KAJIAN YURIDIS TERHADAP PERLINDUNGAN PEMILIK WEBSITE DALAM UPAYA PENCEGAHAN DAN PENANGGULANGAN KRIMINALISASI CYBERCRIME DI INDONESIA

Oleh: Grace Yurico Bawole[1]

ABSTRAK

Tujuan dilakukannya kajan ini adalah untuk mengetahui bagaimana kajian yuridis terhadap perlindungan website dalam upaya pencegahan dan penanggulangan kriminalisasi *cybercrime* di Indonesia. Dengan menggunakan metode penelitian kepustakaan disimpulkan bahwa perlindungan pemilik website dalam upaya pencegahan dan penanggulangan kriminalisasi *cybercrime* di Indonesia secara yuridis sudah dilindungi oleh hukum akan tetapi belum begitu tegas diatur oleh salah satu perundang-undangan yang secara khusus mengatur tentang kriminalisasi *cybercrime ini*. Hal inilah yang menjadi salah satu penyebab semakin maraknya kriminalisasi *cybercrime* yang sangat merugikan pemilik website.

Kata kunci: cybercrime

A. PENDAHULUAN

Teknologi informasi (*information technology*) memegang peranan yang penting, baik di masa kini maupun nanti. Teknologi informasi sangat diyakini akan membawa keuntungan dan kepentingan yang begitu besar untuk semua negara-negara yang ada di dunia. Setidaknya ada 2 (dua) hal yang membuat teknologi informasi dianggap begitu penting dalam memacu pertumbuhan ekonomi dunia, yaitu:

1. Teknologi informasi mendorong permintaan atas produk-produk teknologi informasi itu sendiri, seperti: komputer, modem, sarana untuk membangun jaringan internet dan sebagainya.
2. Untuk memudahkan transaksi bisnis terutama bisnis keuangan di samping bisnis-bisnis umum lainnya.

Pada kenyataannya memang sering terjadi kesenjangan antara negara kaya (maju) dan negara miskin (miskin sekali atau negara berkembang) dalam bidang teknologi informasi sangat lebar jaraknya. Kemajuan teknologi informasi sekarang dan kemungkinannya di masa yang akan datang tidak akan pernah lepas dari dorongan yang dilakukan oleh perkembangan teknologi komunikasi dan teknologi komputer, sedangkan teknologi komputer dan telekomunikasi didorong oleh teknologi mikro elektronika, material dan perangkat lunak. Kimia, fisika, biologi, dan matematika mendasari ini semua.

Perpaduan teknologi komunikasi dan komputer melahirkan internet yang menjadi tulang punggung teknologi informasi. Perkembangan internet dipicu oleh peluncuran pesawat *Sputnik* milik Uni Soviet yang ditanggapi oleh Amerika serikat dengan membuat proyek peluncuran pesawat luar angkasa dan pengembangan internet pada tahun 1960an. Pada awal perkembangannya, internet digunakan atau mengabdi kepada kepentingan kekuasaan khususnya kepentingan militer Amerika Serikat.

Perkembangan teknologi umumnya dan internet pada khususnya tidak bisa dinikmati oleh orang-orang biasa seperti sekarang ini, tetapi bermain dalam tingkat elit. Pengabdian total dunia teknologi terhadap kekuasaan negara adalah inovasi perangkat perang sehingga muncul dari setiap akumulasi kekuasaan kaum bermodal melalui negara adalah perang. Penaklukan antarnegara bukan sekedar memperluas wilayah untuk mesin industry. Kolonialisme berkembang dari rahim kapitalisme yang mengabaikan kemanusiaan.

[1] Dosen Pada Fakultas Hukum Universitas Sam Ratulangi Manado

Seusai perang dingin internet tidak lagi digunakan untuk kepentingan militer, tetapi beralih fungsi menjadi sebuah media yang mampu membawa perubahan dalam kehidupan manusia. Internet tidak lagi hanya digunakan oleh kalangan militer, pemerintah, dan ilmuwan, tetapi juga digunakan oleh pelaku bisnis, politikus, sastrawan, budayawan, musikus, bahkan para penjahat dan teroris. Internet mulai digunakan sebagai alat propaganda politik, transaksi bisnis atau perdagangan, sarana pendidikan, kesehatan, manufaktur, perancangan, pemerintahan, pornografi dan kejahatan lain.

Kehadiran internet telah membuka cakrawala baru dalam kehidupan manusia. Internet yang merupakan sebuah ruang informasi dan komunikasi yang menjanjikan menembus batas-batas antarnegara dan mempercepat penyebaran dan pertukaran ilmu dan gagasan di kalangan ilmuwan dan cendekiawan di seluruh dunia. Internet membawa kita kepada ruang atau dunia baru yang tercipta yang dinamakan *Cyberspace*.

Cyberspace merupakan tempat kita berada ketika kita mengarungi dunia informasi global interaktif yang bernama internet. Istilah ini pertama kali digunakan oleh William Gibson dalam novel fiksi ilmiahnya yang berjudul *Neuromancer*.[2] Cyberspace menampilkan realitas, tetapi bukan realitas yang nyata sebagaimana bisa kita lihat, melainkan realitas virtual (*virtual reality*), dunia maya, dunia yang tanpa batas. Inilah sebenarnya yang dimaksud dengan *borderless world*, karena memang dalam *cyberspace* tidak mengenal batas negara, hilangnya batas dimensi ruang, waktu, dan tempat, sehingga penghuni-penghuninya bisa berhubungan dengan siapa saja dan dimana saja.

Indonesia sebagai negara berkembang memang terlambat dalam mengikuti perkembangan teknologi informasi. Hal ini tidak lepas dari strategi pengembangan teknologi yang tidak tepat karena mengabaikan riset sains dan teknologi. Akibatnya transfer teknologi dari negara industry maju tidak diikuti dengan penguasaan teknologi itu sendiri yang mengantarkan Indonesia kepada negara yang tidak mempunyai basis teknologi.

Dari kacamata Bank dunia, Indonesia dipandang belum memiliki regulasi pengembangan aplikasi informatik generasi baru, terutama yang paling kritis dalam kaitannya dengan perlindungan hak cipta untuk *software*, data dan *integrated circuit*, dan *cybercrime*. Kecemasan terhadap *cybercrime* ini telah menjadi perhatian dunia, terbukti dengan dijadikannya masalah *cybercrime* sebagai salah satu topik bahasan pada Kongres PBB mengenai *The Prevention of Crime and The Treatment of Offender* ke-8 tahun 1990 di Havana, kuba, dan kongres ke-10 di Wina.

Dengan adanya perhatian dunia ini maka Indonesia sebagai salah satu negara yang mulai nampak banyak terjadi masalah *cybercrime*, maka pemerintah Indonesia tidak hanya tinggal diam tetapi terus berupaya untuk mencegah dan menanggulangi terjadinya kriminalisasi *cybercrime* ini salah satunya melalui perlindungan hukum terhadap pemilik website.

B. PERUMUSAN MASALAH

Berdasarkan latar belakang masalah ini maka yang menjadi permasalahan adalah bagaimana kajian yuridis terhadap perlindungan website dalam upaya pencegahan dan penanggulangan kriminalisasi *cybercrime* di Indonesia?

C. METODE PENELITIAN

Dalam menyusun tulisan ini penulis menggunakan metode penelitian kepustakaan (*Library Research*) yakni suatu

[2] Mahzar, Ahmadi., Spritualitas Cyberspace, *Bagaimana teknologi Komputer Mempengaruhi Kehidupan Keberagamaan Manusia*, Mizan, Bandung, 1999, hal. 9.

metode yang digunakan dengan jalan mempelajari buku literatur, perundang-undangan, dan bahan-bahan tertulis lainnya yang berhubungan dengan materi pembahasan yang penulis gunakan untuk menyusun tulisan ini.

D. TINJAUAN PUSTAKA

Web adalah sebuah penyebaran informasi melalui internet. Sebenarnya antara www (world wide web) dan web adalah sama karena kebanyakan orang menyingkat www menjadi web saja. Web merupakan hal yang tidak dapat dipisahkan dari dunia internet. Melalui web setiap pemakai internet bisa mengakses informasi-informasi di situs web yang tidak hanya berupa teks, tetapi juga dapat berupa gambar, suara, film, animasi, dll.

Web adalah suatu kumpulan-kumpulan dokumen yang sangat banyak dan tersebar di beberapa komputer server yang berada di seluruh penjuru dunia dan mempunyai hubungan menjadi satu jaringan yang disebut internet.

Berikut ini adalah definisi web menurut para ahli, yakni:

1. Suwanto Raharjo, S. Si, M. Kom
   Web merupakan salah satu layanan internet yang paling banyak digunakan, dibanding dengan layanan lainnya seperti ftp, gopher, news, atau bahkan email.
2. Wahana Komputer
   Web adalah formulir komunikasi interaktif yang digunakan pada suatu jaringan komputer.
3. A. Taufiq Hidayatullah
   Web adalah bagian paling terlihat sebagai jaringan terbesar dunia yakni internet.
4. Haertalib
   Web adalah sebuah tempat di internet yang mempunyai nama dan alamat.
5. Boone (Thomson)
   Web adalah koleksi sumber informasi seperti grafis yang saling berhubungan satu sama lain dalam internet yang lebih besar.
6. Feri Indayudha
   Web adalah suatu program yang dapat memuat film, gambar, suara, serta music yang ditampilkan dalam internet.
7. Yuhefizar
   Web adalah suatu metode untuk menampilkan informasi di internet, baik berupa teks, gambar, suara maupun video yang interaktif dan mempunyai kelebihan untuk menghubungakan (link) satu dokumen dengan dokumen lainnya (hypertext) yang dapat diakses melaui sebuah browser.

Setelah kita membahas pengertian website maka saat ini perlu juga dijelaskan mengenai *cybercrime* itu sendiri. *Cybercrime* adalah tindak kriminal yang dilakukan dengan menggunakan teknologi komputer sebagai alat kejahatan yang utama. *Cybercrime* ini merupakan kejahatan yang memanfaatkan perkembangan teknologi komputer khususnya internet.

Cybercrime juga dapat diartikan sebagai suatu perbuatan melanggar hukum yang memanfaatkan teknologi komputer yang berbasis pada kecanggihan perkembangan teknologi internet. Dalam perkembangannya kejahatan ini sering juga disebut kejahatan kerah biru atau kejahatan kerah putih.

Untuk mempermudah penanganan kejahatan ini, maka *cybercrime* ini diklasifikasikan dalam beberapa kelompok, yakni:

- *Cyberpiracy* adalah penggunaan teknologi komputer untuk mencetak ulang software atau informasi, lalu mendistribusikan informasi atau software tersebut lewat teknologi komputer.
- *Cybertrespass* adalah *penggunaan* teknologi komputer untuk meningkatkan akses pada sistem komputer suatu organisasi atau individu.

- *Cybervandalism* adalah *penggunaan* teknologi komputer untuk membuat program yang mengganggu proses transmisi elektronik dan menghancurkan data di komputer.

Cybercrime di dunia awal mula berkembang pada tahun 1988 yang pada saat itu lebih dikenal dengan istilah *Cyber Attack*. Pada waktu itu ada seorang mahasiswa yang berhasil menciptakan sebuah *worm* atau virus yang menyerang program komputer dan mematikan sekitar 10% dari seluruh jumlah komputer di dunia yang terhubung ke internet. Pada tahun 1994 seorang bocah sekolah music yang berusia 16 tahun bernama Richard Pryce, atau yang lebih dikenal sebagai "*the hacker*" alias "*Datastream Cowboy*", ditahan lantaran masuk secara illegal ke dalam ratusan sistem komputer rahasia termasuk pusat data dari Griffits Air Force, NASA, dan *Korean Atomic Research Institute* atau Badan Penelitian Atom Korea. Dalam interogasinya dengan FBI, ia mengaku belajar *hacking* dan *cracking* dari seseorang yang dikenalnya lewat internet dan menjadikannya seorang mentor yang memiliki julukan "Kuji". Hebatnya hingga saat ini sang mentor tidak pernah ia ketahui dimana tempatnya.

Perkembangan *cybercrime* di Indonesia sendiri juga sangat pesat, karena walaupun di dunia nyata negara kita dianggap sebagai negara terkebelakang namun untuk masalah kejahatan dunia mata justru sebaliknya. Sudah banyak kasus-kasus yang terjadi di Indonesia menyangkut *cybercrime* ini. Pencurian dan penggunaan account internet milik orang lain. Salah satu kesulitan dari sebuah ISP (*Internet Service Provider*) adalah adanya account pelanggan mereka yang dicuri dan digunakan secara tidak sah. Berbeda dengan pencurian yang dilakukan secara fisik, pencurian account cukup menangkap userid dan password saja. Hanya informasi yang dicuri, sementara itu orang yang kecurian tidak merasakan hilangnya sesuatu yang dicuri. Pencurian baru terasa efeknya jika informasi ini digunakan oleh yang tidak berhak. Akibat dari pencurian ini penggunaan dibebani biaya penggunaan account tersebut.

Kasus seperti di atas banyak terjadi di ISP. Namun yang pernah diangkat adalah penggunaan account curian oleh dua warnet di Bandung yang membajak situs dari pemilik website. Salah satu kegiatan yang sering dilakukan oleh *cracker* adalah mengubah halaman web yang dikenal dengan istilah *deface*. Pembajakan dapat dilakukan dengan mengeksploitasi lubang keamanan. Sekitar 4 (empat) bulan yang lalu, statistik di Indonesia menunjukkan satu (1) situs web dibajak setiap harinya. *Probing* dan *Port Scanning* merupakan salah satu langkah yang dilakukan cracker sebelum masuk ke server yang ditargetkan melalui pengintaian. Caranya dengan melakukan *port scanning* atau *probing* untuk melihat servis-servis apa saja yang tersedia di server target. Sebagai contoh, hasil scanning dapat menunjukkan bahwa server target menjalankan program web server Apache, mail server Sendmail, dan seterusnya. Analogi hal ini dengan dunia nyata adalah dengan melihat-lihat apakah pintu rumah anda terkunci, merek kunci yang digunakan, jendela mana yang terbuka, apakah pagar terkunci (menggunakan firewall atau tidak) dan seterusnya. Yang bersangkutan memang belum melakukan kegiatan pencurian atau penyerangan akan tetapi kegiatan yang dilakukan sudah mencurigakan. Berbagai program yang digunakan untuk melakukan *probing* atau *port scanning* ini dapat diperoleh secara gratis di internet. Salah satu program yang paling popular adalah *nmap* (untuk sistem yang berbasis UNIX, Linux) dan *Superscan* (untuk yang berbasis Microsoft Windows).

Selain mengidentifikasi *port*, *nmap* juga bahkan dapat mengidentifikasi jenis operating system yang digunakan. Sedemikian kompleksnya bentuk kejahatan

mayantara dan permasalahannya menunjukkan perlunya seorang professional yang secara khusus membidangi permasalahan tersebut untuk mengatasi atau setidaknya mencegah tindak kejahatan *cyber* dengan keahlian yang dimiliknya. Demikian pula dengan perangkat hukum atau bahkan hakimnya sekalipun perlu dibekali pengetahuan yang cukup mengenai kejahatan mayantara ini di samping tersedianya sarana yuridis (produk undang-undang) untuk menjerat sang pelaku.

Jenis-jenis *cybercrime* ada bermacam-macam bentuk yakni:

a. Berdasarkan jenis aktivitasnya
   - *Unauthorized Access to Computer and Service*
     Kejahatan yang dilakukan dengan memasuki atau menyusp ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. Biasanya pelaku kejahatan (*hacker*) melakukannya dengan maksud sabotase ataupun pencurian informasi penting dan rahasia. Namun begitu ada juga yang melakukan hanya karena merasa tertantang untuk mencoba keahliannya menembus suatu sistem yang memiliki tingkat proteksi tinggi. Kejahatan ini semakin marak dengan berkembangnya teknologi internet.
   - *Illegal Contents*
     Kejahatan yang dilakukan dengan memasukkan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum. Seperti pemuatan suatu berita yang tidak benar atau bohong yang akan menghancurkan martabat atau harga diri pihak lain, hal-hal yang berhubungan dengan pornografi, pemuatan informasi rahasia negara, agitasi, dan propaganda untuk menentang pemerintahan yang sah.
   - *Data Forgery*
     Kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai *scriptless document* melalui internet. Kejahatan ini biasanya ditujukan pada dokumen-dokumen *e-commerce* dengan membuat seolah-olah terjadi salah ketik yang pada akhirnya akan menguntungkan pelaku.
   - *Cyber Espionage*
     Kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (*computer network system*) pihak sasaran. Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen ataupun data-data pentingnya tersimpan dalam suatu sistem *computerized*.
   - *Cyber Sabotage and Extortion*
     Kejahatan dengan membuat gangguan perusakan atau penghancuran terhadap suatu data program komputer atau sistem jaringan komputer yang terhubung dengan internet. Biasanya kejahatan ini dilakukan dengan menyusupkan suatu *logic bomb*, virus komputer ataupun suatu program tertentu, sehingga data, program komputer atau sistem jaringan komputer tidak dapat digunakan, tidak berjalan sebagaimana mestinya atau berjalan sebagaimana yang dikehendaki oleh pelaku. Dalam beberapa kasus setelah hal tersebut terjadi maka pelaku kejahatan tersebut menawarkan diri kepada korban untuk memperbaiki data program komputer atau sistem jaringan komputer yang telah disabotase tersebut dengan bayaran tertentu.

Kejahatan ini sering disebut *cyberterrorism*.

- *Offense Against Intellectual Property*
  Kejahatan yang ditujukan terhadap Hak atas Kekayaan Intelektual yang dimiliki pihak lain di internet. Contohnya adalah peniruan pada tampilan web page suatu situs milik orang lain secara illegal, penyiaran suatu informasi di internet yang ternyata ini merupakan rahasia dagang orang lain.
- *Infrigements of Privacy*
  Kejahatan yang ditujukan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia. Kejahatan ini biasanya ditujukan terhadap keterangan pribadi seseorang yang tersimpan pada formulir data pribadi secara *computerized* yang apabila diketahui oleh orang lain maka dapat merugikan korban secara materiil maupun immaterial.
- *Cracking*
  Kejahatan dengan menggunakan teknologi computer yang dilakukan untuk merusak sistem keamanan suatu sistem komputer dan biasanya melakukan pencurian tindakan anarkis begitu merekam mendapatkan akses. Biasanya terjadi salah penafsiran antara *hacker* dan *cracker*. Hacker adalah orang yang senang memprogram dan percaya bahwa informasi adalah sesuatu hal yang sangat berharga dan ada yang bersifat dirahasiakan tetapi ada pula yang bersifat dapat dipublikasikan.
- *Carding*

Kejahatan yang menggunakan teknologi komputer untuk melakukan transaksi dengan menggunakan *credit card* orang lain sehingga dapat merugikan orang tersebut baik materiil maupun immaterial.

b. Berdasarkan motif
   - *Cybercrime* yang menyerang individu
     Kejahatan terhadap orang lain dengan motif dendam atau iseng yang bertujuan untuk merusak nama baik, mencoba ataupun mempermainkan seseorang untuk mendapatkan kepuasaan pribadi. Contoh: Pornografi, *cyberstalking*, dll.
   - *Cybercrime* yang menyerang hak cipta (hak milik)
     Kejahatan yang dilakukan terhadap hasil karya seseorang dengan motif menggandakan, memasarkan, mengubah yang bertujuan untuk kepentingan pribadi atau umum demi materi maupun non materi.
   - *Cybercrime* yang menyerang pemerintah
     Kejahatan dengan pemerintah sebagai objek dengan motif melakukan terror, membajak, ataupun merusak keamanan suatu pemerintahan yang bertujuan untuk mengacaukan sistem pemerintahan atau menghancurkan suatu negara.

E. PEMBAHASAN

Pemanfaatan dan penggunaan internet secara meluas ini pada 1 (satu) sisi membawa perubahan paradigma pada bidang kehidupan yang positif, seperti bidang bisnis, politik, sosial, budaya dan sebagainya, tetapi pada sisi lain juga menimbulkan perubahan paradigm dalam studi mengenai kejahatan. Kajian kriminologi yang ada saat ini merupakan kajian terhadap kejahatan yang terjadi di dunia maya (*virtual reality*). Kajian kriminologi bisa mengenai kehidupan dunia maya ini sangat perlu dilakukan mengingat harapan-harapan yang digantungkan begitu tinggi pada internet. Kajian kriminolgis terhadap kehidupan maya semakin mengukuhkan sebuah pendapat bahwa dunia maya, yang realitasnya adalah realitas virtual dan komunitasnya berupa komunitas virtual ternyata memiliki penjahatnya sendiri.

Negara-negara menjadi pioneer dalam bidang ini telah merespon perkembangan abad informasi ini dengan mengubah berbagai paradigm yang meliputi pemanfaatan dan penggunaan internet dalam perundang-undangan yang terkait. Meski demikian, perkembangan internet begitu pesat sehingga perubahan itu harus secara terus menerus diperhatikan agar perundang-undangan yang terbentuk betul-betul dapat mengakomodasi dan melindungi berbagai kepentingan yang terkait.

Negara-negara berkembang dan terbelakang termasuk Indonesia, umumnya tertinggal dalam pengembangan dan pemanfaatan teknologi informasi, karena merasa kesulitan untuk merumuskan suatu perundang-undangan yang mengatur aktivitas di *cyberspace*. Pada saat kesulitan dalam menyusun perundang-undangan itu, serbuan internet dan pemanfaatannya di berbagai bidang tidak bisa dibendung, sehingga dalam menghadapi hal ini dimunculkan pemikiran untuk menggunakan hukum positif yang ada. (*the existing law*).

Penggunaan hukum positif yang ada untuk kejahatan atau perbuatan yang secara *paradigmatic* memiliki perbedaan tentunya tidak membawa keberuntungan bagi berbagai pihak. Perundang-undangan lama (hukum positif saat ini) memiliki paradigmanya sendiri yang melandasi pembuatan atau penciptaan perundang-undangan itu yang diseuaikan dengan zamannya, sedangkan sekarang zaman telah berubah. Konsep ruang dan waktu yang telah melandasi pembuatan hukum positif telah didobrak dengan perkembangan internet. Pendobrakan terhadap konsep ruang dan waktu ini seharusnya diikuti dengan pendobrakan terhadap sistem hukum yang masih mendasari pada konsep itu.

Memberikan perlindungan kepada warga negara dengan harta bendanya merupakan kewajiban pemerintah. Meskipun undang-undang yang mengatur kegiatan di cyberspace belum ada, sedangkan sebagian warga negara yang ada telah menggunakan internet untuk berbagai keperluan, maka secara moril pemerintah memiliki kewajiban untuk melindungi warga negaranya tersebut. Perlindungan ini tentunya diberikan dengan memanfaatkan atau memberlakukan perundang-undangan yang ada dengan berbagai cara seperti penafsiran maupun analogi.

Badan Pembinaan Hukum Nasional dalam sebuah penerbitannya mencoba untuk mengidentifikasikan bentuk-bentuk kejahatan yang berkaitan dengan aktivitas di cyberspace dengan perundang-undangan pidana yang ada. Hasil identifikasi itu berupa pengkategorian perbuatan kejahatan *cyber* (*cybercrime*) ke dalam delik-delik dalam KUHP sebagai berikut:[3]

a. *Joycomputing*
   Merupakan suatu perbuatan seseorang yang menggunakan komputer secara tidak sah atau tanpa izin dan menggunakannya melampaui wewenang yang diberikan. Tindakan ini dapat dikategorikan sebagai tindak pidana pencurian (Pasal 362 KUHP).
b. *Hacking*
   Artinya suatu perbuatan penyambungan dengan cara menambah terminal komputer baru pada sistem jaringan komputer tanpa izin (dengan melawan hukum) dari pemilik sah jaringan komputer tersebut. Tindakan ini dapat dikategorikan sebagai tindak pidana perbuatan tanpa wewenang masuk dengan memaksa ke dalam rumah atau ruangan yang tertutup atau pekarangan atau tanpa haknya

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

berjalan di atas tanah milik orang lain (Pasal 167 dan Pasal 551 KUHP).

c. *The Trojan Horse*
Diartikan sebagai suatu prosedur untuk menambah, mengurangi atau mengubah instruksi pada sebuah program, mengurangi atau mengubah instruksi pada sebuah program, sehingga program tersebut selain menjalankan tugas yang sebenarnya juga akan melaksanakan tugas lain yang tidak sah. Tindakan ini dapat dikategorikan sebagai tindak pidana penggelapan (Pasal 372 dan 374 KUHP). Apabila kerugian yang ditimbulkan menyangkut keuangan negara, tindakan ini dapat dikategorikan sebagai tindak pidana korupsi.

d. *Data Leakage*
Sebagai pembocoran data rahasia yang dilakukan dengan cara menulis data-data rahasia tersebut ke dalam kode-kode tertentu sehingga data dapat dibawa keluar tanpa diketahui oleh pihak yang bertanggung jawab. Tindakan ini dapat dikategorikan sebagai tindak pidana terhadap keamanan negara (Pasal 112, Pasal 113, dan Pasal 114 KUHP) dan tindak pidana membuka rahasia perusahaan atau kewajiban menyimpan rahasia profesi atau jabatan (Pasal 332 dan Pasal 323 KUHP).

e. *Data Diddling*
Suatu perbuatan yang mengubah data valid atau sah dengan cara yang tidak sah, yaitu dengan mengubah input data atau output data. Tindakan ini dapat dikategorikan sebagai tindak pidana pemalsuan surat (Pasal 263 KUHP).

f. Penyia-nyiaan data komputer.
Adalah suatu perbuatan yang dilakukan dengan suatu kesengajaan untuk merusak atau menghancurkan media disket dan media penyimpanan lainnya seperti flashdisk yang berisikan data atau program komputer, sehingga kibat perbuatan tersebut data atau program yang dimaksud menjadi tidak berfungsi lagi dan pekerjaan-pekerjaan yang melalui program komputer tidak dapat dilaksanakan. Tindakan ini dapat dikategorikan sebagai tindak pidana perusakan barang (Pasal 406 KUHP).

Hal-hal yang dilakukan oleh BPHN ini memang sudah cukup baik meskipun baru sebatas pemikiran untuk menanggulangi kekosongan hukum. Akan tetapi perbedaan konsep mengenai ruang dan waktu dari perundang-undangan pidana dengan sifat internet akan membawa kesulitan dalam penerapannya bahkan untuk beberapa pasal dalam penerapan KUHP terhadap beberapa aktivitas di *cyberspace*.

Beberapa kasus penting yang pernah ditangani Polri di bidang *cybercrime* di antaranya adalah:

- *Cyber Smuggling*, berupa laporan pengaduan dari *US Custom* (Pabean Amerika Serikat) adanya tindak pidana penyelundupan via internet yang dilakukan oleh beberapa orang Indonesia, dimana oknum-oknum tersebut telah mendapatkan keuntungan dengan melakukan *Web-hosting* gambar-gambar porno di beberapa perusahaan *Web-hosting* yang ada di Amerika Serikat.
- Pemalsuan Kartu Kredit berupa laporan pengaduan dari warga negara Jepang, Perancis, dan Amerika Serikat tentang tindak pidana pemalsuan kartu kredit yang mereka miliki untuk keperluan transaksi di internet.
- *Hacking situs*, *hacking* beberapa situs termasuk situs Polri yang pelakunya diidentifikasikan berada di *Indonesia*.

Aktivitas di internet tidak bisa dilepaskan dari manusia dan akibat hukumnya terhadap manusia yang ada di dalam kehidupan nyata (*real life/ physical world*) sehingga muncul pemikiran mengenai

perlunya aturan hukum untuk mengatur aktivitas tersebut. Internet memiliki karakteristik yang berbeda dengan dunia nyata sehingga muncul pro dan kontra mengenai bisa tidaknya hukum tradisional/ konvensional (*the existing law*) mengatur aktivitas tersebut atau perlu tidaknya aktivitas di internet diatur oleh hukum.

Pro kontra tersebut disebabkan oleh 2 (dua) hal. *Pertama*, karakteristik aktivitas di internet yang bersifat lintas batas, sehingga tidak lagi tunduk pada batasan-batasan territorial. *Kedua*, sistem hukum tradisional yang justru bertumpu pada batasan-batasan territorial dianggap tidak cukup memadai untuk menjawab persoalan-persoalan hukum yang muncul akibat aktivitas di internet.

Pro kontra masalah ini dibagi menjadi 3 (tiga) kelompok, yaitu:

1) Kelompok pertama secara total menolak setiap usaha untuk membuat aturan hukum bagi aktivitas-aktivitas di internet yang didasarkan atas sistem hukum tradisional. Dengan pendirian seperti ini, maka menurut kelompok ini internet harus diatur sepenuhnya oleh sistem hukum baru yang didasarkan atas norma-norma hukum yang baru pula yang dianggap sesuai dengan karakteristik yang melekat pada internet. Kelemahan utama dari kelompok ini adalah mereka menafikan fakta, meskipun aktivitas internet itu sepenuhnya beroperasi secara virtual, tetapi masih tetap melibatkan masyarakat (manusia) yang hidup di dunia nyata.
2) Kelompok kedua berpendapat bahwa penerapan sistem hukum tradisional untuk mengatur aktivitas-aktivitas di internet sangat mendesak untuk dilakukan. Perkembangan internet dan kejahatan yang melingkupinya begitu cepat sehingga yang paling mungkin untuk pencegahan dan penanggulangannya adalah dengan mengaplikasikan sistem hukum tradisional yang saat ini berlaku. Kelemahan utama kelompok ini merupakan kebalikan dari kelompok pertama, yaitu mereka menafikan fakta bahwa aktivitas-aktivitas di internet menyajikan realitas dan persoalan baru yang merupakan fenomena khas masyarakat informasi yang tidak sepenuhnya dapat direspon oleh sistem hukum tradisional.
3) Kelompok ketiga tampaknya merupakan sintesis dari kedua kelompok di atas. Mereka berpendapat bahwa aturan hukum yang akan mengatur mengenai aktivitas di internet harus dibentuk secara evolutif dengan cara menerapkan prinsip-prinsip *common law* yang dilakukan secara hati-hati dan dengan menitikberatkan kepada aspek-aspek tertentu dalam aktivitas *cyberspace* yang menyebabkan kekhasan dalam transaksi-transaksi di internet. Kelompok ini memiliki pendirian yang cukup moderat dan realistis karena memang ada beberapa prinsip hukum tradisonal yang masih dapat merespon persoalan hukum yang timbul dari aktivitas internet di samping juga fakta bahwa beberapa transaksi di internet tidak dapat sepenuhnya direspon oleh sistem hukum tradisional.

Ada 2 (dua) model yang diusulkan oleh Mieke untuk mengatur kegiatan-kegiatan di cyberspace, yaitu:[4]

- Model Ketentuan Payung (*Umbrella Provisions*) sebagai Upaya Harmonisasi Hukum

  Model ketentuan payung untuk peraturan perundang-undangan yang mengatur kegiatan-kegiatan di *cyberspace*, di satu sisi memiliki kebaikan, yaitu akan menghasilkan suatu *masterpiece* dengan memahami sangat beragamnya hal-hal yang perlu diatur.

[4] Budhijanto, Danrivanto., *Aspek-Aspek Hukum dalam Perniagaan Secara Elektronik (E-Commerce*), FH UNPAD, Bandung, hal. 3.

Namun, di sisi lain kelemahannya adalah menimbulkan konsekuensi logis untuk mempersiapkan dalam waktu yang tidak boleh terlalu lama bagi seluruh rancangan peraturan perundang-undangan yang lebih khusus atau spesifik (baik pada tingkatan yang sederajat maupun pengaturan pelaksanaan teknisnya) agar terhindarkan dari kekosongan hukum.

Model ketentuan payung dapat memuat:

a. Materi-materi pokok saja yang perlu diatur dengan memperhatikan semua kepentingan, antara lain seperti pelaku usaha, konsumen, pemerintah, penegak hukum, dan;
b. Keterkaitan hubungan dengan peraturan perundang-undangan yang telah ada terlebih dahulu dan yang akan datang agar tercipta suatu hubungan sinergis.

- Model *Triangle Regulations* sebagai Upaya Mengantisipasi Pesatnya Laju Kegiatan-kegiatan di *Cyberspace*

Model ini adalah suatu upaya yang lebih menitikberatkan kepada permasalahan manakah yang lebih dulu menjadi prioritas, sehingga mampu secara efisien dan efektif diantisipasi disebabkan pengaturannya lebih spesifik dan menukik. Jadi, tidak perlu adanya pengaturan yang harus memuat seluruh kegiatan di *cyberspace*. Berdasarkan skala prioritas 3 (tiga) regulasi yang dapat disusun terlebih dahulu, yaitu:

a. Pengaturan sehubungan Transaksi Perdagangan elektronika (*E-Commerce*) atau On-line Transaction, yang di dalamnya memuat antara lain tentang *Digital Signature* dan *Certification of Authority*, aspek pembuktian, perlindungan konsumen, anti monopoli dan persaingan sehat, perpajakan, serta asuransi;
b. Pengaturan sehubungan *Privacy Protection* terhadap pelaku bisnis dan konsumen, yang di dalamnya memuat antara lain perlindungan *electronic databases*, *individual/ company records*; dan
c. Pengaturan sehubungan *Cybercrime,* yang di dalamnya memuat antara lain yuridiksi dan kompetensi dari badan peradilan terhadap kasus-kasus yang terjadi dalam *cyberspace*, penipuan melalui komputer atau melalui jaringan telekomunikasi, ancaman dan pemerasan, fitnah atau penghujatan (*defamation*), kegiatan transaksi atas substansi yang berbahaya, eksploitasi seksual dari anak-anak, substansi yang tidak layak untuk ditransmisikan.

Secara radikal *cyberspace* telah mengubah hubungan antara *legally significant* (*online*) *phenomena and physical location.* Peningkatan jaringan komputer global (*global computer network*) telah menghancurkan hubungan antara letak geografis dengan:

1. Kewenangan pemerintah untuk memaksakan *control* atas *online behavior*;
2. Pengaruh online behavior terhadap individu atau barang;
3. Legitimasi pemerintah untuk mengatur fenomena global; dan
4. Kemampuan wilayah untuk memberitahukan kepada orang yang melewati perbatasan mengenai hukum yang berlaku.

Di negara-negara berkembang dan terbelakang pengguna atau pemakai internet umumnya terpusat di kota-kota besar karena struktur dan infrastruktur telekomunikasi lebih mudah didapat, sedangkan ddaerah pedesaan teknologi informasi masih merupakan barang baru. Walaupun demikian, perkembangan pengguna internet menunjukkan angka yang signifikan.

Teknologi informasi tidak akan menjadi besar tanpa bantuan dari pihak lain sebagai pengembang, pemasar, dan pengguna. Ada 3 (tiga) pihak yang kemudian saling menyesuaikan diri menuju apa yang

sekarang popular dengan istilah dunia maya atau *virtual reality* atau mayantara atau disebut juga *electronic world*, yaitu:

- Kemauan dari masyarakat untuk menggunakan teknologi informasi ini. Dalam hal ini masyarakat merupakan pengguna dan dalam optik ekonomi merupakan pangsa pasar.
- Dalam rangka menyongsong pemanfaatan teknologi informasi untuk berbagai bidang, maka industri teknologi informasi harus mempersiapkan diri. Artinya, industri yang bergerak di bidang teknologi informasi harus mempersiapkan diri apabila terjadi permintaan sarana dan prasarana internet.
- Kesiapan pemerintah masing-masing negara terutama bagi negara-negara berkembang dan terkebelakang untuk menerima era internet sebagai bagian penting dari kehidupan.

Urgensi pengaturan nasional atas kegiatan-kegiatan di *cyberspace* dilandasi oleh 3 (tiga) pemikiran utama, yaitu:

a) Perlunya kepastian hukum bagi para pelaku kegiatan di *cyberspace* yang harus diakomodasikan secara memadai dalam regulasi yang telah ada;
b) Upaya untuk mengantisipasi implikasi-implikasi yang ditimbulkan akibat pemanfaatan teknologi informasi; dan
c) Adanya variabel global, yaitu persaingan bebas dan pasar terbuka (WTO/GATT).

Melindungi asset yang telah ditanamkan, apalgi asset itu akan atau telah memberikan kontribusi terhadap keuntungan yang diperoleh perusahaan atau pemerintah, sangat penting. Perlindungan terhadap asset-aset yang dipakai untuk bermain dalam dunia *cyberspace* ini seharusnya merupakan prioritas utama sebab dalam dunia maya tidaka jaminan keamanan. Data, informasi dan berbagai hal yang berharga lalu-lalang dalam sebuah lalu lintas *superhighway* tanpa pengawasan dari pihak keamanan padahal penjahat dengan mata yang tajam berusaha menghentikan atau mengintersepsi data atau informasi yang berharga itu. Sehubungan dengan tidak adanya pengawasan dalam lalu lintas *superhighway* itu, maka masalah kemanan tentunya menjadi tanggung jawab dari mereka yang sengaja menggunakan internet untuk berbagai keperluan.[5]

Mengingat masalah keamanan ini sangat penting maka sistem keamanan internet itu sendiri merupakan asset yang berharga. Hal itu dapat dilihat dari fungsinya sebagai benteng pertahanan ataupun sebagai pelindung dari berbagai data penting baik yang terdapat di ruang publik maupun ruang privat sebuah situs. Meskipun masalah keamanan ini sangat penting dalam dunia *cyberspace*, tetapi ada saja yang tidak memperhatikan atau kurang perhatian terhadap sistem keamanan internet yang digunakan pada sebuah situs yang dikelolanya.

Kurangnya perhatian terhadap masalah kemanan internet ini menyebabkan sistus yang dikelola dapat dengan mudah diserang, disusupi, dirusak dan diberi virus yang berbahaya. Dari hasil survai yang dilakukan oleh peneliti menganggap masalah keamanan ini penting, tetapi belum menjadi perhatian utama. Meskipun mereka memandang masalah ini penting, tetapi dalam kenyataannya situs mereka berhasil di-*hack*. Ada beberapa faktor penyebab sehingga situs mereka berhasil di-*hack*, yaitu:

- Kurangnya perhatian terhadap ungkapan yang menyatakan bahwa dalam dunia internet tidak ada jaminan keamanan yang menyebabkan mereka kurang memperhatikan masalah keamanan. Hal ini dapat timbul karena

[5] Raharjo, Agus., *CYBERCRIME (Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi)*, Citra Aditya Bakti, Bandung, 2002, hal. 250.

ada anggapan bahwa pengakses adalah orang baik-baik, orang yang hanya mencari informasi tanpa merusak situs yang dikunjungi. Sebuah anggapan yang keliru dan salah besar. Anggapan ini umumnya muncul dari pengelola situs pelayanan publik milik pemerintah.

- Berdasarkan anggapan itu, maka mereka membangun sistem keamanan internet secara sederhana, murah dan mudah didapat. Sistem keamanan internet yang mereka bangun umumnya berbasis password, sebuah sistem keamanan yang sebetulnya sangat rapuh dan mudah ditembus apalagi dengan adanya berbagai macam aplikasi pemecah password seperti *crack* (UNIX), *viper* (*perl script*) dan *cracker jack* (DOS).
- Untuk membangun sistem keamanan internet yang baik memerlukan biaya yang besar, akibatnya mereka beranggapan keamanan internet penting, tetapi untuk memakai sistem keamanan yang mahal dan handal belum terlalu mendesak. Jika situs yang dikelola bisa diamankan dengan sistem keamanan yang murah, jadi tiodaklah perlu dengan yang mahal.

Beberapa cara yang dapat digunakan untuk mengamankan sistem informasi berbasis internet adalah[6]:

1. Mengatur akses (*access control*)
   Salah satu cara yang umum digunakan untuk mengamankan informasi adalah dengan mengatur akses ke informasi melalui *mekanisme authentication* dan *access control*. Implementasi dari mekanisme ini antara lain dengan menggunakan password. Di sistem UNIX dan Windows NT, untuk masuk dan menggunakan sistem komputer, pemakai harus melalui proses *authentication* dengan menuliskan *userid* (*user identification*) dan password.
2. Menutup *service* yang tidak digunakan
   Dalam sebuah sistem seringkali perangkat keras dan perangkat lunak diberikan beberapa servis yang dijalankan sebagai default, seperti pada sistem UNIX yang sering dipasang dari vendornya adalah *finger*, *telnet*, *ftp*, *smtp*, *pop*, *echo*, dan sebagainya.untuk mengamankan sistem servis maka server yang tidak diperlukan dimatikan.
3. Memasang proteksi
   Untuk lebih meningkatkan keamanan sistem informasi, proteksi dapat ditambahkan. Proteksi ini dapat berubah filter lebih khusus *firewall*. Filter dapat digunakan untuk memfilter e-mail, informasi, akses atau bahkan dalam level packet. Ada program filter internet yang bernama *Zeeksafe*. Program ini bisa memblokir situs-situs yang tidak diinginkan selama pengguna surfing di internet. Selain itu ada juga *We-Blocker* yang menentukan parameter apa saja yang akan membatasi akses ke website yang dianggap tidak layak dilihat.
4. *Firewall*
   Firewall merupakan sebuah perangkat yang diletakkan antara internet dengan jaringan internet. Informasi yang ke luar atau masuk harus melalui *firewall* ini. Tujuan utama dari firewall adalah untuk menjaga (prevent) agar akses ke dalam maupun ke luar dari orang yang tidak berwenang (*unauthorized access*) tidak dapat dilakukan. Firewall bekerja dengan mengamati paket *Internet Protocol* (IP) yang melewatinya. Detail dari konfigurasi bergantung kepada masing-masing *firewall*. Firewall dapat berupa

[6] Rahardjo, Budi., *Keamanan Dalam Teknologi Informasi*, Gradhika Bakti Praja, Semarang, 2001, hal. 51.

sebuah perangkat keras yang sudah dilengkapi dengan perangkat lunak tertentu sehingga pemakai (administrator) tinggal melakukan konfigurasi dan firewall tersebut. Firewall juga dapat berupa perangkat lunak yang ditambahkan pada sebuah server (baik UNIX maupun Windows NT) yang dikonfigurasikan menjadi *firewall*. Firewall biasanya melakukan 2 (dua) fungsi, yaitu fungsi *Internet Protocol* (IP) *filtering* dan fungsi *proxy*.

5. Pemantau adanya serangan
   Sistem pemantau (*monitoring system*) digunakan untuk mengetahui adanya tamu tidak diundang (*intruder*) atau adanya serangan (attack). Nama lain dari sistem ini adalah *Intruder Detection System* (IDS). Sistem ini dapat memberi tahu administrator melaui e-mail maupun melaui mekanisme lain seperti *pager*. Ada beberapa cara untuk memantau adanya intruder, baik yang sifatnya aktif maupun pasif. *Intruder Detection System* (IDS) cara yang pasif misalnya dengan memonitor *log file*. Beberapa contoh dari Intruder Detection System (IDS), antara lain:
   1) *Autobuse*, mendeteksi probing dengan memonitor log file.
   2) *Courtney* dan *portsentry*, mendeteksi *probing (port scanning)* dengan memonitor *packet* yang lalu lalang. *Portsentry* bahkan dapat memasukkan *Internet Protocol* (IP) penyerang dalam *filter tcpwrapper*.
   3) *Shadow* dari SANS.
   4) *Snort*, mendeteksi pola (*pattern*) pada paket yang lewat dan mengirimkan *alert* jika pola tersebut terdeteksi. Pola-pola atau *rules* disimpan dalam berkas yang disebut *library* yang dapat dikonfigurasi sesuai dengan kebutuhan.
6. Pemantau integritas sistem
   Sistem ini dijalankan secara berkala untuk menguji integritas sistem. Salah satu contoh program yang umum digunakan di sistem UNIX adalah program *Tripwire*. Program ini dapat digunakan untuk memantau adanya perubahan pada berkas. Pada mulanya program ini dijalankan dan membuat database mengenai berkas-berkas atau direktori yang ingin kita amatai beserta *signature* dari berkas tersebut. Signature berisi informasi mengenai besarnya berkas, kapan dibuatnya, pemiliknya, hasil *checksum* atau *hash* dan sebagainya. Apabila ada perubahan pada berkas tersebut, maka keluaran dari *hash function* akan berada dengan yang ada di database sehingga ketahuan adanya perubahan.
7. Audit: mengamati berkas *log*
   Segala kegiatan penggunaan sistem dapat dicatat dalam berkas yang biasanya disebut *log file* atau *log* saja. Berkas log ini sangat berguna untuk mengamati penyimpangan yang terjadi. Kegagalan untuk masuk ke sistem (*login*) misalnya tersimpan dalam berkas log. Untuk itu pada administrator diwajibkan untuk rajin nmemelihara dan menganalisis berkas log yang dimilikinya.
8. *Back up* secara rutin
   Biasanya *intruder* masuk ke dalam sistem dan merusak sistem dengan menghapus berkas-berkas yang ditemui. Jika intruder ini berhasil menjeboil sistem dan masuk sebagai superuser, maka ada kemungkinan dia dapat menghapus seluruh berkas. Untuk itu, adanya back up yang dilakukan secara rutin merupakan sebuah hal yang essensial. Bayangkan jika yang berhasil dihapus oleh *intruder* itu adalah data-data rahasia apalagi data rahasia keamanan negara.

9. *Penggunaan* enkripsi untuk meningkatkan keamanan
   Salah satu mekanisme untuk meningkatkan keamanan adalah dengan menggunakan teknologi enkripsi. Data-data yang dikirimkan diubah sedemikian rupa sehingga tidak mudah disadap. Banyak servis di internet yang masih menggunakan *plain text* untuk *authentication* seperti penggunaan pasangan *userid* dan *password*. Informasi ini dapat dilihat dengan mudah oleh program penyadap atau pengendus (*sniffer*). Untuk meningkatkan keamanan *server world wide web* dapat digunakan enkripsi pada tingkat socket. Dengan menggunakan enkripsi, orang tidak bisa menyadap data-data (transaksi) yang dikirimkan dari/ ke server *www*. Salah satu mekanisme yang cukup popular adalah dengan menggunakan *Secure Socket Layer* (SSL) yang mulanya dikembangkan oleh *Netscape*. Selain server *www* dari *Netscape* dapat dikonfigurasi agar memiliki fasilitas *Secure Socket Layer* (SSL) dengan menambahkan software tambahan (SSLeay-implementasi *Secure Socket Layer* (SSL) atau *Open Secure Socket Layer* (SSL) yaitu implementasi *Open Source* dari *Secure Socket Layer* (SSL).
   Penggunaan *Secure Socket Layer* (SSL) memiliki permasalahan yang bergantung kepada lokasi dan hukum yang berlaku. Hal ini disebabkan pemerintah melarang ekspor teknologi enkripsi (kriptografi) dan paten *Public Key Partners* atas *Rivest Shamir Adleman* (RSA) *public key cryptography* yang digunakan pada *Secure Socket Layer* (SSL).
10. *Telnet* atau *shell* aman
    Telnet atau *remote login* digunakan untuk mengakses sebuah *remote site* atau komputer. Akses ini dilakukan dengan menggunakan hubungan TCP/IP dengan menggunakan *userid* dan *password*. Informasi tentang *userid* dan *password* ini dikirimkan melalui jaringan komputer secara terbuka. Akibatnya, ada kemungkinan seorang yang nakal melakukan *sniffing* dan mengumpulkan informasi tentang pasangan *userid* dan *password* ini meskipun cara ini biasanya membutuhkan akses *root*. Untuk menghindari hal ini, enkripsi dapat digunakan untuk melindungi adanya *sniffing*. Paket yang dikirimkan dienkripsi dengan algoritma DES atau Blowish yang menggunakan kunci session yang dipertukarkan via *Rivest Shamir Adleman* (RSA) sehingga tidak dapat dibaca oleh orang yang tidak berhak.

Password dapat saja menjadi sistem pengaman yang baik asalkan tidak membiarkan *password* itu digunakan untuk jangka waktu yang tidak terlalu lama dan selalu dalam pengawasan. Penggunaan *password* yang sama dan terlalu lama sangat berbahaya, karena dalam keadaan administrator lemah, cracker dapat masuk ke sistem dan mengeksploitasinya. Kelemahan dari pengelolaan *password* seperti ini terutama terjadi pada hari-hari dimana administrator libur atau pada hari-hari dimana jam kerja diliburkan.

F. PENUTUP

Perlindungan pemilik website dalam upaya pencegahan dan penanggulangan kriminalisasi *cybercrime* di Indonesia secara yuridis sudah dilindungi oleh hukum akan tetapi belum begitu tegas diatur oleh salah satu perundang-undangan yang secara khusus mengatur tentang kriminalisasi *cybercrime ini*. Hal inilah yang menjadi salah satu penyebab semakin maraknya kriminalisasi *cybercrime* yang sangat merugikan pemilik website.

Pemerintah Indonesia harus secepat mungkin menyusun dan mengesahkan undang-undang yang khusus mengatur

tentang kriminalisasi *cybercrime* di Indonesia sebagai bentuk adanya kepastian hukum dalam upaya untuk mencegah timbulnya kejahatan internet yang semakin banyak dan untuk menanggulangi kejahatan internet yang sudah terjadi sampai saat ini.

DAFTAR PUSTAKA

Badan Pembinaan Hukum Nasional, *Perkembangan Pembangunan Hukum Nasional tentang Hukum Teknologi dan Informasi*, BPHN Departemen Kehakiman RI, 1996.

Budhijanto, Danrivanto., *Aspek-Aspek Hukum dalam Perniagaan Secara Elektronik (E-Commerce*), FH UNPAD, Bandung.

Mahzar, Ahmadi., Spritualitas Cyberspace, *Bagaimana Teknologi Komputer Mempengaruhi Kehidupan Keberagamaan Manusia*, Mizan, Bandung, 1999.

Raharjo, Agus., *CYBERCRIME (Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi)*, Citra Aditya Bakti, Bandung, 2002.

Rahardjo, Budi., *Keamanan Dalam Teknologi Informasi*, Gradhika Bakti Praja, Semarang, 2001.