ISSN : 1693 - 0819

KEBIJAKAN REGULASI HUKUM PIDANA DALAM MENANGANI KEJAHATAN TEKNOLOGI INFORMASI

Oleh : Sugiarto
(Staf Pengajar UNISRI Surakarta)

ABSTRACT

The development of information technology, besides having positive impact, it also has negative ones. The positive impact is the trend on technological development with all human creativity forms and the negative one is the emerging crime modus in Cyber world. The existing instruments of positive crime code (KUHP) still has difficulties in handle the development of IT crime, especially in relation with evident system or evidential means (article 184 KUHAP verse 1 character c which still has not been acknowledging computer data as the evident due to digital in nature). Additionally, there are several articles which are inappropriate to be implemented in IT crime, that is fine which are very light (can be replaced with jail) in IT crimes which can result in huge financial loss, even it can paralyze networking system.

The emerging of the Acts No. 11/2008 on Electronic Information and Transaction is expected to be able in providing secured, fair feeling and law authorization for the user and provider of informational technology and also able to overcome information technology crimes.

Keywords: Regulation policy, crime code, information technology crimes.

A. PENDAHULUAN

Latar Belakang Masalah

Hukum pidana memiliki arti yang penting dalam wacana hukum di Indonesia. Betapa tidak !, karena dalam hukum pidana memuat aturan-aturan yang menentukan perbuatan-perbuatan yang tidak boleh dilakukan dengan disertai ancaman yang berupa pidana (nestapa) dan menentukan syarat-syarat pidana dapat dijatuhkan (Moeljatno, 1993 : 1). Dengan demikian materi hukum pidana sarat dengan nilai kemanusiaan (Ahmad Babiej, 2006:1)

Mengingat materi hukum pidana sarat dengan nilai-nilai kemanusiaan, maka hukum pidana dapat digambarkan sebagai pedang bermata dua. Satu sisi hukum pidana bertujuan menegakkan nilai kemanusiaan, namun di sisi lain, penegakan hukum pidana justru memberikan sanksi kenestapaan bagi manusia yang melanggarnya.

Perihal kesesuaian antara hukum pidana dengan masyarakat di mana hukum pidana tersebut diberlakukan, menjadi salah satu syarat baik atau buruknya hukum pidana (Ahmad Babiej, 2006:2). Artinya, hukum pidana dianggap baik jika memenuhi dan sesuai dengan nilai-nilai yang berkembang di masyarakat. Namun demikian, kenyataan menunjukkan bahwa hingga sekarang hukum pidana Indonesia masih mempergunakan hukum pidana warisan Belanda.

Sehingga secara filosofis, politis, dan sosiologis, pemberlakuan hukum pidana warisan kolonial ini jelas menimbulkan problem tersendiri bagi bangsa Indonesia.

Menurut Undang-undang No. 1 tahun 1946, hukum pidana Indonesia yang disebut dengan KUHP, wujud aslinya adalah *Wetboek van Strafrecht* yang masih menggunakan bahasa Belanda (Sudarto, 1981:71). KUHP yang beredar di pasaran, adalah KUHP yang diterjemahkan dari bahasa Belanda oleh beberapa pakar hukum pidana, seperti Moeljatno, dan R. Susilo maupun terjemahan dari Badan Pembinaan Hukum Nasional (Tim Penerjemah BPHN, 1988).

Dilihat dari usianya, KUHP dapat dianggap telah usang dan sangat tua, walaupun Indonesia telah beberapa kali merubah materi KUHP, namun perubahan ini tidak sampai kepada masalah substansial atau masalah pokoknya. Di Belanda sendiri, KUHP saat ini telah banyak mengalami perkembangan, antara lain penghilangan pidana mati, penambahan pidana kerja sosial, serta denda yang dibuat dengan system kategorisasi.

Sudarto menyebutkan bahwa, ada tiga substansi atau masalah pokok dalam hukum pidana, yaitu kesalahan, sifat melawan hukumnya perbuatan dan pidana (Sudarto, 1990:86). Sedangkan Barda Nawawi Arief, menyebutkan bahwa tiga substansi atau masalah pokok hukum pidana tersebut meliputi masalah kesalahan atau pertanggungjawaban pidana, masalah pidana dan pemidanaan, maupun masalah tindak pidana atau kejahatan (Barda Nawawi Arief, 1996:87).

Berkenaan dengan tindak pidana atau kejahatan, KUHP bersifat positivis, dalam arti harus dicantumkan dalam Undang-Undang (asas legalitas formal). Dengan demikian, KUHP tidak memberikan tempat bagi hukum yang hidup di tengah-tengah masyarakat yang tidak tertulis dalam perundang-undangan. Tindak pidana atau kejahatan yang muncul, akibat perkembangan teknologi informasi seperti *money laundering, cyber crime*, belum tercover dalam KUHP.

B. PERMASALAHAN

Berdasarkan latar belakang masalah tersebut di atas dapat dikemukakan permasalahan sebagai berikut:

"Bagaimanakah kebijakan regulasi hukum pidana dalam rangka menangani kejahatan teknologi informasi?"

C. PEMBAHASAN

Untuk menjawab pertanyaan tersebut di atas, maka pada tulisan ini secara berturut-turut akan dibahas tentang perkembangan teknologi informasi dan modus-modus kejahatan, dan selanjutnya akan dibahas tentang kebijakan regulasi hukum pidana dalam menangani kejahatan teknologi informasi.

1. Perkembangan Teknologi Informasi dan Modus-Modus Kejahatan.

Sue Titus Reid mengemukakan bahwa kejahatan adalah tindakan yang disengaja melanggar hukum pidana yang dilakukan tanpa adanya suatu pembelaan atau pembenaran yang diakui secara hukum dan diberi sanksi oleh negara (Sue Titus Reid, 1979:5). Sutherland dalam Soerjono Soekamto mengemukakan bahwa ciri pokok dari kejahatan adalah merupakan perbuatan yang merugikan negara dan terhadap perbuatan itu negara bereaksi dengan memberikan hukuman sebagai upaya pamungkas (Soejono Soekamto, 1981:45). Francis Fukuyama menjelaskan bahwa ada kaitan yang erat antara modal sosial dan kejahatan. Kejahatan

itu muncul atau terjadi karena tiadanya modal sosial (Robert D. Putnam, 1993:82; Francis Fukuyama, 2005:34).

Seiring dengan berkembangnya teknologi internet *(cyberspace)* menyebabkan munculnya kejahatan yang disebut dengan *cybercrime* atau kejahatan melalui jaringan internet. Internet atau *interconnected network* adalah konvergensi telematika yang merupakan perpaduan teknologi komputer, media dan teknologi informasi. Internet merupakan jaringan komputer yang terdiri dari ribuan bahkan jutaan jaringan komputer independen yang dihubungkan satu dengan yang lainnya. Jaringan ini dapat dimanfaatkan untuk kepentingan sosial, ekonomi, politik, militer, bahkan untuk propaganda maupun terorisme.

Internet menawarkan berbagai kemudahan-kemudahan bertransaksi tanpa mempertemukan para pihak secara fisik atau material menembus batas-batas yurisdiksi antarnegara. Internet telah membawa seseorang ke dalam dunia baru yang disebut *cyberspace*, yang dalam perkembangannya tidak hanya membawa efek positif, tetapi juga efek negatif.

Cyberspace sebagai wahana komunikasi (Tubagus Ronny Rahman Nitibaskoro, 2001:53) yang berbasis komputer, banyak menawarkan realitas baru dalam berinteraksi di dunia maya. Adanya interaksi antarpengguna *cyberspace* telah banyak terseret ke arah terjadinya penyelewengan hubungan sosial berupa kejahatan yang khas yang memiliki karakteristik berbeda dengan tindak pidana konvensional yang selama ini sudah dikenal. Namun ada juga yang berpandangan bahwa kejahatan melalui komputer memiliki kesamaan bentuk dengan kejahatan yang ada di dunia nyata.

Andi Hamzah mengemukkan bahwa kejahatan komputer diartikan sebagai penggunaan komputer secara ilegal (Andi Hamzah, 1989:26). Sedangkan Petrus Reinhard Golose, mengemukakan bahwa dalam kasus kejahatan dunia maya, baik korban maupun pelaku tidak berhadapan langsung dalam satu tempat kejadian perkara. Dalam berbagai kasus baik korban maupun pelaku dapat berada dalam negara yang berbeda. Hal ini menggambarkan bahwa kejahatan dunia maya merupakan salah satu bentuk kejahatan lintas negara *(transnational crime)*, dan tak terbatas *(boundless)*, tanpa kekerasan *(non violence)*, tidak ada kontak fisik *(no physically contact)*, dan tanpa nama *(anonimity)* (Petrus Reinhard Golose, 2006:19). Inilah sebabnya JE. Sahetapy mengatakan bahwa kejahatan erat kaitannya dengan hasil budaya, artinya semakin tinggi tingkat budaya dan semakin modern suatu bangsa, maka semakin modern pula kejahatan itu, baik dilihat dari bentuk, sifat, dan cara pelaksanaannya (Abdul Wahid, 2002:21).

Secara umum, kejahatan di bidang TI dapat dikategorisasikan menjadi dua kelompok. *Pertama*, kejahatan biasa yang menggunakan teknologi informasi sebagai alat bantunya. Dalam kejahatan ini terjadi peningkatan modus dan operandinya dari semula menggunakan peralatan biasa, sekarang telah memanfaatkan teknologi informasi. *Kedua*, kejahatan yang muncul setelah adanya internet, di mana sistem komputer sebagai korbannya. Contoh dari kejahatan kelompok ini adalah pengrusakan situs internet, pengiriman virus atau program-program komputer yang tujuannya merusak sistem kerja komputer (Heru Sutadi, 2003:14)

Berdasarkan jenis aktifitas yang dila kukannya *cybercrime* dapat digolongkan menjadi beberapa jenis (James O. Brian, 1999: 6) antara lain : (1) *unauthorized acces* adalah kejahatan

yang terjadi ketika seseorang memasuki atau menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa ijin atau tanpa sepengetahuan pemilik sistem, (2) *illegal contents* adalah kejahatan yang dilakukan dengan memasukkan data atau informasi ke dalam internet, (3) penyebaran virus secara sengaja, (4) data forgeri adalah kejahatan yang dilakukan dengan tujuan memalsukan data pada dokumen penting yang ada di internet, (5) *cyber espionage* adalah kejahatan yang memanfaatkan jaringan internet, (6) *sabotage and extortion* adalah jenis kejahatan yang dilakukan dengan membuat gangguan, perusakan dan penghancuran terhadap suatu data (7) *cyberstalking* adalah kejahatan yang dilakukan untuk mengganggu atau melecehkan seseorang dengan memanfaatkan komputer, (8) *carding* adalah kejahatan yang dilakukan untuk mencuri kartu kredit milik orang lain dan digunakan dalam transaksi perdagangan di internet, (9) *cracker* adalah kejahatan dengan cara memanfaatkan kemampuannya untuk hal-hal yang negatif, (10) *cybersquatting* adalah kejahatan yang dilakukan dengan mendaftarkan domain dan nama perusahaan orang lain, (11) *tiposquatting* adalah kejahatan yang membuat dominan plesetan, (12) *hijacking* adalah kejahatan dengan melakukan pembajakan hasil karya orang lain, dan (13) *cyberterorism* adalah kejahatan yang dilakukan dengan cara mengancam pemerintah atau warga negaranya termasuk *cracking* ke situs pemerintah atau militer.

Berdasarkan motif kejahatan yang dilakukannya, *cybercrime* dapat digolongkan menjadi dua jenis yaitu (1) *cybercrime* sebagai tindakan murni kriminal, dan (2) *cybercrime* sebagai kejahatan abu-abu (Setiadi, 2005:20).

Berdasarkan sasaran kejahatan, *cybercrime* dapat dikelompokkan menjadi tiga kategori, yaitu: (1) *cybercrime* yang menyerang individu *(against person)*, (2) *cybercrime* yang menyerang hak milik *(against property)*, dan *cybercrime* yang menyerang pemerintah *(against goverment)* (Setiadi, 2005:20).

2. Kebijakan Regulasi Hukum Pidana dalam Menangani Kejahatan Teknologi Informasi

Pesatnya perkembangan teknologi informasi beserta penyebaran produk-produknya sangat dimungkinkan karena adanya globalisasi dan dampaknya terasa pula dalam bidang hukum. Hukum, teknologi informasi, dan globalisasi merupakan 3 bidang yang saling berhubungan. Dalam globalisasi (karena kemajuan teknologi informasi), hukum bergerak diantara memper tahankan hukumnya sendiri atau menyesuaikan dengan hukum negara lain.

Kemajuan teknologi informasi, memungkin kan setiap orang dapat melakukan hubungan hukum dengan orang lain di belahan dunia manapun. Akibat dari kemajuan ini dibutuhkan hukum untuk mengatur perilaku manusia, memecahkan masalah-masalah yang timbul, sebagai sosial kontrol (Marwan Mas, 2004:80-94). Persoalannya adalah kecepatan yang dimiliki oleh hukum tidak seiring dengan kecepatan globalisasi dan teknologi informasi, sehingga timbul kesan bahwa hukum selalu tertinggal dalam mengatur aktivitas perilaku manusia. Ketertinggalan hukum bukan merupakan indikasi bahwa hukum termarginalisasi, akan tetapi ada beberapa hal yang menyebabkan. *Pertama*, adanya perbedaan kepentingan dan kemauan politik dari badan pembuat hukum (SoetandyoWignyosubroto, 2008:8), *Kedua*, proses pembuatan undang-undang membutuhkan waktu yang lama (William J. Chambliss & Rob-

ert B. Seidman, 1971:12), padahal perkembangan teknologi berjalan sangat cepat sehingga dengan proses yang demikian lama menyebabkan hukum yang terbentuk menjadi usang dari sisi teknologi. *Ketiga*, hukum memerlukan kepastian dan ketepatan, sehingga substansi atau materi yang hendak diatur dapat dipergunakan oleh para penegak hukum maupun oleh mereka yang diatur (Lawrence M. Friedman, 2009:13-17).

Persoalan yang timbul diantara hukum, teknologi informasi dan globalisasi berpusat pada satu titik yaitu manusia. Karena berbicara masalah hukum tidak semata-mata bersifat normatif melainkan membahas persoalan manusia. Oleh karena itu persoalan hukum yang paling mendasar adalah persoalan manusia (Esmi Warasih, 2005:84). Manusia merupakan mahluk yang monodualis yaitu sebagai mahluk individu dan mahluk sosial (Suroto, 1985:5), bahkan oleh Notonagoro disebutnya sebagai mahluk monopluralis artinya manusia terdiri dari banyak unsur (monodualis-monodualis) yang merupakan satu kesatuan, misalnya jiwa - raga, individu – sosial, mandiri - terikat dan sebagainya (Notonagoro, 1975:42). Sehingga persoalan kemanusiaan memiliki dimensi yang luas, yang meliputi sosial, hukum, budaya, ekonomi, dan sebagainya.

Berkembangnya teknologi informasi karena globalisasi adalah merupakan wujud dari rutinitas manusia yang ditunjukkan untuk kepentingan manusia. Hukum bertujuan untuk mengatur perilaku manusia, akan tetapi tiap hari kita jumpai kejahatan. Teknologi informasi dikembangkan untuk membuat hidup manusia lebih mudah berkomunikasi, akan tetapi banjir informasi yang menyesatkan *(pornografi, cybercrime)*. Dengan globalisasi berharap meningkatnya kesejahteraan rakyat, akan tetapi banyak rakyat yang tertindas. Tujuan yang dicapai adalah kekayaan dan kekuasaan (Robert Gilpin, 1987:111-119). Negara-negara besar dan kuat lebih banyak memberikan pengaruh bahkan kerap kali memaksakan sekalipun dengan dalih bermacam-macam. Sebaliknya negara kecil atau negara yang lemah secara politik dan ekonomi bersifat tergantung di tingkat global (Dochak Latief, 2001:103). George Washinton pernah berkata bahwa merupakan suatu kegilaan bagi suatu negara mengharapkan pertolongan negara lain tanpa memperhatikan negara yang membantunya. Lebih jelas pendapat dari Jhon Foster Dulles yang menyatakan bahwa Amerika tidak mempunyai teman, tetapi Amerika selalu mempunyai kepentingan tertentu (Dochak Latief, 2001:103).

Sistem hukum modern yang diterapkan Indonesia saat ini tidak secara otomatis menjamin keadilan. Hal ini masih sangat tergantung pada bagaimana penegak hukum menggunakan atau tidak menggunakan hukum. Penggunaan hukum tersebut tidak berarti melakukan pelanggaran hukum, melainkan semata-mata menunjukkan hukum dapat digunakan untuk tujuan lain selain mewujudkan keadilan. Disinilah letak tragedi hukum modern (Satjipto Rahardjo, 2009:X).

Pemikiran Satjipto Rahardjo dengan hukum progresifnya yang menegaskan bahwa hukum hendaknya mampu mengikuti perkembangan jaman, mampu menjawab perubahan jaman dengan segala dasar didalamnya serta mampu melayani masyarakat dengan menyandarkan aspek moralitas dari sumber daya manusia penegak hukum itu sendiri (Satjipto Rahardjo, 2006:IX).

Permasalahannya adalah bahwa dalam penegakan hukum yang seringkali dihadapi adalah ketika terkait dengan penyampaian informasi, komunikasi dan/atau transaksi secara

elektronik khususnya dalam hal pembuktian dan hal yang terkait dengan perbuatan hukum yang dilaksanakan melalui sistem elektronik (sistem komputer).

Dalam hukum kita meskipun masih relatif sederhana, sebenarnya sudah sejak lama memperluas penafsiran asas dan normanya ketika menghadapi persoalan kebendaan yang tidak berwujud, misalnya dalam kasus pencurian listrik sebagai perbuatan pidana. Namun dalam kegiatan *cybers* tidak lagi sederhana karena kegiatannya tidak lagi dibatasi oleh teritori suatu negara, yang mudah diakses kapan dan darimanapun. Kerugian dapat terjadi baik pada pelaku transaksi maupun pada orang lain yang tidak pernah melakukan transaksi.

Kegiatan melalui media elektronik atau komputer meskipun bersifat virtual (maya) dapat diketegorikan sebagai tindakan atau perbuatan hukum yang nyata. Secara yuridis kegiatan pada ruang siber tidak dapat didekati dengan ukuran dan kualifikasi hukum konvensional saja sebab jika cara ini ditempuh akan terlalu banyak kesulitan dan hal yang lolos dari pemberlakuan hukum. Kegiatan dalam ruang siber adalah kegiatan virtual yang berdampak sangat nyata meskipun alat buktinya bersifat elektronik. Dengan demikian, subjek pelakunya harus dikualifikasikan pula sebagai orang yang telah melakukan perbuatan hukum secara nyata.

Ketentuan-ketentuan mengenai *cybercrime* dalam KUHP masih bersifat global, namun berdasarkan tingkat kemungkinan terjadinya kasus dalam dunia maya dan kategorisasi kejahatan *cyber* secara khusus diatur dalam KUHP dan disusun berdasarkan tingkat intensitas terjadinya kasus tersebut yang berkaitan dengan kejahatan *hacking* antara lain : (1). Ketentuan yang berkaitan dengan delik pencurian, (2). Yang berkaitan dengan pengrusakan/pengahncuran barang, (3). Yang berkaitan dengan perbuatan memasuki atau melintasi wilayah orang lain.

Delik pencurian, di atur dalam Pasal 362 KUHP dan variasinya diatur dalam Pasal 363 KUHP; yakni tentang pencurian dengan pemberatan; Pasal 364 KUHP tentang pencurian ringan, Pasal 365, tentang pencurian yang disertai dengan kekerasan; Pasal 367 KUHP, tentang pencurian di lingkungan keluarga. Pasal 362 KUHP berbunyi: "*Barangsiapa mengambil barang sesuatu, yang seluruhnya atau sebagian kepunyaan orang lain, dengan maksud untuk dimiliki secara melawan hukum, diancam karena pencurian, dengan pidana penjara paling lama lima tahun atau pidana denda paling banyak Sembilan ratus rupiah*".

Menurut hukum pidana, pengertian benda diambil dari penjelasan Pasal 362 KUHP yaitu segala sesuatu yang berwujud atau tidak berwujud seperti listrik, dan mempunyai nilai di dalam kehidupan ekonomi dari seseorang. Data atau program yang tersimpan di dalam media penyimpanan disket atau sejenisnya yang tidak dapat diketahui wujudnya dapat berwujud dengan cara menampilkan pada layar penampil komputer (*screen*) atau dengan cara mencetak pada alat pencetak (*printer*). Dengan demikian data atau program komputer yang tersimpan dapat dikategorikan sebagai benda seperti pada penjelasan Pasal 362 KUHP. Kendatipun demikian dalam sistem pembuktian kita terutama yang menyangkut elemen penting dari alat bukti (Pasal 184 KUHAP ayat (1) huruf c) masih belum mengakui data komputer sebagai bagiannya karena sifatnya yang digital. Padahal dalam kasus *cybercrime* data elektronik seringkali menjadi barang bukti yang ada. Karenanya sangat

realistis jika data elektronik dijadikan sebagai bagian dari alat bukti yang sah.

Menurut pengertian *computer related crime*, pengertian mengambil adalah dalam arti meng-copy atau mereka data atau program yang tersimpan di dalam suatu disket dan sejenisnya ke disket lain dengan cara memberikan instruksi-instruksi tertentu pada komputer sehingga data atau program yang asli masih utuh dan tidak berubah dalam posisi semula.

Menurut penjelasan pasal 362 KUHP, barang yang sudah diambil dari kekuasaan pemiliknya itu, juga harus berindah dari tempat asalnya, padahal dengan mengambil adalah melepaskan kekuasaan atas benda itu dari pemiliknya untuk kemudian dikuasai dan perbuatan itu dilakukan dengan sengaja dengan maksud untuk dimiliki sendiri, sehingga perbuatan meng-copy yang dilakukan dengan sengaja tanpa ijin dari pemiliknya dapat dikategorikan sebagai perbuatan "mengambil" sebagaimana yan dimaksud dengan penjelasan Pasal 362 KUHP.

Dalam sistem jaringan (*network*), peng-copy-an data dapat dilakukan secara mudah tanpa harus melalui izin dari pemilik data. Hanya sebagian kecil saja dari data internet yang tidak dapat "diambil" oleh para pengguna internet. Pencurian bukan lagi hanya berupa pengambilan barang/benda berwujud saja, tetapi juga termasuk pengambilan data secara tidak sah.

Penggunaan fasilitas *Internet Service Provider* (ISP) untuk melakukan kegiatan *hacking* erat kaitannya dengan delik pencurian yang diatur dalam Pasal 362 KUHP. Pencuri biasanya lebih mengutamakan memasuki sistem jaringan perusahaan financial, misalnya penyimpanan data kartu kredit, situs-situs belanja *on-line* yang ditawarkan di media internet dan data yang didapatkan secara melawan hukum itu diharapkan memberi keuntungan bagi si pelaku.

Ketentuan mengenai perbuatan perusakan, penghancuran barang, diatur dalam Pasal 406-412 KUHP. Pasal 406 KUHP berbunyi : *(1) Barangsiapa dengan sengaja melawan hukum menghancurkan, merusakkan, membikin tidak dapat dipakai lagi atau menghilangkan barang sesuatu yang seluruhnya atau sebagian adalah kepunyaan orang lain, diancam dengan pidana dipenjara paling lama dua tahun delapan bulan atau denda paling banyak empat ribu lima ratus rupiah; (2) Dijatuhkan pidana yang sama terhadap orang, yang dengan sengaja dan melawan hukum membunuh, merusakkan, membikin tidak dapat digunakan atau menghilangkan hewan yang seluruhnya atau sebagian adalah kepunyaan orang lain.*

Berdasarkan pengertian-pengertian mengenai perbuatan "menghancurkan, merusak, membuat tidak dapat dipakai lagi dan menghilangkan", maka dapat disimpulkan bahwa makna dalam perbuatan-perbuatan tersebut terdapat kesesuaian yang pada intinya perbuatan tersebut menyebabkan fungsi dari data atau program dalam suatu jaringan menjadi berubah/berkurang.

Perbuatan penghancuran atau perusakan barang yang dilakukan *cracker* dengan kemampuan *hacking*-nya bukanlah perbuatan yang bisa dilakukan oleh semua orang awam. Kemampuan tersebut dimiliki secara khusus oleh orang-orang yang mempunyai keahlian dan kreatifitas dalam memanfaatkan sistem, program, maupun jaringan. Motif untuk kejahatan ini sangat beragam yakni misalnya motif ekonomi, politik, pribadi atau motif kesenangan semata.

Ketentuan yang Berkaitan dengan Perbuatan Memasuki atau Melintasi

Wilayah Orang Lain diatur dalam Pasal 167 KUHP yang berbunyi : *(1) Barangsiapa memaksa masuk ke dalam rumah, ruangan atau pekarangan tertutup yang dipakai orang lain dengan melawan hukum atau berada di situ dengan melawan hukum, dan atas permintaan yang berhak atau suruhannya tidak pergi dengan segera, diancam dengan pidana penjara paling lama Sembilan bulan atau denda paling banyak empat ribu lima ratus rupiah; (2) Barangsiapa masuk dengan merusak atau memanjat, dengan menggunakan anak kunci palsu, perintah palsu atau pakaian jabatan palsu atau barang siapa tidak setahu yang berhak lebih dulu bukan karena kekhilafan masuk dan kedapatan di situ pada waktu malam, dianggap memaksa masuk; (3) Jika mengeluarkan ancaman atau menggunakan sarana yang dapat menakutkan orang, diancam dengan pidana penjara paling lama satu tahun empat bulan; (4) Pidana tersebut dalam ayat (1) dan (3) ditambah sepertiga jika yang melakukan kejahatan dua orang atau lebih dengan bersekutu.*

Dari Pasal 167 KUHP, menurut Andi Hamzah (1989) ada beberapa hal yang menyulitkan aparat penegak hukum dalam upaya penanganan kejahatan komputer, antara lain: (1). Apakah komputer dapat disamakan dengan rumah, ruangan atau pekarangan tertutup; (2). Berkaitan dengan cara masuk ke rumah atau ruangan tertutup, apakah test *key* atau *password* yang digunakan oleh seseorang untuk berusaha masuk ke dalam suatu sistem jaringan dapat dikategorikan sebagai kunci palsu, perintah palsu atau pakaian palsu.

Pasal yang berkaitan dengan perbuatan memasuki atau melintasi wilayah orang lain adalah Pasal 551 KUHP yang berbunyi: *"Barang siapa tanpa wewenang berjalan atau berkendaraan di atas tanah yang oleh pemiliknya dengan cara jelas di larang memasukinya, diancam dengan pidana denda paling banyak dua ratus dua puluh lima rupiah"*. Berkaitan dengan pasal ini, ada beberapa hal yang tidak sesuai lagi untuk diterapkan dalam upaya penanggulangan kejahatan *hacking*, yaitu pidana denda yang sangat ringan –dapat mengganti pidana kurungan- padahal hacking dapat merugikan finansial yang tidak sedikit bahkan mampu melumpuhkan kegiatan dari pemilik suatu jaringan yang berhasil dimasuki oleh pelaku dan perbuatan *hacking* ini merupakan awal dari maraknya kejahatan-kejahatan tradisional dengan sarana komputer dilakukan. Misalnya: pencurian, penipuan, penggelapan, pemalsuan dan lain-lain. Sebagai contoh: Seseorang yang dapat masuk ke suatu jaringan komputer perusahaan akan dengan mudah melakukan transaksi fiktif yang ia kehendaki atau melakukan perbuatan curang lainnya. Penanggulangan terhadap *cybercrime* dalam bentuk *hacking* perlu diimbangi dengan pembenahan dan pembangunan sistem hukum pidana secara menyeluruh, yakni meliputi pembangunan kultur, struktur dan substansi hukum pidana. Dalam hal ini kebijakan hukum pidana menduduki posisi yang strategis dalam pengembangan hukum pidana modern. Istilah kebijakan berasal dari bahasa Inggris *policy* atau dalam bahasa Belanda *politiek* yang secara umum dapat diartikan sebagai prinsip-prinsip umum yang berfungsi untuk mengarahkan pemerintah dalam mengelolah, mengatur atau menyelesaikan urusan-urusan publik, masalah-masalah masyarakat atau bidang-bidang penyusunan peraturan perundang-undangan dan pengaplikasian hukum/peraturan, dengan suatu

tujuan yang mengarah pada upaya mewujudkan kesejahteraan atau kemakmuran masyarakat (warga negara) (Wisnubroto, 1999:10). Oleh karena itu istilah kebijakan hukum pidana dapat pula disebut dengan istilah politik hukum pidana.

Lahirnya Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, diharapkan dapat meningkatkan efektifivas dan efisiensi pelayanan publik serta membuka kesempatan yang seluas-luasnya kepada setiap orang untuk memajukan pemikiran dan kemampuan di bidang penggunaan dan pemanfaatan teknologi informasi seoptimal mungkin dan bertanggung jawab selain itu juga diharapkan dapat memberikan rasa aman, adil, dan kepastian hukum bagi pengguna dan penyelenggaraan teknologi informasi termasuk penanggulangan kejahatan dunia maya (*cybercrime*).

Hukum positif selain KUHP yang saat ini dapat dipergunakan untuk menangani kejahatan dunia maya (*cybercrime*), disamping diatur dalam Undang-undang Nomor 11 Tahun 2008 khususnya Pasal 27 sampai dengan Pasal 52, juga diatur dalam Peraturan Perundang-undangan lain, yaitu: (1) *Undang-undang Nomor 36 Tahun 1999 Tentang Telekomunikasi*, meliputi: (a) pasal 22 dan Pasal 50, yakni memberikan ancaman pidana bagi perbuatan memanipulasi akses ke jaringan telekomunikasi; (b) Pasal 38 dan Asal 55 yakni memberikan ancaman pidana bagi mereka yang menimbulkan gangguan fisik dan elektromagnetik terhadap penyelenggaraan telekomunikasi; (c) Pasal 40 dan Pasal 56, memberi ancaman pidana bagi mereka yang menyadap informasi melalui jaringan telekomunikasi; (2) *Undang-undang Nomor 19 Tahun 2002 tentang Hak Cipta*, khususnya Pasal 1 Ayat 8, menjelaskan bahwa program komputer adalah sekumpulan instruksi yang diwujudkan dalam bentuk bahasa, skema, kode maupun bentuk yang lain yang apabila digabungkan dengan media yang dapat dibaca dengan komputer akan mampu membuat komputer bekerja untuk melakukan fungsi-fungsi khusus atau untuk mencapai hasil yang khusus, termasuk persiapan dalam merancang instruksi tersebut. Dalam Pasal 30 mengatur mengenai jangka waktu hak cipta untuk program komputer berlaku selama 50 tahun, (3) *Undang-undang Nomor 8 Tahun 1997 tentang Dokumen Perusahaan*, khususnya Pasal 12, menjelaskan bahwa dokumen perusahaan yang berupa mikrofilm, dan media lainnya (alat penyimpan informasi yang bukan kertas, dan mempunyai tingkat pengamanan yang dapat menjamin keaslian dokumen yang dialihkan atau ditransformasikan) diakui sebagai alat bukti yang sah., (4) *Undang-undang Nomor 20 Tahun 2001 Tentang Perubahan Atas Undang-undang Nomor 31 Tahun 1999, tentang Pemberantasan Tindak Pidana Korupsi*, menjelaskan bahwa alat bukti petunjuk tidak hanya dapat diperoleh dari keterangan saksi, surat, dan keterangan terdakwa sebagaimana diatur dalam KUHAP tetapi juga dapat diperoleh dari alat bukti yang lain yang berupa informasi yang diucapkan, dikirim, diterima, atau disimpan secara elektronik (email), telegram, teleks, faximile, dan dari dokumen yakni setiap rekaman data atau informasi yang dapat dikeluarkan dengan atau tanpa bantuan suatu sarana, baik yang tertuang diatas kertas, bentuk fisik apapun selain kertas, maupun yang terekam secara elektronik, yang berupa tulisan, suara, gambar, peta, rancangan foto, huruf, tanda, angka, atau perforasi yang memiliki makna., (5) *Undang-undang Nomor 25 Tahun 2003 Tentang*

Pencucian Uang, khususnya Pasal 2 Ayat 1 q, menjelaskan bahwa salah satu jenis tindak pidana penipuan adalah dilakukan melalui internet dan Pasal 38 huruf b menjelaskan bahwa informasi yang diucapkan, dikirimkan, diterima, dan disimpan secara elektronik dengan alat optik atau yang serupa dengan itu adalah merupakan alat bukti yang sah, dan (6) *Undang-undang Nomor 23 Tahun 2007 Tentang Perdagangan Orang*, khususnya Pasal 29, mengatur alat bukti selain sebagaimana yang diatur dalam KUHP, yaitu yang berupa informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan alat optik atau serupa dengan itu dan data rekaman atau informasi yang dapat dilihat, dibaca, didengar, dan dapat dikeluarkan dengan atau tanpa bantuan suatu sarana, baik yang tertuang dikertas, benda fisik apapun selain kertas, atau yang terekam secara elektronik.

Jika kita cermati hukum positif kita berdasarkan ketentuan peraturan perundang-undangan sebagaimana telah disebutkan diatas secara normatif, mampu untuk menangani kejahatan penyalahgunaan pemanfaatan teknologi informasi. Agustinus Dewaria, berpendapat bahwa internet hanya metode, situs bisa dilihat seperti rumah, data sama dengan barang milik orang, oleh karena itu hukum bisa ditegakkan meskipun dengan hukum positif yang lama (sebelum lahirnya Undang-undang Nomor 11 Tahun 2008), apalagi setelah disahkannya Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Undang-undang ini dengan tegas menyebutkan bahwa untuk kepentingan penyidikan, penuntutan, dan pemeriksaan dipersidangan, selain ketentuan yang diatur dalam KUHAP dan peraturan perundangan lainnya, informasi elektronik dan/ atau dokumen elektronik adalah merupakan alat bukti yang sah (Pasal 44 Undang-undang Nomor 11 Tahun 2008).

Beberapa contoh kasus penyalahgunaan pemanfaatan teknologi informasi dapat dipaparkan sebagai berikut:

1. Hacker, Dani Firmansyah konsultan Teknologi Informasi (TI) PT Danareksa di Jakarta, pada Sabtu 17 April 2004 berhasil membobol situs (*Craking*) Pusat Tabulasi Nasional Pemilu http://www.tnp.kpu.go.id milik Komisi Pemilihan Umum (KPU) di Hotel Borobudur Jakarta Pusat dan mengubah nama-nama partai di dalamya menjadi nama-nama "unik" semisal Partai Kolor Ijo, Partai Mbah Jambon, Partai Jambu, dan sebagainya. Modus dengan mengelos sistem keamanan server http://www.tnp.kpu.go.id dengan cara XSS atau *Cross Site Scripting* dan *SQL Injection*. Barang bukti: log file kabinet, server warnet Yogyakarta, server Danareksa, server KPU, Grafik koneksi berupa webalizer, sabtu buah cd *software*, satu buku file dan satu buku komputer. Majelis hakim Pengadilan negeri Jakarta Pusat yang diketuai Hamdi SH, pada persidangan kamis 23 Desember 2004, menetapkan vonis 6 bulan 21 hari kepada Dani Firmansyah. Hukuman didasarkan pada UU RI Nomor 36 Tahun 1999 tentang Telekomonikasi Pasal 22c jo. Pasal 38 jo Pasal 50 dan Subsider Pasal 406 KUHP (menghancurkan dan merusakkan barang).

2. Cyber Fraud (CC Fraud), Benny Wong pada 14 Juli 2004 melakukan transaksi di "Hardy's Supermarket" Bambulan Gianyar Bali, dengan menggunakan kartu kredit City Bank bernomor 4541 7900 1413 0605 atas nama Wahyu Nugroho. Saat itu transaksi berhasil dilakukan. Pada tanggal yang sama, Benny Wong kembali berbelanja di "Hardy's Supermarket" Sanur Bali dengan menggunakan empat kartu

kredit palsu yaitu Mastercard dari BNI, Visa dari Standart Cartered Bank, serta Mastercard dan Visa dari Citibank. Namun transaksi gagal dilakukan karena Kartu Kredit yang digunakan diketahui Palsu. Pada tanggal 14 September 2004 Majelis Hakim Pengadilan Negeri Denpasar yang dipimpin oleh Hakim Ketua Arif Supratman SH memberikan "hadiah" kepada terdakwa berupa putusan hukuman penjara selama 3 (tiga) tahun. Sembilan kemudian, tepatnya 6 Juni 2005, Majelis Hakim Pengadilan Negeri Gianyar Bali yang dipimpin oleh Hakim Ketua Gede Ginarsa dan Jaksa Penuntut Umum Ida Ayu Suratni memvonis untuk terdakwa yang sama dengan putusan penjara selama 2 (dua) tahun 8 (delapan) bulan. Secara keseluruhan, hukuman atas terdakwa pemalsuan kartu kredit di Bali itu adalah 5 (lima) tahun 8 (delapan) bulan. Putusan Pengadilan terhadap Benny Wong di Pengadilan Negeri Denpasar dan Pengadilan Negeri Gianyar tersebut, didasarkan pada Pasal 263 KUHP (Pemalsuan Surat-Barang siapa membuat surat palsu..., jika pemakaian tersebut dapat menimbulkan kerugian, karena pemalsuan surat, diancam dengan pidana penjara paling lama enam tahun).

3. Cyber Sex (pornography), Anggota Satuan *Cyber Crimes* Direktorat kriminal Khusus Kepolisian Daerah Metropolitas Jakarta Raya, Rabu 28 Juli 2004 sekitar pukul 11.15 wib, telah menangkap Johnny Indrawan Yusuf alias Hengky Wiratman alias Irwan Soenaryo asal Malang, Jawa Timur terkait dengan kasus perdagangan VCD Porno dan alat bantu seks melalui jeringan internet dalam situs http://www.vcdpomo.com. Nama domain http://www.vcdpomo.com itu sendiri terdaftar pada Network solution, LLc 13200 Woodland Park Drive, Herdon, VA 200171-3025, Amerika Serikat. Domainya terdaftar pada 4 Juli 2003 dan akan berakhir pada 4 Juli 2008 atas nama Lily Wirawan/Johny Jusuf dengan alamat : 20 Sill Wood Place, Sidney, 2171, Australia. Situs tersebut juga memiliki IP Addres: 69.50.194.230 yang terdaftar di ATJEU PUBLISHING, LLC 5546 West Irma, Glendale, AZ, United States. Terdakwa diancam hukuman Pidana penjara paling lama 2 (dua) tahun 8 (delapan) bulan, karena melanggar Pasal 282 KUHP (Kejahatan Terhadap Kesusilaan).

Dari kajian normatif hukum yang diatur dalam peraturan perundangan sebagai mana tersebut diatas sebetulnya telah mampu untuk menangani masalah kejahatan penyalahgunaan pemanfaatan teknologi informasi, namun demikian jika dikaji dari perspektif sosiologi yang mengatakan bahwa hukum adalah bagian dari lingkungan sosialnya, maka bekerjanya hukum tersebut sangat dipengaruhi oleh subsistem-subsistem sosial yang lain seperti sosial, budaya, politik, dan ekonomi. Demikian pula jika membicarakan hukum sebagai satu sistem, maka norma-norma hukum yang diatur dalam peraturan perundang-undangan tersebut hanya merupakan bagian dari subsistem yang lain, yaitu struktur hukum dan budaya hukum. Oleh karena itu norma-norma hukum tersebut dapat berjalan dengan baik apabila lembaga-lembaga hukum yang diciptakan oleh sistem hukum tersebut memberikan dukungan atas bekerjanya norma hukum yang ada serta lembaga-lembaga tersebut mampu memberikan pelayanan hukum secara teratur sesuai dengan keinginan masyarakat. Selain harus didukung oleh struktur hukum yang ada juga harus didukung oleh kesadaran masyarakat untuk melaksanakan hukum tersebut.

Dengan meminjam teori Robert B. Seidman dapat dijelaskan bahwa bekerjanya norma-

norma hukum sebagaimana telah diatur dalam peraturan perundangan sangat dipengaruhi oleh kekuatan-kekuatan personal dan sosial. Oleh karena itu dalam rangka menegakkan norma-norma hukum tersebut faktor manusia merupakan faktor yang sangat dominan karena membicarakan penegakan hukum tidak hanya semata-mata berpegangan pada kebenaran hukum sebagaimana tercantum dalam peraturan perundangan melainkan berhadapan dengan nilai-nilai maupun pola-pola perilaku yang ada dalam masyarakat.

D. KESIMPULAN

Berdasarkan pembahasan tersebut diatas dapat dikemukakan kesimpulan sebagai berikut :

Berkembangnya Teknologi Informasi selain berdampak positif juga menimbulkan dampak negatif. Dampak positifnya adalah menambah trend perkembangan teknologi dengan segala bentuk kreatifitas manusia dan dampak negatifnya adalah menimbulkan modus kejahatan baru dalam dunia *Cyber*.

Hukum pidana positif (KUHP) belum dapat sepenuhnya menjangkau kejahatan teknologi Informasi, sehingga perlu ada pembaharuan hukum positif yang mengatur masalah kejahatan TI. Karena kejahatan ini memiliki karakteristik yang berbeda dengan kejahatan konvensional.

Instrumen hukum pidana positif (KUHP) yang ada masih kesulitan untuk menanggulangi perkembangan kejahatan TI, terutama berkaitan dengan sistem pembuktian atau alat bukti (pasal 184 KUHAP ayat 1 huruf c masih belum mengakui data komputer sebagai alat bukti karena sifatnya digital). Selain itu, terdapat beberapa pasal yang tidak sesuai lagi untuk diterapkan dalam upaya penanggulangan kejahatan TI, yaitu pidana denda yang sangat ringan (dapat mengganti pidana kurungan) pada hal kejahatan TI dapat merugikan finasiil yang tidak sedikit, bahkan mampu melumpuhkan sistem jaringan.

Lahirnya UU No. 11 tahun 2008, tentang Informasi dan Transaksi Elektronik diharapkan mampu memberikan rasa aman, adil, dan kepastian hukum bagi pengguna dan penyelenggara Teknologi Informasi serta mampu menanggulangi kejahatan Teknologi Informasi.

DAFTAR PUSTAKA

Abdul Wahid, 2002, *Kriminologi dan Kejahatan Kontemporer*, Lembaga Penerbitan Malang : Fakultas Hukum Unisma.

Andi Hamzah, 1989, *Aspek-aspek Pidana di Bidang Komputer*, Jakarta: Sinar Grafika.

Barda Nawawi Arief, 1996, *Bunga Rampai Hukum Pidana*, Bandung : Citra Aditya Bakti

Dochak Latief, 2001, *Pembangun Ekonomi dan Kebijakan Ekonomi Global*, Surakarta: UMS Press.

Esmi Warasih, 2005, *Pranata Hukum Sebuah telaah sosiologi*, Semarang: PT. Suryandaru Utama.

Francis Fukuyama, 2005, *Goncangan sosial kodrat manusia dan tata sosial baru*, Jakarta: Gramedia Pustaka Utama.

Lawrence M. Friedman, 2009, *The Legal System a Social Science Perspective*. Alih bahasa M. Khozim, Bandung : Nusa Media.

Marwan Mas, 2004, *Pengantar Ilmu Hukum*, Jakarta: Ghalia Indonesia.
Moeljatno, 1993, *Asas-asas Hukum Pidana*, Jakarta : Rineka Cipta
……., 1994, *Kitab Undang-Undang Hukum Pidana*, Jakarta : Bina Aksara
Notonagoro, 1975, *Pancasila Secara Ilmiah Populer*, Jakarta: Pancuran Tujuh.
Satjipto Rahardjo, 2004, *Sosiologi Hukum. Perkembangan Metode dan Pilihan Masalah*, Sunkarta : Universitas Muhammadiyah Press
……., 2006, *Membedah Hukum Progresif*, Jakarta : PT Kompas Media Nusantara.
———————, 2009, *Penegakan Hukum Suatu tinjauan Sosiologis*, Yogyakarta: Genta Publishing.
Soerjono Soekanto, Hengkie Liklikuwata, Mulyana W. Kusumah, 1981, *Kriminologi Suatu Pengantar*, Jakarta: Ghalia Indonesia.
Soetandyo Wignyosoebroto, 2008, *Hukum dan Masyarakat*, Malang : Bayu Media Publishing.
Sudarto, 1981, *Hukum dan Hukum Pidana*, Bandung : Alumni
……., 1990, *Hukum Pidana I*, Semarang : Fakultas Hukum Undip
Sue Titus Reid, 1979, *Crime and Criminology*, New York : Hot Rinehart and Winston.
Sunoto, 1985, *Mengenal Filsafat Pancasila. Pendekatan melalui etika pancasila*, Yogyakarta: Hanindita.
Tim Penerjemah Badan Pembinaan Hukum Nasional, 1988, Departemen Kehakiman, *Kitab Undang-Undang Hukum Pidana*, Jakarta : Pustaka Sinar Harapan
Tubagus Rony Rahman Niti Baskara, 2001, *Ketika Kejahatan Berdaulat : Sebuah Pendekatan Kriminologi, Hukum dan Sosiologi*, Jakarta : Peradaban
Robert B. Seidman, 1972, *Law and Development*, A. General Model, dalam *Law and Society Review*, No VI.
Robert D Putnam, 1993, *Making Democracy Work*, Princenton, Princenton University Press.
Robert Gilpin, 1987, *The Political Economic of International Relation*, New Jersey : Prosedon University Press.
R.Susilo, t.th., *Kitab Undang-Undang Hukum Pidana, serta Komentar-komentarnya lengkap pasal demi pasal*, Bogor : Polite
William J. Chambliss & Robert B. Seidman, 1971, *Law, Order and Power*, Mas Adisson – Wesly: Reading.
Wishnubroto,1999, *Kebijakan Hukum Pidana dalam Penanggulangan Penyalahgunaan Komputer*, Yogyakarta : Universitas Atma Jaya.

Jurnal

Ahmad Bahiej, *Sejarah dan Problematika Hukum Pidana Material di Indonesia*, Sosio Religia, Vol.5 No. 2 Februari 2006.

Heru Sutadi, Cybercrime, apa yang bisa diperbuat?, http://www.sinarharapan.co.id/berita/0304/05/iptp01.html 2003.

James O. Brian, *Management Information System*, *Mc Graw-Hill*, 1999, h. 21, Donny Budi Utoyo, *Kajian Sosial Komunitas Maya Hacker/Craker dalam "Jurnal Hukum Teknologi"*, Volume 2 Nomor 1 Tahun 2005, LKHT FH UI, Depok

Setiadi, *Penegakan Hukum terhadap Pelaku Tindak Pidana Internet Banking*, dalam Jurnal Hukum Teknologi, Volume nomor 1 Tahun 2005, LKHT FH UI, Depok.

3. Peraturan Perundang-undangan

Kitab Undang-Undang Hukum Pidana (KUHP).

Undang-undang Nomor 8 Tahun 1997 tentang Dokumen Perusahaan.

Undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi.

Undang-undang Nomor 20 Tahun 2001 tentang Perubahan Atas Undang-undang Nomor 31 Tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi.

Undang-undang Nomor 19 Tahun 2002 tentang Hak Cipta.

Undang-undang Nomor 25 Tahun 2003 tentang Pencucian Uang.

Undang-undang Nomor 21 Tahun 2007 tentang Pemberantasan Tindak Pidana Perdagangan Orang.

Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Heru Sutadi, *Cybercrime, Apa yang bisa diperbuat ?*. http://www.sinarharapan.co.id/berita/0304/05/hpi.01.html, 2003, diakses 10 Juni 2009

Petrus Reinhard Golose, *Penegakan Hukum Cyber Crime dalam Sistem Hukum Indonesia dalam Seminar Pembuktian dan Penanganan Cyber Crime di Indonesia*, FHUI, Jakarta

(Footnotes)

[*] Dosen Negeri Dipekerjakan di FKIP Uniseti, saat ini sedang studi di Program Doktor Ilmu Hukum Universitas Sebelas Maret Surakarta