harus mempertimbangkan hal ini sebagai suatu kenyataan sosial."[128]

Pandangan J. Andenaes diatas jelas menggambarkan suatu pandangan yang tidak semata-mata bertolak dari sudut teori ilmu hukum atau suatu filsafat hukum secara murni, tetapi merupakan suatu pandangan yang lebih bersifat pragmatis. Pandangan pragmatis yang berhubungan dengan kenyataan-kenyataan social memang merupakan salah satu faktor yang sepatutnya dipertimbangkan oleh pembuat undang-undang dalam melakukan suatu kebijakan kriminal.[129]

Dari pendapat tersebut di atas, penulis berpendapat bahwa hukum pidana sangat penting dalam hal untuk mencegah terjadinya balas-membalas atas suatu tindakan yang pada prinsipnya melanggar norma-norma dan hukum yang berlaku.

Dengan demikian, penekanan penggunaan instrumen hukum pidana sebagai salah satu cara menanggulangi kejahatan ini dapat dipahami, karena ketentuan hukum pidana dianggap sebagai bagian *integral* dari upaya untuk melakukan pencegahan dan penanggulangan kejahatan. Lebih spesifik lagi, karena hanya dalam hukum pidana lah, fungsi *deterent* (menakut-nakuti) mempunyai legitimasi kuat, karena substansi hukuman dalam hukum pidana adalah penjatuhan sanksi pidana berupa penderitaan. [130]

---

[128] *Ibid.*

[129] *Ibid.*

[130] Dalam bukunya yang berjudul Lehrbuch des Peinlichen Rechts (1801), Feuerbach mengemukakan teorinya mengenai tekanan jiwa (*Psychologische Zwang Theorie*). Feuerbach beranggapan bahwa suatu ancaman pidana merupakan usaha preventif terjadinya tindak pidana. Apabila orang telah mengetahui sebelumnya bahwa ia diancam pidana karena melakukan tindak pidana, diharapkan akan menekan hasratnya untuk melakukan perbuatan tersebut. M. Karfawi,

Dengan demikian, hukum pidana diposisikan sebagai bagian penting dari sebuah kebijakan hukum, baik itu dalam fungsinya sebagai pelengkap ketentuan hukum administratif[131], atau murni dimaksudkan sebagai sarana kebijakan penal (*penal policy),* khususnya pada tahap kebijakan yudikatif/aplikatif penegakan hukum pidana (*in concreto).* [132] dan hal tersebut berlaku secara universal.

Dilihat dari perspektif hukum pidana, kebijakan penegakan hukum di Indonesia termasuk salah satu tugas pembangunan di bidang hukum, di samping pembentukan hukum dan pembangunan prasarana dan sarana hukum. Kebijakan penegakan hukum terutama kebijakan penegakan hukum pidana (*criminal law enforcement policy)* bermuara pada kebijakan kesejahteraan sosial (*social welfare policy)* sebagaimana dicantumkan dalam Pembukaan Undang-Undang Dasar 1945.

Perkembangan karakteristik hukum yang mengatur tindak pidana pada dasarnya merupakan respons terhadap perkembangan sosial, kultur dan politik ditengah masyarakat, yang pada akhirnya sangat mempengaruhi perkembangan substansi hukum pidana di Indonesia.[133] Perkembangan ini tidak dapat dihindari terutama menghadapi perkembangan kejahatan global yang turut memberi warna baru tindak pidana di Indonesia. Dimana pengaruh tindak pidana yang bersifat lintas batas teritorial dan berdampak sangat membahayakan, atau tindak pidana yang pada dasarnya sangat potensial merugikan kepentingan nasional dan/atau masyarakat internasional telah mewarnai wajah kejahatan di Indonesia sekarang ini.

"Asas Legalitas dalam Usul Rancangan KUHP (Baru) dan Masalah masalahnya", *Jurnal Arena Hukum*, Juli 1987, hal. 9-15.

[131] Menurut Muladi, dalam ini fungsi hukum pidana bersifat menunjang sanksi-sanksi administratif untuk ditaatinya norma-norma hukum administrasi. Dengan demikian keberadaan tindak pidana ini sepenuhnya bergantung pada hukum lain. Lebih lanjut lihat Muladi, dalam Prinsip-prinsip Dasar Hukum Pidana Lingkungan dalam Kaitannya dengan Undang-Undang No 23 Tahun 1997. Jurnal Hukum Pidana dan Kriminologi. Vol I. Nomor 1/1998, hal. 9.

[132] Barda Nawawi Arif. *Masalah Penegakan Hukum Pidana dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan.* Jakarta: Kencana Prenada Media Group, 2007, hal. 77.

[133] Contoh hukum administrative yang didalamnya memuat ketentuan pidana salah satunya dapat dilihat dalam ketentuan undang-undang Perbankan. Dengan demikian, ketika kejahatan ini dilakukan, maka secara yuridis hal tersebut dikatagorikan sebagai tindak pidana administrative (administrative penal law) atau tidak pidana yang mengganggu kesejahteraan masyarakat. (public welfare offences). Bandingkan dengan Muladi *Loc.,Cit,* hal. 4.

Dikaitkan dengan permasalahan apakah fungsionalisasi hukum pidana dapat memberikan efek jera dan dapat memberikan rasa keadilan bagi korban, memang tidak mudah. Tetapi sebagaimana tergambar dalam uraian tujuan pemidanaan nampak bahwa pemidanaan khususnya dengan sanksi pidana (penjara yang paling utama) akan memberikan dampak pencegahan secara khusus maupun secara umum. Secara khusus ditujukan kepada pelaku yang bersangkutan agar tidak mengulangi lagi perbuatannya, sehingga efek jera dapat dicapai. Hal ini juga terkait dengan efektifitas sanksi pidana dalam mencapai tujuan pidana.

Barda Nawawi Arief, mengemukakan bahwa mengetahui pengaruh bekerjanya pidana ini memang tidak mudah, karena seperti dikatakan oleh Johannes Andenaes, bekerjanya hukum pidana selamanya harus dilihat dari keseluruhan konteks kulturnya. Ada saling pengaruh antara hukum dengan faktor-faktor lain yang membentuk sikap dan tindakan-tindakan kita.[134] Lebih lanjut dikatakannya, sangatlah sulit untuk melakukan evaluasi terhadap efektivitas dari *general deterrence* karena mekanisme penangkalan/ awal pencegahan (*deterrence*) itu tidak diketahui. Kita tidak dapat mengetahui hubungan yang sesungguhnya antara sebab dan akibat. Orang mungkin melakukan kejahatan atau mengulanginya lagi tanpa hubungan dengan ada tidaknya undang-undang atau pidana yang dijatuhkan. Efektivitas hukum pidana tidak dapat diukur secara akurat, hukum hanya merupakan salah satu sarana kontrol sosial; kebiasaan, keyakinan agama, dukungan dan pencelaan kelompok, penekanan dari kelompok-kelompok interest, dan pengaruh dari pendapat umum merupakan sarana-sarana yang lebih efisien dalam mengetahui tingkah laku manusia dari pada sanksi hukum.[135]

Berkaitan dengan efek jera kepada pelaku, dalam kejahatan mayantara/ *cyber crime,* atau pada kejahatan pada umumnya, maka ukuran efektivitas terletak pada aspek pencegahan khusus *(special prevention)* dari pidana. Jadi, ukurannya terletak pada masalah seberapa jauh sanksi pidana mempunyai pengaruh terhadap si pelaku/terpidana. Ada dua aspek pengaruh pidana terhadap terpidana, yaitu aspek pencegahan awal *(deterent aspect)* dan aspek perbaikan (*reformative*

---

[134]Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana, Op.Cit.*, hal. 249.
[135] *Ibid.*, hal. 250.

aspect). Aspek pertama *(deterent aspect)* baisanya diukur dengan menggunakan *indicator recidivis*. Berdasarkan indikator inilah RM Jackson, menyatakan bahwa suatu pidana adalah efektif apabila si pelanggar tidak dipidana kembali dalam suatu periode tertentu. Selanjutnya ditegaskan bahwa efektivitas adalah suatu pengukuran dari perbandingan antara jumlah pelanggar yang dipidana kembali dengan dan yang tidak dipidana kembali. Penelitian dengan indikator *recidivis* ini sulit dilakukan di Indonesia, karena data yang ada biasanya sangat sumir yaitu hanya mengemukakan jumlah residivis pada tiap akhir bulan atau akhir tahun.

Aspek kedua, yaitu aspek perbaikan (*reformation aspect*) berhubungan dengan masalah perubahan sikap dari terpidana. Seberapa jauh pidana penjara dapat merubah sikap terpidana masih belum dapat dijawab secara memuaskan. Hal ini disebabkan pada problem metodologis yang belum terpecahkan dan belum ada kesepakatan, khususnya mengenai:

1. Apakah ukuran untuk menentukan telah adanya tanda-tanda perbaikan, atau adanya perubahan sikap pada diri si pelaku. Ukuran *recidivis rate* dan *reconviction rate* masih banyak yang diragukan.
2. Berapa lamanya periode tertentu untuk melakukan evaluasi terhadap ada tidaknya perubahan sikap setelah terpidana menjalani pidana penjara.[136]

Kesulitan dan keadaan tersebut juga berlaku terhadap efetivitas upaya penal khususnya melalui sarana sanksi pidana penjara terhadap pelaku kejahatan mayantara/*cyber crime*, Namun, dapat dikatakan bahwa pemberian dengan saran penal melalui sanksi pidana penjara, dalam kejahatan mayantara/*cyber crime* akan memberikan efek atau dampak pencegahan *(deterent aspect)* dan aspek perbaikan (*reformative aspect*) terhadap si pelaku dan juga terhadap masyarakat pada umumnya..

Fungsionalisasi atau operasionalisasi hukum pidana diarahkan pada penegakan hukum pidana yang didasarkan pada peraturan perundang-undangan yang sudah ada, yaitu:

1. Kitab Undang-Undang Hukum Pidana (KUHP).
2. Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi.

---

[136] *Ibid.*, hal. 254.

3. Undang-Undang No.19 Tahun 2002 tentang Hak Cipta
4. Undang-Undang Nomor 32 Tahun 2002 tentang Penyiaran.
5. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
6. dan Undang-Undang lainya yang terkait dan mengancamkan sanksi pidana.

Bagaimana para pelaku kejahatan mayantara *(cyber crime)* dapat dipertanggungjawabkan atas tindakannya berdasarkan undang-undang nasional harus dilihat secara lebih mendalam berdasarkan kualifikasi perbuatan sesuai dengan unsur-unsur tindak pidana yang diatur di dalam berbagai undang-undang tersebut.

3.4. Pertanggungjawaban Pidana Kejahatan Mayantara

Pertanggungjawaban pidana pada hakikatnya mengandung makna pencelaan pembuat (subjek hukum) atas tindak pidana yang telah dilakukannya. Oleh karena itu, pertanggungjawaban pidana mengandung didalamnya pencelaan objektif dan pencelaan subjektif. Artinya, secara objektif si pembuat telah melakukan tindak pidana (perbuatan terlarang/melanggar hukum dan diancam pidana menurut hukum yang berlaku) dan secara subjektif si pembuat patut dicela atau dipersalahkan/dipertanggungjawabkan atas tindak pidana yang dilakukannya itu sehingga ia patut dipidana.

Bertolak dari pengertian demikian, maka dalam arti luas, persyaratan pertanggungjawaban pidana pada dasarnya identik dengan persyaratan pemidanaan (penjatuhan pidana/tindakan). Ini berarti, asas-asas pertanggungjawaban pidana juga identik dengan asas-asas pemidanaan pada umumnya, yaitu asas legalitas dan asas culpabilitas. Bahkan dapat pula dinyatakan bahwa sistem pertanggungjawaban pidana dalam arti luas tidak dapat dilepaskan dari keseluruhan sistem (aturan) pemidanaan.

Persyaratan dan asas-asas pertanggungjawaban pidana yang dikemukakan di atas merupakan hal-hal yang sudah diterima secara umum dan konvensional dalam doktrin/teori maupun dalam peraturan perundang-undangan (hukum positif). Permasalahannya adalah seberapa jauh doktrin/teori dan ketentuan-

ketentuan hukum positif yang konvensional itu dapat juga diterapkan dalam masalah pertanggungjawaban pidana *cyber crime*.

Telah dikemukakan di atas bahwa untuk adanya pertanggungjawaban pidana pertama-tama harus dipenuhi persyaratan objektif, yaitu perbuatannya harus merupakan tindak pidana menurut hukum yang berlaku. Dengan perkataan 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 materiel/substantif maupun hukum pidana formal.

Selain berdasarkan hukum positif, juga perlu didukung ilmu pengetahuan hukum pidana, karena obyek ilmu pengetahuan hukum pidana terutama adalah mempelajari asas-asas dan peraturan-peraturan hukum pidana yang berlaku, menghubungkan asas-asas/peraturan-peraturan yang satu dengan yang lainnya, mengatur penempatan asas-asas/ peraturan-peraturan tersebut dalam suatu sistematika, agar dengan demikian dapat dipahami pengertian yang objektif dari pengaturan-pengaturan yang berlaku (hukum pidana posistif) yang merupakan tujuan dari ilmu pengetahuan hukum pidana. [137]

Tugas utama dari ilmu pengetahuan hukum pidana adalah untuk mempelajari dan menjelaskan (interpretasi) hukum (tindak) pidana yang berlaku pada suatu waktu dan negara tertentu. Ia mempelajari norma-norma dalam hubungannya dengan pemidanaan (konstruksi), dan kemudian menerapkan hukum pidana yang berlaku secara teratur dan berurutan (sistematika). Dengan perkataan lain ia mengolah suatu tindak pidana yang sudah terjadi kemudian dihubungkan dengan penerapan hukum pidana yang berlaku.[138]

Untuk melakukan hal tersebut diatas, bukanlah persoalan mudah. Banyak masalah-masalah yang menjadi kendala dalam mewujudkan penegakan hukum. Salah satunya adalah belum responsifnya undang-undang yang mengatur tentang jenis kejahatan dengan teknik dan modus operandi yang baru.

---

[137] E.Y Kanter dan S.R Sianturi, *Asas-asas Hukum Pidana di Indonesia dan Penerapannya*. Jakarta : Storia Grafika : 2002. hal. 32.
[138] *Ibid.*, hal. 33.

Pendekatan dari sudut politik kriminal terlihat pula dari pendapat Van Bemmelen yang mengemukakan sebagai berikut :[139] Jika kita mendekati hukum pidana bukan dari sudut pidananya tetapi dari sudut ketentuan-ketentuan pemerintah dan larangan serta dari sudut penegakan ketentuan-ketentuan itu (yakni penegakan hukum), dan khususnya dari sudut hukum acara pidana, maka kita tidak lagi begitu condong untuk membuang hukum pidana. Jika kita mendekati hukum pidana dari sudut ketentuan-ketentuan pemerintah dan larangan, kita sadar bahwa perbuatan-perbuatan tertentu yang melawan hukum yang tidak mungkin akan diterima oleh masyarakat. Makar terhadap kepala negara tidak mngkin dapat diterima oleh negara. Begitupun masyarakat tidak mungkin dapat menerima bahwa manusia secara bebas membunuh orang lain atau sengaja merusak, menghilangkan atau mengambil sesuatu benda milik orang lain tanpa ijin pemiliknya.

Pertanggungjawaban kejahatan mayantara/*cyber crime* tentunya harus didasarkan pada sumber hukum perundang-undangan yang berlaku saat ini (baik didalam KUHP maupun dalam undang-undang khusus di luar KUHP). Peraturan perundang-undangan di luar KUHP, yang dapat dikaitkan dengan perkembangan kejahatan yang menggunakan teknologi canggih di bidang informasi dan telekomunikasi. Ketentuan pidana yang dapat diterapkan dalam rangka pertanggungjawaban pidana kepada pelaku kejahatan mayantara *cyber crime* berupa tindak pidana khusus dan tindak pidana umum.

3.4.1. Pertanggungjawaban Pidana Kejahatan Mayantara menurut KUHP

Sistem hukum pidana materiil yang saat ini berlaku di Indonesia terdiri dari keseluruhan sistem peraturan perundang-undangan (*statutory rules*) yang ada dalam KUHP (sebagai induk aturan umum) dan undang-undang khusus diluar KUHP. Keseluruhan peraturan perundang-undangan (*statutory rules*) di bidang hukum pidana substantif itu terdiri dari aturan umum (*general rules*) dan aturan khusus (*special rules*). Aturan umum terdapat di dalam KUHP (Buku I), dan

---

[139] Van Bemmelen, *ons strafrecht 1, het matierel strafrecht algemeen deel, Zesde herzeine drunk*, H.D. Tjeenk Willink, Groningen, 1979, hal. 21-22. dalam Barda Nawawi Arief, Kebijakan Legislatif dalam Penanggulangan Kejahat dengan Pidana Penjara, Semarang: BP Undip, 1996, hal. 20.

aturan khusus terdapat di dalam KUHP (Buku II dan III) maupun dalam undang-undang khusus di luar KUHP. Aturan khusus ini pada umumnya memuat perumusan tindak pidana tertentu, namun dapat pula memuat aturan khusus yang menyimpang dari aturan umum. Dengan demikian sistem hukum pidana substantif yang berlaku ini dapat digambarkan sebagai berikut :

Merujuk kepada Sistem hukum pidana materil yang saat ini berlaku di Indonesia, terhadap kejahatan *cyber*, setidaknya ada dua pendapat yang berkembang sejalan dalam menangani kasus kejahatan yang berhubungan dengan komputer yang secara tidak langsung juga berkaitan dengan masalah *cyber crime* yakni;

1. Pendapat pertama menyatakan bahwa KUHP mampu untuk menangani kejahatan di bidang komputer (*computer crime*). Pendapat ini didasarkan pada pertimbangan bahwa kejahatan komputer sebenarnya bukanlah kejahatan baru dan masih terjangkau oleh KUHP untuk menanganinya. Pengaturan untuk menangani kejahatan komputer sebaiknya diintegrasikan ke dalam KUHP dan bukan ke dalam undang-undang tersendiri.
2. Pendapat yang kedua, mengatakan bahwa kejahatan yang berhubungan dengan komputer (*computer crime*) memerlukan ketentuan khusus dalam KUHP atau undang-undang tersendiri yang mengatur tindak pidana dibidang komputer. Pertimbangan dari pendapat kedua ini dilatarbelakangai oleh:
   a. Bahwa hukum pidana yang ada tidak siap menghadapi kejahatan komputer, karena tidak segampang itu menganggap kejahatan komputer berupa pencurian data sebagai suatu pencurian. Kalau dikatakan pencurian harus ada barang yang hilang. Sulitnya pembuktian dan kerugian besar yang mungkin terjadi melatarbelakangi pendapatnya yang mengatakan perlunya produk hukum baru untuk menangani kejahatan komputer agar dakwaan terhadap pelaku kejahatan tidak meleset.
   b. Perlu adanya ketentuan baru yang mengatur permasalahan tindak pidana komputer. Tindak pidana yang menyangkut komputer

haruslah ditangani secara khusus, karena cara-caranya, lingkungan, waktu dan letak dalam melakukan kejahatan komputer adalah berbeda dengan tindak pidana lain.

Ketentuan-ketentuan yang terdapat dalam KUHP tentang *cyber crime* masing bersifat global. Namun berdasarkan tingkat kemungkinan terjadinya kasus dalam dunia maya (*cyber*) dan kategorisasi kejahatan *cyber* menurut *draft convention on cyber crime* maupun pendapat para ahli, Teguh Arifiyadi mengkategorikan beberapa hal yang secara khusus diatur dalam KUHP dan disusun berdasarkan tingkat intensitas terjadinya kasus tersebut yaitu[140]:

1. **Tindak Pidana berkaitan dengan pencurian**

   Delik tentang pencurian dalam dunia maya termasuk salah satu delik yang paling populer diberitakan media masa. Delik pencurian diatur dalam Pasal 362 KUHP, Pasal 363 KUHP, Pasal 364 KUHP, Pasal 365 dan Pasal 367 KUHP. Pengertian benda diambil dari penjelasan Pasal 362 KUHP segala sesuatu yang berwujud atau tidak berwujud dan mempunyai nilai di dalam kehidupan ekonomi dari seseorang.

   Dalam sistem jaringan (*network*), peng-copy-an data dapat dilakukan secara mudah tanpa harus melalui izin dari pemilik data. Pencuri biasanya lebih mengutamakan memasuki sistem jaringan perusahaan finansial seperti penyimpanan data kartu kredit, komputer-komputer di bank atau situs-situs belanja *online* yang ditawarkan di media internet dan data yang didapatkan secara melawan hukum itu diharapkan memberi keuntungan bagi si pelaku.

2. **Tindak Pidana berkaitan dengan perusakan/penghancuran barang**

   Dalam kejahatan komputer (*computer crime*), perbuatan perusakan, penghancuran barang mempunyai pengertian suatu perbuatan yang

---

[140] Teguh Arifiyadi. "Cyber Crime dan Upaya Antisipasinya Secara Yuridis (I)", http://. wordpress.com/2009/04/23/cyber-crime-dan-upaya-antisipasinya.secarayuridis/ Teguh+Arifiyadi+Cyber+Crime+dan+Upaya+Antisipasinya+Secara+Yuridis&cd=6&hl= id&ct=clnk&gl=I d&client= firefox-a *cyber crime*/Portal Departemen Komunikasi dan Informatika Republik Indonesia. html.

dilakukan dengan suatu kesengajaan untuk merusak / menghancurkan media disket atau media penyimpan sejenis lainnya yang berisikan data atau program komputer sehingga akibat perbuatan tersebut data atau program yang dimaksud menjadi tidak berfungsi lagi dan pekerjaan-pekerjaan yang melalui proses komputer tidak dapat dilaksanakan. Ketentuan mengenai perbuatan perusakan, penghancuran barang diatur dalam pasal 406-412 KUHP. Perbuatan penghancuran atau perusakan barang yag dilakukan *cracker* dengan kemampuan *hacking*nya bukanlah perbuatan yang bisa dilakukan oleh semua orang awam.

3. Tindak Pidana berkaitan dengan pornografi

Hadirnya media internet secara global menyebabkan siapa saja dapat untuk mengakses situs-situs yang tersedia secara mudah. Ketentuan tentang pornografi dalam dunia maya dikaitkan dengan kasus yang pernah terjadi di Indonesia penulis mengetengahkan kasus Indrawan Yusuf alias Hengky Wiratman alias Irwan Soenaryo seorang pria asal Malang. Dalam kasus ini anggota Satuan *cyber crime* Direktorat Kriminal Khusus Kepolisian Daerah Metropolitan Jakarta Raya, terkait dengan kasus perdagangan VCD porno dan alat bantu seks melalui jaringan internet dalam situs http://www.vcdporno.com. Terdakwa diancam hukuman Pidana Penjara paling lama 2 (dua) tahun 8 (delapan) bulan, karena melanggar Pasal 282 KUHP

4. Tindak Pidana tentang penipuan

Ketentuan yang berkaitan dengan penipuan yakni perbuatan memanipulasi keterangan untuk mencari keuntungan melalui media internet dapat "ditafsirkan" sebagai perbuatan menyesatkan yang ada dalam delik penipuan seperti yang tertuang dalam pasal 378 KUHP dan pasal 379a KUHP apabila hal tersebut berkaitan dengan pembelian barang). Contoh dari perbuatan ini adalah seseorang yang dengan sengaja melakukan transaksi pada situs-situs belanja *online* secara fiktif atau seseorang yang melakukan penipuan dengan memanfaatkan sarana suatu situs/*web* bahkan melalui fasilitas *e-mail* dengan memberikan janji-janji palsu.

5. Tindak Pidana berkaitan dengan perbuatan memasuki atau melintasi wilayah orang lain

Apabila ada seorang asing hendak masuk ke sistem jaringan komputer tersebut tanpa ijin dari pemilik terminal ataupun penanggung jawab sistem jaringan komputer, maka perbuatan ini dikategorikan sebagai *hacking*. Kejahatan komputer jenis *hacking* atau *cracking* (apabila ia melakukan perusakkan atau gangguan) sangat berbahaya karena apabila seseorang berhasil masuk ke dalam sistem jaringan orang lain, maka ia akan mudah untuk mengubah ataupun mengganti data yang ada sebelumnya pada sistem jaringan. Perbuatan mengakses ke suatu sistem jaringan tanpa ijin tersebut dapat dikategorikan sebagai perbuatan tanpa wewenang masuk dengan memaksa ke dalam rumah atau ruangan yang tertutup atau pekarangan tanpa haknya berjalan di atas tanah milik orang lain, sehingga pelaku dapat diancam pidana berdasarkan Pasal 167 KUHP dan Pasal 551 KUHP.

6. Tindak Pidana tentang penggelapan

Perbuatan penggelapan dengan memanfaatkan internet erat kaitannya dengan perbuatan memanipulasi data atau program pada suatu sistem jaringan komputer. Perbuatan ini dapat dijerat dengan Pasal 372 KUHP dan Pasal 372 KUHP, apabila perbuatan penggelapan dengan sarana internet tersebut mendatangkan kerugian bagi keuangan negara, maka dapat diterapkan delik korupsi .

7. Tindak Pidana terhadap ketertiban umum

Apabila kita meninjau kembali pasal 154, maka dapat kita lihat bahwa pasal tersebut termasuk pasal yang menuntut delik pers. Pelaku dalam tindak pidana ini memanfaatkan fungsi internet sebagai salah satu media publikasi yang disalahgunakan untuk kepentingan sendiri atau golongannya.

8. Tindak Pidana tentang pemalsuan surat

Kemampuan komputer tidak hanya sebagai media untuk menyimpan dan mengolah data. Kemampuan komputer juga dapat membuat gambar-gambar, foto-foto dengan tidak menutup kemungkinan terjadinya pemalsuan-pemalsuan surat berharga, apalagi ditambah dengan hadirnya media internet dimana setiap orang yang mempunyai kemampuan khusus dapat men-

download program-program yang berisikan data tentang surat berharga seperti kartu kredit bahkan memungkinkan dilakukannya pemalsuan identitas seperti, K.T.P, SIM, akte kelahiran, paspor dan lain sebagainya. Pemalsuan yang dilakukan dengan sarana komputer sebagai data *diddling* mempunyai pengertian yakni suatu perbuatan yang mengubah data valid / sah dengan cara yang tidak sah dan dengan mengubah input / masukan data atau output / keluaran data. Apabila dikaitkan dengan delik-delik yang ada dalam KUHP, maka data *diddling* dapat dikategorikan sebagai perbuatan tanpa wewenangnya memalsukan surat / pemalsuan surat, dapat diancam dengan pidana berdasarkan Pasal 263 KUHP. Surat menurut Pasal 263 adalah segala surat yang ditulis dengan tangan, dicetak, maupun ditulis dengan mesin tik dan lain-lain.

9. Tindak Pidana tentang pembocoran rahasia;

Ketentuan yang berkaitan dengan perbuatan membocorkan rahasia negara (termasuk didalamnya perbuatan dengan menggunakan sarana internet) diatur dalam pasal 112, 113 KUHP dan Pasal 114 KUHP serta perbuatan membocorkan rahasia perusahaan yang diatur dalam Pasal 322 KUHP dan Pasal 323 KUHP.

Kaitannya dengan kejahatan komputer ialah bahwa dengan pemanfaatan komputer pembukaan rahasia negara dapat dilakukan kepada pihak yang tidak berwenang untuk menerima rahasia tersebut.

Sedangkan perbuatan membocorkan rahasia perusahaan dapat dikategorikan sebagai kejahatan membuka rahasia, sehingga si pelaku dapat diancam dengan pidana berdasarkan Pasal 322 KUHP Pasal 323 KUHP.

10. Tindak Pidana tentang perjudian

Ada puluhan ribu lebih situs-situs di internet yang menyediakan fasilitas perjudian dari yang model klasik yang hanya memainkan fungsi tombol *keyboard* sampai yang sangat canggih yang menggunakan pemikiran matang dan perhitungan-perhitungan adu keberuntungan. Tidak diperlukan lagi perizinan-perizinan khusus untuk membuat sebuah usaha perjudian via internet. Cukup dengan bermodalkan sebuah *web* dengan fasilitas perjudian

menarik, setiap orang dapat memiliki 'rumah perjudian' di internet. Ketentuan tentang perjudian dalam KUHP diatur dalam pasal 303 dan 303 bis.

Dari apa yang telah diuraikan diatas, dalam prakteknya fungsionalisasi hukum pidana dengan mempergunakan KUHP memang telah berjalan. Dikatakan demikian kerena ketentuan-ketentuan KUHP telah berfungsi, beroperasi atau bekerja dan terwujud secara kongkrit, dengan menghukum para pelaku tindak pidana *cyber*.

Sebagai contoh kongkrit Fungsionalisasi KUHP dalam kejahatan *cyber*, penulis memberikan beberapa contoh kasus yang telah diputus oleh Pengadilan, yakni :

1. Kasus Petrus Pangkur

   Putusan Pengadilan Negeri Sleman No: 94/Pid.B/2002/PN.SLMN. yang menghukum terdakwa Petrus Pangkur karena melakukan *carding*. Dalam persidangan, Jaksa Penuntut Umum mengajukan dakwaan kesatu Pasal 363 ayat (1) ke-5 KUHP dan dakwaan kedua Pasal 378 KUHP. Terdakwa Petrus Pangkur dipidana selama 1 tahun 3 bulan, karena telah terbukti secara sah dan meyakinkan bersalah melakukan tindak pidana penipuan dalam dakwaan kedua. Dakwaan kesatu tidak terbukti secara sah dan meyakinan karena dakwaan kesatu yang diajukan oleh Penuntut Umum tidak dapat memenuhi unsur "mengambil". [141]

2. Kasus Beny Wong

   Kasus *carding* lainnya yang berhasil diungkap adalah kasus yang dilakukan oleh Beny Wong. Pada tanggal 14 Juli 2004 terpidana melakukan transaksi di "Hardy's Supermarket" Batubulan Gianyar, Bali dengan menggunakan kartu kredit Citibank bernomor 4541 7900 1413 0605 atas nama Wahyu Nugroho. Saat itu transaksi berhasil dilakukan.

   Pada tanggal yang sama, Beny Wong kembali berbelanja di "Hardy's Supermarket" Sanur, Bali. Dengan menggunakan empat kartu kredit palsu

---

[141] Dikutip dari http://widodo-cybercrimelaw.blogspot.com/2009/02/pidana-kerja-sosial-dan-pidana.html. diakses tanggal 9 juli 2009.

yaitu Mastercard dari BNI, Visa dari Standard Chartered Bank, serta Mastercard dan Visa dari Citibank. Namun transaksi gagal dilakukan karena Kartu Kredit yang digunakan diketahui palsu.

Dalam persidangan tanggal 14 September 2004 Majelis Hakim Pengadilan Negeri Denpasar yang dipimpin oleh Hakim Ketua Arif Supratman SH memberikan "hadiah" kepada terdakwa berupa putusan hukuman penjara selama 3 (tiga) tahun.

Sembilan bulan kemudian, tepatnya 6 Juni 2005, Majelis Hakim Pengadilan Negeri Gianyar Bali yang dipimpin oleh Hakim Ketua Gede Ginarsa dan Jaksa Penuntut Umum Ida Ayu Surasmi memvonis untuk terdakwa yang sama dengan putusan hukuman penjara selama 2 (dua) tahun 8 (delapan) bulan. Secara keseluruhan, hukuman atas terdakwa pemalsuan kartu kredit di Bali itu adalah 5 (lima) tahun 8 (delapan) bulan.

Putusan Hukuman terhadap Beny Wong di Pengadilan Negeri Denpasar dan Pengadilan Negeri Gianyar Bali tersebut, didasarkan pada Pasal 263 KUHP tentang pemalsuan surat (barang siapa membuat surat palsu..., jika pemakaian tersebut dapat menimbulkan kerugian, karena pemalsuan surat, diancam dengan pidana penjara paling lama enam tahun).[142]

3. Kasus Buyung.

Salah satu *carding* yang sempat populer adalah tertangkapnya *carder* asal Bandung. Buyung alias Sam, mahasiswa berusia 25 tahun yang menggunakan kartu kredit orang lain untuk transaksi melalui internet. Nilainya mencapai sekitar DM 15 ribu. Aksi ini dilakukan melalui warnet selama satu tahun. Kasus ini diserahkan Polda Jabar ke Mabes Polri. Pertimbangannya karena kejahatan yang dilakukan tersangka berdampak ke

---

[142] Unit *Cyber crime* Satuan Reserse Ekonomi Direktorat Reserse Kriminal Polda Jateng. Disampaikan pada Seminar Penegakan Hukum *Cyber crime*. Fakultas Hukum Universitas Kristen Satya Wacana Salatiga. Semarang, 2 Juni 2006.

berbagai negara, sehingga pengusutannya membutuhkan keterlibatan pihak interpol.

Terbongkarnya kejahatan Buyung berawal dari berita teleks Interpol Wiesbaden No. 0234203 tertanggal 6 September 2001 yang melaporkan adanya penipuan melalui internet dan diduga melibatkan seorang WNI yang bertindak sebagai pemesan barang bernama Buy.

Menurut Kapolda Jabar waktu itu, saat ini untuk sementara kepolisian akan menjerat sang mahasiswa dengan Kitab Undang-Undang Hukum Pidana (KUHP) soal pencurian dan penipuan mengingat perangkat hukum yang lebih tepat, terutama soal *cyberlaw* dan *cybercrime* di Indonesia belum ada.

Belum jelas bagaimana kasus ini ditindaklanjuti sebab pihak kepolisian juga kurang terbuka pada pers. Kabarnya Buyung dilepas setelah diberi semacam wejangan oleh sejumlah praktisi TI dan pihak kepolisian untuk tidak mengulangi perbuatannya. Buyung juga didesak agar memberi pesan moral kepada para *carder* lain agar tidak melanjutkan aksinya[143].

3.4.2. Pertanggungjawaban Pidana Kejahatan Mayantara menurut Hukum Khusus (*Lex Specialis*)

Dalam praktek penegakan hukum terhadap tindak pidana mayantara, disamping mempergunakan ketentuan hukum yang diatur oleh KUHP, juga dipergunakan ketentuan hukum diluar KUHP, atau yang disebut dengan Hukum Khusus (*Lex Specialis*).

Mengenai pengertian hukum khusus ini, Andi Hamzah mengatakan bahwa hukum pidana khusus diartikan sebagai hukum pidana materiel maupun hukum pidana formil.[144] Sementara Pompe, seorang sarjana hukum pidana Belanda membuat pengertian tentang hukum pidana khusus (materiel dan formil) dengan menyebut dua kriteria, yang menunjukkan hukum pidana khusus, yaitu orang-

---

[143]Diakses pada situs http://www.google.co.id/url?sa =t&source=webcontent Web&t= res&cd=1&url =http%3A%2F%2Fwww.apricot.net%2Fapricot2007%2Farsip%2Fidstream %2 Fsesi 3%2FAPRICO T%2520BALI% 25202007.ppt&ei= o39a SvKrNYe VkAXIx ITUBQ&usg=AFQjCNHoPDmNDGzoj3h91K0CStfaH3hLZA 9 Juli 2009.

[144] Andi Hamzah, *Perkembangan Hukum Pidana Khusus*. Jakarta: Melton Putra, 1991, hal. V

orangnya yang khusus, maksudnya subjeknya atau pelakunya yang khusus dan yang kedua ialah *perbuatannya* yang khusus.[145]

Lebih lanjut Pompe menunjuk patokan pasal 103 KUHP yaitu jika ketentuan undang-undang diluar KUHP banyak menyimpang dari ketentuan umum hukum pidana, maka itu merupakan hukum pidana khusus.[146] Jadi menurut pompe, bukan saja materielnya yang menyimpang dari ketentuan umum hukum pidana (Buku I KUHP), tetapi juga hukum acaranya banyak yang menyimpang dari hukum acara pidana umum (KUHP).[147]

Sudarto, salah seorang pakar hukum pidana Indonesia membagi tiga kelompok yang bisa dikualifikasikan sebagai undang-undang pidana khusus, yakni:

1. Undang-undang yang tidak dikodifikasikan.
2. Peraturan-peraturan hukum administratif yang memuat sanksi pidana.
3. Undang-undang yang memuat hukum pidana khusus (*ius singulare, ius speciale*), yang memuat delik-delik untuk kelompok orang tertentu atau berhubungan dengan perbuatan tertentu.[148]

Penerapan ketentuan pidana khusus terhadap kejahatan mayantara terkait erat dengan persyaratan pertanggungjawaban pidana, yang pada dasarnya identik dengan asas-asas pemidanaan pada umumnya, yaitu asas legalitas dan culpabilitas.[149] Bahkan dapat pula dinyatakan bahwa sistem pertanggungjawaban pidana dalam arti luas tidak dapat dilepaskan dari keseluruhan sistem aturan pemidanaan.

Telah dikemukakan di atas bahwa untuk adanya pertanggungjawaban pidana pertama-tama harus dipenuhinya persayaratan objektif, yaitu perbuatannya harus merupakan tindak pidana menurut hukum yang berlaku. Dengan perkataan lain, untuk adanya pertanggungjawaban pidana, pertama-tama harus dipenuhinya asas

---

[145] *Ibid.*, hal. 2.
[146] *Ibid.*,
[147] Pasal 103 KUHP menyatakan bahwa "Ketentuan-ketentuan dalam Bab I sampai Bab VIII buku ini juga berlaku bagi perbuatan- perbuatan yang oleh ketentuan perundang-undang an lainnya diancam dengan pidana, kecuali jika oleh undang-undang ditentukan lain".
[148] Sudarto, *Kapita Selekta Hukum Pidana.* Bandung: Alumni, Cetakan Ke-3, 2003, hal. 63-64.
[149] Barda, Nawawi Arief, *Tindak Pidana Mayantara Perkembangan Kajian Cybercrime di Indonesia.* Jakarta : Rajawali Press 2005, hal. 73.

legalitas, yaitu harus ada dasar/sumber hukum (sumber legitimasi) yang jelas, baik di bidang hukum pidana materiel/ subtantif maupun hukum pidana formal.

Bertolak dari persyaratan objektif yang konvensional (asas legalitas) pertanggungjawaban *cyber crime* tentunya harus didasarkan pada sumber hukum perundang-undangan yang berlaku saat ini, dalam hal ini KUHP dan UU Pidana Khusus.

Dalam praktek penegakan hukum berdasarkan ketentuan undang-undang pidana khusus berbagai perundang-undangan yang dapat diterapkan/ digunakan adalah:

1. **Undang-Undang Nomor 20 Tahun 2001 Tentang Tindak Pidana Korupsi**

   Contoh fungsionalisasi hukum pidana terhadap kejahatan berdimensi mayantara dengan mempergunakan instrumen UU Korupsi dapat dilihat dalam kasus Liauw Joen Tjin alias A een, yang melakukan penggelapan uang di bank BRI Cab. Katamso Yogyakarta, melalui komputer.[150]

   Dalam kasus ini, Liauw Joen Tjin alias A een bersama-sama dengan Dalip Jamhari (karyawan BRI Cab. Katamso Yogyakarta, terdakwa mengkliringkan beberapa cek/Bilyet giro BRI Cab. Brigjen Katamso Yogyakarta melalui Bank Niaga Cabang Yogyakarta.

2. **Undang-Undang No 36 Tahun 1999 tentang Telekomunikasi**

   Lahirnya UU No 36 Tahun 1999 tentang Telekomunikasi didasari atas pertimbangan bahwa penyelenggaraan telekomunikasi mempunyai arti strategis dalam upaya memperkukuh persatuan dan kesatuan bangsa, memperlancar kegiatan pemerintahan, mendukung terciptanya tujuan pemerataan pembangunan dan hasil-hasilnya, serta meningkatkan hubungan antarbangsa. Indonesia sangat menyadari bahwa pengaruh globalisasi dan perkembangan teknologi telekomunikasi yang sangat pesat telah mengakibatkan perubahan yang mendasar dalam penyelenggaraan dan cara pandang terhadap telekomunikasi.

---

[150] Kasus penggelapan uang di bank melalui komputer (*clearing*) ini merupakan kasus pertama di Indonesia yang muncul ke permukaan (ke pengadilan).

Dikaitkan dengan ketertinggalan KUHP dalam mengatisipasi terjadinya delik baru terkait kemajuan teknologi seperti kejahatan komputer, pencurian pulsa dan delik-delik lain yang berkaitan dengan teknologi informasi, maka menjadi suatu hal yang sangat logis apabila dalam UU ini dicantumkan juga ketentuan pidana.

Delik-delik yang berkaitan dengan kejahatan mayantara dalam Undang-undang ini adalah sebagai berikut :

a. Memanipulasi akses ke jaringan telekomunikasi (pasal 50 jo 22)
b. Menyadap informasi melalui jaringan telekomunikasi (pasal 56 jo. 40). Kongkritisasi penerapan hukum pidana terhadap kasus kejahatan berdimensi mayantara tersebut dapat dilihat dalam kasus Dani Xnuxer yang melakukan *Defacing* terhadap situs KPU.

3. Undang-Undang 15 Tahun 2003 tentang Terorisme

Beberapa waktu lalu di tahun 2004, Kepolisian RI berhasil menangkap pelaku pembuat situs yang ditengarai merupakan situs yang digunakan oleh Kelompok Jaringan teroris di Indonesia untuk melakukan propaganda terorisme melalui Internet.

Domain situs teroris http://www.anshar.net dibeli dari kartu kredit curian (hasil *carding*). Hasil penelusuran menunjukkan, situs tersebut dibeli atas nama Max Fiderman. Max Fiderman tentunya bukan nama asli, alias nama samaran. Max Fiderman sebenarnya orang baru di belantara *carding*. Setelah menguasai sedikit ilmunya, Max diduga berhasil dibujuk untuk membeli domain http://www.anshar.net dengan kartu kredit curian.

4. Undang-Undang Nomor 32 tahun 2002 tentang Penyiaran.

Undang-Undang Nomor 32 tahun 2002 tentang Penyiaran (menggantikan Undang-Undang Nomor 24 tahun 1997), antara lain mengatur tindak pidana sebagai berikut:

a. Pasal 57 juncto Pasal 36 ayat (5) mengancam pidana terhadap siaran yang:
   1) bersifat fitnah, menghasut,menyesatkan dan/ atau bohong;
   2) menonjolkan unsur kekerasan, cabul, perjudian, penyalahgunaan narkotika dan obat terlarang; atau

3) mempertentangkan suku, agama, ras, dan antar golongan.

b. Pasal 57 juncto Pasal 36 ayat (6) mengancam pidana terhadap siaran yang memperolokkan, merendahkan, melecehkan, dan/ atau mengabaikan nilai-nilai agama, martabat manusia Indonesia, atau termasuk hubungan internasional.

c. Pasal 58 juncto 46 ayat (3) mengancam pidana terhadap siaran iklan niaga yang didalamnya memuat:

1) Promosi yang dihubungkan dengan ajaran suatu agama, ideologi, pribadi dan/atau kelompok yang menyinggung perasaan dan/atau merendahkan martabat agama lain, ideologi lain, pribadi lain, atau kelompok lain;
2) Promosi minuman keras atau sejenisnya dan bahan atau zat adiktif;
3) Promosi rokok yang memperagakan wujud rokok;
4) Hal-hal yang bertentangan dengan kesusilaan masyarakat dan nilai-nilai agama; dan
5) Eksploitasi anak dibawah umur 18 tahun.

Dibandingkan dengan UU Penyiaran yang lama (UU No. 24/1997), patut dicatat hal-hal sebagai berikut:

a. Didalam Undang-Undang Nomor 32 tahun 2002 tidak ada penentuan kualifikasi delik (sebagai kejahatan atau pelanggaran) sehingga dapat menimbulkan masalah juridis. Sementara itu, di dalam Undang-Undang Penyiaran yang lama (Undang-Undang Nomor 24 tahun 1997), disebutkan secara tegas kualifikasi deliknya, yaitu ada yang dinyatakan sebagai kejahatan dan ada yang berupa "pelanggaran".

b. Perumusan delik pada Pasal 57 juncto Pasal 36 ayat (5) dan ayat (6) Undang-undang Nomor 32 tahun 002 mirip dengan perumusan delik dalam Pasal 64 dan Pasal 65 Undang-Undang Nomor 24 tahun 1997 yang berdasarkan Pasal 76 Undang-Undang Nomor 24 tahun 1997 dinyatakan sebagai "kejahatan".

c. Perumusan delik pada Pasal 58 Undang-Undang Nomor 32 tahun 2002 mirip dengan Pasal 73 juncto Pasal 42 ayat (2) a dan Pasal 74 juncto Pasal 42 (2) b, c, d Undang-Undang Nomor 24 tahun 1997, yang oleh Pasal 76 Undang-undang lama ini dinyatakan sebagai "pelanggaran"

d. Dengan tidak adanya kualifikasi yuridis yang jelas didalam Undang-Undang Nomor 32 tahun 2002, hal ini tidak dapat menimbulkan masalah dalam penerapannya (termasuk pertanggungjawaban pidananya).

5. Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (ITE)

Berbagai contoh kasus kejahatan mayantara/ *cyber crime* yang berhasil diungkap di atas, menunjukkan bahwa kejahatan mayantara ini cenderung mengalami peningkatan. Dilihat dari segi motivasi dan modus yang dilakukan, hal ini pun mengalami berbagai kemajuan. Teknik-teknik yang dipergunakan semakin hari semakin sulit untuk dilacak.

Berbagai upaya mulai dari pencegahan, penanganan kasus dan pemidanaan terhadap para pelaku kejahatan mayantara/*cyber crime* saat ini masih menimbulkan permasalahan. Berbagai penanganan kasus, dengan menggunakan berbagai undang-undang hingga saat ini menunjukkan bahwa aturan perundang-undangan yang spesifik mengatur tentang kejahatan kejahatan mayantara *cyber crime* memang belum memadai.

Pada tahun 2008 diundangkan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (ITE) membawa harapan baru dan tantangan bagi para aparatur penegak hukum dan pemerhati terjadinya tindak pidana mayantara, untuk kembali memperhatikan dan mempelajari unsur-unsur dan sistem perlindungan hukum guna memaksimalkan penegakan hukum terhadap kasus-kasus kejahatan mayantara.

Secara garis besar, arah kebijakan penanggulangan tindak pidana mayantara dalam Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (ITE) dilandaskan kepada pemikiran

bahwa perkembangan dan kemajuan Teknologi Informasi yang demikian pesat telah menyebabkan perubahan kegiatan kehidupan manusia dalam berbagai bidang yang secara langsung telah memengaruhi lahirnya bentuk-bentuk perbuatan hukum baru. bahwa penggunaan dan pemanfaatan Teknologi Informasi harus terus dikembangkan untuk menjaga, memelihara, dan memperkukuh persatuan dan kesatuan nasional berdasarkan peraturan perundang-undangan demi kepentingan nasional, bahwa pemanfaatan Teknologi Informasi berperan penting dalam perdagangan dan pertumbuhan perekonomian nasional untuk mewujudkan kesejahteraan masyarakat, bahwa pemerintah perlu mendukung pengembangan Teknologi Informasi melalui infrastruktur hukum dan pengaturannya sehingga pemanfaatan Teknologi Informasi dilakukan secara aman untuk mencegah penyalahgunaannya dengan memperhatikan nilai-nilai agama dan sosial budaya masyarakat Indonesia.[151] Dari hal tersebut, dikaitkan dengan fungsi hukum pidana sebagai sebuah *"punishment"*, maka yang seharusnya dikembangkan menyangkut dua unsur pokok, yaitu :

a. Mencegah terjadinya tindak pidana mayantara.
b. Penindakan kepada pelaku tindak pidana mayantara. [152]

Lahirnya Undang-Undang ITE merupakan instrumen untuk melindungi masyarakat dari bahaya tindak pidana mayantara. Akan tetapi patut diwaspadai bahwa karakteristik tindak pidana mayantara, bersifat khusus dan merupakan *extra ordinary crime,* karena banyak melibatkan aspek yang kompleks, dan bersifat *transnasional crime,* karena melintasi batas-batas negara. Dengan demikian, strategi penanggulangan dan pemberantasannya harus secara khusus pula. Oleh karena itu diperlukan profesionalisme dan kehandalan para penegak hukum untuk memahami

---

[151] Lihat konsideran menimbang UU No 11 Tahun 2008 Poin c,d,e dan f

[152] H.L. Packer menyatakan, pembenaran dari punishment didasarkan pada satu atau dua tujuan sebagai berikut :

1. Mencegah terjadinya kejahatan atau perbuatan yang tidak dikehendaki atau perbuatan yang salah (*the prevention of crime or undesired conduct or offending conduct)*
2. untuk mengenakan penderitaan atau pembalasan yang layak kepada si pelanggar *(the diserved infliction of suffering on evildoers/retribution for perceived wrong doing)*. Herbert Packer., *The Limit Of Criminal Sanction,* dalam Muladi dan Barda Nawawi Arief, *Teori-teori dan Kebijakan Pidana,* Bandung : Almuni, 1992, hal. 6.

ketentuan hukumnya dan melakukan penegakan hukum yang konsisten dan berkesinambungan. Disamping dukungan masyarakat melalui advokasi dan pemberdayaan seluruh lapisan masyarakat, sehingga diharapkan tindak pidana mayantara ini dapat ditekan bahkan diberantas.

Dalam catatan beberapa literatur dan situs-situs yang mengetengahkan kejahatan mayantara/*cyber crime*, berpuluh jenis kejahatan yang berkaitan dengan dunia *cyber*, maka perbuatan yang termasuk dalam kategori kejahatan umum yang difasilitasi teknologi informasi antara lain penipuan kartu kredit, penipuan bursa efek, penipuan perbankan, pornografi anak, perdagangan narkoba, serta terorisme. Sedang kejahatan yang menjadikan sistem dan fasilitas teknologi informasi sebagai sasaran di antaranya adalah *denial-of-service attack, defacing, cracking* ataupun *phreaking.*

Kejahatan internet yang marak di Indonesia meliputi penipuan kartu kredit, penipuan perbankan, *defacing, cracking*, transaksi seks, judi *online* dan terorisme dengan korban selain berasal dari negara-negara luar seperti AS, Inggris, Australia, Jerman, Korea serta Singapura, juga beberapa daerah di tanah air. Larangan mengenai kejahatan mayantara, seperti telah diuraikan diatas, pada dasarnya telah diatur dalam beberapa perundang-undangan di KUHP, UU Perbankan, terorime dll. Bahkan di dalam Undang-Undang No. 36 Tahun 1999 tentang Telekomunikasi dilekatkan sanksi pidana bagi para pelaku yang melakukan perbuatan tanpa hak, tidak sah, atau memanipulasi: a. akses ke jaringan telekomunikasi; dan atau b. akses ke jasa telekomunikasi; dan atau c. akses ke jaringan telekomunikasi khusus.[153] Ancaman pidana yang dapat dijatuhkan yaitu pidana penjara paling lama 6 (enam) tahun atau denda paling banyak Rp 600.000.000,00 (enam ratus juta rupiah).[154] Lantaran besarnya dampak yang ditimbulkan dalam kejahatan mayantara, tampaknya UU ITE tidak mengenal ampun siapapun yang terlibat para pelaku, baik itu orang perseorangan maupun korporasi yang terbukti melakukan tindak pidana mayantara diancam dengan pidana penjara dan denda.

---

[153] Pasal 22 UU No 36 Tahun 1999
[154] Pasal 50 UU No 36 Tahun 1999

Adapun delik-delik yang diatur oleh Undang-Undang No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) adalah sebagai berikut :

Tindak pidana yang berkaitan dengan Komputer sebagai Alat Kejahatan:

a. Tindak Pidana Perjudian

Ketentuan mengenai perjudian diatur dalam Pasal 27 ayat (2), yang melarang "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". Bagi para pelaku tindak pidana ini dapat diancamkan pidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah). [155]

b. Tindak Pidana Pencemaran Nama Baik

Selanjutnya dalam Pasal 27 ayat (3) dinyatakan bahwa 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. Bagi para pelaku tindak pidana ini dapat diancamkan pidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

c. Tindak Pidana Pemerasan dan Pengancaman

Hal ini mengatur 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. Bagi para pelaku tindak pidana ini dapat diancamkan pidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

---

[155] Pasal 45 ayat 1 UU No 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

d. Tindak Pidana tentang Berita Bohong dan Penyebaran Kebencian

Pasal 28 UU No 11 Tahun 2008 menyebutkan bahwa berita bohong dan penyebaran informasi yang menimbulkan rasa kebencian diancam dengan pidana. Secara lebih lengkap sebagai berikut :

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). Terhadap perbuatan ini, bagi para pelaku tindak pidana dapat diancamkan pidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

e. Tindak Pidana tentang Ancaman Kekerasan

Pasal 29 Undang-Undang No 11 Tahun 2008 menyatakan : 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. Terhadap perbuatan ini diancam dengan dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp2.000.000.000,00 (dua miliar rupiah).[156]

f. Tindak Pidana tentang Akses Tidak Sah (*illegal access*)

Akses tidak sah merupakan perbuatan yang dilakukan dengan sengaja dan tanpa hak melakukan akses secara tidak sah terhadap seluruh atau sebagian sistem komputer, dengan maksud untuk mendapatkan data komputer atau maksud-maksud lainnya demi memperoleh manfaat secara melawan hukum, biasanya, berkaitan erat

---

[156] Pasal 45 ayat 3 UU No 11 Tahun 2008

dengan suatu sistem komputer yang terhubung dengan sistem komputer lain. Terhadap rumusan ini, UU No 11 Tahun 2008 tentang ITE, telah mengatur perbuatan ini sebagai sebuah tindak pidana, hal ini dapat kita lihat di dalam ketentuan Pasal 30 yang menyatakan bahwa:

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.

Terhadap pebuatan diatas, bagi para pelaku pelanggar pasal 30 ayat (1) diancam dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 600.000.000,00 (enam ratus juta rupiah). Sementara untuk pelanggar pasal 30 ayat (2) diancamkan pidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp 700.000.000,00 (tujuh ratus juta rupiah). Dan untuk pelanggar pasal 30 ayat 3, diancam dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp 800.000.000,00 (delapan ratus juta rupiah).

g. **Tindak Pidana tentang *Illegal Interception in The Computers, Systems and Computer Networks Operation***

Pasal 31 Undang-Undang No. 11 Tahun 2008 mengatur tentang intersepsi secara tidak sah terhadap komputer, sistem, dan jaringan operasional komputer, yang dirumuskan sebagai berikut :

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 atas 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. Terhadap perbuatan ini diancamkan pidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp 800.000.000,00 (delapan ratus juta rupiah).

Selanjutnya dalam pasal Pasal 32 Undang-Undang No. 11 Tahun 2008 diatur juga tentang pencurian data (*data theft*), yaitu kegiatan memperoleh data komputer secara tidak sah, baik untuk digunakan sendiri ataupun untuk diberikan kepada orang lain. Secara lengkap Pasal 32 menentukan sebagai berikut :

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.

Terhadap pelanggaran Pasal 32 ayat (1) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp 2.000.000.000,00 (dua miliar rupiah). Sedangkan terhadap pelanggaran sebagaimana dimaksud dalam Pasal 32 ayat (2) dipidana dengan pidana penjara paling lama 9 (sembilan) tahun dan/atau denda paling banyak Rp 3.000.000.000,00 (tiga miliar rupiah). Selanjutnya, bagi 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).

h. Tindak Pidana tentang *System Interference* (mengganggu sistem komputer)

Pasal 33 UU No 11 Tahun 2008 menyatakan bahwa 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 diancam pidana dengan dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp10.000.000.000,00 (sepuluh miliar rupiah).

i. Tindak Pidana terhadap Kegiatan Menyalahgunakan Peralatan Komputer (*misuse of devices*)

Ketentuan hal tersebut diatur dalam Pasal 34 ayat (1) yang menentukan sebagai berikut :

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.

Terhadap pelanggaran diatas, Pasal 50 Undang-Undang No 11 Tahun 2008 mengancamkan pidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp10.000.000.000,00 (sepuluh miliar rupiah).

j. Tindak Pidana tentang Mengganggu Data Komputer (*data interference*)

Pasal 35 Undang-Undang No 11 Tahun 2008 tentang ITE melarang 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. Sanksi pidana bagi para pelanggar pasal ini dicantumkan dalam pasal 51 ayat (1) dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp12.000.000.000,00 (dua belas miliar rupiah).

Sebenarnya sebelum dikeluarkannya Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Teknologi Elektronik, hukum pidana telah difungsionalisasikan dalam kasus-kasus kejahatan mayantara *(cyber crime)*. Namun sayangnya kesemua peraturan tersebut dirasakan masih terlalu sempit dan parsial. Akibatnya hal ini belum mampu menjerat pelaku kejahatan mayantara secara maksimal.

Memperhatikan lingkup luas dan karakteristik tindak pidana mayantara, maka pemberantasan tindak pidana ini tidak bisa dilakukan dengan tindakan biasa-biasa saja. Namun sayangnya sampai saat ini, hasil dan reaksi atas penanganan kejahatan ini masih belum memadai. Pemberantasan tindak pidana mayantara masih terkeasan dilakukan dengan biasa-biasa saja, seakan-akan kejahatan ini bisa ditangani seperti menangani kejahatan biasa (*ordiniary crime)* yang individual, tidak terorganisir, bersakala lokal dan berdampak kecil bagi kehidupan masyarakat dan negara. Meskipun masih menjadi tanda tanya apakah dengan keluarnya undang-undang baru tersebut dapat memberikan perlindungan

bagi masyarakat akan bentuk kejahatan ini,mengingat undang-undang ini belum lama diberlakukan. Tetapi kita harus tetap optimis, karena harus disadari bahwa proses bekerjanya hukum itu sendiri tidak hanya mengandalkan aturan atau undang-undang yang baik, tetapi juga dipengaruhi oleh tiga komponen penting yang saling terkait satu sama lain sebagaimana digambarkan dalam *Model of Law and Development* oleh *Robert B. Seidman.*[157]

Dinyatakan bahwa komponen bekerjanya hukum meliputi tiga unsur yang saling terkait dan saling mempengaruhi, yaitu proses pembuatan hukum (*law making process)* dalam hal ini keberpihakan hukum juga ditentukan siapa yang membuatnya, proses penegakan hukum (*law implementing processes)* dalam hal ini para aparat penegak hukum/pelaksana hukum akan sangat menentukan terlaksananya tidaknya hukum tersebut, dan pemakai hukum (*role occupant)* tidak lain adalah masyarakat sendiri, sejauhmana kesadaran hukum masyarakat juga sangat menentukan dalam tegaknya hukum tersebut.[158]

Dalam menganalisis norma hukum tentang dan/atau yang berkaitan dengan kejahatan mayantara yang telah secara legal disahkan dan berlaku di Indonesia sebagai hukum positif dapat mengacu kepada dua pendekatan

Pendekatan Pertama, mengacu kepada pandangan sosiologi hukum. Membandingkan tuntutan perlindungan hukum kejahatan mayantara dengan norma hukum yang sudah ada (*existing laws*) Yaheznel Dror mengatakan, kesenjangan antara realitas perilaku sosial masyarakat, dengan norma hukum yang sah berlaku merupakan ruang yang bisa menimbulkan ketegangan (*tension*).[159] Adanya kesenjangan ini membuka kemungkinan penyesuaian dengan cara menemukan hukum atau membuat hukum yang baru. Penyesuaian hukum ini juga dapat dilakukan hakim di pengadilan atas suatu peristiwa kongkrit (*in concreto).*

Dari pendekatan pertama ini, dikaitkan dengan penegakan hukum kejahatan mayantara, permasalahan penegakan hukum yang timbul adalah :

---

[157] Robert B. Saidman, *The State Law and Development, St.* Martin's Press, New York : 1978, hal. 75-77.
[158] *Ibid.*, hal. 75-77.
[159] Yehezkel Dror, *Law In Social Change,* dalam *Sociology of Law.* Pinguin Books, First Published, 1969, hal. 90.

1. Perumusan tindak pidana di dalam KUHP kebanyakan masih bersifat konvensional dan belum secara langsung dikaitkan dengan perkembangan *cyber crime*. Di samping itu, mengandung berbagai kelemahan dan keterbatasan dalam menghadapi perkembangan teknologi informasi dan *high tech crime*. Hal ini akan semakin pelik jika dikaitkan dengan adanya asas-asas pembatas dalam hukum pidana sehubungan dengan asas legalitas, dimana salah satunya adalah *lex certa*. Akibatnya sulit untuk menerapkan begitu saja pasal-pasal di dalam KUHP terhadap kejahatan-kejahatan berdimensi *cyber*. Hal ini dapat dimaklumi karena *cyber crime* berada dalam lingkungan elektronik dan dunia maya yang sulit diidentifikasikan secara pasti, sedangkan asas konvensional bertolak dari perbuatan real dan kepastian hukum. Selanjutnya, *cyber crime* berkaitan erat dengan perkembangan teknologi canggih yang sangat cepat berubah sedangkan asas legalitas konvensional bertolak dari sumber hukum formal yang statis.
2. Belum memadainya kualitas aparat penegak hukum, khususnya hakim, dalam menangani kasus-kasus *cyber crime*. Sebagaimana diketahui, salah satu permasalah mendasar dalam penegakan hukum kejahatan mayantara adalah minimnya pengetahuan hakim akan jenis kejahatan ini. Tidak mengherankan apabila dalam banyak kasus *cyber crime*, penggalian fakta persidangan masih terkesan perkara *cyber crime* merupakan kejahatan biasa. Lemahnya penekanan poin bagi *cyberlaw* ini dikarenakan pihak jaksa penuntut, pengacara, bahkan hakim tidak ada keinginan untuk membedah kasus *cyber crime* dari perspektif *cyberlaw* itu sendiri.[160] Chasiany Tandjung, ketua majelis hakim yang memeriksa

---

[160] Dalam kasus Mustika Ratu. Com, yang merupakan perkara *cybercrime* pertama dan diharapkan mampu menjadi *landmak* bagi kasus-kasus yang terkait dengan *cyberlaw*, Pakar Hukum Atip Latifulhayat berkomentar keras, karena dalam persidangan tersebut sama sekali tidak menggali persoalan *cyberlaw*. Atip berpendapat bahwa kasus mustika ratu.com merupakan sebuah potret pengadilan kita yang menampilkan kemalasan-kemalasan dari mereka yang seharusnya memberikan pencerahan dalam perkara *cyberlaw*. Hal serupa juga pernah diungkapkan Hinca Panjaitan kepada *hukumonline* saat menghadiri persidangan kasus ini. Ketika itu, saksi ahli Murgiana Haq, mantan President *Asean Intellectual Property Association* (A-IPA) memberikan kesaksiannya. Hinca tidak melihat adanya penerapan konsep-konsep *cyberlaw* dalam pemeriksaan

perkara *mustika-ratu.com,* mengakui bahwa dalam persidangan pihaknya tidaklah memiliki pengetahuan yang berkaitan dengan internet.

Pendekatan Kedua, mengacu kepada empat hal :

1. Apakah norma hukum tentang kejahatan mayantara yang sudah ada jika dibandingkan dengan instrumen/konvensi internasional telah memuat norma hukum baru ;
2. Apakah sudah menciptakan pelayanan standar yang semakin tinggi;
3. Apakah telah melegalisasi adanya sanksi hukum yang semakin tinggi;
4. Apakah adanya institusi yang mendukung penegakan hukum kejahatan mayantara

Apabila dikaitkan dengan peraturan internasional yang telah ada, UU ITE telah mengadopsi berbagai ketentuan internasional yang terkait dengan penanggulangan *cyber crime*. Kebijakan kriminalisasi *cyber crime* dalam UU ITE tertuang dalam BAB XI, mulai dari pasal 45 sampai dengan pasal 52 telah memuat ketentuan pidana seperti yang terdapat dalam Konvensi *Cyber crime* Dewan Eropa (*Council of Europe Cyber crime Convection),* dan mengacu pada konvensi *Cyber crime 2001* di Budapest.

Terkait dengan optimalisasi pelayanan yang berstandar tinggi, UU ITE Khususnya dalam pasal 15 ayat 1 telah mewajibkan setiap penyelenggara Sistem Elektronik harus menyelenggarakan Sistem Elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya Sistem Elektronik sebagaimana mestinya, dan harus bertanggungjawab terhadap penyelenggaraan sistem elektroniknya. Selanjutnya Pasal 16 ayat 1 telah menyaratkan pula kepada penyelenggara Sistem Elektronik wajib mengoperasikan Sistem Elektronik yang memenuhi persyaratan minimum sebagai berikut:

1. Dapat menampilkan kembali Informasi Elektronik dan/atau Dokumen Elektronik secara utuh sesuai dengan masa retensi yang ditetapkan dengan Peraturan Perundang-undangan;

---

perkara. Sumber : www. Hukumonline.com/ Kasus mustika-ratu.com, Tidak Ada Manfaatnya bagi Bahan Pembelajaran *Cyberlaw* (12/10/01)

2. Dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan, dan keteraksesan Informasi Elektronik dalam Penyelenggaraan Sistem Elektronik tersebut;
3. Dapat beroperasi sesuai dengan prosedur atau petunjuk dalam Penyelenggaraan Sistem Elektronik tersebut;
4. Dilengkapi dengan prosedur atau petunjuk yang diumumkan dengan bahasa, informasi, atau simbol yang dapat dipahami oleh pihak yang bersangkutan dengan Penyelenggaraan Sistem Elektronik tersebut; dan
5. Memiliki mekanisme yang berkelanjutan untuk menjaga kebaruan, kejelasan, dan kebertanggungjawaban prosedur atau petunjuk.

Sedangkan dari segi sanksi Pidana, ketentuan UU ITE telah secara komprehnsif melegalisasi sanksi hukum yang tinggi, hal ini dapat dilihat dari pengancaman pidana penjara (berkisar 5-10 tahun) dan denda (berkisar antara 600 Juta sampai dengan 10 milyar Rupiah) bagi para pelaku tindak pidana menurut ketentuan UU ITE.

Sementara dari sisi institusi yang mendukung penegakan hukum, UU ITE di dalam pasal 43, telah memerintahkan bahwa Selain Penyidik Pejabat Polisi Negara Republik Indonesia, Pejabat Pegawai Negeri Sipil tertentu di lingkungan Pemerintah yang lingkup tugas dan tanggung jawabnya di bidang Teknologi Informasi dan Transaksi Elektronik diberi wewenang khusus sebagai penyidik sebagaimana dimaksud dalam Undang-Undang tentang Hukum Acara Pidana untuk melakukan penyidikan tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik. Disamping itu Pihak kepolisian Indonesia telah membentuk suatu unit penanggulangan kejahatan mayantara dengan nama *Cyber crime Unit* yang berada di bawah kendali Direktrorat Reserse Kriminal Polri.

Dari pendekatan kedua ini, dikaitkan dengan penegakan hukum kejahatan mayantara, permasalahan penegakan hukum yang timbul adalah :

1. Formulasi delik dalam UU ITE hanya terfokus pada kejahatan komputer atau sistem komputer, bukan pada perumusan kejahatan yang dilakukan dengan komputer atau dengan menyalahgunakan sistem komputer atau sistem elektronik. Hal ini tentunya sangat riskan, mengingat kejahatan mayantara/ *cyber crime* bisa terjadi untuk semua tindak pidana. Lebih

lanjut, dengan perumusan yang demikian, dikaitkan dengan *Model Law Organization for Economic Co-operation and Development* (OECD), hal ini bisa menimbulkan apa yang dinamakan *under and overcriminalization.* Hal ini sesungguhnya telah dibatasi dengan asas-asas yang mencakup hal sebagai berikut :

a. Berdasarkan atas kenyataan, perlindungan rahasia pribadi lebih bersifat perdata dan administratif, maka sudah selayaknya apabila hukum pidana digunakan sebagai sarana terakhir (*ultimum remedium).*

b. Masing-masing ketentuan pidana yang dibuat harus secara tepat dan teliti menggambaran perbuatan yang dilarang dan harus dihindarkan perumusan yang bersifat samar dan umum *(precision principle)*

c. Perbuatan yang dikriminalisasikan harus digambarkan secara jelas dalam ketentuan hukum pidana *(clearness principle)*

d. Perumusan pelanggaran terhadap kerahasiaan pribadi harus dilakukan dengan menghindarkan perumusan yang bersifat global. Asas kulpabilitas menghendaki adanya pertimbangan terhadap keraguan yang disebabkan karena kepentingan yang dirusakkan, perbuatan yang dilakukan, status pelaku tindak pidana dan sebagainya *(principle of differentiation)*

e. Perbuatan yang dilakukan dengan kesengajaan. Kriminalisasi perbuatan-perbuatan culpa menysaratkan pembenaran khusus (*priciple of intents).*

f. Pemidanaan hanya dilakukan atas permintaan si korban (*principle of victim application*).[161]

2. Di dalam UU ITE telah diatur tentang pertanggungjawaban pidana korporasi. (vide pasal 52 ayat (4)). Selanjutnya dalam penjelasan pasal 52 ayat (4) tersebut dijelaskan bahwa ketentuan ini dimaksudkan untuk menghukum setiap perbuatan melawan hukum yang memenuhi unsur sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 37 yang

---

[161] Muladi dan Barda Nawai Arif, *Bunga Rampai Hukum Pidana.* Bandung, Alumni, 1992, hal. 43.

dilakukan oleh korporasi *(corporate crime)* dan/atau oleh pengurus dan/atau staf yang memiliki kapasitas untuk:

a. Mewakili korporasi;
b. Mengambil keputusan dalam korporasi;
c. Melakukan pengawasan dan pengendalian dalam korporasi;
d. Melakukan kegiatan demi keuntungan korporasi.

Dengan demikian, dapat dikatakan, bahwa sistem pertanggungjawaban pidana korporasi yang dianut rezim UU ITE tetap menyaratkan bahwa yang melakukan pertanggungjawaban adalah orang-perorangan, karena sama sekali tidak ada ketentuan tentang pertanggungjawaban pidana terhadap korporasi/badan-badan tersebut.

3. Dalam kaitannya dengan point ke 2 diatas, maka hal tersebut akan menimbulkan permasalahan tentang jenis pidana apa yang harus dikenakan terhadap korporasi tersebut, karena tidak dimuat ketentuan mengenai aturan pidana pengganti denda untuk korporasi apabila tidak membayar.
4. Di dalam UU ITE, sanksi pidana yang bisa diterapkan adalah pidana penjara dan denda. Dari persfektif pemidanaan hal ini merupakan hal yang sangat sentral, karena menyangkut masalah penentuan sanksi apa yang sebaiknya digunakan atau dikenakan kepada si pelanggar. Hal ini terkait erat dengan persoalan bahwa hukum pidana harus menghindari usaha pengendalian perbuatan dengan tidak menggunakan sanksi pidana yang efektif karena menimbulkan krisis pelampauan batas dari pidana (*the crisis of overreach of the criminal law).* [162] Dikaitkan dengan hasil penelitian yang pernah dilakukan oleh Fakultas Hukum Universitas Diponegoro, ternyata pidana penjara sebenarnya merupakan pidana yang kurang efektif. [163] Mengingat *cyber crime* merupakan kejahatan yang menggunakan atau bersaranakan teknologi komputer, maka diperlukan modifikasi jenis sanksi pidana bagi pelakunya. Jenis sanksi pidana

---

[162] Muladi, *Politik Hukum Pidana,* Jakarta: Rajagrafindo Persada ,1997, hal. 34-35.
[163] Muladi dan Barda Nawawi Arief, *Teori-teori dan Kebijakan Pidana.* Bandung: Citra Aditya bakti, 1984, *Op.,Cit,* hal. 119.

tersebut adalah tidak diperbolehkannya/dilarang si pelaku untuk menggunakan komputer dalam jangka waktu tertentu. Bagi pengguna komputer yang sampai pada tingkat ketergantungan, sanksi atau larangan untuk tidak menggunakan komputer merupakan derita yang berat.

5. Belum adanya kesamaan persepsi diantara aparat penegak hukum dalam memandang *cyber crime*. Kepala Kepolisian Daerah Kalimantan Barat, Brigadir Jenderal Polisi Raden Nata Kesuma mengakui banyak kasus kejahatan dunia maya (*cyber crime*) yang lolos dari jeratan Undang-Undang No. 11/2008 tentang Informasi dan Transaksi Elektronik, karena kurangnya pemahaman terhadap UU ITE. karena ketidakpahaman penegak hukum, tidak sedikit para pelaku kejahatan ini lolos dari pertanggungjawaban hukum.
6. Pasal 2 UU ITE yang mengatur persoalan yuridiksi masih bersifat tradisional, yakni prinsip teritorial, prinsip teritorial yang diperluas, dan nasionalitas aktif. Terhadap hal ini, penulis setuju dengan pendapat Barda Nawawi Arif yang berpendapat terhadap tindak pidana mayantara seharusnya yang diberlakukan adalah prinsip ubikuitas. Yang dimaksud dengan prinsip atau azas *ubikuitas* adalah prinsip yang mengatakan bahwa delik-delik yang dilakukan atau terjadi di sebagian wilayah teritorial negara dan sebagian di luar wilayah teritorial suatu negara (ekstra teritorial) harus dapat dibawa ke dalam yurisdiksi setiap negara yang terkait.

3.5. *Locus Delicti* kaitannya dengan Aspek Yurisdiksi Kejahatan Mayantara.

Selain persoalan yang berkaitan dengan pengaturan dalam hukum/undang-undang pidana nasional, kejahatan mayantara/*cyber crime* juga menimbulkan persoalan yang berkaitan dengan yurisdiksi khususnya nantinya berkaitan pula dengan kompetensi pengadilan suatu negara mana yang berwenang memeriksa dan mengadili perkara kejahatan mayantara. Hal ini, menjadi persoalan karena sebagaimana telah dikemukakan pada pembahasan hakikat pengertian kejahatan mayantara dan juga karakteristik kejahatan mayantara, dimana bentuk kejahatan

ini merupakan kejahatan transnsasional, yang dapat terjadi lintas negara. Kejahatan mayantara dapat dilakukan disuatu negara tertentu dan menimbulkan disuatu negara lain. Dalkam hal seperti ini tentu menimbulkan persoalan dari aspek penetuan tempat terjadinya tindak pidana *(locus delicti)*.

Memang telah disadari, walaupun Kongres PBB telah menghimbau negara-negara anggota untuk menanggulangi c*yber crime* dengan sarana penal, namun kenyataannya tidaklah mudah. Kongres PBB X/2000 sendiri mengakui, bahwa ada beberapa kesulitan untuk menanggulangi c*yber crime* dengan sarana penal, antara lain:

1. Perbuatan jahat yang dilakukan berada di lingkungan elektronik. Oleh karena itu, penanggulanggan *cyber crime* memerlukan keahlian khusus, prosedur investigasi dan kekuatan/ dasar hukum yang mungkin tidak tersedia pada aparat penegak hukum di negara yang bersangkutan;
2. *Cyber crime* melampaui batas-batas negara, sedangkan upaya penyidikan dan penegakan hukum selama ini dibatasi dalam wilayah teritorial negaranya sendiri;
3. Struktur terbuka dari jaringan komputer internasional memberi peluang kepada pengguna untuk memilih lingkungan hukum (negara) yang belum mengkriminalisasikan *cyber crime*. Terjadinya "*data havens*" (negara tempat berlindung singgahnya data, yaitu negara yang tidak memprioritaskan pencegahan penyalahgunaan jaringan komputer) dapat menghalangi usaha negara lain untuk memberantas kejahatan itu.[164]

Terhadap hal ini, persoalan Jurisdiksi (Point b dan c) merupakan persoalan yang mendapat perhatian yang mendalam. Memperhatikan ciri-ciri pokok kejahatan mayantara/*cyber crime*, terutama berkaitan dengan penggunaan alat dan jaringan global. Dari aspek alat, dapat diatur mengenai pembatasan-pembatasan penggunaan alat, misalnya, komputer dilarang digunakan untuk mengambil sebagian atau seluruhnya data milik orang lain yang tersimpan dalam suatu *web-site* yang tidak bersifat publik.[165]

Adapun mengenai jaringan global, sifat pengaturan kejahatan siber

---

[164] Ahmad M. Ramli, Op.,Cit. hal. 23.
[165] T.R. Nitibaskara, *Ketika Kejahatan Berdaulat*. Op.,Cit. hal. 46.

dengan adanya faktor ini harus didekati dengan lebih hati-hati, karena bersentuhan dengan berbagai negara. Aspek global ini, menimbulkan keadaan seakan-akan *borderless state* (tanpa batas-batas negara). Keadaan ini mengakibatkan pelaku, korban dan tempat terjadinya perbuatan pidana (*locus delicti*) berbeda-beda negara. Untuk peristiwa pidana di mana pelaku dan korban berbeda kewarganegaraan, tetapi tindak pidana melibatkan kontak fisik, maka secara yuridis penyelesaiannya mudah. KUHP kita telah mengatur peristiwa semacam itu. Yang menjadi persoalan, jika warga negara asing yang melakukan *cyber crime*, dan korbannya bukan dari negara asalnya atau dari negara tempat tinggal pelaku, melainkan berada di wilayah kedaulatan negara yang lain lagi. Di sini, mengenai *locus delicti* menjadi persoalan. Di mana sesungguhnya kejahatan itu dilangsungkan di tempat pelaku atau di negara korban, hukum pidana negara mana yang dilanggar.[166]

Bisa jadi, ketiga negara berbeda-beda dalam merumuskan tindakan pelaku. Menurut undang-undang yang berlaku di negara korban, tindakan pelaku tergolong sebagai tindak pidana yang dapat dikenai sanksi pidana yang berat. Bagi negara di mana pelaku tinggal, terdapat kemungkinan perbuatan tersebut dilihat hanya sebagai kenakalan (*delinquency*). Dan untuk negara di mana pelaku berasal, perbuatan itu sama sekali bukan merupakan perbuatan pidana, karena ketentuan hukum yang mengatur bahwa tindakan itu sebagai perbuatan yang dilarang belum ada.

Dalam hukum internasional, dikenal tiga jenis jurisdiksi, yakni jurisdiksi untuk menetapkan undang-undang *(the jurisdiction to prescribe)*, jurisdiksi untuk penegakan hukum *(the jurisdiction to enforce)*, dan jurisdiksi untuk menuntut *(the jurisdiction to adjudicate)*.[167]

Dalam kaitannya dengan penentuan hukum yang berlaku dikenal beberapa

---

[166] Seringkali ditemukan fakta, semakin banyak kasus yang terjadi merupakan kejahatan siber lintas batas negara, yang mengakibatkan hukum nasional suatu negara menjadi mandul. Singapura misalnya, telah memiliki seperangkat peraturan seperti: The Electronic Act 1998 (Undang-undang transaksi Elektronik), Computer Misuse Act (CMA) dan Electronic Communication Privacy Act (ECPA), tidak dapat menjangkau pelaku kejahatan siber yang tidak berada di dalam wilayah kedaulatannya, meskipun pribadi atau institusi negara itu tengah menjadi korbannya.

[167] H. Ahmad M. Ramli, *Cyber Law dan HAKI dalam Sistem Hukum Indonesia*, Bandung : Refika Aditama, 2004, hal . 20.

asas yang biasa digunakan, yaitu : pertama, *subjective territoriality,* yang menekankan bahwa keberlakuan hukum ditentukan berdasarkan tempat perbuatan dilakukan dan penyelesaian tindak pidananya dilakukan di negara lain. Kedua, *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. Ketiga, *nationality* yang menentukan bahwa negara mempunyai jurisdiksi untuk menentukan hukum berdasarkan kewarganegaraan pelaku. Keempat, *passive nationality* yang menekankan jurisdiksi berdasarkan kewarganegaraan korban. Kelima, *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, *dan* keenam, asas *Universality.*[168]

Apabila asas-asas tersebut dikaitkan dengan asas-asas yang ada di KUHP, sesungguhnya juga sudah terjangkau dengan berlakunya asas teritorialitas, bahwa hukum pidana Indonesia dapat diterapkan pada kejahatan yang terjadi di dalam wilayah teritorial Indonesia. Kejahatan mayantara (*cyber crime*) yang merugikan kepentingan hukum yang ada di wilayah Indonesia dapat diartikan bahwa tempat terjadinya adalah di wilayah Indonesia, hal ini sesuai dengan ajaran tempat terjadinya tindak pidana menurut akibat. Apalagi, jika pelaku dan peralatan yang digunakan untuk melakukan kejahatan berada di Indonesia, maka berlaku asas teritorialitas, Pasal 2 KUHP: Ketentuan pidana dalam perundang-undangan Indonesia diterapkan bagi setiap orang yang melakukan sesuatu tindak pidana di Indonesia.[169]

Asas *Universality* selayaknya memperoleh perhatian khusus terkait dengan penanganan hukum kasus-kasus kejahatan mayantara/*cyber crime*. Asas ini disebut juga sebagai *"universal interest jurisdiction"*. Pada mulanya asas ini menentukan bahwa setiap negara berhak untuk menangkap dan menghukum para pelaku pembajakan. Asas ini kemudian diperluas sehingga mencakup pula

---

[168] *Ibid.*

[169] Tim Penerjemah KUHP BPHN Depkeh RI, *Kitab Undang-undang Hukum Pidana KUHP*, Jakarta : Sinar Harapan, 1981, hal . 13.

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, cracking, carding, hacking and viruses,* namun perlu dipertimbangkan bahwa penggunaan asas ini hanya diberlakukan untuk kejahatan sangat serius berdasarkan perkembangan dalam hukum internasional.[170]

Sejauh hukum pidana yang berlaku saat ini yaitu KUHP, asas universalitas yang diatur di dalam Pasal 4 belum mengatur dan belum dapat menjangkau bentuk kejahatan mayantara *(cyber crime)* khususnya yang dilakukan di luar wilayah Indonesi. Oleh karena itu, untuk ruang siber dibutuhkan suatu hukum baru yang menggunakan pendekatan yang berbeda dengan hukum yang dibuat berdasarkan batas-batas wilayah. Ruang siber dapat diibaratkan sebagai suatu tempat yang hanya dibatasi oleh *screens and passwords*. Secara radikal ruang siber telah mengubah hubungan antara *legally significant (online) phenomena and physical location.*[171]

Berdasarkan karakteristik khusus yang terdapat dalam ruang siber dimana pengaturan dan penegakan hukumnya tidak dapat menggunakan cara-cara tradisional, beberapa ahli berpandangan bahwa sebaiknya kegiatan-kegiatan dalam *cyberspace* diatur oleh hukum tersendiri, dengan mengambil contoh tentang tumbuhnya *the law of merchant (lex mercatoria)* pada abad pertengahan. Asas, kebiasaan dan norma yang mengatur ruang siber ini yang tumbuh dalam praktek dan diakui secara umum disebut sebagai *Lex Informatica.*[172]

Terhadap hal tersebut, muncul beberapa teori jurisdiksi dalam ruang siber, beberapa teori tersebut adalah sebagai berikut :

1. *The Theory of the Uploader and the Downloader*[173], berdasarkan teori ini, suatu negara dapat melarang dalam wilayahnya, kegiatan *uploading* dan *downloading* yang diperkirakan dapat bertentangan dengan kepentingannya. Misalnya, suatu negara dapat melarang setiap orang untuk *uploading* kegiatan perjudian atau kegiatan perusakan lainnya

---

[170] H. Ahmad Ramli, *Loc.Cit.* hal. 20.
[171] *Ibid.*
[172] *Ibid.*, hal 21.
[173] *Ibid.*, hal. 22.

dalam wilayah negara, dan melarang setiap orang dalam wilayahnya untuk *downloading* kegiatan perjudian tersebut. Minnesota adalah salah satu negara bagian pertama yang menggunakan jurisdiksi ini.

2. Teori *The Law of the Server*. Pendekatan ini memperlakukan *server* di mana *webpages* secara fisik berlokasi, yaitu di mana mereka dicatat sebagai data elektronik. Menurut teori ini sebuah *webpages* yang berlokasi di server pada Stanford University tunduk pada hukum California. Namun teori ini akan sulit digunakan apabila *uploader* berada dalam jurisdiksi asing. Ketiga, *The Theory of International Spaces*. Ruang siber dianggap sebagai *the fourth space*. Yang menjadi analogi adalah tidak terletak pada kesamaan fisik, melainkan pada sifat internasional, yakni *sovereignless quality*.[174]

Dalam membicarakan masalah jurisdiksi di ruang maya ("mayantara" atau *"cyberspace"*), Masaki Hamano dalam tulisannya berjudul *"Comparative Study in the Approach to Jurisdiction in Cyberspace"* mengemukakan terlebih dahulu adanya jurisdiksi yang didasarkan pada prinsip-prinsip tradisional. Menurutnya ada tiga kategori jurisdiksi tradisional, yaitu "jurisdiksi legislatif" *("legislative jurisdiction"* atau *"jurisdiction to prescribe")*, "jurisdiksi judisial" *("judicial jurisdiction"* atau *"jurisdiction to adjudicate")*, dan "jurisdiksi eksekutif" *("executive jurisdiction"* atau *"jurisdiction to enforce")*.[175]

Mengacu pada pengertian ketiga jurisdiksi di atas, maka dapat dikatakan bahwa jurisdiksi tradisional berkaitan dengan batas-batas kewenangan negara di tiga bidang penegakan hukum. Pertama, kewenangan pembuatan hukum substantif (oleh karena itu disebut jurisdiksi legislatif, atau dapat juga disebut "jurisdiksi formulatif"). Kedua, kewenangan mengadili atau menerapkan hukum

---

[174] *Ibid.*

[175] Barda Nawawi Arief, *Perbandingan Hukum Pidana*, Jakarta: Rajagrafindo Persada, 2002, hal. 28.

(oleh karena itu disebut jurisdiksi judisial atau aplikatif). Ketiga, kewenangan melaksanakan/memaksakan kepatuhan hukum yang dibuatnya (oleh karena itu disebut jurisdiksi eksekutif).[176]

Ketiga bidang jurisdiksi tradisional yang mempunyai "batas-batas" tertentu itu, saat ini sering dipermasalahkan sehubungan dengan *"online activity"* di ruang cyber ("dunia tak bertuan yang tak mengenal batas"). Oleh karena itu bermunculan beberapa artikel yang berkaitan dengan masalah *"cyberjurisdiction"*. [177]

Masaki Hamano membedakan pengertian *"cyberjurisdiction"* dari sudut pandang dunia *cyber/virtual* dan dari sudut hukum. Dari sudut dunia virtual, *"cyberjurisdiction"* sering diartikan sebagai "kekuasaan sistem operator dan para pengguna *("users")* untuk menetapkan aturan dan melaksanakannya pada suatu masyarakat di ruang *cyber/virtual*". Dari sudut hukum, *"cyberjurisdiction"* atau *"jurisdiction in cyber-space"* adalah "kekuasaan fisik pemerintah dan kewenangan pengadilan terhadap pengguna internet atau terhadap aktivitas mereka di ruang cyber" *("physical government's power and court's authority over Netusers or their activity in cyber-space")*.[178]

Jadi membicarakan masalah yurisdiksi *cyber* pada hakikatnya berkaitan dengan masalah kekuasaan atau kewenangan, yaitu siapa yang berkuasa/berwenang mengatur dunia internet. Mengenai masalah ini, David R. Johnson dan David G. Post dalam artikelnya berjudul *"And How Should the Internet Be Governed?"* sebagaimana dikutip Barda Nawawi Arief, mengemukakan empat model yang bersaing, yaitu: (1) pelaksanaan kontrol dilakukan oleh badan-badan pengadilan yang saat ini ada *("the existing judicial forums")*; (2) Penguasa nasional melakukan kesepakatan internasional mengenai *"the governance of Cyberspace"*; (3) pembentukan suatu organisasi internasional baru *("A New International Organization")* yang secara khusus menangani

---

[176]Ibid.,hal.29
[177] *Ibid.*
[178] *Ibid.*

masalah-masalah di dunia Internet; dan (4) pemerintahan/ pengaturan sendiri *("self-governance")* oleh para pengguna Internet.[179]

Johnson dan Post mendukung model ke-4 *("self-governance")*.[180] Oleh karena itu keduanya berpendapat, bahwa penerapan prinsip-prinsip tradisional dari *"Due Process and personal jurisdiction"* tidak sesuai dan mengacaukan apabila diterapkan pada *cyberspace*.[181] Menurut mereka, *cyberspace* harus diperlakukan sebagai suatu ruang yang terpisah dari dunia nyata dengan menerapkan hukum yang berbeda untuk *cyberspace ("cyberspace should be treated as a separate "space" from the "real world" by applying distinct law to cyberspace")*.[182]

Pandangan Johnson dan Post (selanjutnya disingkat "J-P") itu banyak mendapat tanggapan/kritik. Lawrence Lessig menyatakan, bahwa pembahasan "J-P" lebih merupakan suatu alasan/dalih dari perspektif normatif daripada argumentasi analitik. Kalau pandangan "J-P" benar, bahwa dunia *cyber* beserta aktivitasnya harus dibedakan dari dunia riel, maka orang yang berhubungan di ruang cyber bukanlah orang yang sesungguhnya *("are not real people")*, benda/barang di ruang *cyber* bersifat *"intangible"*, dan kerugian/perlukaan yang ditimbulkannya bersifat *"imma-teriel"*. Hal demikian tentunya, menurut Lessig, merupakan dalil/hal yang menggelikan *("ridiculous proposition")* dan tidak benar menurut pandangan umum. Menurut Lessig, "orang tetap orang, baik sebelum dan setelah mereka menjauh dari layar komputer" *("People remain people before and after they step away from the computer screen")*. Selanjutnya dinyatakan, bahwa cyberspace bukannya suatu "wilayah aman di luar bumi" *("extra-terrestrial safety-zone")*; para penjahat dan pelanggar penyalahgunaan jabatan tidaklah aman dari pengadilan karena sesuatu immunitas di luar dirinya *("out-of-body immunity")*.[183]

Menurut Christopher Doran, pandangan "J-P" mengenai tidak dapat diterapkannya jurisdiksi personal terhadap para terdakwa Internet, bukanlah

---

[179] *Ibid.*, hal. 30.
[180] *Ibid.*
[181] *Ibid.*
[182] *Ibid.*
[183] *Ibid.*, hal. 31.

pandangan yang menonjol/berpengaruh. Ada pendapat pro dan kontra dalam berbagai kasus di USA mengenai berlakunya jurisdiksi personal terhadap terdakwa cyberspace.[184] Masaki Hamano juga menyatakan, bahwa ide "J-P" ini tidak terwujud dalam kenyataan. Sekalipun banyak kasus-kasus hukum yang berhubungan dengan dunia cyber, namun pengadilan-pengadilan di Amerika Serikat telah menerima pendekatan tradisional terhadap sengketa jurisdiksi cyberspace daripada menyusun seperangkat hukum baru yang lengkap mengenai cyberlaw. Adalah benar bahwa ada keterbatasan kemampuan negara untuk mengatasi problem yurisdiksi yang ditimbulkan oleh Internet. Akan tetapi, adalah juga benar bahwa cyberspace tidak sama sekali bebas dari peraturan-peraturan pemerintah.[185]

Bila dicermati, kesulitan utama negara-negara dalam menghadapi kejahatan mayantara atau *cyber crime* bukan hanya terletak pada aturan hukum saja, melainkan dalam penegakkan hukumnya *(law enforcement)* lebih mengalami kesulitan. Pelaku yang melakukan tindak pidananya dari luar wilayah kedaulatan, nyaris sulit dijangkau. Perhatian serius masyarakat internasional terhadap masalah kejahatan mayantara sangat beralasan karena dalam kenyataan keseharian ulah para *cracker* dan *hacker* dapat mengakibatkan dampak yang luas dan sangat fatal.[186]

---

[184] *Ibid.*

[185] *Ibid.*

[186] Sebagai contoh dampak bahaya dari cybercrime adalah : Virus "I Love You" dan "Love Bug" serta berbagai variasinya yang menyebar dengan cepat diketahui berasal dari Filipina. Berdasarkan prakiraan, virus "I Love You" dapat merasuki 10 juta komputer dalam jaringan dunia dan menimbulkan kerugian finansial yang besar pada jaringan komputer di Malaysia, Jerman, Belgia, Perancis, Belanda, Swedia, Hongkong, Inggris Raya, dan Amerika Serikat. Virus ini menyebabkan ATM-ATM di Belgia tak berfungsi beberapa waktu. Harian KOMPAS Senin, 06 Oktober 2003. Contoh kasus lainnya, Pada tahun 2004, kegiatan bisnis di Inggris sempat mengalami kerugian sekitar 2.4 milyar poundsterling akibat kejahatan yang dilakukan secara elektronik,. Menurut survei, dapat dilaporkan bahwa:

- 90% dari 200 perusahaan di Inggris pernah mengalami serangan penetrasi yang ilegal yang berusaha masuk ke sistem komputer perusahaan mereka.
- 89% merasa pernah dirugikan akibat data-data informasi penting mereka telah dicuri dan lolos keluar melalui jaringan internet
- 97% dari responden pernah mengalami serangan virus komputer yang telah merugikan mereka sekitar 71 poundsterling
- Sementara kerugian akibat penipuan/pemalsuan data finansial (financial fraud) telah merugikan mereka sekitar 9% yaitu sebesar 68 juta poundsterling. Diakses tgl 20 Nopember 2008 pada situs http:// anaklanang. wordpress.com/2008/08/10/kasus-kasus-cybercrime-dunia-anda-perlu-tahu-ini/

Dari uraian di atas tergambar bahwa dalam dimensi internasional masyarakat bangsa-bangsa menyetujui bahkan menghimbau agar negara-negara menggunakan sarana pidana untuk menanggulangi kejahatan mayantara (*cyber crime*). Namun demikian, uapaya non penal juga tetap dilakukan, yang sifatnya pada pencegahan dan pemberian kesadaran dan pemahaman kepada masyarakat.

Pengaturan dalam hukum nasional, juga tergambar bahwa setidak-tidaknya akan menghadapi persoalan berkaitan dengan asas universalitas untuk dapat menjangkau kejahatan mayantara (*cyber crime*). Permasalahan asas universalitas ini bagi Negara Indonesia sesungguhnya dapat diatasi, misalnya dengan memperluas rumusan Pasal 4 KUHP, dengan memasukkan rumusan bahwa bentuk kejahatan yang menggunakan sarana komputer yang menimbulkan kerugian atau melanggar kepentingan hukum negara, badan hukum atau perorangan di dalam Indonesia apabila dilakukan di luar Negara Indonesia, berlaku hukum pidana Indonesia.

Pada umumnya, tempat tindak pidana (locus delicti) adalah ditempat dimana tindak pidana itu telah dilakukan oleh petindak dan ketika itu pula tindak pidana telah sempurna (*vooltoid*) semua unsur-unsur tindak pidana terpenuhi. Namun, untuk kejahatan mayantara. Dalam teori/ asas hukum pidana, mengenai tempat terjadinya tindak pidana (*Locus Delicty*) ada empat ajaran, yaitu: [187]

1. Ajaran tindakan badaniah. Untuk menentukan tempat kejadian, pusat perhatian adalah kepada tempat dimana petindak ketika melakukan suatu tindak pidana dan unsur-unsur tindak pidana pada ketika itu sudah sempurna.
2. Ajaran tempat bekerjanya alat. Tempat kejadian adalah dimana alat yang digunakan bekerja dan telah membuat sempurna suatu tindak pidana.
3. Ajaran akibat dari tindakan. Tempat tindak pidana adalah ditempat terjadinya suatu akibat yang merupakan penyempurnaan dari tindak pidana yang telah terjadi.

---

[187]S.R. Sianturi, *Op.Cit.*, hal. 113-114.

4. Ajaran berbagai tempat tindak pidana. Menurut ajaran ini tempat tindak pidana adalah gabungan dari ketiga-tiganya atau dua diantara ajaran-ajaran tersebut.

Kejahatan mayantara/*cyber crime*, sebagaimana telah dikemukakan pada pembahasan di muka, bahwa melihat karakteristiknya, kejahatan mayantara termasuk kejahatan transnasional (*transnational crime*), karena kejahatan tersebut dapat dilakukan di suatu negara tertentu dan akibatnya terjadi di negara tertentu lainnya. Kejahatan transnasional (*transnational crime*), menurut Romli Atmasasmita,[188] adalah kejahatan yang bersifat transnasional, yaitu:

1. Kejahatan yang dilakukan di lebih dari satu negara;
2. Kejahatan dilakukan di satu negara akan tetapi persiapan, perencanaan dan direktif atau kontrol dilakukan di negara lain;
3. Kejahatan dilakukan di satu negara akan tetapi melibatkan organisasi kriminal yang melakukan kejahatan di lebih dari satu negara; atau
4. Kejahatan dilakukan di satu negara akan tetapi akibat yang sangat substansial terjadi di negara lain.

Kejahatan mayantara/*cyber crime*, memenuhi sifat kejahatan transnasional, sehingga persoalan locus delicti berkaitan dengan yurisdiksi sebagaimana diuraikan di atas menjadi permasalahan. Maka, selain secara teoritis terdapat beberapa ajaran, dimasa mendatang KUHP harus mengatur secara jelas untuk bentuk tindak pidana lintas negara (transnasional).

Dalam Konsep RUU KUHP mengenai hal tempat berlakunya akibat atau permasalahan yurisdiksi dirumuskan sbb:

Pasal 3 (Asas wilayah atau territorial) RUU KUHP:

Ketentuan pidana dalam peraturan perundang-undangan Indonesia berlaku bagi setiap orang yang melakukan:

1) tindak pidana di wilayah Negara Republik Indonesia.
2) tindak pidana dalam kapal atau pesawat udara Indonesia; atau
3) tindak pidana di bidang teknologi informasi yang akibatnya dirasakan

---

[188] Romli Atmasasmita, *Pengantar Hukum Pidana Internasional Bagian II*, Jakarta: Hecca Press, 2004, hal. 120.

atau terjadi di wilayah Indonesia dan dalam kapal atau pesawat udara Indonesia.

Pasal 4 (Asas Nasional Pasif) RUU KUHP:

Ketentuan pidana dalam peraturan perundang-undangan Indonesia berlaku bagi setiap orang di luar wilayah Negara Republik Indonesia yang melakukan tindak pidana terhadap:

1) warga negara Indonesia; atau
2) kepentingan negara Indonesia yang berhubungan dengan:
   a) keamanan negara atau proses kehidupan ketatanegaraan.
   b) martabat Presiden dan/atau Wakil Presiden dan pejabat Indonesia di luar negeri.
   c) pemalsuan dan penipuan segel, cap negara, meterai, uang/mata uang, kartu kredit, perekonomian, perdagangan, dan perbankan Indonesia;
   d) keselamatan/keamanan pelayaran dan penerbangan;
   e) keselamatan/keamanan bangunan, peralatan, dan aset nasional (negara Indonesia);
   f) keselamatan/keamanan peralatan komunikasi elektronik;
   g) tindak pidana jabatan/korupsi; dan/atau
   h) tindak pidana pencucian uang.

Pasal 10 (tempat tindak pidana)

Tempat tindak pidana adalah:

1) tempat pembuat melakukan perbuatan yang dilarang oleh peraturan perundang-undangan; atau

tempat terjadinya akibat yang dimaksud dalam peraturan perundang-undangan atau tempat yang menurut perkiraan pembuat akan terjadi akibat tersebut.[189]

Menurut penulis bahwa RUU KUHP telah memuat ketentuan mengenai tindak pidana yang berkaitan dengan informatika, pilihan yang efektif dan efisien untuk penanggulangan kejahatan mayantara adalah dengan tetap dicantumkannya

---

[189]Rancangan Undang-undang Republik Indonesia tentang Kitab Undang-undang Hukum Pidana. *Pasal 3, Pasal 4, Pasal 10.*

jenis kejahatan mayantara dalam RUU KUHP baru, akan tetapi sifatnya hanya secara umum dan pengaturan spesifik tentang kejahatan ini diatur dalam UU khusus.

Sehubungan dengan masalah pengaturan mengenai *locus delicti* dan kaitannya dengan aspek yurisdiksi yang berkaitan dengan kejahatan mayantara atau *cyber crime*, di dalam Rancangan Undang-Undang KUHP ada ketentuan mengenai perluasan asas berlakunya hukum pidana dan tempat terjadinya tindak pidana yang berorientasi pada perbuatan dan akibat, sehingga diharapkan nantinya dapat menjaring tindak pidana/kejahatan mayantara atau *cyber crime* yang dilakukan di luar wilayah Indonesia tetapi akibatnya terjadi di Indonesia.

BAB IV
PENUTUP

4.1. Kesimpulan

Teknologi dan sistem informasi dengan basis peralatan komputer selain telah mengantarkan umat manusia, masyarakat, bangsa dan negara menuju pada kemajuan baik secara ekonomis, maupun kesejahteraan, pada sisi yang lain telah menimbulkan dampak negatif. Dampak negatif dari kemajuan teknologi dan sistem informasi tidak dapat dihindari, oleh karena ada beberapa pihak yang sengaja memanfaatkan untuk tujuan dan kepentingan tertentu yang dapat merugikan pihak lain. Perkembangan internet sebagai bagian dari teknologi dan sistem informasi yang menghadirkan *cyberspace* dengan realitas virtualnya menawarkan kepada manusia berbagai harapan dan kemudahan. Akan tetapi di balik itu, timbul persoalan berupa kejahatan yang dinamakan *cyber crime* yang kemudian dikenal sebagai kejahatan mayantara. Kejahatan mayantara/*Cyber crime* merupakan tindak pidana yang berkaitan dengan jaringan telekomunikasi internet, umumnya terkait erat dengan persoalan kerahasiaan, integritas dan keberadaan data dan sistem komputer atau tindak pidana yang menggunakan komputer sebagai alat kejahatan dan juga tindak pidana yang berkaitan dengan komputer sebagai media, yakni terkait dengan isi atau muatan data atau sistem komputer.

Berdasarkan pembahasan yang telah diuraikan pada bab-bab sebelumnya, dapat diambil beberpa kesimpulan berkaitan dengan pokok permasalahan, sebagai berikut:

1. Penanggulangan kejahatan mayantara/*cyber crime* di Indonesia harus dilakukan dengan upaya penal yaitu dengan menggunakan sarana hukum dan sanksi pidana. Meskipun disadari bahwa sarana penal membawa dampak negatif, namun pencegahan terhadap kejahatan mayantara hanya akan membawa hasil apabila sanksi pidana dikedepankan (*primum remedium*), hal ini dengan mengingat dan mempertimbangkan korban atau akibat dari kejahatan mayantara dapat sangat luas dan secara

finansial dapat menimbulkan kerugian yang besar. Namun demikian, sebagai langkah pencegahan tetap diperlukan adanya upaya non-penal, yaitu memberikan kesadaran kepada masyarakat akan keberbahayaan kejahatan mayantara, sehingga masyarakat juga menyadari untuk tidak melakukan kejahatan dengan menggunakan sarana teknologi informasi. Bentuk kejahatan mayantara yang secara faktual telah menimbulkan kerugian harus dilakukan penanggulangannya dengan hukum dan sanksi pidana, sedangkan kejahatan mayantara yang bersifat potensial, dapat dilakukan dengan uapaya pencegahan secara non hukum pidana.

2. Fungsionalisasi hukum pidana, atau memfungsikan atau mengoperasionalisasikan hukum pidana dapat diartikan sebagai penegakan hukum pidana, diharapkan dapat memberikan efek penangulangan dan pencegahan baik pencegahan secara khusus (*special prevention*) kepada para pelaku agar tidak mengulangi lagi kejahatannya, maupun pencegahan secara umum (*general prevention*) kepada masyarakat agar tidak melakukan kejahatan mayantara/*cyber crime).* Terhadap kejahatan *cyber crime* ini, hukum pidana Indonesia, baik itu yang tertuang dalam KUHP (ketentuan hukum umum/*lex generalis*) maupun ketentuan hukum khusus (*lex specialis*) telah difungsionalisasikan dalam menindak para pelaku kejahatan. Namun hal tersebut belum dapat dilakukan secara maksimal karena adanya keterbatasan dalam sumber daya manusia aparat penegak hukum kita. Salah satu buktinya adalah belum terciptanya kesamaan persepsi diantara para penegak hukum terhadap penafsiran mengenai kategori beberapa perbuatan *cybercrime*. Hal ini bisa terjadi karena minimnya pengetahuan para aparat penegak hukum terhadap kejahatan *cybercrime*.
3. Meskipun Indonesia belum memiliki undang-undang khusus tentang kejahatan mayantara/*cyber crime,* namun secara prinsip, berbagai undang-undang yang sudah ada, baik di dalam KUHP maupun undang-undang khusus lainnya telah difungsikan untuk menanggulangi bentuk-bentuk kejahatan mayantara/*cyber crime.* Khusus Undang-undang ITE telah memberikan harapan baru bagi maksimalisasi penegakan hukum

terhadap para pelaku kejahatan *cyber crime*, karena secara substansial UU ITE telah mengadopsi berbagai ketentuan internasional yang terkait dengan penanggulangan *cyber crime*. Lebih lanjut, dari segi sanksi pidana, ketentuan UU ITE telah secara komprehensif melegalisasi sanksi hukum yang tinggi dibandingkan dengan ketentuan hukum pidana umum yang selama ini diterapkan terhadap para pelaku kejahatan *cyber*.

4. *Locus delicti* (tempat terjadinya tindak pidana) kaitannya dengan aspek yurisdiksi kejahatan mayantara, sampai saat ini masih dirasakan menimbulkan permasalahan, karena hukum pidana Indonesia belum dapat menjangkau kejahatan mayantara yang dilakukan di luar wilayah Indonesia meskipun kerugian atau akibatnya di dalam wilayah Indonesia. Diharapkan dimasa depan Indonesia mengatur tentang yurisdiksi kejahatan mayantara yang dapat dilakukan di luar wilayah Indonesia tetapi menimbulkan akibat/kejahatan di dalam negeri, atau sebaliknya. Ketentuan yurisdiksi ini perlu diatur di dalam ketentuan umum Buku I KUHP.

4.2. Saran

Berdasarkan pembahasan dan kesimpulan tersebut diatas, penulis mengajukan beberapa saran sebagai berikut:

1. Penanggulangan dan penegakan hukum terhadap kejahatan mayantara pertama-tama harus dilakukan dengan menggunakan sarana penal/sarana hukum pidana, mengingat korban atau akibat dari kejahatan mayantara sangat luas. Namun demikian, sarana non hukum pidana juga tetap dilakukan misalnya dengan memberikan sosialisasi dan pemahaman kepada masyarakat tentang besarnya keberbahayaan kejahatan mayantara.
2. Pada masa mendatang perlu diatur rumusan tindak pidana yang khusus mengatur mengenai bentuk-bentuk kejahatan mayantara/*cyber crime* dengan unsur-unsur tindak pidana yang lebih jelas dengan sanksi yang proporsional. Pengaturan dapat dimasukkan ke dalam KUHP sebagai salah satu bentuk kejahatan dalam satu bab tersendiri.

3. Para penegak hukum (Penyidik, Jaksa Penunut Umum, dan Hakim termasuk para Penasihat Hukum) yang menangani perkara kejahatan mayantara/*cyber crime* harus mempersamakan persepsi dalam persoalan mengenai penafsiran delik-delik dalam ruang lingkup kejahatan *cyber*, untuk mewujudkan hal tersebut, perlu dikembangkan pemahaman kepada para penegak hukum mengenai teknologi informasi agar penafsiran mengenai suatu bentuk *cybercrime* ke dalam pasal-pasal dalam KUHP atau undang-undang lain tidak membingungkan.
4. Perlu dirumuskan di dalam RUU KUHP, tentang *locus delicti* (tempat terjadinya tindak pidana) kaitannya dengan yurisdiksi yang berkaitan dengan kejahatan mayantara/*cyber crime* khususnya perlu diperluas rumusan mengenai tempat terjadinya tindak pidana, meliputi tindak pidana yang dilakukan di luar Indonesia yang mengakibatkan terjadinya tindak pidana (korban) di wilayah Indonesia. Hal ini menyangkut perluasan asas teritorialitas maupun rumusan tempat terjadinya tindak pidana (*locus delicti)*, perlu dirumuskan di dalam ketentuan umum KUHP.

DAFTAR PUSTAKA

I. Buku

Agus, Raharjo. *Cyber Crime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, Bandung: PT Citra Aditya Bakti, 2002.

Amrullah, M. Arief. *Politik Hukum Pidana Dalam Perlindungan Korban Kejahatan Ekonomi Bidang Perbankan,* Malang: Bayumedia Publishing, 2007.

Apeldoorn, L.J. van. *Pengantar ilmu Hukum*, Jakarta: Pradnya Paramita, 1981.

Arief, Barda Nawawi. *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*, Jakarta: Kencana Predana Media Group, 2007

_____. *Antisipasi Penanggulangan Cybercrime Dengan Hukum Pidana*. Jakarta: Perdana Kencana Group, 2007.

_____. *Tindak Pidana Mayantara, Perkembangan Kajian Cyber Crime di Indonesia*, Jakarta: RajaGrafindo, 2006.

_____. *Kapita Selekta Hukum Pidana,* Bandung: Citra Aditya Bakti, 2003.

_____. *Perbandingan Hukum Pidana,* Jakarta: RajaGrafindo, 2002.

_____. *Bunga Rampai Kebijakan Hukum Pidana*, Bandung : Citra Aditya Bakti, 1996.

_____. *Kebijakan Legislatif Dalam Penanggulangan Kejahatan Dengan Pidana Penjara*, Semarang: Ananta, 1994.

Casey, Eoghan. *Digital Evidence and Komputer Crime*, London : A Harcourt Science and Technology Company, 2001.

Cyber-Crime: *Issues, Data Sources, and Feasibility of Collecting Police-Reported Statistics*, Canadian Centre for Justice Statistics. Published by authority of the Minister responsible for Statistics Canada, 2002.

Dror, Yehezkel. *Law In Social Change,* dalam *Sociology of Law.* Pinguin Books, First Published, 1969.

Encyclopedia of crime and justice. volume 4, New York: Free Press, 1983.

Hamzah, Andi. *Perkembangan Hukum Pidana Khusus.* Jakarta: Melton Putra, 1991.

Kanter, E.Y dan Sianturi, S.R. *Asas-asas Hukum Pidana di Indonesia dan Penerapannya.* Jakarta : Storia Grafika : 2002.

Muladi. *Politik Hukum Pidana,* Jakarta: Rajagrafindo Persada ,1997.

Muladi dan Arief, Barda Nawawi. *Bunga Rampai Hukum Pidana*, Bandung: Alumni, 1992.

_____. *Teori-teori dan Kebijakan Pidana.* Bandung: Citra Aditya bakti, 1984.

Nitibaskara, Tubagus Rony Rahman. *Ketika Kejahatan Berdaulat* (sebuah pendekatan kriminologi, hukum dan sosiologi). Jakarta: Peradaban, 2001.

Rahardjo, Satjipto. *Membedah Hukum Progresif,* Jakarta: Penerbit Kompas, 2007.

Ramli, Ahmad M. *Cyber Law dan HAKI dalam Sistem Hukum Indonesia*, Bandung : Refika Aditama, 2004.

Reksodiputro, Mardjono. *Kemajuan Pembangunan Ekonomi dan Kejahatan*, Jakarta: PPKPH UI, 1994.

_____. *Sistem Peradilan Pidana Indonesia* (Melihat Kejahatan dan Penegakan Hukum dalam batas-batas toleransi), Jakarta: Pusat Keadilan dan Pengabdian Hukum, 1994.

Romli Atmasasmita. *Pengantar Hukum Pidana Internasional Bagian II*, Jakarta: Hecca Press, 2004.

Sahetapy, J.E. *Suatu Studi Khusus Mengenai Ancaman Pidana Mati Terhadap Pembunuhan Berencana*, Jakarta: Rajawali Press. 1982.

_____. *Kausa Kejahatan*, Surabaya: Pusat Studi Kriminologi Fakultas Hukum Unair, 1979.

Saidman, Robert B, *The State Law and Development, St.* Martin's Press, New York : 1978.

Santoso, Topo dan Zulfa, Eva Achjani. *Kriminologi*, Jakarta: Raja Grafindo Persada, 2002.

Sianturi, S.R. *Asas-asas Hukum Pidana di Indonesia dan Penerapannya,* Jakarta: Alumni Ahaem-Petehaem, 1985.

Soekanto, Soerjono. *Ringkasan Metode Penelitian Hukum Empiris.* Cet. I. Jakarta : Ind.Hill.Co, 1990.

_____, *Pengantar Penelitian Hukum*, Jakarta: Universitas Indonesia Press.

Stephenson, Peter, *Investigating Computer-Related Crime*: A Hanbook For Corporate Investigators London, New York, CRC Press: Washington D.C:, 2000.

Sudarto, *Kapita Selekta Hukum Pidana.* Bandung: Alumni, Cetakan Ke-3, 2003.

Sutherland, Edwin H. dan Donald R. Cressey. *Principles of Criminology*, Sixth Edition, New York: Lippincott Company, 1960.

Tim Penerjemah KUHP BPHN Depkeh RI. *Kitab Undang-undang Hukum Pidana KUHP*, Jakarta : Sinar Harapan, 1981.

Wignjosoebroto, Soetandyo. *Hukum dalam Masyarakat, Perkembangan dan Masalah.* Malang: Bayu Media, 2008.

_____, *Hukum Paradigma: Metode dan Dinamika Masalahnya*, Jakarta: Lembaga Studi dan Advokasi Masyarakat (ELSAM), 2002.

II. Jurnal Dan Makalah

Atmasasmita, Romli. "Pengaruh Konvensi Internasional terhadap Perkembangan Asas-Asas Hukum Pidana Nasional", Makalah dalam Seminar Tentang Asas-Asas Hukum Pidana Nasional, Semarang 26 –28 April, 2004.

Barry C, Collin. "The Future of CyberTerrorism, Proceedings of 11th Annual International Symposium on Criminal Justice Issues", The University of Illinois at Chicago, dikutip dari makalah Vladimir Golubev, *cyber-crime and legal problems of usage network the INTERNET*, 1996.

Golose, Petrus Reinhard. "Perkembangan Cyber Crime dan Upaya Penanggulangannya di Indonesia Oleh Polri", Jakarta: *Buletin Hukum Perbankan dan Kebanksentralan*, Volume 4 Nomor 2, Agustus, 2006.

Karfawi, M. "Asas Legalitas dalam Usul Rancangan KUHP (Baru) dan Masalah masalahnya", *Jurnal Arena Hukum*, Juli 1987.

Manap, Nazura Abdul. *Cyber-crimes: Problems and Solutions Under Malaysian Law*, makalah pada seminar nasional Money Laundering dan Cybercrime dalam Perspektif Penegakan Hukum di Indonesia, diselenggarakan oleh Laboratorium Hukum Pidana FH Universitas Surabaya, 24 Februari 2001.

Mohammad Nuh. "Regulasi, Sistem Keamanan Serta Kepastian Penegakan Hukum dalam ITE" Seminar Sehari Menteri Komunikasi dan Informatika, Jakarta: FH Usakti, 6 Agustus 2008.

Muladi. Prinsip-prinsip Dasar Hukum Pidana Lingkungan dalam Kaitannya dengan Undang-Undang No 23 Tahun 1997. Jurnal Hukum Pidana dan Kriminologi. Vol I. Nomor 1/1998.

Ramli, Ahmad M. "Instrumen Hukum Internasional tentang Cyber Crime dan Antisipasi Implementasinya dalam Hukum Pidana Nasional, Makalah Seminar Nasional Information Technology Security dan Cyber Crime", Jakarta: *Kementrian Komunikasi dan Informasi RI*, 9 Desember 2003.

Renata, Philip. "Type of Cyber Crime", *Suplemen BisTek Warta Ekonomi*, No. 24 edisi Juli 2000.

Unit *Cyber crime* Satuan Reserse Ekonomi Direktorat Reserse Kriminal Polda Jateng. Disampaikan pada Seminar Penegakan Hukum *Cyber crime*. Fakultas Hukum Universitas Kristen Satya Wacana Salatiga. Semarang, 2 Juni 2006.

III. Website

Budi Rahardjo. *Pernak Pernik Peraturan dan Pengaturan Cyberspace di Indonesia,* http://budi.insan.co.id, diakses tanggal 22 Januari 2008.

Sterling, Bruce. "The Hacker Crackdown, Law and Disorder on the electronic Frontier", *Massmarket Paperback*, electronic version available at http://www.lysator.liu.se/etexts/hacker, 1990.

Cyberspace. http://www.bartleby.com/59/23/cyberspace.html diakses tanggal 13 September 2008.

Cyber crime" dan "Cyber-Terrorism" Manfaatkan Perkembangan Teknologi. Harian KOMPAS Senin, 06 Oktober 2003.

Purwanto, Eddy dan Tim Sub Bag Jaringan Informasi IPTEK. JIIPP dikutip dari http:// www. litbang. depkes.go.id/tik/media/Pengantar_WWW.doc.

Gambar skema USENET, http://upload.wikimedia.org/wikipedia commons/thumb/f/f4/ Usenet_servers_and_clients.svg/ 370px-Usenet_servers_and_clients.svg.png. diakses pada tanggal 20 Nopember 2008.

Packer, Herbert L. " The Limits of Criminal Sanction", http://my--anne1.blogspot.com /2009/01/analisis-yuridis -penerapan-sistem.html, diakses tanggal 20 Nopember 2008.

http://dictionary.cambridge.org/define.asp?key=19297&dict=CALD di akses tanggal 13 September 2008.

http:// anaklanang. wordpress.com/2008/08/10/kasus-kasus-cybercrime-dunia-anda-perlu-tahu-ini/