Kebijakan Hukum Dalam Mengurangi Kejahatan Akibat Dampak Kemajuan Komputer

Oleh: **Iskandar Z. Nasibu**

Abstract

Computer crime in global community of internet user public is a thing which can be realized or unconsciously, intentionally or involuntary is done. This thing happened because development of information technology and level of public intelectuality is increases.

Keeps abreast of technology in the computer area, especially in area Information And Communivation technology (ICT), badness by using computer technology has come up with phase to worry so that law footing to become a real footing that was public required.

Law challenged to do regulation, investigation, even where necessary determines penalty system based on justice and rule of law in standing computer technology progress.

Kata Kunci: Kebijakan Hukum, Kejahatan, Komputer, Globalisasi,

Pendahuluan

Perkembangan kemajuan teknologi dewasa ini membawa perubahan pola hidup manusia dalam bergaul, bersosialisasi, bahkan melakukan aktifitas ekonomi dalam skala lokal, regional, maupun global (Yaffe, 2001). Dapat dikatakan bahwa teknologi komputer membawa manusia pada manusia tanpa jiwa, artinya semakin kehilangan kesempatan untuk berinteraksi secara sosial, karena semakin banyak waktu dihabiskan di depan internet, televisi, dan media lainnya.

Mengikuti perkembangan teknologi komputer tersebut, khususnya di bidang *Information And Communivation technology* (ICT), menimbulkan berbagai akses, baik yang sifatnya positif maupun negatif, sehingga dunia hukum ditantang untuk melakukan *regulasi*, *investigasi*, sampai kalau perlu menentukan *penalty system* berdasarkan keadilan dan kepastian hukum.

Kejahatan dengan menggunakan teknologi komputer telah sampai pada tahap mencemaskan. Kemajuan teknologi komputer tak disangkal lagi, selain membawa ke dunia revolusioner yang serba praktis ternyata memiliki sisi gelap yang mengerikan, seperti *pornografi* (Kasus Anggota DPR Pusat Yahya Zaini dengan Artis Maria Eva), perang informasi (konfrontasi Indonesia dan Malaisya masalah perbatasan laut), *hacker*, pembobolan ATM (Sebagai contoh kasus di Indonesia, kejahatan komputer yang baru terdengar adalah kasus klick BCA yang terjadi tahun

2001, dengan jenis kejahatan *typosquatting*), *plagiat* dalam karya tulis, intimidasi atau pengancaman kepada pemimpin negara (kasus Presiden Indonesia Susilo Bambang Yudoyono yang diancam oleh sekelompok tertentu untuk dibunuh), bahkan yang santer terdengar dan sangat mengelitik kita semua adalah kejahatan terorisme digital.

Gambaran sisi gelap dari dampak negatif kemajuan teknologi komputer tersebut di atas kiranya hanya merupakan sedikit dari berbagai kasus yang muncul kepermukaan. Penulis yakin masih banyak kasus lain yang belum terungkap atau belum muncul di tengah-tengah kemajuan globalisasi yang saat ini masih menyimpan misteri dan sewaktu-waktu akan meledak. Selain itu dampak negatif kemajuan kejahatan komputer yang saat ini telah populer di tengah-tengah masyarakat terbatas pada kejahatan yang sudah dipublikasikan, karena tidak menutup kemungkinan masih banyak yang tersimpan rapi.

Diperkirakan kejahatan dengan menggunakan teknologi komputer ini telah menyebabkan kerugian yang cukup besar. Namun data statistik dan grafik yang benar-benar akurat masih agak sulit untuk didapatkan. Hal ini disebabkan karena ada beberapa kejahatan komputer yang tidak terdeteksi oleh korban, tidak dilaporkannya kejahatan ini kepada pihak yang berwenang, OECD memperkirakan 75-80 % pelanggaran komputer tidak dilaporkan.

Menurut British Crime Survey, para korban tidak melaporkannya karena tidak mengalami kerugian atau kerusakan yang signifikan, polisi tidak melakukan apapun untuk menanggulangi kejahatan ini, ataupun polisi memang kurang mengerti ataupun tidak terlalu tertarik terhadap hal kejahatan dalam bentuk baru ini.

Sulitnya untuk mengkalkulasi keseluruhan kerugian yang diderita oleh seluruh korban. Namun menurut data yang dibuat oleh para penegak hukum dan ahli komputer di Amerika, menyebutkan bahwa sekurang-kurangnya $ 5 X 1000,000,000 kerugian yang diderita akibat kejahatan ini. Dan pada kenyataannya mungkin terjadi lebih banyak lagi.

Namun, patut kita sayangkan pihak yang dirugikan ternyata mencari jalan "damai" dengan alasan penegakan hukum dalam kasus ini dapat mengganggu kepercayaan masyarakat terhadap sistem Internet Banking. Inilah salah satu gambaran pragmatisme pelaku bisnis kita, yang secara tidak langsung telah membunuh penegakan hukum melalui media internet di Indonesia. Untuk kasus sebesar ini saja, ternyata pihak yang dirugikan tidak bersedia menggunakan pendekatan hukum, belum lagi kerugian yang diderita oleh orang perorangan yang tidak dilaporkan oleh pihak berwajib, misalnya seorang yang kehilangan dana di rekeningnya setelah melakukan transaksi jual-beli di internet karena kredit cardnya telah di-*hack* seseorang. Berbagai kasus kejahatan komputer di Indonesia, wajar saja bila kita kesulitan untuk menghitung kerugian seseorang akibat kejahatan yang dilakukan melalui komputer.

Kejahatan Komputer/ Cyber Crime

Dengan semakin populernya Inter-Net sebagai (*the network of the networks*), masyarakat penggunanya (*internet global community*) seakan-akan mendapati suatu dunia baru yang dinamakan *cyberspace*, sebagaimana dipopulerkan oleh William Gibson dalam novel *scifinya Neuromancer* yang merupakan khayalan tentang adanya alam lain pada saat teknologi telekomunikasi dan informatika bertemu. Di alam baru ini bagi kebanyakan netter tidak ada hukum. Karena tidak adanya kedaulatan dalam jaringan komputer ini, mereka beranggapan bahwa tidak ada satupun hukum suatu negara yang berlaku, karena hukum network tumbuh dari kalangan mayarakat global penggunanya. "Alam baru" ini seakan-akan menjadi suatu jawaban dari impian untuk melampiaskan kebebasan berkomunikasi (*free flow of information*) dan kebebasan mengemukakan pendapat (*freedom of speech*) tanpa mengindahkan lagi norma-norma yang berlaku dalam kehidupan sehari-hari.

Substansi *cyberspace* sebenarnya adalah keberadaan informasi dan komunikasi yang dalam konteks ini dilakukan secara elektronik dalam bentuk visualisasi tatap muka interaktif. Komunikasi virtual (*virtual communication*) tersebut yang dipahami sebagai virtual reality sering disalahpahami sebagai "alam maya", padahal keberadaan sistem elektronik itu sendiri adalah konkrit di mana komunikasi virtual sebenarnya dilakukan dengan cara representasi informasi digital yang bersifat diskrit.

Sehubungan dengan itu, Wiener dan Bigelow mencetuskan *Cybernetics Theory*, mengenai suatu pendekatan interdisipliner terhadap sistem kendali dan komunikasi dari hewan, manusia, mesin dan organisasi. Uniknya teori tersebut sebenarnya lebih menekankan pada pentingnya umpan balik dari sistem komunikasi itu sendiri. Teori tersebut menyiratkan bahwa dalam memahami suatu informasi yang disampaikan pada suatu sistem komunikasi yang baik harus dengan memperhatikan umpan balik dari sistem tersebut. Sebagai catatan, Wiener juga mengakui bahwa istilah *Cyber* sebenarnya pernah digagas oleh Ampere yang namanya digunakan sebagai satuan kuat arus. Oleh karena itu jika ditilik dari asal usulnya, istilah *cyber* sebenarnya erat hubungannya dengan kawat listrik. Sehingga tidak mengherankan, jika istilah tersebut juga digunakan untuk organ buatan listrik *Cyborg* yang merupakan singkatan dari *Cybernetics Organics.*

Pada awalnya istilah *cyber law* sebagaimana dipahami oleh masyarakat sekarang ini kurang tepat jika digunakan untuk merujuk pada hukum yang tumbuh dalam medium *cyberspace* (Flamm, 1987) . Istilah *cyberspace law* justru lebih tepat untuk itu. Namun demikian, Istilah telematika paling tepat digunakan karena lebih memperlihatkan hakekat keberadaannya dan layak untuk digunakan sebagai definisi guna melakukan pengkajian hukum selanjutnya. Istilah telematika merujuk pada hakekat *cyberspace* sebagai suatu sistem elektronik yang lahir dari perkembangan dan konvergensi telekomunikasi, media dan informatika.

Dengan demikian kemajuan teknologi komputer, teknologi informasi, dan teknologi komunikasi menimbulkan suatu tindak pidana baru yang memiliki karakteristik yang berbeda dengan tindak pidana konvensional. Penyalahgunaan komputer sebagai salah satu dampak dari ketiga perkembangan tersebut tidak terlepas dari sifatnya yang khas sehingga membawa persoalan baru yang agak rumit untuk dipecahkan, berkenaan dengan masalah penanggulangannya.

Saat ini hampir seluruh organisasi tidak terlepas dari kemungkinan terjadinya kejahatan komputer atau pelanggaran komputer. Sebelumnya penting bagi penulis untuk menyampaikan berbagai teori dan definisi tentang kejahatan melalui komputer. Beberapa definisi mengenai kejahatan komputer atau penyalahgunaan komputer, antara lain:

Ade Maman Suparman (2005: 190), kejahatan komputer/ cyber crime adalah segala macam penggunaan jaringan komputer untuk tujuan kriminal dan atau kriminal berteknologi tinggi dengan menyalahgunakan kemudahan teknologi digital. Menurut beliau bentuk-bentuk kejahatan tersebut dapat berupa; *spionase*, informasi, pencurian data, pemalsuan *credit card*, penyebaran virus, pornografi anak, penyebaran e-mail bermasalah, hingga kampanye sara, terorisme dan *ekstriminimse* di internet.

Selanjutnya menurut Kongres PBB ke X, *cyber crime that ini the narrow sense means, any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them.* Dalam pengertian yang lebih luas lagi adalah *any illegal behaviour committed by means, or in relation to, a computer system or network, including such crimers as illegal possession, of fering or distributing information by means of a computer system or network.*

Kemudian definisi yang dikemukakan oleh *Organization of European Community Development* (OECD), bahwa *Any illegal, unethicall or unauthorized behavior relating to the authomatic processing and/or the transmission of data.* Definisi tersebut menyatakan kejahatan komputer termasuk segala akses illegal atau secara tidak sah terhadap suatu transmisi data. Di sini terlihat bahwa segala aktifitas yang tidak sah dalam suatu sistem komputer merupakan kejahatan.

Sementara pendapat yang dikemukakan oleh Andi Hamzah lebih memperluas pengertian dengan mengemukakan bahwa pengertian kejahatan komputer adalah segala aktifitas tidak sah yang memanfaatkan komputer untuk tidak pidana. Sekecil apapun dampak atau akibat yang ditimbulkan dari penggunaan komputer secara tidak sah atau ilegal merupakan suatu kejahatan.

Varian Dan Bentuk *Cyver Crime*

Pada dasarnya manifestasi dari *cyber crime* muncul dalam berbagai macam atau varian seperti berikut ini:

Pertama, *Recreational hackers*, yaitu suatu kejahatan yang dilakukan oleh *netter* tingkat pemula untuk sekedar mencoba, kekuranghandalan sistem sekuritis suatu perusahaan.

Kedua, *criminal minded hackers*, yaitu pelaku kejahaan biasanya memiliki motivasi untuk mendapatkan keuntungan finansial, sabotase dan penghancuran data.

Ketiga, *political hacker*, yaitu melakukan pengrusakan terhadap ratusan situs web untuk mengkampanyekan program-programnya, bahkan tidak jarang dipergunakan untuk menempelkan pesan untuk mendiskreditkan lawannya.

Keempat, *denial of service attack* atau *unprecedented* yaitu bertujuan untuk memacetkan sistem dengan menggangu akses dari pengguna yang *legitimate*. Taktik yang dipergunakan adalah dengan mengirim atau membanjiri situs web dengan data yang tidak perlu. Pemilik situs *web* menderita kerugian karena untuk mengendalikan atau mengontrol kembali situs *web* memakan waktu yang tidak sedikit.

Kelima, *insiders* atau *internal hackers* yaitu kejahatan yang dilakukan dalam perusahan sendiri. Modus operandinya dengan menggunakan karyawan yang kecewa atau bermasalah dengan perusahaan.

Keenam, viruses, yaitu program penggangu dengan penyebaran virus yang dapat menular ke aplikasi internet. Sebelumnya pola penularan virus hanya bisa melalui floppy disk.

Ketujuh, *piracy* atau pembajakan komputer yaitu pihak produsen *software* dapat kehilangan *profit* karena karyanya dapat dibajak melalui *download* dari internet dan di *copy* dalam *CD ROOM*, yang selanjutnya di perbanyak secara ilegal atau tanpa seijin penciptanya.

Kedelapan, *Fraud* yaitu segala jenis manipulasi informasi keuangan dengan tujuan mengeruk keuntungan sebesar-besarnya, sebagai contoh adalah harga tukar saham yang menyesatkan melalui rumor. Situs lelang fiktif dengan mengeruk uang masuk dari peserta lelang dan baranngnya telah dikirim, bahkan identitas pelakunya tidak dapat dilacak.

Kesembilan, *gambling* atau perjudian di dunia *cyber* yang berskala global sulit dijerat dengan hukum nasional. Kegiatan *gambling* dapat diputar kembali di negara yang merupakan *tex heaven* seperti Cayman Islands merupakan surga bagi *money laundring*, bahkan termasuk di Indonesia sering dijadikan sebagai negara tujuan *money laundring* yang uangnya diperoleh dari hasil kejahatan yang berskala International.

Kesepuluh, *pornography*. Sisi gelap dunia *cyber* selain mendatangkan berbagai kemudahan dengan mengatasi kendala dan ruang dan waktu, di sisi lain *cyber space* telah melahirkan dunia *pornography* yang megkhawatirkan berbagai kalangan. Hal ini dapat dilakukan dengan cara *cyber stalking*. *Cyber stalking* sendiri dapat dimaknai sebagai segala bentuk kiriman *e-mail* yang tidak dikehendaki oleh *user* yang sering memadati *folder* serta tidak jarang dengan pemaksaan walaupun email sampah itu tidak dikehendaki oleh *user*, bahkan tidak jarang secara paksa memperoleh identitas personal secara detail calon para korbannya.

Kesebelas, *hate sites*. Situs ini sering dipergunakan untuk saling menyerang dan melontarkan komentar-

komentar yang tidak sopan dan *vulgar* yang dikelola oleh para *ekstrimis*. Penyerangan terhadap lawan atau *oppenent* sering mengangkat isu rasial, perang program, dan promosi kebijakan atau suatu pandangan.

Keduabelas, *criminal communications*. Pada dasarnya para ahli yang mengeluti komputer telah mendeteksi bahwa teknologi komputer telah dijadikan sebagai alat yang handal dan modern untuk melakukan komunikasi antar para *gangster*, anggota sindikat obat bius, komunikasi antar *hooligan* di dunia sepak bola.

Selain varian dan bentuk seperti yang diuraikan di atas, ahli komputer dari Jerman yakni Sieber mengklasifikasikan kejahatan komputer sebagai berikut: Pertama, *fraud by computer manipulation*. Kedua, *computer espionage and software theft*. Ketiga, *computer sabotage*. Keempat, *theft or service*. Kelima, *unauthorized access to data processing system*. Keenam, *traditional business offences assited by data processing*.

Di Indonesia pola-pola kriminalitas atau *modus operandi* berbasikan teknologi digita sempat dialami di beberapa tempat. Misalnya dibulan Januari 1986 muncul kasus pembobolan Hongkong Bank di Jakarta yang mengakibatkan kerugian 96 Miliar. Selain itu ada juga kejadian bulan April 2001 tentang kasus penyadapan kartu kredit di Surabaya dan Denpasar (Suherman, 2005: 193).

Teknologi digita komputer telah melahirkan tantangan tersendiri bagi *law maker* dan penegak hukum dalam menghadapi kasus transaksi melalui *electronic transfer*. Pada umumnya kesulitan yang dihadapi penegak hukum adalah, masalah pengenaan hukum yang tepat kepada tersangka. Penerapan pasal yang disangkakan terhadap tersangka masih menjadi persoalan karena berkaitan dengan teknologi/ jaringan akses komunikasi (Pasal 362 KUHP atau 378 KUHP atau UU No 36 tahun 1999 tentang Telekomunikasiyang sekarang sudah diganti dengan UU No 11 tahun 2008 tentang Informasi dan Transaksi Elektronik). Kesulitan lain yang dihadapi adalah kemampuan penyidik terhadap pengetahuan komputer sangat kurang/terbatas.

Kebijakan Hukum Terhadap Kejahatan Komputer

Perkembangan global internet menyiratkan adanya harapan-harapan akan terjadinya perubahan ruang dan jarak. Perkembangan tersebut juga diramalkan akan menuju pada terbentuknya entitas dengan sistem tingkah laku tertentu, melalui pola-pola pengujian dengan unsur-unsur dominan berupa pengalaman dan budaya dalam penggunaan informasi. Semua itu pada gilirannya harus diakui oleh hukum mana pun di semua belahan bumi, yang tentu saja berbeda-beda impaknya terhadap kaitan antara hukum dengan ekonomi, politik ataupun ideologi.

Hubungan antara hukum dan teknologi internet tentu saja akan menjadi unik. Dunia *cyber* sebagai manifestasi sistem informasi dan telekomunikasi yang terpadu dalam suatu jaringan global, adalah ruang tanpa batas yang dapat diisi dengan sebanyak mungkin kategori. Baik yang sudah ada, akan ada, dan mungkin akan terus berkembang. Mulai perdagangan,

perhubungan, kesehatan, sampai militer, dan sebagainya, dan seterusnya. Bahkan anda sendiri dapat membentuk komunitas dari tingkatan keluarga, arisan sampai pada tingkatan sebuah negara di dunia *cyber* yang tiada batas (*unlimited world*).

Hukum dan alat perlengkapannya tentu juga terus berkembang. Dengan demikian yang menjadi masalah adalah apakah hukum dapat berkembang sepesat dan secepat perkembangan dunia cyber? Bahkan pada taraf *unlimited* yang bisa melanda semua kategori yang sempat terpikirkan manusia seperti UU *Commerce*. Terus berkembangnya pemanfaatan teknologi internet untuk berbagai kegiatan konvensional sehari-hari telah membuka jalan bagi kebebasan cyber. Baik untuk kegiatan bisnis maupun dalam kegiatan awam sehari-hari, segala sesuatu yang terjadi dalam dunia *cyber* dapat dilakukan dengan mudah, bebas, canggih, cepat, efisien. Tak perlu lagi bertemu muka secara langsung. Semua ini tentu akan menimbulkan masalah apabila tidak atau belum secara utuh diatur oleh hukum.

Secara definitif, kebijakan publik adalah perbuatan hukum atau keputusan hukum yang dilaksanakan oleh pejabat pemerintah yang fungsinya adalah mengarahkan jalannya kehidupan masyarakat. Dalam konteks munculnya istilah *cyber crime*, maka idealnya kebijakan publik yang dimaksudkan di sini adalah menyangkut kebijakan hukum itu sendiri terhadap *cyber crime*.

Di negara-negara maju seperti Amerika Serikat, menyadari bahwa cyber crime yang serius telah mengadakan upaya bersiaga mengembangkan polisi cyber serta telah membentuk Computer Emergency Response Team (CERT). Sementara di negara-negara Eropa seperti Inggris, Italia, Prancis Dan Jerman telah membentuk suatu institusi yang ditugaskan untuk cyber crime investigation dengan nama National Criminal Intellegence Service (NCIS).

Perserikatan Bangsa-Bangsa (PBB) sendiri dalam Kongres ke VIII tentang *Prevention Of Crime And The Treatment Of Offenders*, membahas pencegahannya,dengan menghasilkan beberapa rekomendasi sebagai berikut:

1. menghimpun negara anggota untuk mengintensifkan upaya-upaya preventif dalam menangulangi penyalahgunaan komputer dengan tindakan sebagai berikut:
   a. melakukan modernisasi hukum pidana formil maupun materil;
   b. tindakan pencegahan dan pengamanan komputer;
   c. meningkatkan kepekaan warga masyarakat dan aparat penegak hukum terhadap pentingnya pencegahan kejahatan komputer;
   d. training atau pelatihan bagi penegak hukum, khususnya mendalami kejahatan ekonomi dan computer crime;
   e. dalam kerangka edukasi, etika penggunaan komputer menjadi kurikulum bidang studi informatika;
   f. mengadopsi kebijakan perlindungan korban kejahatan komputer serta

menyadari pentingnya korban untuk melapor.

2. para negara anggota untuk berpartisipasi aktif dalam Forum Internasional yang menyangkut pencegahan kejahatan komputer;
3. merekomendasikan pada Commite On Crime Prevention Control yang merupakan unit PBB untuk melakukan diseminasi membantu negara anggota dalam menghadapi kejahatan komputer. Mempertimbangkan kasus kejahatan dalam hal mengimplementasikan perjanjian ekstradisi di bidang *cyber crime*.

Dalam konteks hukum nasional, upaya pengembangan teknologi komputer yang lebih terstruktur kemudian dilakukan melalui serangkaian kebijakan hukum yang dimulai sejak dikeluarkannya Keppres No. 186 tahun 1998 tentang Tim Koordinasi Telematika Indonesia (TKTI). Susunan keanggotaan TKTI tersebut dalam perkembangannya diatur kembali dan ditetapkan dengan Keppres No. 50 tahun 2000. Berdasarkan Keppres tersebut, terdapat 4 tugas utama TKTI, yaitu: Pertama, merumuskan kebijaksanaan pemerintah di bidang telematika. Kedua, menetapkan pentahapan dan prioritas pembangunan serta pemanfaatan telematika di Indonesia. Ketiga, melakukan pemantauan dan pengendalian atas penyelenggaraan telematika di Indonesia. Keempat, melaporkan perkembangan Telematika di Indonesia kepada Presiden.

Selanjutnya pada tanggal 21 Februari 2001, Presiden RI yang kala itu dijabat oleh Abdurrahman Wahid mengeluarkan 2 buah Instruksi Presiden yang sangat terkait dengan pengembangan teknologi komputer. Pertama, Inpres No. 1 tahun 2001 tentang Pusat Informasi Berbasis Teknologi Informatika di Komplek Kemayoran. Kedua, Inpres No. 2 tahun 2001 tentang Penggunaan Komputer Dengan Aplikasi Berbahasa Indonesia.

Kemudian pada tanggal 26 April 2001, dikeluarkan Inpres No. 6 tahun 2001 tentang Pengembangan dan Pendayagunaan Telematika di Indonesia. Inpres ini memuat Kerangka Kebijakan Pengembangan dan Pendayagunaan teknologi komputer di Indonesia. Arah pengembangan teknologi komputer sebagaimana dimaksud dalam kerangka kebijakan tersebut terdiri dari:

a. teknologi komputer untuk mempersatukan bangsa dan memberdayakan rakyat;
b. teknologi komputer dalam masyarakat dan untuk masyarakat;
c. teknologi komputer merupakan Infrastruktur Informasi Nasional;
d. teknologi komputer merupakan usaha sektor swasta dan iklim usaha;
e. peningkatan kapasitas dan teknologi;
f. Government On-line;
g. Membentuk Tim Koordinasi Telematika Indonesia.

Selanjutnya Indonesia juga harus memperhatikan pengaturan hukum teknologi komputer terutama mengenai *cyber crime* yang ada dalam KUHP, yang semakin tertinggal jauh dari perkembangan komputer itu sendiri. Setidaknya ada beberapa hal yang harus dilakukan untuk memperbaharui buku II KUHP yang mengatur tindak pidana. Tim perumus

KUHP baru Indonesia harus benar-benar kerja keras untuk menafsirkan kejahatan dengan menggunakan komputer.

Perkembangan teknologi informasi yang telah diuraikan di atas menunjukkan eksistensinya sebagai suatu arena tempat berbagai kepentingan masyarakat saling bersaing. Pada titik inilah hukum dengan kekuatan memaksanya dalam mengatur perilaku pemerintah dan masyarakat memiliki kedudukan yang penting sebagai sarana untuk mengelola konflik. Tujuannya tentu saja adalah kesejahteraan sosial sesuai dengan prinsip negara modern yang dianut Indonesia. Dengan demikian, agar hukum tersebut dapat terlaksana dengan baik, pemerintah seharusnya dapat memahami terlebih dahulu perspektif dari masyarakat yang bersangkutan.

Mengacu pada berbagai kebijakan publik yang terkait dengan telematika tersebut, pemerintah melakukan pendekatan yang berbeda dengan yang pernah dilakukan oleh pemerintah Amerika Serikat. Sebagaimana telah diuraikan sebelumnya, pemerintah Amerika Serikat memprioritaskan kepentingan pertahanan keamanan nasional terlebih dahulu sebelum membuat kebijakan untuk mendorong sektor sosial dan ekonomi yang terkait. Kebijakan tersebut terbukti memajukan riset dan pengembangan teknologi telematika, sehingga secara teknis Amerika Serikat telah memiliki basis yang tangguh untuk pengembangannya lebih lanjut.

Sebaliknya Indonesia mengalami tahap perkembangan teknologi telematika yang sangat berbeda dengan Amerika Serikat. perbedaan yang cukup signifikan adalah kenyataan praktek di mana Amerika Serikat telah menjadi bangsa *inventor*, Indonesia justru masih menjadi bangsa *user*. Kesenjangan yang dibahasakan sebagai digital divide tersebut memang telah coba diatasi dengan mengeluarkan Inpres No. 6 tahun 2001. Akan tetapi, walaupun penyusunan materinya telah diupayakan komprehensif, Inpres tersebut gagal dalam menjelaskan masalah terpenting yang dihadapi bangsa Indonesia dengan adanya *digital divide* tersebut. Selanjutnya Inpres tersebut juga tidak menjelaskan sama sekali karakter, sikap, atau pandangan hidup dari masyarakat yang bersangkutan, sehingga tidak jelas keterkaitan yang spesifik antara arahan-arahan tersebut dengan manfaatnya bagi masyarakat yang bersangkutan.

Penutup

Kejahatan *cyber* dalam komunitas global masyarakat pengguna internet adalah suatu hal yang dapat disadari atau tanpa disadari, sengaja atau tidak sengaja dilakukan. Hal ini terjadi karena perkembangan tekhnologi informasi dan tingkat intelektualitas/intelegensia masyarakat yang semakin meningkat.

Menguatnya eksistensi negara modern membuat hukum menjadi pijakan yang sangat dibutuhkan masyarakat dalam melakukan berbagai aktifitasnya. Walaupun bukan satu-satunya motif, namun masyarakat tampaknya menilai bahwa sistem hukum nasional, khususnya berbagai peraturan yang ada, belum cukup

menjamin adanya perlindungan secara memadai. Oleh karenanya, tuntutan-tuntutan untuk membentuk atau merevisi berbagai peraturan yang sudah ada kerap dikemukakan baik melalui forum diskusi publik, kalangan lembaga swadaya masyarakat, maupun dari kalangan akademisi. Pemerintah sebagai institusi yang memiliki otoritas tampaknya juga tanggap terhadap tuntutan tersebut, sehingga dampak negatif kemajuan teknologi komputer tidak akan terasa.

Daftar Pustaka

Flamm, Kenneth, 1987, *Targeting the Computer-Government Support and International Competition*, The Brookings Institution, Washington D.C

Hamzah, Andi , *Aspek-aspek Pidana di Bidang Komputer*,

Suherman, Ade Maman, 2005, *Aspek Hukum Dalam Ekonomi Global*, Cetakan Kedua, Ghalia Indonesia. Bogor.

Unions Nations Conggres X, *Workshop On Crimes Related To The Computer Network*, Back Ground Paper, tanpa tahun.

Yaffe, David, James Petras, Peter Marcuse, William K. Tabb, 2001, *Globalisasi Dalam Perspektif Sosialis*, diterjemahkan oleh Ken Budha Kusumandaru & Sutardji, Cubuc dan Sumbu, Yogyakarta.

Kitab Undang- Undang Hukum Pidana (KUHP)

UU No 32 tahun 2002 tentang *Penyiaran*.

UU No 11 tahun 2008 tentang *Informasi Teknologi dan Elektronik*

Inpres No. 2 tahun 2001 tentang *Penggunaan Komputer Dengan Aplikasi Berbahasa Indonesia*

Inpres No. 6 tahun 2001 tentang *Pengembangan dan Pendayagunaan Telematika di Indonesia*

Keppres No. 186 tahun 1998 tentang *Tim Koordinasi Telematika Indonesia* (TKTI)