

# KEBIJAKAN KRIMINAL PENANGGULANGAN KEJAHATAN TELEMATIKA

Dini Dewi Heniarti<sup>#</sup>, Husni Syawali<sup>#</sup>, dan Diana Wiyanti<sup>#</sup>

<sup>#</sup>Dosen Tetap Fakultas Hukum Unisba

---

## Abstract

The rush development of information technology has created the super modern and smarter hardware and software for information and communication process which may fulfill the needs of society at this fields. Furthermore, it has changed the mindset and the business activity in industrial, trade, government and other live sectors and it influence the social live and law. Actually there is also negative impact which is caused by the development of information technology such as the possibility for new crime on data security. However, there are, at least three approach models can be used to prevent or control the negative impact of this development, there are; first, traditional approach (through law enforcement), second, making new interpretation, and third, making new criminal policy.

Key words : Technology, communication, information.

---

## 1. PENDAHULUAN

### 1.1 Latar Belakang Masalah

Masyarakat berpendapat bahwa sekarang kita memasuki era informasi, sebagaimana dikatakan oleh Edmon Makarim :

*"Banyak pendapat yang menyatakan bahwa internet mempunyai kelebihan sebagai suatu jaringan global dari suatu jaringan komputer dengan berbagai fasilitas kemudahan. Hanya sedikit orang yang kritis mempertanyakan, apakah media komunikasi elektronik ini dapat mempunyai akibat hukum bagi penggunaannya? Alam baru yang dinamakan dengan cyberspace (dunia maya) sering dianggap tidak ada hukumnya, sebagai suatu ruang baru tanpa hukum. Akibatnya orang pun menjadi liar dalam menampilkan informasi".<sup>1</sup>*

Istilah *cyberspace* sebenarnya lahir dari konsep *computer* dan *communication*, konsep itu lebih dikenal dengan konvergensi telematika, yaitu keterpaduan antara teknologi telekomunikasi, media, dan informatika. Istilah senada dikemukakan oleh Suwarno,<sup>2</sup> bahwa telematika merupakan persenyawaan (konvergensi) telekomunikasi dan telematika. Penulis

dalam hal ini juga mempergunakan telematika walaupun bukan satu-satunya terminologi.

Telekomunikasi merupakan salah satu media manusia berinteraksi, dalam hal ini interaksi yang dilakukan dalam jarak jauh. Telekomunikasi memiliki pengertian sendiri karena memiliki karakteristik sendiri.<sup>3</sup>

Di era perkembangan teknologi sekarang ini, informasi menjadi hal yang sangat vital, bagaimana orang mencari informasi sesuai dengan kebutuhannya dan keakuratan informasi tersebut menjadi hal yang tidak kalah penting juga, arus komunikasi yang berkembang sangat cepat memerlukan suatu instrument hukum komunikasi yang baik, yang dapat menunjang perkembangan arus informasi.

Pesatnya kemajuan teknologi komunikasi, media, dan informatika atau disingkat dengan teknologi telematika serta meluasnya perkembangan infra struktur informasi global telah merubah pola pikir dan cara kegiatan bisnis di bidang industri, perdagangan, pemerintahan, pendidikan, dan berbagai sektor kehidupan lainnya.

Perkembangan teknologi telematika membawa dampak permasalahan baik dalam kehidupan sosial maupun hukum. Dampak permasalahan tersebut terletak pada karakteristik teknologi telematika itu

---

<sup>1</sup> Edmon Makarim, *Cyberlaw antara Wacana dan Kenyataan*, Tempo, 3 February, 2002, hlm. 3.

<sup>2</sup> Suwarso, *Makalah pada Seminar Hukum Nasional Strategi Penanggulangan Kejahatan dalam bidang Telematika* kerjasama Universitas Semarang dengan Dirjen Pos dan Telekomunikasi, 2002, hlm. 1.

---

<sup>3</sup> Agus Budi Riswandi, *Hukum dan Internet di Indonesia*, UII Pres, 2003, hlm. 3.

sendiri, yang menciptakan pola perilaku antara individu dengan masyarakat.

Perubahan perilaku tersebut baik positif maupun negatif akan menimbulkan masalah baru dalam hal pengawasan dan pengaturannya. Perlu diperhatikan kiranya bahwa kemajuan teknologi komunikasi tersebut memiliki sisi gelap baik kecanggihan dan kemampuannya dalam menyediakan berbagai macam kemudahan. Sekalipun pada akhirnya perangkat hukum akan digunakan untuk mencegah dan menindak orang yang menyalahgunakan atau melanggar aturan penggunaannya, namun akan lebih baik apabila etika atau moral dijadikan landasan untuk mengendalikan manusia dari perbuatan yang merugikan atau perbuatan yang tidak terpuji.<sup>4</sup>

Dalam dunia nyata (*real*) manusia berkomunikasi biasanya secara kasat mata (*face to face*), sedangkan seiring dengan perkembangan teknologi informasi misalnya manusia dalam melakukan aktivitas internet baik untuk keperluan bisnis, pendidikan, kesehatan, pemerintahan tidak secara *face to face* melainkan dengan jarak jauh bahkan lintas batas negara. Fenomena semacam ini menggambarkan kepada kita bahwa dunia sudah menyatu.

Dalam dunia bisnis transaksi perdagangan melalui sarana elektronik mengalami dilema. Di satu sisi model transaksi perdagangan melalui sarana elektronik menawarkan biaya rendah, efisiensi, dan praktis. Namun di sisi lain dengan beberapa nilai tambah dari model transaksi perdagangan melalui media elektronik telah menciptakan keraguan-keraguan dari pelaku kalangan bisnis.<sup>5</sup>

Permasalahan yang muncul kemudian adalah masalah keamanan dan beraktivitas dengan melalui media elektronik, bahkan aktivitas ini telah menimbulkan dimensi kejahatan baru. Volodymyr Golubev.<sup>6</sup> Menyebutnya sebagai "*The new form of anti social behavior.*"

---

<sup>4</sup> Tien Sumartini Saefullah, *Peranan Etika atau Moral dalam kegiatan Cyberspace Sebagai Salah Satu Upaya Penegakkan Hukum*, Jurnal Syiar Madani, vol. IV. No.1. 2003, hlm.1.

<sup>5</sup> Ibid. hlm. 39.

<sup>6</sup> Barda Nawawi Arief, *Perbandingan Hukum Pidana*, Raja Grafindo Persada, Jakarta, 2002, hlm. 252. selanjutnya dikatakan beberapa julukan lainnya antara lain sebagai kejahatan dunia maya (*cyber/virtual space offence*), dimensi baru ini *hi tech*, *transnational crime* dan dimensi baru dari *white collar crime*.

Kejahatan dalam bidang telematika ini merupakan sisi gelap dari kemajuan teknologi yang mempunyai dampak yang sangat luas bagi seluruh bidang kehidupan modern saat ini. Beberapa bentuk kejahatan telematika terdapat dalam bidang, antara lain:<sup>7</sup>

- a. Penggunaan kartu kredit milik orang lain.
- b. Transaksi perbankan.
- c. Pemanfaatan kode rahasia (PIN) milik orang lain untuk penarikan uang tunai dari ATM.
- d. Perikatan atau kontrak elektronik.
- e. Penggunaan domain milik orang lain yang melanggar hak atas kekayaan intelektual.
- f. Membuat, menyediakan, mengirimkan, atau menghapus data komputer yang mengakibatkan terganggunya fungsi sistem.
- g. Membuat, menyediakan, mengirimkan, atau menghapus data elektronik yang mengakibatkan kerugian ekonomi bagi orang lain.
- h. Mengakses jaringan komputer dengan maksud mencuri data (*hacker*).

Dari berbagai contoh kejahatan telematika yang dikemukakan di atas dapat disimpulkan bahwa kejahatan yang dilakukan merupakan tindak pidana yang selama ini telah di kenal yaitu pencurian, pemalsuan, kejahatan kesusaan, penggunaan hak milik orang lain tanpa izin, akan tetapi pelaksanaan tindak pidana tersebut dilakukan dengan menggunakan jaringan dan atau jasa telekomunikasi. Adapun beberapa kasus yang menonjol dan terjadi di Indonesia antara lain:

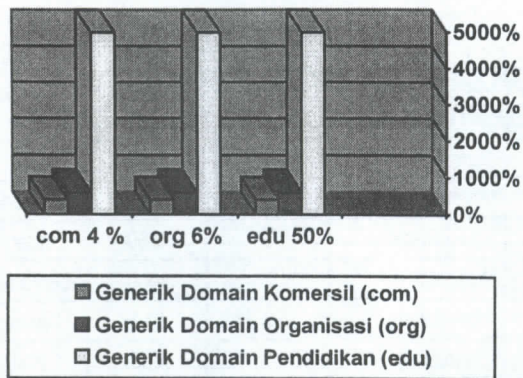
### 1. Kasus hacking murni.

Berikut ini grafik korban *Hacker* di Indonesia berdasarkan domainnya yang terdata dari tahun 1986-2000, jumlahnya: 16 kasus (data dari sumber yang cukup valid: Attrition.org). jumlah ini tidak menunjukkan situasi yang sebenarnya karena banyak yang tidak terdata atau *dark number*, karena para korban masih enggan melaporkan kepada Polri.

---

<sup>7</sup> Sutrisman, *Makalah pada Seminar Nasional, Strategi Penanggulangan Kejahatan dalam Bidang Telematika*, kerjasama Universitas Semarang dengan Dirjen Pos dan Telekomunikasi Dephub RI, 2002, hlm. 2.

### Korban Hacker di Indonesia (Tahun 1986-2000).



(Sumber: <http://www.attrition.org>)

Di bawah ini adalah data tanggal penyerangan, nama-nama situs yang menjadi korban di Indonesia serta nama *hacker* yang melakukannya. Dengan beberapa contoh website yang menjadi korban kejahatan dan akibat-akibat yang ditimbulkannya. Data ini pun belum mencerminkan kejadian yang sesungguhnya (lebih banyak), serta belum terdatakan kerugian finansial/ekonomi.

### Website di Indonesia yang menjadi Korban Hacking (Tahun 1996-2000).

Tanggal	Nama Situs Korban	Nama Hacker
28 Oktober 2000	Planetdata.co.id	Troya
27 Oktober 2000	Matahari.co.id	Antihackerlink
26 Oktober 2000	Asaba.co.id	Reboot
25 Oktober 2000	Kabelvision.co.id	-
24 Oktober 2000	Commerce.net.id	Stolen
07 Oktober 2000	Astek.co.id	Hitler Crew
14 Juli 2000	Deka.co.id	SuBZero
14 Juli 2000	Trisakti.ac.id	SuBZero
24 Mei 2000	Rad.net.id	Antihackerlink
12 September 1999	Webprimus.inptek.net.id	HPT
24 Agustus 1999	Redhat.or.id	Stroomtrooper
21 Agustus 1999	Satelindo.co.id	Mozy
01 Agustus 1998	Bit.net.id	Kao Tik Team
19 Januari 1998	Polri.mil.id	Kecoak E
18 Januari 1998	Abri.mil.id	Kecoak E
23 Desember 1996	Bppt.go.id	Phait

(Sumber: <http://www.attrion.org>)

Dari data tersebut terlihat bahwa pada tanggal 18 dan 19 Januari 1998 situs Polri dan ABRI menjadi

korban namun tidak berdaya untuk mengungkap tersangkanya, adapun *hacker* yang sering melakukannya dan berasal dari Indonesia adalah: Kecoak E, Phait, dan Antihackerlink, sedangkan yang lainnya sulit untuk diidentifikasi kemungkinan besar *hacker* tersebut dari luar negeri.

Akibat yang ditimbulkan dari ulah para *hacker* tersebut adalah sebagai berikut:

- Planetdata.co.id penampilannya tertutup habis, yang muncul cuma tulisan Hacked!!. Troya Rulezzz, Ferial yang membobol situs ini juga memberi pesan-pesan. Ferizal misalnya menulis, *I knew I love you before I met you (dedicated for datu)*. Situs aslinya sendiri hingga akhir Oktober 2000 belum pulih.
- Situs Matahari tiba-tiba berubah menjadi Khaterina, dibawahnya tertera tulisan *I really love you so much*. *Hacker* tersebut menuliskan nama Iwan dan Kaht dan Gambar Hati. Mengaku sebagai Chikebum, salah satu kelompok dari anti *hackerlink*, membobol situs matahari karena frustrasi akibat putus cinta.  
Sebelumnya situs milik perusahaan terkait dengan group Lippo, kabelvision juga diserang, tidak teridentifikasi siapa yang melakukannya. Di halaman web hanya tertera: *sorry*, <http://www.kabelvision.co.id> *stiiil under heavy attack*.
- Situs Astek.co.id. milik PT. Jamsostek pada tanggal 6 Oktober 2000 berubah tampilannya, tertera gambar Adolf Hitler lengkap dengan logo nazi dan tulisan HC, craker ini menamakan dirinya Hilter Crew, dibagian bawah situs ada teks tentang Yahudi juga link ke [www.hitler.org](http://www.hitler.org).
- Situs Universitas Trisakti ([trisakti.ac.id](http://trisakti.ac.id)) pada pertengahan Juli tahun 2000 berubah wajah, seseorang yang menamakan dirinya SubZero menyusup dan mengubah halaman tersebut. Halaman web berwarna hitam itu diisi oleh tulisan *SubZero owns you* dan ketikan besar berbunyi Hacked by Subzero. Ia juga meninggalkan email atas nama [Ch4m313.on@hotmail.com](mailto:Ch4m313.on@hotmail.com).
- Situs Rad.net, perusahaan *Internet Service Provider* (ISP) juga kebobolan, terjadi pada tanggal 24 Mei 2000, pelakunya Antihackerlink, mereka mengubah tampilan situs dengan menuliskan nama Antihackerlink besar-besar, di bawah tulisan: *exist without skin colour, without nationally, with out religions bias*. Pelakunya juga meninggalkan e-mail, [antihackerlink@antionline.Org](mailto:antihackerlink@antionline.Org).

- f. Satelindo.co.id, dibubuhi sebuah gambar dengan tulisan dibawahnya, *I caal that one ... "The Last War,"* pelakunya Mozy pada Agustus tahun lalu selain teks singkat juga meninggalkan e-mail di [mozy@usa.com](mailto:mozy@usa.com).
- g. Polri.mi.id dan Abri.mil.id, situs milik Polri di susupi oleh Kecoak Elektronik terjadi pada tanggal 19 Januari 1998, si kecoak mengubah halaman depan situs dengan tulisan Tritura 98. Isinya berupa tuntutan agar menurunkan harga, rombak kabinet, dan bebaskan tapol. Juga disertakan hujatan kepada pemerintah. Bersamaan dengan itu situs Polri di ubah tampilan tetapi tidak merusak server, situs milik TNI, [abri.mil.id](mailto:abri.mil.id), dibagian atas tertulis, *the cruel, violent, and corrupted*.
- h. Situs BPPT, di rusak dan di serang oleh mereka yang menamakan dirinya *Portuguese Hackers Againt Indonesia Tiranny* (Phait) melakukan *mass hack* ke situs Badan Pengkajian dan Penerapan Teknologi (BPPT), pada tanggal 23 Desember 1996. Pelakunya mengatakan bahwa serangan itu bukan melawan rakyat Indonesia, melainkan pemerintah Indonesia.

## 2. Kasus bermotif ekonomi/penyalahgunaan kartu kredit.

Berikut ini adalah data para *hacker* yang bermotivasikan *ekonomi atau sengaja menipu belanja pada website e'commerce* dengan menggunakan nomor kartu kredit untuk orang lain, secara melawan hukum. Pelakunya, lazim disebut dengan *carder* karena modus ini bukan cara *hacking* yang sesungguhnya, sebagian tertangkap oleh reserse Polda Jawa Tengah dan Polda D.I. Yogyakarta.

### a. Kasus di Semarang.

Berdasarkan laporan dari *MasterCard Intemational Security & Risk Management* tanggal 13 November 2000 yang berpusat di Singapura. Dasar laporan tersebut dari keluhan perusahaan komputer *Greywolf Computer Services* yang berada di kota Weirton negara bagian West Virginia Amerika Serikat, pemiliknya Mr. Mark Bunner pada tanggal 17 November 2000, melaporkan ke *MasterCard* telah di tipu oleh orang Indonesia sebanyak 14.644,41 US\$. Dari laporan ini dapat diketahui siapa pelakunya di Indonesia, dari kota mana transaksi dilakukan:

### Tersangka Yang Paling Sering Melakukan Transaksi

No	Nama Tersangka	Jumlah Transaksi	Kerugian (US\$)	Kota
1	Beny Sum	4	3500	Salatiga
2	Aryanto Surya	2	2010	Ungaran
3	Banu Pradipto	3	1500	Ungaran
4	Adhenico.a	2	4000	Semarang
5	Kurniawan	3	840	Salatiga
6	Suriapuspa	2	600	Salatiga
7	Ferdinan Kesi	1	300	Salatiga
8	Januar Maulana	1	280	Salatiga
	Jumlah	18	13010	

(Sumber : *Mastercard Internasional Security & Risk Management*).

Penyidikan terhadap para tersangka tersebut dan modus operandi yang mereka lakukan adalah sebagai berikut; pada tanggal 15 November 2000 tersangka Adhenico A. Kurniawan (Nico), umur 20 tahun seorang mahasiswa UNIKA-Salatiga di tangkap oleh Reserse Polda Jawa Tengah, dalam laporan Polisi No:A/133/XI/2000/Serse tanggal 15 November 2000, ia dituduh melakukan tindak pidana sebagaimana dalam pasal 378 KUHP, 363 KUHP.

### b. Kasus di Yogyakarta.

Adapun rekap data dari kasus yang terjadi di Yogyakarta adalah sebagai berikut (terlampir):

1. Jumlah Kasus (tersangka dicurigai) : 127 kasus.
2. Dapat disidik tuntas : 5 kasus.
3. Belum bisa disidik : 118 kasus.

Beberapa kasus penggunaan nomor-nomor kartu kredit secara tidak syah (penipuan) melalui cara menggunakan internet yang tersangkanya dapat di tangkap, sedangkan dalam proses untuk diajukan ke persidangan oleh penyidik Polri di Yogyakarta dan Semarang atau pun yang ditangani oleh penyidik di Mabes Polri. Dengan jumlah tersangka lebih dari 10 orang, perkembangan terakhir seluruh kasus *cybercrime* yang tercatat Polri atau dilaporkan oleh korbannya adalah sebagai berikut:

## 1. Kasus hacking/cracking

### Kasus Hacking/Cracking di Indonesia (November 2001- Februari 2002).

No	Modus Operandi	Jumlah	Korban	Pelaku	Catatan
1	DDOS Attack	3	1 Korea 2 Jepang	1 Bali 1 Jakarta 1 Bandung	
2	Defacing	2	2 Jepang	1 Jakarta 1 Bandung	
3	Cracking	1	1 Jakarta	1 Bandung	
4	Phreaking	0	0	0	0
5	Lain-lain	1	1 Jakarta	1 Bandung	Nimda Attack
	Jumlah Total	7	7	7	

## 2. Kasus kejahatan umum dengan internet sebagai media.

### Kasus Kejahatan Umum yang menggunakan Internet di Indonesia. (November 2001 – February 2002).

No	Modus Operandi	Total	Korban	Tersangka	Catatan
1	Penipuan Kartu Kredit	10	3 Singapura 3 USA 3 Australia 1 Inggris	1 Bali 1 Jakarta 1 Batam 2 Bandung 3 Semarang	
2	Valis Hit & Run	1	1 Australia	1 Jakarta 1 Manila	
3	Penipuan Internet Banking	2	1 Semarang 1 Jakarta	1 Jakarta	
4	Pornografi Anak	1	1 Jakarta	1 Jakarta 1 USA	
5	Terorisme	1	1 USA	1 Bandung	E-mail
6	Peyelundupan Senpi	0	0	0	0
7	Narkoba	1	1 Jakarta	1 Bandung	Narcotics
	Jumlah	15	15	15	

Kejahatan dalam bidang telematika ini mendapat perhatian dalam seminar RUU PTI. Dalam *International Information Industry Congress (IIIC) 2000 Millenium Congress*, yang diselenggarakan di Quebec dan *Information Technology Association of Canada (ITAC)*, juga sangat mengkuatirkan masalah ini yang menyatakan bahwa *Cybercrime* sebagai dampak dari *hi tech* (CC) merupakan sisi paling buruk dari masyarakat informasi "*Cybercrime is part of the seamy side of the information society*".<sup>8</sup>

Kejahatan dimensi baru yang ditimbulkan akibat perkembangan teknologi telematika seyogyanya mendapat perhatian bersama untuk menanggulangnya. Dalam menghadapi kejahatan telematika sebagian berpendapat bahwa penerapan sistem hukum tradisional untuk mengatur aktivitas-aktivitas di dunia *online* ini sangat mendesak untuk dilakukan, tanpa harus menunggu akhir perdebatan akademis mengenai sistem hukum yang paling pas, pertimbangan pragmatis yang didasarkan atas meluasnya akibat yang ditimbulkan telah memaksa negara manapun untuk segera membentuk aturan hukum mengenai hal tersebut. Untuk itu semua yang paling mungkin adalah dengan mengaplikasikan sistem hukum tradisional yang saat ini berlaku, sambil menunggu kebijakan formulasi. Model pendekatan semacam ini rupanya sudah mulai dilakukan oleh aparat penegak hukum di Indonesia. Beberapa contoh kasus yang berkembang misalnya kasus *domain name* dengan menggunakan nama mustika ratu.com. Dalam kasus ini aparat penegak hukum mencoba menggunakan hukum konvensional semacam UU Merek, UU Persaingan Usaha Tidak Sehat, dan Kitab Undang-Undang Hukum Pidana. Dalam hal alat pembuktian pun hakim saat ini mulai didorong untuk melakukan terobosan-terobosan hukum berkaitan dengan kehadiran *digital signature* dalam transaksi *e-commerce* atau *internet payment system* melalui model interpretasi hukum.

## 1.2 Identifikasi Masalah

Perkembangan pesat ilmu pengetahuan di bidang telematika membawa implikasi bentuk-bentuk kejahatan baru, dimana dalam hal ini perlu ada suatu kebijakan dalam penanggulangannya. Oleh karena itu dari latar belakang permasalahan tersebut dapat diidentifikasi masalahnya sebagai berikut:

1. Bagaimana kebijakan penanggulangan kejahatan telematika melalui sarana penal?
2. Bagaimana kebijakan penanggulangan kejahatan telematika melalui sarana non penal?

## 1.3 Tujuan Penelitian

1. Untuk mengetahui bagaimana kebijakan kriminal penanggulangan kejahatan telematika melalui sarana penal.
2. Untuk mengetahui bagaimana kebijakan kriminal penanggulangan kejahatan telematika melalui sarana non penal.

## 1.4 Manfaat Penelitian

Dari hasil penelitian ini diharapkan dapat memberikan kontribusi baik secara teoritis maupun secara praktis.

1. Secara Teoritis, penelitian ini diharapkan dapat menambah wawasan dan pengetahuan bagi peneliti, khususnya mengenai kebijakan kriminal dalam penanggulangan kejahatan telematika.
2. Secara Praktis, penelitian ini diharapkan dapat menambah wawasan bagi masyarakat luas khususnya dalam bidang Pembaharuan Hukum Pidana.

## 2. PEMBAHASAN

Perkembangan pesat ilmu pengetahuan di bidang telematika membawa implikasi bentuk-bentuk kejahatan baru, dimana dalam hal ini perlu ada suatu kebijakan dalam penanggulangannya.

Perkembangan ilmu pengetahuan teknologi telematika merupakan salah satu program dalam pembangunan nasional. Pesatnya perkembangan teknologi telematika selain mengandung aspek kemanfaatan juga bisa berdampak kriminogen.

Dalam suatu pertimbangan "*Milan Plan Action*" hasil kongres PBB ke VII dinyatakan:<sup>9</sup>

*"The past years have witnessed rapid and farreaching social and economic transormation in many countries. Development is not criminogenics per se sepecially where is fruit are equitable distributes*

<sup>8</sup> Ibid. hlm. 240.

<sup>9</sup> Barda Nawawi Arif, *Bunga Rampai Kebijakan Hukum Pidana*, Citra Aditya Bhakti, 1996, hlm. 9.

*among all the peoples, thus contributing to the improvement of overall social conditions, however, unbalanced or inadequately planned development contributes to increases of criminality."*

Dari pernyataan kongres PBB tersebut terlihat suatu penegasan bahwa, pembangunan itu pada hakikatnya tidak bersifat kriminogen apabila hasilnya didistribusikan secara pantas dan adil kepada semua rakyat serta menunjang kondisi sosial, akan tetapi pembangunan bersifat kriminogen atau dapat meningkatkan kriminalitas apabila pembangunan itu tidak direncanakan secara rasional, perencanaannya tidak seimbang, mengabaikan nilai-nilai kultural dan moral serta tidak mencakup strategi perlindungan masyarakat yang integral.

Oleh karena itu kebijakan pembangunan dalam bidang teknologi juga harus diletakkan secara integral dengan kebijakan pembangunan nasional. Dampak negatif dari perkembangan teknologi telematika adalah terjadinya kejahatan dimensi baru. Hukum (hukum pidana-penal) akan dipanggil, walaupun tidak selalu demikian, untuk mengatasi hal tersebut karena hukum hanyalah salah satu sarana kontrol sosial.

Sehubungan dengan hal ini, Sudarto pernah mengemukakan,<sup>10</sup> bahwa apabila hukum pidana hendak dilibatkan dalam usaha mengatasi segi-segi negatif dari perkembangan masyarakat/modernisasi (antara lain penanggulangan kejahatan), maka hendaknya dilihat dalam hubungan keseluruhan politik kriminal atau *social defence planning*, dan ini pun harus merupakan bagian integral dari rencana pembangunan nasional.

Hukum pidana sebagai sarana terakhir dalam penanggulangan kejahatan, artinya apabila hendak menggunakan hukum pidana maka harus betul-betul memperhatikan prinsip-prinsip pembatas agar tidak digunakan secara serampangan. Akan tetapi dalam kasus-kasus tertentu hukum pidana akan dipanggil.

Upaya penanggulangan kejahatan dengan menggunakan sanksi (hukum) pidana merupakan cara yang paling tua, setua peradaban manusia itu sendiri. Sampai saat ini pun hukum pidana masih diandalkan sebagai salah satu politik kriminal, bahkan pada akhir-akhir ini pada bagian akhir produk perundang-

undangan hampir selalu dicantumkan sub bab tentang ketentuan pidana.<sup>11</sup>

Hukum pidana merupakan salah satu sarana penal yang digunakan untuk menanggulangi kejahatan, dimana penal *policy* ini merupakan bagian yang integral dari seluruh kebijakan kriminal dan kebijakan sosial. Penggunaan sarana penal ini antara lain adalah dengan melakukan pembaharuan hukum pidana (*penal reform*). Dengan demikian pembaharuan hukum pidana merupakan bagian dari kebijakan hukum pidana (*penal policy*).

Makna dan hakikat pembaharuan hukum pidana berkaitan erat dengan latar belakang dan urgensi diadakannya pembaharuan hukum pidana yang dapat ditinjau dari aspek sosio politik, sosio filosofis, dan sosio kultural atau dari beberapa aspek kebijakan; khususnya kebijakan sosial, kebijakan kriminal, dan kebijakan penegakan hukum, artinya pembaharuan hukum pidana pada hakikatnya harus merupakan perwujudan dan perubahan terhadap berbagai aspek dan kebijakan yang melatarbelakangi. Dengan demikian pembaharuan hukum pidana pada hakekatnya mengandung makna reorientasi dan reformasi hukum pidana yang sesuai dengan nilai-nilai sentral sosio politik, sosio filosofis, dan sosio kultural dengan pendekatan yang berorientasi kepada pendekatan kebijakan (*policy oriented*) dan pendekatan yang berorientasi pada nilai (*value oriented approach*).<sup>12</sup>

Selain alasan-alasan tersebut di atas pembaharuan hukum pidana didasarkan pada alasan adaptif yaitu dengan melihat kecenderungan-kecenderungan internasional. Kebijakan kriminal (politik kriminal) merupakan suatu usaha yang rasional dari masyarakat dalam menanggulangi kejahatan.<sup>13</sup> Defenisi dari *Marc Ancel* merumuskan sebagai "*the rational organization of the control of crime by society*".<sup>14</sup>

<sup>10</sup> Sudarto, *Hukum dan Hukum Pidana*, 1981, hlm. 104.

<sup>11</sup> Barda Nawawi Arif, *Beberapa Aspek Kebijakan Penegakkan dan Pengembangan Hukum Pidana*, Citra Aditya Bhakti, 1998, hlm. 39.

<sup>12</sup> Barda Nawawi Arif, *Bunga Rampai Kebijakan Hukum Pidana*, Op.cit, hlm.31.

<sup>13</sup> Sudarto, *Ibid*, hlm.38.

<sup>14</sup> Barda Nawawi Arif, *Bunga Rampai Kebijakan Hukum Pidana*, Op. Cit, hal.2. Selanjutnya dikatakan, bertolak dari pengetahuan Marc Ancel, G. Peter Hoefnagles mengemukakan bahwa "*criminal policy is the rational organization of the social reaction to crime*".

Kebijakan atau penanggulangan kejahatan pada hakikatnya merupakan bagian yang integral dari upaya perlindungan masyarakat (*social defence*) dan upaya mencapai kesejahteraan masyarakat (*social welfare*). Oleh karena itu dapat dikatakan bahwa tujuan akhir atau tujuan utama dari politik kriminal adalah kesejahteraan masyarakat. Selanjutnya G. Peter Hoefnagels mengatakan.<sup>15</sup>

*"Criminal policy as a science of policy is part a larger policy; the law enforcement policy, the legislative and enforcement policy is in turn part of social policy".*

Dari uraian Hoefnagels terlihat bahwa upaya penanggulangan kejahatan dapat ditempuh dengan pendekatan kebijakan, dalam arti:

1. Ada keterpaduan (integralitas) antara politik kriminal dengan politik sosial.
2. Ada upaya keterpaduan antara upaya penanggulangan kejahatan dengan penal dan non penal.
3. Ada keterpaduan antara *treatment offender's* dengan *treatment of society*.
4. Ada keterkaitan antara penyembuhan *simptomatik* dengan *causative*.
5. Ada keterpaduan antara *treatment of offender's* dengan *treatment of the victim*.
6. Ada keterpaduan antara *individual/personal responsibility* dengan *structural /functional responsibility*.
7. Ada keterpaduan antara sarana formal/tradisional/*legal system* dengan *extra legal system*.

Dari uraian di atas tampak bahwa kejahatan dalam bidang telematika tidak dapat ditanggulangi hanya melalui sarana penal (hukum pidana), karena hukum pidana mempunyai batas-batas kemampuan. Mengingat berbagai keterbatasan dan kelemahan, dengan demikian penggunaan atau intervensi penal seyogyanya dilakukan dengan hati-hati, cermat, hemat, selektif, dan limitatif. Hal yang sama dikemukakan oleh Jeremi Bentham bahwa;<sup>16</sup> hukum pidana jangan digunakan apabila "*groundless, needless, unprofitable, or inefficacious*." Hal ini senada seiring ditegaskan

dalam kongres-kongres PBB bahwa upaya non penal merupakan "*The basic strategies crime prevention*."

## 2.1 Pembaharuan Hukum Pidana sebagai Bagian dari Kebijakan Kriminal.

Perkembangan telematika ditandai dengan adanya konvergensi antara aspek teknologi dan bisnis. Konvergensi ini meliputi beberapa hal, yakni: konvergensi perangkat (*equiepmnt*), konvergensi jaringan (*network*), konvergensi jasa (*services*), konvergensi pasar (*market*), dan konvergensi konsumen (*costumer*). Dengan kemunculan perangkat-perangkat (keras maupun lunak) dan jaringan-jaringan serta sektor-sektor jasa baru, terkait dengan keberadaan internet sebagai suatu jaringan telekomunikasi global (*global telecommunication network*) atau sering juga disebut jalan raya informasi (*information super highway*),<sup>17</sup> orang mulai membayangkan terjadinya konvergensi pasar dan konvergensi konsumen itu.

Selanjutnya dalam bidang perdagangan telah melahirkan model transaksi (*e-commerce*), dalam bidang pendidikan (*e-learning*), pemerintahan (*e-govemment*), bisnis (*e-bussines*), dan politik (*e-democracy*), dengan demikian telematika tidak hanya dapat dimanfaatkan untuk bertelekomunikasi tetapi dapat dipergunakan untuk perdagangan, pendidikan, politik, dan akan memberikan nilai tambah apabila dikelola dengan baik.

Dalam rangka pemberdayaan telematika, pemerintah Indonesia sangat *concern* dalam mengembangkan kerangka hukumnya, terbukti saat ini sedang disusun RUU Pemanfaatan Teknologi Informasi dan RUU *Cyberlaw*.

Karakteristik dari *super highway information* juga telah mendorong banyak negara untuk membuat aturan-aturan hukumnya. Aturan hukum ini dimaksudkan untuk memberikan tindakan preventif maupun represif atau kemungkinan pelanggaran-pelanggaran hukum melalui teknologi telematika.

Dengan demikian dapat dipahami bahwa hukum senantiasa berdialektika dengan aspek non hukum. Sejalan dengan pemahaman ini tidak menutup

<sup>15</sup> Ibid.

<sup>16</sup> Nigel Walker dalam Barda Nawawi Arif, *Beberapa Aspek Kebijakan Penegakan dan Pengembangan Hukum Pidana*, Op. Cit. hlm. 48. lihat juga Herbert L. Packer, *The limit of criminal sanction*, 1968, hlm. 366.

<sup>17</sup> Edmon Makarim, *Hukum dan Telematika (cyberlaw)*, [http://www.cyberlaw.lkht.org/asp/hukum telematika](http://www.cyberlaw.lkht.org/asp/hukum%20telematika).



kemungkinan juga hukum berdialektika dengan perkembangan teknologi.<sup>18</sup>

Kebijakan hukum pidana (*penal policy*) merupakan bagian dari upaya kebijakan kriminal. Salah satu masalah sentral dari penanggulangan kejahatan telematika melalui *penal reform* adalah masalah kriminalisasi.

Dalam hal ini apa-apa sajakah yang dapat dikategorikan/dikriminalisasikan sebagai tindak pidana dalam bidang telematika. Kebijakan kriminalisasi merupakan suatu kebijakan dalam menetapkan suatu perbuatan yang semula bukan tindak pidana (tindak pidana) menjadi suatu tindak pidana (perbuatan yang dapat di pidana).<sup>19</sup>

Dalam *work shop "Computer Related Crime"* yang diselenggarakan dalam kongres PBB X tahun 2000 dinyatakan bahwa negara-negara anggota harus berusaha melakukan harmonisasi ketentuan-ketentuan yang berhubungan dengan kriminalisasi, pembuktian, dan prosedur (*States should seek harmonization, evidence, and procedure*).<sup>20</sup> Dengan demikian masalahnya bukan sekedar membuat kebijakan formulasi legislatif, akan tetapi bagaimana ada harmonisasi kebijakan penal diberbagai negara. Ini berarti kebijakan kriminalisasi tindak pidana dalam bidang telematika bukan semata-mata masalah nasional, akan tetapi terkait juga dengan kebijakan regional dan internasional.

Kebijakan kriminalisasi tindak pidana bidang telematika tidak boleh dilakukan secara serampangan agar tidak terjadi krisis kelebihan perbuatan yang dikriminalisasikan (*The crisis of criminalization*), krisis kelebihan batas kemampuan pidana (*The crisis of over each of the criminal law*), dan melebihi beban aparat penegak hukum (*over velasting*). Selain itu hal-hal yang perlu diperhatikan dalam hal kriminalisasi adalah prinsip-prinsip pembatas (*The limiting principles*),<sup>21</sup>

mengkaitkan begitu saja kejahatan telematika dengan kejahatan-kejahatan tradisional tidak begitu gampang. Untuk adanya pencurian dan penggelapan misalnya diperlukan perbuatan mengambil barang kepunyaan orang lain. Kesulitan timbul apabila si pelaku mengambil deposit uang berkaitan dengan *cash dispensers*. Demikian pula apabila menyangkut tindak pidana penipuan (*fraud*). Hal ini sulit ditetapkan apabila yang dicurangi adalah komputer. Sepanjang yang menyangkut pemalsuan, masalah yang timbul adalah apakah *electronically stored data* termasuk dokumen yang dipalsukan, padahal untuk ini biasanya diisyaratkan adanya pernyataan yang dapat dilihat dan dibaca. Oleh karena itu dalam kebijakan formulasi perlu dilakukan pendekatan-pendekatan. Pendekatan yang pertama dilakukan adalah pendekatan global (*global approach*), yang menghendaki adanya pengaturan baru yang bersifat umum. Pendekatan lain disebut juga sebagai pendekatan evolusioner (*evolutionary approach*) yang berusaha untuk mengadakan pembaharuan atau amandemen terhadap perumusan-perumusan kejahatan tradisional, dengan menambah objek dan cara-cara dilakukannya kejahatan tersebut.<sup>22</sup>

Mengenai sumber atau dasar hukum atau landasan legislasi untuk menyatakan suatu perbuatan dapat dipidana konsep RKUHP tetap mempertahankan asas legalitas formal tetapi diimbangi dengan perumusan materil yang memberi tempat kepada hukum yang hidup,<sup>23</sup> atau hukum tidak tertulis. Dalam dokumen internasional dan KUHP negara lain juga terlihat perkembangan/pengakuan ke arah asas legalitas materil, misal dalam Pasal 15 Ayat (2) ICCPR yang menyatakan:

*"No one shall be held quilty of any criminal offence on account of any act of mission wich did not constitute a the time when it was committed. Nor shaal or hevier penalty be imposed tha the one that was applicable at the time when the criminal offence wa cimmitted. If subsequent to the commision of the offence, provision is made by lawa for the imption of a lighter penalty, the offender shall benefit thereby."*

Dalam pasal tersebut diakui adanya *General principle of law recognized by the community of nations*, sebagai sumber hukum. Seiring dengan

<sup>18</sup> Agus Budi Riswandi, *Hukum dan Internet di Indonesia*, Op. Cit. hlm. 59. selanjutnya dikatakan bahwa dalam posisi yang demikian ada tiga kemungkinan yang akan timbul, yakni pertama, hukum akan dipengaruhi perkembangan teknologi, kedua hukum akan mempengaruhi perkembangan teknologi, dan ketiga hukum dan teknologi akan saling mempengaruhi (bersinergi).

<sup>19</sup> Barda Nawawi Arif, *Perbandingan Hukum Pidana*, Op. Cit. hlm. 269.

<sup>20</sup> Dokumen A/CONF 187/15, *Report of the Tenth UN Congress on The Prevention of Crime and the Treatment of Offenders*, 19 Juli 2000, hlm.27.

<sup>21</sup> Sudarto, *Hukum dan Hukum Pidana*, Op. Cit, hlm. 44.

<sup>22</sup> Muladi dan Barda Nawawi Arif, *Bunga Rampai Hukum Pidana*, Alumni, Bandung, 1992.hlm 31. selanjutnya dikatakan pendekatan ketiga tersebut kompromitis, yaitu gabungan keduanya.

<sup>23</sup> Ibid.

timbulnya hukum-hukum baru bahkan timbulnya delik-delik baru, maka ada beberapa kelompok yang responsif atas realitas ini.<sup>24</sup> *Kelompok pertama*: menolak setiap usaha untuk membuat peraturan hukum bagi aktivitas di ruang maya yang didasarkan atas sistem hukum tradisional/konvensional. Mereka beralasan bahwa yang layaknya sebagai surga demokrasi (*democratic paradise*) yang menjanjikan wahana bagi adanya lalu lintas ide secara bebas dan terbuka tidak boleh dihambat dengan regulasi/aturan yang didasarkan atas sistem hukum tradisional yang bertumpu pada batasan-batasan teritorial. *Kelompok kedua*: berpendapat bahwa penerapan sistem hukum tradisional untuk mengatur aktivitas di ruang maya mendesak untuk dilakukan. *Kelompok ketiga*: berpendapat bahwa aturan hukum yang akan mengatur aktivitas di ruang maya harus dibentuk secara evolutif dengan cara menerapkan sistem *common law* secara hati-hati. Kelompok ini berpendirian moderat dan realistis karena memang ada beberapa prinsip hukum tradisional yang masih responsif terhadap persoalan hukum yang timbul. Oleh karena itu maka dilihat dari sudut kebijakan (*penal policy*), kebijakan kriminalisasi bukan sekedar menetapkan/merumuskan atau memformulasikan perbuatan apa yang dapat di pidana (termasuk sanksi pidananya), melainkan juga mencakup masalah bagaimana kebijakan formulasi legislasi disusun dalam suatu kesatuan hukum pidana yang harmonis dan terpadu sehingga ada harmonisasi materi/subtansi dan harmonisasi kebijakan formulasi.

## 2.2 Yurisdiksi Kejahatan Telematika

Berbicara masalah yurisdiksi pidana (*criminal jurisdiction*), berlaku beberapa prinsip, yaitu:<sup>25</sup>

1. Prinsip teritorial (*territorial principle*), yaitu menunjuk kepada dimana pelanggaran itu dilakukan.
2. Prinsip nasionalistis (*nationality principle*), yaitu menunjuk kepada kepentingan kebangsaan orang yang melakukan pelanggaran/kejahatan.
3. Prinsip universal (*universality principle*), yaitu menunjuk kepada menjaga seseorang yang melakukan pelanggaran/kejahatan.
4. Prinsip personal pasif (*passive personality principle*), yaitu menunjuk kepada *nationality* atau

kebangsaan orang yang dirugikan (korban oleh kejahatan). Selanjutnya Lord Mcmillan mengemukakan pengertian yurisdiksi teritorial sebagai berikut:<sup>26</sup>

*"It is an essential attribute of the sovereignty of this realm, as of all sovereign independent states, that it should process jurisdiction over all person and things within its territorial limits and all causes civil and criminal arising within these limits."*

Dari pengertian tersebut dapat disimpulkan bahwa pertama beradanya seseorang atau benda secara fisik dalam suatu wilayah negara sudah menimbulkan yurisdiksi negara terhadap benda atau orang tersebut, sehubungan dengan hal ini Akehurst mengemukakan bahwa *territorial principle* sebagai berikut:<sup>27</sup>

*"Every state claim jurisdiction over crime's committed into its own territory, even by foreigners. Some time a criminal act may begin in one state and be complete in another: for instance, a man may shoot across a frontier and kill some one on the other side. In such circumstance both state have jurisdiction, the state where the act commenced has jurisdiction under the subjective territorial principle, and the state where the act is completed has jurisdiction under the objective territorial principle (also some time called the effect doctrine, based on the fact that the injurious effect, although not the act or mission is self, occurred on the territory of the state)."*

Dari pengertian tersebut dapat disimpulkan bahwa, yurisdiksi teritorial mengandung prinsip teritorial subjektif dengan menitikberatkan kepada dimana kejahatan tersebut diselesaikan beserta akibatnya.

Berdasarkan fakta empiris bahwa kejahatan dalam bidang telematika banyak dilakukan di wilayah *on line activity/cyber*, maka patut dikemukakan pendapat Masaki Hamano yang membedakan pengertian *cyber jurisdiction* dari sudut pandang dunia virtual dan sudut pandang hukum. Dari sudut virtual sering diartikan sebagai kekuasaan sistem operator dan para pengguna/*user* untuk menetapkan aturan dan melaksanakannya pada suatu masyarakat di ruang *cyber/virtual*. Sedangkan dari sudut hukum, *cyber*

<sup>24</sup> Agus Budi Riswandi, *Hukum dan Internet*, Op. Cit. hlm.67-68.

<sup>25</sup> Harris D.J. *Cases and Material an International Law, third edition, sweet and Maxwell, London 1983*, hlm. 210.

<sup>26</sup> Starke J.G. *Introduction to International Law, Butterwothrs, 1989*, hlm. 202.

<sup>27</sup> Peter Malanzuk, *Akehurst Modern Introduction to International Law*, Roudlege, Seven Edition, 1999, hlm. 111.

*jurisdiction* adalah kekuasaan fisik pemerintah dan kewenangan pengadilan terhadap pengguna internet atau terhadap aktivitas mereka di ruang *cyber* (*physical government's power and courts authority over net user or their activity in cyber space*).<sup>28</sup>

Jadi membicarakan masalah yurisdiksi pada hakikatnya berhadapan dengan masalah kekuasaan atau kewenangan, yaitu siapa yang berkuasa atau berwenang mengatur dunia *cyber*. Mengenai hal ini David R. Jhonson dan David G. Post dalam artikelnya berjudul "*And how Should be governed?*". Mengemukakan empat model yang bersaing, yaitu:<sup>29</sup>

1. Pelaksanaan kontrol saat ini dilakukan oleh badan-badan pengadilan yang ada saat ini (*the exiting 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 masalah-masalah di dunia internet.
4. Pemerintahan/pengaturan sendiri (*self governance*) oleh para pengguna internet.

Jhonson dan Post mendukung hal yang keempat. Keduanya berpendapat bahwa tidak dapat diterapkan dan akan mengacaukan apabila diterapkan pada dunia *cyber*. Pendapat kedua orang tersebut banyak mendapat kritikan, karena menganggap orang yang berhubungan di dunia *cyber* bukanlah orang sungguhan. Sebagai salah satu contoh bahwa kaidah-kaidah konvensional atau pendekatan tradisional adalah yang dilakukan oleh pengadilan Indonesia dalam kasus *domain name* dengan menggunakan nama *mustikaratu.com*. Dalam kasus ini para aparat penegak hukum mencoba menggunakan hukum konvensional semacam UU Merek, UU Persaingan Usaha Tidak Sehat, dan Kitab Undang-undang Hukum Pidana. Dalam hal pembuktian pun hakim sudah mulai didorong untuk melakukan terobosan hukum berkaitan dengan kehadiran *digital signature* dalam transaksi *e-commerce* atau *internet pay system* melalui model interpretasi hukum. Hal senada dikemukakan oleh

Qodry Azizy sebagai berikut:<sup>30</sup> mengingat perkembangan hukum yang statis perlu ada perubahan yang sistematis, disamping perlu adanya keberanian pemaknaan atau interpretasi hukum oleh hakim agar tidak ketinggalan dan akan memenuhi rasa keadilan.

Hal yang menyangkut masalah yurisdiksi, maka seyogyanya untuk RUU PTI apabila menambah/memperluas hal-hal yang belum ditegaskan dalam KUHP misalnya dalam KUHP berlakunya asas personal/nasional aktif dan asas universal hanya untuk delik-delik tertentu, oleh karena itu dapat diperluas juga dalam tindak pidana ini. Perluasan asas universal ini untuk melindungi jaringan komunikasi global. Jadi disini mengandung asas *ubikuitasi* (*Ubiquityomnipresence*).

Sehubungan masyarakat berkembang dengan pesat, sementara hukum sangat statis, sehingga ada perubahan yang sistematis, disamping adanya keberanian pemaknaan atau interpretasi hukum oleh hakim agar tidak ketinggalan zaman dan akan memenuhi rasa keadilan masyarakat.

Sehubungan dengan masalah tersebut maka kebijakan kriminalisasi harus terpadu dengan kebijakan penegakan hukum (*law enforcement policy*). Kebijakan penanggulangan kejahatan telematika tidak bisa hanya melalui upaya penal (*penal policy*), harus disertai upaya non penal misalnya mempengaruhi pandangan masyarakat mengenai kejahatan dan penghukuman (*influencing view of society on crime and punishment by mass media*), pencegahan tanpa kejahatan (*prevation without punishment*). Untuk pencegahan tanpa kejahatan bisa melalui penyehatan masyarakat, pengamanan dari sisi teknologi atau yang disebut juga dengan istilah *techno prevention*, dan dari sisi pemerintah harus segera merampungkan UU PTI sebagai *umbrella act*, melakukan pembaharuan terhadap hukum pidana, hukum perdata baik materil maupun formil, perlindungan konsumen dalam *e-commerce*, sedangkan dari sisi pelanggan/*user* bisa melalui peningkatan pengamanan terhadap sistem/saran/alat yang digunakan, menjaga kerahasiaan nomor kode *password* pribadi.

<sup>28</sup> Barda Nawawi Arif, *Perbandingan Hukum Pidana*, Op. Cit. hlm. 276.

<sup>29</sup> Barda Nawawi Arif, *Capita Selecta Hukum Pidana*, Op. Cit. hlm. 248.

<sup>30</sup> Qodry Azizy, *Elektisisme Hukum Nasional, kompetisi antara Hukum Islam dan Hukum Umum*, Gama Media, 2003. hlm.177.

## 2.3 Penemuan Hukum

Hukum berfungsi sebagai perlindungan kepentingan manusia. Agar kepentingan manusia terlindungi, hukum harus dilaksanakan. Pelaksanaan hukum dapat berlangsung normal, damai, tetapi dapat terjadi juga karena pelanggaran hukum. Dalam hal ini, hukum yang telah dilanggar ini harus ditegakkan. Melalui penegakan hukum inilah hukum menjadi kenyataan. Dalam memanfaatkan hukum ada tiga unsur yang harus diperhatikan yaitu : kepastian hukum (*rechtssicherheit*), kemanfaatan (*zweckmassigkeit*), dan keadilan (*gerechtigkeit*).<sup>31</sup>

Kalau kita berbicara hukum pada umumnya kita hanya melihat kepada peraturan hukum dalam arti kaedah atau peraturan perundang-undangan, terutama bagi praktisi. Padahal undang-undang itu tidak sempurna, karena tidak mungkin untuk mengatur segala kegiatan kehidupan manusia secara tuntas. Ada kalanya undang-undang itu tidak lengkap dan ada kalanya tidak jelas, akan tetapi meskipun demikian tetap harus dilaksanakan.

Oleh karena undang-undang tidak lengkap, maka hakim harus mencari hukumnya. Ia harus melakukan penemuan hukum (*rechtvinding*).

Penemuan hukum lazimnya diartikan sebagai proses pembentukan hukum oleh hakim atau petugas-petugas hukum lainnya yang diberi tugas melaksanakan hukum terhadap peristiwa-peristiwa konkrit.

Penemuan hukum adalah kegiatan terutama hakim dalam melaksanakan undang-undang bila terjadi peristiwa konkrit. Undang-undang sebagaimana kaedah pada umumnya adalah untuk melindungi kepentingan manusia. Oleh karena itu harus dilaksanakan atau ditegakkan. Untuk dapat melaksanakannya undang-undang harus diketahui orang. Agar dapat memenuhi asas "setiap orang dianggap tahu akan undang-undang", maka undang-undang harus tersebar luas dan harus jelas. Kejelasan undang-undang ini sangat penting, oleh karena itu setiap undang-undang selalu dilengkapi dengan penjelasan yang dimuat dalam Tambahan Lembaran Negara.

Ketentuan undang-undang tidak dapat diterapkan begitu saja secara langsung kepada peristiwanya. Untuk dapat menerapkannya harus diberi arti atau

dijelaskan atau ditafsirkan atau disesuaikan dengan peristiwanya. Setiap peraturan hukum bersifat abstrak dan pasif. Abstrak karena umum sifatnya dan pasif karena tidak akan menimbulkan akibat hukum kalau tidak terjadi peristiwa konkrit.<sup>32</sup>

Boleh dikatakan setiap undang-undang perlu dijelaskan, perlu ditafsirkan terlebih dahulu. Interpretasi atau penafsiran merupakan salah satu metode penemuan hukum yang bersifat memberi penjelasan yang gamblang mengenai teks undang-undang agar ruang lingkup kaedah dapat ditetapkan sehubungan dengan peristiwa tertentu. Penafsiran oleh hakim merupakan penjelasan yang harus menuju kepada pelaksanaan yang dapat diterima oleh masyarakat mengenai peraturan hukum terhadap peristiwa yang konkrit. Metode interpretasi adalah sarana atau alat untuk mengetahui makna undang-undang. Pembenerannya terletak pada kegunaannya untuk melaksanakan ketentuan yang konkrit.

Ada beberapa metode interpretasi, walaupun bukan merupakan metode yang diperintahkan kepada hakim untuk digunakan dalam penemuan hukum, tetapi merupakan penjabaran putusan-putusan hakim. Dari alasan-alasan atau pertimbangan-pertimbangan yang sering digunakan oleh hakim dalam menemukan hukumnya dapat disimpulkan adanya metode interpretasi menurut Bahasa (gramatikal), teleologis dan sosiologis, sistematis atau logis, histories, perbandingan hukum (*comparative*), dan futuristis.<sup>33</sup>

Interpretasi gramatikal merupakan cara penafsiran yang paling sederhana untuk mengetahui makna ketentuan undang-undang dengan menguraikannya menurut bahasa.

Interpretasi teleologis dan sosiologis yaitu suatu metode yang ditetapkan berdasarkan tujuan kemasyarakatan. Dalam hal ini undang-undang yang masih berlaku sudah tidak sesuai lagi diterapkan kepada peristiwa, hubungan, kebutuhan, dan kepentingan masa kini. Disini peraturan perundang-undangan disesuaikan dengan hubungan dan situasi sosial yang baru.

Penafsiran sistematis adalah menafsirkan undang-undang sebagai bagian dari keseluruhan sistem perundang-undangan, dengan demikian menafsirkannya tidak boleh menyimpang dari sistem.

<sup>31</sup> Sudikno Mertokusumo, *Bab-bab Penemuan Hukum*, Citra Aditya Bhakti, 1993, hlm. 1.

<sup>32</sup> Ibid, halaman 13.

<sup>33</sup> Ibid, hlm. 14.

Interpretasi histories adalah menafsirkan dengan jelas sejarah terjadinya, yaitu menurut sejarah undang-undang dan sejarah hukum.

Interpretasi komparatif adalah menafsirkan dengan jalan memperbandingkan misalnya dengan hukum beberapa negara, dan juga bagi hukum yang timbul dari perjanjian internasional.

Interpretasi futuristis adalah metode penemuan hukum yang bersifat antisipasi dengan berpedoman pada undang-undang yang belum mempunyai kekuatan hukum.

Di lihat dari hasil penemuan hukum dibedakan antara interpretasi restriktif dan ekstensif. Interpretasi restriktif adalah penjelasan atau penafsiran yang bersifat membatasi, sedangkan penafsiran ekstensif melampaui batas-batas yang ditetapkan oleh penafsiran gramatikal.

### 3. KESIMPULAN

Ada dua pendapat yang berbeda tentang cara pencegahan dan penanggulangan melalui sarana penal (hukum/sanksi pidana) yang disebabkan oleh kegiatan telematika.

1. Mengaplikasikan sistem hukum tradisional yang berlaku guna mencegah dan menanggulangi perkembangan kejahatan telematika yang begitu cepat. Cara yang ditempuh adalah antara lain adanya keberanian untuk melakukan penafsiran sebagai langkah antisipasi guna meminimalisir perkembangan kejahatan telematika. Dalam penerapan hukum tradisional tersebut perlu memperhatikan adanya harmonisasi antara hukum pidana material dengan hukum pidana formal, misalnya dalam masalah pembuktian harus disesuaikan dengan perkembangan teknologi.
2. Kejahatan telematika perlu diatur dalam sistem hukum yang baru sesuai dengan karakteristik teknologi telematika. Pendekatan yang digunakan adalah pendekatan global (*global approach*) yang menghendaki adanya peraturan baru yang bersifat umum terhadap kejahatan telematika dan pendekatan evolusioner (*evolutionary approach*) yang berusaha mengadakan pembaharuan (amandemen) terhadap perumusan tentang kejahatan tradisional dengan menambah objek dan cara yang dilakukan dalam kejahatan telematika.

### DAFTAR PUSTAKA

#### Buku

- Arif, Barda Nawawi. 1996. *Bunga Rampai Kebijakan Hukum Pidana*. Citra Aditya Bhakti.
- . 1998. *Beberapa Aspek Kebijakan Penegakkan dan Pengembangan Hukum Pidana*. Citra Aditya Bhakti.
- . 2002. *Perbandingan Hukum Pidana*, Jakarta : Raja Grafindo Persada.
- Azizy, Qodry. 2003. *Elektisisme Hukum Nasional, kompetisi antara Hukum Islam dan Hukum Umum*. Gama Media.
- D.J., Harris 1983. *Cases and Material an International Law. third edition*. London : sweet and Maxwel.
- J.G., Starke 1989. *Introduction to International Law. Butterwothrs*.
- Malanzuk, Peter, 1999. *Akeuhurst Modern Introduction to International Law*. Roudlege. Seven Edition.
- Mertokusumo, Sudikno. 1993. *Bab-bab Penemuan Hukum*. Citra Adiyta Bhakti.
- Muladi dan Barda Nawawi Arif, 1992. *Bunga Rampai Hukum Pidana*. Bandung : Alumni.
- Riswandi, Agus Budi. 2003. *Hukum dan Internet di Indonesia*. Yogyakarta. UII Pres.
- Saefullah, Tien Sumartini. 2003. *Peranan Etika atau Moral dalam kegiatan Cyberspace Sebagai Salah Satu Upaya Penegakkan Hukum.*, Jurnal Syiar Madani, vol. IV. No.1. 2003.
- Sudarto. 1981. *Hukum dan Hukum Pidana.*
- Sutrisman. 2002. *Makalah pada Seminar Nasional, Strategi Penanggulangan Kejahatan dalam Bidang Telematika*, kerjasama Universitas Semarang dengan Dirjen Pos dan Telekomunikasi Dephub RI.
- Suwarso. 2002. *Makalah pada Seminar Hukum Nasional Strategi Penanggulangan Kejahatan dalam bidang Telematika* kerjasama Universitas Semarang dengan Dirjen Pos dan Telekomunikasi.

#### Dokumen

- Dokumen A/CONF 187/15, *Report of the Tenth UN Congress on The Prevention of Crime and the Treatment of Offenders*, 19 Juli 2000.

#### Internet

- Edmon Makarim. *Hukum dan Telematika (cyberlaw)*, [http://www.cyberlaw.lkht.org/asp/hukum telematika](http://www.cyberlaw.lkht.org/asp/hukum%20telematika).

#### Majalah

- Edmon Makarim. *Cyberlaw antara Wacana dan Kenyataan*, Tempo, 3 February, 2002.