KEBIJAKAN FORMULASI HUKUM PIDANA TERHADAP TINDAK PIDANA TEKNOLOGI INFORMASI

SKRIPSI

Diajukan Sebagai Salah Satu Syarat
Untuk Menempuh Ujian
Sarjana Hukum

Oleh:

RAHMAT HIDAYAT
50 2011 376

FAKULTAS HUKUM
UNIVERSITAS MUHAMMADIYAH PALEMBANG
2015

UNIVERSITAS MUHAMMADIYAH PALEMBANG
FAKULTAS HUKUM

PERSETUJUAN DAN PENGESAHAN

Judul Skripsi : KEBIJAKAN FORMULASI HUKUM PIDANA TERHADAP TINDAK PIDANA TEKNOLOGI INFORMASI

Nama : **RAHMAT HIDAYAT**
Nim : **50 2011 041**
Program Studi : **Ilmu Hukum**
Program Kekhususan : **Hukum Pidana**

Pembimbing,

Reny Okprianti, SH., M.Hum. ( )

Palembang, 2015

PERSETUJUAN OLEH TIM PENGUJI:

Ketua : **Nur Husni Emilson, S.H., Sp.N., MH** ( )

Anggota : **1. Hendri S, S.H., M.Hum** ( )

2. Dr. Hj. Lilies Anisa, SH., MH. ( )

DISAHKAN OLEH
DEKAN FAKULTAS HUKUM
UNIVERSITAS MUHAMMADIYAH PALEMBANG

Dr. Hj. SRI SUATMIATI, SH, M.Hum
NBM/NIDN 791348/0006046009

MOTTO :

Yakinlah ada sesuatu yang menantimu selepas banyak kesabaran (yang kujalani) yang akan membuatmu terpana hingga kau lupa pedihnya rasa sakit.

(Iman Ali bin Ali Thalib AS)

Kupersembahkan kepada:

- *Ayahanda Agusdin dan Ibunda Asmawati*
- *Saudara-saudaraku tersayang*
- *Seseorang yang akan mendampingiku*
- *Ira Novita, SH & M. Rizki Alkahfi*
- *Sahabat-sahabatku*
- *Alamamaterku.*

Judul Skripsi: KEBIJAKAN FORMULASI HUKUM PIDANA TERHADAP TINDAK PIDANA TEKNOLOGI INFORMASI

Penulis,
RAHMAT HIDAYAT

Pembimbing,
RENY OKPRIANTI, SH., M.Hum

ABSTRAK

Yang menjadi permasalahan adalah:

1. Bagaimanakah kebijakan formulasi hukum pidana terhadap tindak pidana teknologi informasi
2. Bagaimanakah kebijakan penegakan hukum dalam upaya penanggulangan tindak pidana teknologi informasi ?

Selaras dengan tujuan yang bermaksud menelusuri prinsip-prinsip hukum, terutama yang ada sangkut paut dengan kebijakan penanggulangan tindak pidana teknologi informasi melalui hukum pidana, maka jenis penelitiannya adalah penelitian hukum *normatif* yang bersifat *deskriptif* (menggambarkan) dan tidak bermaksud untuk menguji hipotesa.

Teknik pengumpulan data

Teknik pengumpulan data sekunder dititik beratkan pada penelitian kepustakaan (*library research*) dengan cara mengkaji:

a. Bahan hukum primer, yaitu bahan hukum yang bersifat mengikat seperti undang-undang, peraturan pemerintah, dan semua ketentuan peraturan yang berlaku
b. Bahan hukum sekunder, yaitu bahan hukum seperti hipotesa, pendapat para ahli maupun peneliti terdahulu, yang sejalan dengan permasalahan dalam skripsi ini
c. Bahan hukum tersier, yaitu bahan hukum yang menjelaskan bahan hukum primer dan bahan hukum sekunder seperti kamus bahasa, ensiklopedia, dan lainnya.

Teknik pengolahan data

Setelah data terkumpul, maka data tersebut diolah guna mendapatkan data yang terbaik. Dalam pengolahan data tersebut, penulis melakukan kegiatan editing, yaitu data yang diperoleh diperiksa da diteliti lagi mengenai kelengkapan, kejelasan dan kebenarannya, sehingga terhindar dari kekurangan dan kesalahan.

Analisa data

Analisa data dilakukan secara *kualitatif* yang dipergunakan untuk mengkaji aspek-aspek *normatif* atau *yuridis* melalui metode yang bersifat *deskriptif analitis* yang menguraikan gambaran dari data yang diperoleh dan

menghubungkan satu sama lain untuk mendapatkan suatu kesimpulan yang bersifat umum.

Berdasarkan hasil penelitian dapat disimpulkan sebagai berikut:

1. Kebijakan formulasi hukum pidana terhadap tindak pidana teknologi informasi adalah: Harus memperhatikan harmonisasi internal dengan sistem hukum pidana atau aturan pemidanaan umum yang berlaku saat ini. Tidaklah dapat dikatakan terjadi harmonisasi/sinkronisasi apabila kebijakan formulasi berada diluar sistem hukum pidana yang berlaku saat ini.
2. Kebijakan penegakan hukum dalam upaya penanggulangan tindak pidana teknologi informasi adalah:
    a. Adanya aturan perundang-undangan khusus yang mengatur dunia *cyber*
    b. Adanya lembaga yang akan menjalankan peraturan yaitu polisi, jaksa dan hakim khusus mengenai *cybercrime*
    c. Adanya fasilitas atau sarana untuk mendukung pelaksanaan peraturan itu
    d. Kesadaran hukum dari masyarakat yang terkena peraturan.

KATA PENGANTAR

Assalamu'alaikum Wr. Wb.

Alhamdulillah penulis panjatkan puji syukur kehadirat Allah SWT, serta shalawat dan salam kepada junjungan kita Nabi Besar Muhammad SAW beserta keluarga dan para sahabat, penulis dapat menyelesaikan skripsi ini dengan judul: ***"KEBIJAKAN FORMULASI HUKUM PIDANA TERHADAP TINDAK PIDANA TEKNOLOGI INFORMASI"***

Penulisan skripsi ini adalah untuk memenuhi syarat mendapatkan gelar Sarjana Hukum pada Fakultas Hukum Universitas Muhammadiyah Palembang.

Penulis menyadari bahwa skripsi ini masih banyak kekurangan, kekeliruan, dan kekhilafan semua ini tidak lain karena penulis adalah sebagai manusia biasa yang tak luput dari kesalahan dan banyak kelemahan, akan tetapi berkat adanya bantuan dan bimbingan serta dorongan dari berbagai pihak, akhirnya kesukaran dan kesulitan tersebut dapat dilalui oleh karena itu dalam kesempatan ini penulis menyampaikan rasa terima kasih yang mendalam kepada:

1. Bapak Dr. H.M.Idris, SE., Msi, selaku Rektor Universitas Muhammadiyah Palembang.
2. Ibu Dr. Hj. Sri Suatmiati, SH., M.Hum, selaku Dekan Fakultas Hukum Universitas Muhammadiyah Palembang.
3. Wakil Dekan I, II, III dan IV Fakultas Hukum Universitas Muhammadiyah Palembang.

4. Ibu Luil Maknun, SH., MH, selaku Ketua Bagian Hukum Pidana pada Fakultas Hukum Universitas Muhammadiyah Palembang.
5. Ibu Reny Okprianti,SH., M.Hum, selaku Pembimbing Skripsi yang telah banyak memberikan petunjuk-petunjuk dan arahan-arahan dalam penulisan dan penyusunan skripsi ini.
6. Ibu Khalisah Hayatuddin, SH., M.Hum, selaku Pembimbing Akademik pada Fakultas Hukum Universitas Muhammadiyah Palembang.
7. Bapak dan Ibu Dosen serta Karyawan dan Karyawati Fakultas Hukum Universitas Muhammadiyah Palembang.
8. Ayahanda dan Ibunda, Kakanda dan Adinda, serta seluruh keluarga yang telah banyak memotivasi penulis untuk meraih gelar kesarjanaan ini.

Semoga skripsi ini dapat memberikan manfaat bagi semua pihak yang membacanya, akhirnya segala kritik dan saran penulis terima guna perbaikan dimasa-masa mendatang.

Wassalamu'alaikum Wr. Wb.

Palembang, Pebruari 2015

Penulis,

RAHMAT HIDAYAT

DAFTAR ISI

Halaman

BAB. I

PENDAHULUAN

A. Latar Belakang

Pada awal sejarah, manusia bertukar informasi melalui bahasa. Maka bahasa adalah teknologi. Bahasa memungkinkan seseorang memahami informasi yang disampaikan oleh orang lain. Tetapi bahasa yang disampaikan dari mulut ke mulut hanya bertahan sebentar saja, yaitu hanya pada saat si pengirim menyampaikan informasi melalui ucapannya itu saja. Setelah ucapan itu selesai, maka informasi yang berada di tangan si penerima itu akan dlupakan dan tidak bisa disimpan lama. Selain itu jangkauan suara juga terbatas. Untuk jarak tertentu, meskipun masih terdengar, informasi yang disampaikan lewat bahasa suara akan terdegradasi bahkan hilang sama sekali.

Penemuan teknologi elektronik seperti radio, tv, komputer mengakibatkan informasi menjadi lebih cepat tersebar di area yang lebih luas dan lebih lama tersimpan. Dalam perkembangnnya, kolaborasi antara penemuan komputer dan penyebar informasi melalui komputer melahirkan apa yang dikenal dengan istilah *internet* (*internconnected network*-jaringan yang saling terhubung).

Revolusi tersebut tidak dapat dipungkiri menjadi ujung tombak era globalisasi yang kini melanda hampir seluruh dunia. Apa yang disebut dengan globalisasi pada dasarnya bermula dari abad ke-20, yakni pada saat terjadi revolusi transportasi dan elektronik yang menyebarluaskan dan mempercepat

perdagangan antar bangsa, disamping pertambahan dan kecepatan lalu lintas barang dan jasa.

Proses globalisasi tersebut melahIrkan fenomena yang mengubah model komunikasi konvensional dengan melahirkan kenyataan dalam dunia maya (*virtual reality*) yang dikenal sekarang ini dengan *internet*. *Internet* berkembang demikian pesat sebagai kultur masyarakat modern, dikatakan sebagai kultur karena melalui *internet* berbagai aktifitas masyarakat *cyber* seperti berpikir, berkreasi, dan bertindak dapat dekspresikan didalamnya, kapanpun dan dimanapun. Kehadirannya telah mebentuk dunia tersendiri yang dikenal dengan dunia maya (*cyberspace*) atau dunia semu yaitu sebuah dunia komunikasi berbasis komputer yang menawarkan realitas yang baru berentuk *virtual* (tidak langsung dan tidak nyata).[1]

Komunitas masyarakat yang ikut bergabung didalamnya pun kian hari semakin meningkat. Kecenderungan masyarakat untuk berkonsentrasi dalam *cyberspace* merupakan bukti bahwa *internet* telah membawa kemudahan-kemudahan bagi masyarakat. Bagi sebagian orang munculnya fenomena ini telah mengubah perilaku manusia dalam berinteraksi dengan manusia lain, baik secara individual maupun secara kelompok. Di samping itu, kemajuan teknlogi tentunya akan berjalan bersama dengan munculnya perubahan-perubahan di bidang kemasyarakatan.

---

[1]Agus Rahardjo, *Cybercrime Pemahaman Dan Upaya Pencegahan Kejahatan Berteknologi*, Citra Adtya Bakti, Bandung, 2002, hlm. 20

Sebagaimana dikatakan Satjipto Raharjo,[2] banyak alasan yang dapat dikemukakan sebagai penyebab timbulnya suatu perubahan di dalam masyarakat tetapi perubahan dalam penerapan hasil-hasil teknologi modern dewasa ini banyak disebut-sebut sebagai salah satu sebab bagi terjadinya perubahan sosial. Perubahan-perubahan tersebut dapat mengenai nlai-nilai sosial, pola-pola perikelakuan, organisasi, susunan lembaga-lembaga masyarakat dan wewenang interaksi sosial dan lain sebagainya.

Kemajuan teknologi informasi khususnya media *internet,* dirasakan banyak memberikan manfaat seperti dari segi keamanan, kenyamanan dan kecepatan. Contoh sederhana, dengan dipergunakan *internet* sebaga sarana pendukung dalam pemesanan/reservasi tiket (pesawat terbang, kereta api), hotel, pembayaan taghan telepon, listrik, telah membuat konsumen semakin nyaman dan aman dalam mejalankan aktivitasnya. Kecepatan melakukan transaksi perbankan melalui *e-banking*, memanfaatkan *e-commerce* untuk mempermudah melakukan pembelian dan penjualan suatu barang serta menggunakan *e-library* dan *e-learning* untuk mencari referensi atau informasi ilmu pengetahuan yang dilakukan secara *on line* karena dijembatani oleh teknologi *internet* baik melalui komputer atau pun *hand phone*.

Pemanfaatan teknologi *internet* juga tidak dapat dipungkiri membawa dapak negatif yang tidak kalah banyak dengan manfaat positif yang ada. *Internet* membuat kejahatan yang selama ini bersifat konvensional seperti pengancaman, pencurian, pencemaran nama baik, pornografi, perjuadian penipuan hingga tindak

---

[2]Satjipto Rahardjo, *Hukum Dan Masyarakat*, Angkasa, Bandung, 1980, hlm. 96

pidana terorisme kini melalui media *internet* beberapa jenis tindak pidana tersebut dapat dilakukan secara *on line* oleh individu maupun kelompok dengan resiko tertangkap yang sangat kecil denga akibat kerugian yang lebih besar baik untuk masyarakat maupun negara.

Perkembangan teknlogi infrmasi yang demikian pesatnya haruslah diantisipasi dengan hukum yang mengaturnya. Dampak negatif tersebut harus diantisipasi dan ditanggulangi dengan hukum yang terkait kejahatan teknologi informasi dan komunikasi. Secara internasioanal hukum yang terkait kejahatan teknologi informasi digunakan adalah hukum tegnlogi informasi (*law of information technology*), hukum dunia maya (*virtual world law*) dan hukum mayantara. Sejalan dengan istilah tersebut Barda Nawawi Arief menyatakan:[3] tindak pidana mayantara, identik dengan tindak pidana di ruang siber (*cyber space*) atau yang biasa juga dikenal dengan *cybercrime*.

Sehubungan dengan tindak pidana di dunia maya yang terus berkembang pemerintah telah melakukan kebijakan dengan terbitnya Undang-undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang diundangkan pada tanggal 21 April 2008. Undang-undang ITE merupakan payung hukum pertama yang mengatur khusus terhadap dunia maya (*cyber law*) di Indonesia.

\Berbagai komentar di media televisi, surat kabar, majalah maupun komunitas dunia maya bermunculan terhadap keluarnya UU ITE. Pada saat seminar dan sosialisasi Undang-undang Informasi dan Transaksi Elektronik yang

---

[3]Barda Nawawi Arief, *Sari Kuliah Perbandingan Hkum Pidana*, Raja Grafindo Persada, Jakarta, 2006, hlm. 268

diadakan BEM Fisikom Universitas Indnesia, beberapa masaah yang diangkat oleh para peserta seminar seperti pasal tentang penghinaan dan pencemaran nama baik yang dianggap membelenggu kebebasan berekspresi, pasal mengenai pornografi, kesiapa aparat serta belum termuatnya aturan terhadap *spamming*, *warm* juga virus komputer di dalam undang-undang tersebut.

Opini yang bersifat pro maupun kontra terhadap pemidanaan di dunia maya memang wajar dalam iklim demokrasi serta kebebasan berpendapat sekarang ini. Pemidanaan terhadap larangan-larangan di dalam UU ITE dikarenakan kegiatan di alam maya (*cyber*) meskipun bersifat virtual tetapi dikatagorikan sebagai tindakan dan perbuatan hukum yang nyata. Secara yuridis untuk ruang siber sudah tidak pada tempatnya lagi untuk mengkatagorikan sesuatu dengan ukuran dan kualitas konvensional untuk dapat dijadikan obyek dan perbuatan, sebab jika cara ini yang ditempuh akan terlalu banyak kesulitan dan hal-hal yang lolos dari jerat hukum. Kegiatan *cyber* adalah kegiatan virtual tetapi berdampak sangat nyata meskipun alat buti bersifat elektronik, dengan demikian subyek pelakunya harus dikualifikasikan pula sebagai telah melakukan perbuatan hukum secara nyata.

Menurut Barda Nawawi Areif, kebijakan kriminal merupakan suatu kebijakan dalam menetapkan suatu perbuatan yang semula bukan tindak pidana (tidak dipidana). Jadi pada hakekatnya, kebijakan krimnalisasi terhadap tindak pidana teknologi informasi merupakan bagian dari kebijakan kriminal (*criminal policy*) dengan menggunakan sarana hukum pidana (*penal*) dan oleh karena itu termasuk bagian dari "kebijakan hukum pidana" (*penal policy*), khususnya

kebijakan formulasinya. Selanjutnya menurut Barda Nawawi Arief kebijakan kriminal bukan sekedar kebijakan menetapkan/merumuskan/memformulasikan perbuatan apa yang dapat dipidana (termasuk sanksi pidananya), melainkan juga mencakup masalah bagaimana kebijakan formulasi/legislasi itu disusun dalam suatu kesatuan sistem hukum pidana (kebijakan legislatif) yang harmonis da terpadu.[4]

Bertolak dari pengertian di atas maka upaya atau kebijakan untuk melakukan penanggulangan tindak pidana di bidang teknologi informasi yang dilakukan dengan menggunakan "*penal*" (hukum pidana), maka dibutuhkan kajian terhadap materi/substansi (*legal substance reform*) tindak pidana teknologi informasi saat ini. Dalam penanggulangan melalui hukum pidana (*penal policy*) perlu diperhatikan bagaimana memformulasikan (kebijakan legistatif) suatu peraturan perundang-undangan yang tepat untuk menanggulangi tindak pidana di bidang teknologi informasi pada masa yang akan datang, seta bagaimana mengaplikasikan kebijakan legislatif (kebijakan yudikatif/yudisial atau penegaka nukum pidana *in concreto*) tersebut oleh aparat penegak hukum atau pengadilan.

Bertitik tolak dari Latar belakang tersebut di atas, penulis merasa tertarik untuk melakukan penelitian lebih mendalam yang hasilnya akan dituangkan kedalam tulisan yang berbentuk skripsi dengan judul: "KEBIJAKAN FORMULASI HUKUM PIDANA TERHADAP TINDAK PIDANA TEKNOLOGI INFORMASI"

---

[4]Barda Nawawi Arief, *Kapita Selekta Hukum Pidana*, Citra Aditya Bakti, Bandung, 2003, hlm. 259

B. Permasalahan

Adapun yang menjadi perasalahan adalah sebaga berikut:

1. Bagaimanakah kebijakan formulasi hukum pidana terhadap tindak pidana teknologi informasi ?
2. Bagaimanakah kebijakan penegakan hukum dalam upaya penanggulangan tindak pidana teknologi informasi ?

C. Ruang Lingkup dan Tujuan

Ruang lingkup penelitian terutama dititik beratkan pada penelusuran terhadap kebijakan formulasi hukum pidana terhadap tindak pidana teknologi informasi saat ini dan kebijakan penegakan hukum dalam penanggulangan tindak pidana teknologi informasi, tanpa menutup kemungkinan menyinggung pula hal-hal lain yang ada kaitannya.

Tujuan penelitian adalah:

1. Untuk mengetahui dan menjelaskan kebijakan formulasi hukum pidana terhadap tindak pidana teknologi informasi sat ini.
2. Untuk mengetahui dan memahami kebijakan penegakan hukum dalam upaya penanggulangan tindak pidana teknologi informasi.

Hasil penelitian ini dipergunakan untuk melengkapi pengetahuan teoritis yang diperoleh selama studi di Fakultas Hukum Universitas Muhammadiyah Palembang dan diharapkan bermanfaat sebagai tambahan informasi bagi ilmu pengetahuan, khususnya hukum pidana, sekaligus merupakan sumbangan pemikiran yang dipersembahkan kepada alamamater.

D. Metode Penelitian

Selaras dengan tujuan yang bermaksud menelusuri prinsip-prnsip hukum, terutama yang bersangkut paut dengan kebijakan penanggulangan tindak pidana teknologi informasi melalui hukum pidana, maka jenis penelitiannya adalah penelitian hukum *normatif* yang bersifat *deskriptif* (menggambarkan) dan tidak bermaksud untuk menguji hipotesa.

Teknik pengumpulan data

Teknik pengumpula data sekunder dititik beratkan pada penelitian kepustakaan (*library research*) dengan cara mengkaji:

a. Bahan hukum primer, yaitu bahan hukum yang bersifat mengikat seperti undang-undang, peraturan pemerintah, dan semua ketentuan peraturan yang berlaku
b. Bahan hukum sekunder, yaitu bahan hukum seperti hipotesa, pendapat para ahli maupun peneliti terdahulu, yang sejalan dengan permasalahan dalam skripsi ini
c. Bahan hukum tersier, yaitu bahan hukum yang menjelaskan bahan hukum primer dan bahan hukum sekunder seperti kamus bahasa, ensiklopedia, dan lainnya.

Teknik penglahan data

Setelah data terkumpul, maka data tersebut diolah guna mendapatkan data yang terbaik. Dalam pengolahan data tersebut, penulis melakukan kegiatan *editing*, yaitu data yang diperoleh diperiksa dan diteliti lagi mengenai kelengkapan kejelasan dan kebenarannya, sehingga terhindar dari kekurangan dan kesalahan.

Analisa data

Analisa data dilakukan secara *kualitatif* yang dipergunakan untuk mengkaji aspek-aspek *normatif* atau *yuridis* melalui metode yang bersifat *deskriptif analitis* yang menguraikan gambaran dari data yang diperoleh dan menghubungkan satu sama lain untuk mendapatkan suatu kesimpulan yang bersifat umum.[5]

E. Sistematika Penulisan

Sesuai dengan buku pedoman penyusunan skripsi Fakultas Hukum Universitas Muhammadiyah Palembang, penulisan skripsi ini secara keseluruhan tersusun dalam 4 (empat) bab dengan sistematika sebagai berikut:

Bab. I. Pendahuluan, berisi mengenai latar belakang, permasalahan, ruang lingkup dan tujuan, metode penelitian, serta sistematika penulisan

Bab. II. Tinjauan pustaka, memaparkan tinjauan pustaka yang menyajikan mengenai pengertian dan landasan pemahaman kebijakan penaggulangan kejahatan, tindak pidana teknologi informatika, yursdiksi hukum pidana dalam tindak pidana teknologi informasi.

Bab. III. Pembahasan, yang berisikan paparan tentang hasil penelitia secara khusus menguraikan dan menganalisa permasalahan yang diteliti mengenai bagaimanakah kebijakan formulasi hukum pidana terhadap tindak pidana tegnologi informasi saat ini dan juga mengenai

---

[5]Bambang Sunggono, *Metode Penelitian Hukum*, Raja Grafindo Persada, Jakarta, 1997, hlm. 129

bagaimanakah kebijakan penegakan hukum dalam upaya penanggulangan tindak pidana teknologi informasi.

Bab. IV. Penutup, pada bagian penutup ini merupakan akhir pembahasan skripsi ini yang diformat dalam kesimpulan dan saran-saran.

BAB. II

TINJAUAN PUSTAKA

A. Pengertian dan Landasan Pemahaman Kebijakan Penanggulangan Kejahatan

Hakekat pembangunan nasional adalah pembangunan bertujuan untuk mewujudkan manusia Indonesia seutuhnya dan masyarakat Indonesia seluruhnya untuk mencapai masyarakat adil, makmur dan sejaktera merata materiil dan spirituil berdasarkan Pancasila dan UUD 1945. Salah satu bagian pembangunan nasional adalah pembangunan dibidang hukum, yang dikenal dengan istilah pembaharuan hukum (*law reform*). Pembaharuan hukum nasional sebagai bagian dari rangkaian pembangunan nasional ini dilakukan secara menyeluruh dan terpadu baik hukum pidana, hukum perdata, maupun hukum administrasi, dan meliputi juga hukum formil maupun hukum materielnya.

Upaya pembaharuan hukum tidak terlepas dari kebijakan public dalam mengendalikan dan membentuk pola sampai seberapa jauh masyarakat diatur dan diarahkan. Dengan demikian sangat penting untuk menyadarkan para perancanghukum dan kebijakan public bahkan para pendidik, bahwa hukum dan kebijakan publik yang diteritkan akan mempunyai implikasi yang luas dibidang sosial, ekonomi dan politik. Sayangnya spesialisasi baik dalam pekerjaan, pendidikan maupun riset yang dilandasi dua disiplin tersebut (hukum dan ilmu

sosial), sehingga pelbagai imformasi yang bersumber dari keduanya tidak selalu bertemu (*converge*) bahkan seringkali tidak sama dan sebangun (*incongruent*).

Istilah kebijakan berasal dari bahasa Inggris *policy* atau dalam bahasa Belanda *politie*. Black's Law Dictionary mengidentifikasikan *policy* sebagai :

> "*The general principles by which a government is guided in its management ofpublic affairs... or principles and standart regarded by the legislature or by the courts as being of fundamental concern to the whole of society in measures, as applied to a law, ordinance, or rule of law, denotes its general purpose or tendency considered as directed to the welfare or the welfare or prosperity of the state community*" [6]

Secara umum kebijakan dapat diartikan sebagai prinsip-prinsip umum yang berfungsi untuk mengarahkan pemerintah dalam mengelola, 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).[7]

Upaya perindungan masyarakat (*social defence*) dan upaya mencapai kesejahteraan masyarakat (*social welfare*) pada hakkatnya merupakan bagian integral dari kebijakan atau upaya penangulangan kejahatan.[8] Kongres PBB ke-4 mengenai *Prevention of Crime and The Treatment of Offender* tahun 1970 yang tema sentralnya membicarakan masalah "*Crime and Develompent*" menegaskan

---

[6]Henry Cambell Balck, *Black's Law Dictionary*, Seventh Edition, St. Paulmin West Publicing. Co, 1999, hlm. 117

[7]Wisnusubroto, *Kebijakan Hukum Pidana dalam Peanggulangan Penyalahgunaan Komputer*, Universitas Atmajaya, Yogyakarta, 1999, hlm. 3

[8]Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana*, Raja Grafindo Persada, Jakarta, 2006, hlm. 2

keterpaduan tersebut: "*Any dichotomy between a country's policies for social defence and its planning for national development was unreal by definitions*"[9]

Penegasan perlunya penanggulangan kejahatan diintegrsikan dengan keseluruhan kebijakan sosial, juga dikemukakan dalam kongres PBB ke-5 tahun 1975 di Geneva dalam membahas masalah *criminal legislation, judicial procedures, and other form of social control in the prevention of crime*, menyatakan: "*The many esencies of criminal policy should be coordinated and the whole should be integrated into a general social policy of each country*". [10]

Kebijakan penanggulangan kejahatan atau yang biasa dikenal dengan istilah "politik kriminal" menurut Sudarto merupakan suatu usaha yang rasional dari masyarakat dalam menanggulangi kejahatan.[11] Defenisi ini diambl dari defenisi Marc Ancel yang merumuskan politik kriminal sebagai "*the rational organization of the control of crime by society*".

Tujuan penanggulangan kejahatan yaitu perlindungan masyarakat ntuk mencapai kesejahteraan masyarakat. Perumusan tujuan dari politik criminal yang demikian dinyatakan dalam salah satu laporan kursus latihan ke-34 yang diselenggarakan oleh UNAFEI di Tokyo tahun 1973 sebagai berikut:[12]

> *Most of group members agreed some discussion that "protection of the society could be accepted as the final goal of criminal policy although not the ultimate aim of society, which might perhaps be described by terms like "happiness of citizens", "a wholesome and cultural living", "social welfare" or "equality".*

---

[9]*Ibid,* hlm. 5

[10]Nyoman Serikat Putra Jaya, *Beberapa Pemikiran ke Arah Pengembangan Hukum Pidana*, Citra Aditya Bakti, Bandung, 2008, hlm. 190

[11]Sudarto, *Hukum dan Hukum Pidana*, Alumni, Bandung, 1977

[12]Barda Nawawi Arief, Bunga Rampa Kebijakan Hukum Pidana, *Op. Cit*, hlm. 2

Kesepakatan dari hasil kursus tersebut dapat menjadi landasan dalam kebijakan kriminal sebagai upaya penangglangan kejahatan untuk kesejahteraan social (*social welfare*) dan untuk perlindungan masyaraat (*social deence*).

B. Tindak Pidana Teknologi Informasi

Di era global ini berbagai hal positif bias dimanfaatkan oleh setiap bangsaterutama bidang teknologi, kemauan teknologi juga menyimpan kerawanan yang tentu saja sangat membahayakan. Bahkan hanya soal kejahatan konvensional yang gagal diberantas akibat terimbas oleh pola-pola modernitas yang gagal mengedepankan prinsip humantas, tetapi juga munculnya kejahatan di alam maya yang telah menjadi realitas dunia.

Memang tidak bisa diingkari oleh siapapun, bahwa tenologi itu dapat menjadi alat perubahan ditengah masyarakat. Demikian pentingnya fungsi teknologi, hingga sepertinya masyarakat dewasa ini sangat tergantung dengan teknologi, baik untuk hal-hal positif maupun negatif. Pada perkembangannya *internet* juga membawa sisi negatif, dengan membuka peluang munculnya tindakan-tindakan anti sosial yang selama ini dianggap tidak mungkin terjad atau tdak akan terpikirkan terjadi. Sebuah teori menyataka bahwa *crime is product of society it self*, yang secara sederhana dapat diartikan bahwa semakin tinggi tingkat intelektualitassuatu masyarakat maka aan semakin canggih dan beraneka-ragam pulalah tingkat kejahatan yang dapat terjadi.[13]

---

[13]Abdul Wahib da Mohammad Labib, *Kejahatan Mayantara (Cybercrime)*, Rafika Aditama, Bandung, 2005, hlm. 39

Salah satu contoh saat ini adalah kejahatan maya atau biasa disebut "cybercrime" (tindak pidana mayantara), merupakan bentuk fenomena baru dalam tindak kejahatan sebagai dampak langsung dari perkembangan teknologi informasi. Beberapa sebutan diberikan pada jenis kejahatan baru ini di dalam berbagai tulisan, antara lain: sebagai kejahatan dunia maya (*cyber space/virtual space offence*), dimensi baru dai "*hi-tech crime*", dimensi baru dari "*transnational crime*" dan dimensi baru dari "*white coller crime*".[14]

White collar crime menurut Jo Ann Miller, umumnya dibagi ke dalam 4 (empat) jenis, yaitu: Kejahatan korporasi, kejahatan birokrasi, malpraktek, dan kejahatan individu.[15] Sementara itu *cybercrime* memiliki ciri khas tersendiri yaitu para pelaku umumnya orang muda yang menguasai teknologi informasi dan dilakukan secara ekstra hati-hati dan sangat meyakinkan serta membutuhkan keahlian tambahan atau pertolongan orang lain.[16]

Kekhawatiran akan tindak kejahatan ini dirasakan diseluruh aspek bidang kehidupan. ITAC (*Information Technology Assosiation of Canada*) pada *International Information Industry Congress* (IIIC) 2000 *Millenium Congress* di Quebec tanggal 19 September 2000 menyatakan bahwa "*cybercrime is a real and growing threat to economic and social development around the world.*

---

[14]Barda Nawawi Arief, *Antisipasi Penanggulangan "cybercrime" dengan hukum pidana*,, Makalah pada Seminar Nasional mengenai "*cyberlaw*", di STHB, Bandung, Hotel Grand Aquila, 9 April 2001

[15]Sutanto, Hermawan Sulistyo, dan Tjuk Sugiarto, *Cybercrime-Motif dan Penindakan*, Pensil 324, Jakarta, hlm. 13

[16]*Ibid*, hlm. 20

Information technology touches every aspect of human life and so can electronically enable crime".[17]

Istilah *cybercrime* saat ini merujuk pada suatu tindakan kejahatan yang berhubungan dengan dunia maya (*cyberspace*) dan tindakan kejahatan yang menggunakan komputer. Ada ahli yang menyamakan antara tindakan kejahatan *cyber* (*cybercrime*) dengan tindakan kejahatan komputer, dan ada ahli yang membedakan diantara keduanya. Meskipun belum ada kesepahaman mengenai defenisi kejahatan tenologi informasi, namun ada kesamaan pengertian universal mengenai kejahatan komputer.

Kejahatan teknologi informasi atau kejahatan komputer memang identik dengan *cybercrime*, banyak literatur baik nasional maupun internasional yang mendefenisikan terhadap istilah tersebut. *The U.S Departement of Justice* meberikan pengertian "*cybercrime is any illegal act requiring knowledge of computer technologi for it perpetration investigation or prosecution*". Computer crime dapat diartikan sebaga kejahatan di bidang komputer secara umum dapat diartikan sebagai pengguna computer secara illegal.[18] Abdul Wahib dan Mohammad Labib menyatakan bahwa kejahatan dunia maya adalah kejahatan yang berkaitan dengan pemanfaatan sebuah teknologi informasi tanpa batas serta memilki karakteristik yang kuat dengan sebuah rekayasa teknologi yang

---

[17]Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana Dalam Menanggulangi Kejahatan*, Kencana Prenada Media Group, Jakarta, 2007, hlm. 240

[18]Andi Hamzah, *Aspek-aspek Pidana di Bidang Komputer*, Raja Grafindo Persada, Jakarta, 1998, hlm. 4

mengandalkan pada tingkat keamanan yang tinggi dan kredibilitas dari sebuah informasi yang disampaikan dan diakses oleh penguna *internet*.[19]

Barda Nawawi Arief menunjuk pada kerangka (sistematik), *Draft Convention on Cybercrime* dari Dewan Eropa (Draft No.25, Desember 2000) yang mendefenisikan *cybercrime* sebagai "*crime related to technology, computers and the internet*" atau secara sederhana berarti kejahatan yang berhubungan dengan teknologi, computer dan *internet*.[20] Pengertian lain diberikan oleh Organization of European Community Development, yaitu "*any illegal, unethical or unauthorized behavior relating the automatic processing and/or the transmission data*".

Cybercrime pada dasarnya tindak pidana yang berkenaan dengan informasi, sistem informasi (*information system*) itu sendiri, serta sistem komunikasi yang merupakan sarana untuk penyampaian/pertukaran informasi itu kepada pihak lainnya (*transmitter/originator to recipient*).[21] Menurut Sutanto, secara garis besar *cybercrime* terdiri dari dua jenis, yaitu:[22]

1. Kejahatan yang menggunakan technology informasi (TI) sebagai fasilitas. Contoh-contoh dari aktivitas *cybecrime* jenis pertama ini adalah pembajakan (*copyright* atau hak cipta intelektual dan lain-lain), pornografi, pemalsuan dan pencurian kartu kredit (*carding*), penipuan lewat *e-mail*, penipuan dan pembobolan rekening bank, perjudian *on line*, terorisme, situs sesat, materi-mater *internet* yang berkaitan dengan SARA (seperti penyebaran kebencian etnik dan ras atau agama), transaksi dan penyebaran obat terlarang, transaksi seks, dan lain-lain.
2. Kejahatan yang menjadikan sistem dan fasilitas teknologi informasi (TI) sebagai sarana. *Cybercrime* jenis ini bukan memanfaatkan komputer dan *internet* sebagai media atau sarana tindak pidana, melainkan

---

[19]Abdul Wahib dan Mohammad Labib, *Op. Cit*, hlm. 40

[20]Barda Nawawi Arief, Kapita Selekta Hukum Pidana, *Op. Cit*, hlm. 243

[21]*Ibid*

[22]Sutanto, Hermawan Sulistyo dan Tjuk Sugiarto, *Op. Cit*, hlm. 21

menjadikannya sebagai sarana. Contoh dari jenis-jenis tindak kejahatan antara pengaksesan ke suatu sistem secara illegal (*hacking*) perusahaan situs *internet* dan *server* data (*cracking*), serta *defacting*.

Menurut Freddy Haris, *cybercrime* merupakan suatu tidak pidana dengan karateristik-karakteristik sebagai berikut:

1. *Unauthorized access* (dengan maksud ntuk memfasilitasi kejahatan)
2. *Unauthorized alteration or destruction of data*
3. Mengganggu/merusak operasi komputer
4. Mencegah/menghambat akses pada komputer.[23]

Sedangkan kualifikasi kejahatan dunia maya (*cybercrime*), sebagaimana dikutif oleh Barda Nawawi Arief, adalah kualifikasi *cybercrime* menurut *Convention on Cybercrime* 2001 di Budapest Hongaria, yaitu:[24]

1. *Illegal acces*, yaitu sengaja memasuki atau mengakses sistem komputer tanpa hak.
2. *Illegal interception*, yaitu sengaja dan tanpa hak mendengar atau menangkap secara diam-diam pengiriman dan pemancaran data komputer yang tidak bersifat publik ke , dari atau di dalam sistem komputer dengan menggunakan alat bantu teknis
3. *Data interference*, yaitu sengaja dan tanpa hak melakukan perusakan, penghapusan, perubahan atau penghapusan data komputer
4. *System interference*, yaitu sengaja melakukan gangguan atau rintangan serius tanpa hak terhadap berfungsinya sistem komputer
5. *Misuse of Devices*, penyalahgunaan perlengkapan komputer, termasuk program computer, password komputer, kode masuk (*access code*)
6. *Computer related Forgery,* Pemalsuan (dengan sengaja dan tanpa hak memasukkan, mengubah, menghapus data autentik menjadi tidak autentik dengan maksud digunakan sebagai data autentk)
7. *Computer Related Fraud*, penipuan (dengan sengaja da tanpa hak menyebabkan hilangnya barang/kekayaan orang lain dengan cara memasukkan, mengubah, menghapuskan data komputer atau dengan mengganggu berfungsinya komputer/sistem komputer, dengan tujuan

---

[23]Freddy Haris, *Cybercrime dari Perspektif Akademis*, Lembaga Kajian Hukum dan Teknologi Fakultas Hukum UniversitasIdonesia, Jakarta, hlm. 4

[24]Barda Nawawi Arief, Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan, *Op. Cit*, hlm. 24

untuk memperoleh keuntungan ekonomi bagi dirinya sendiri atau orang lain)

8. *Content-Related Offences*
   Delik-delik yang berhubungan dengan pornografi anak (*child pornography*)
9. *Offences Related to Infringements of copyright and Related Rights*
   Delik-delik yang terkait dengan pelanggaran hak cipta.

Beberapa bentuk kejahatan yang berhubungan erat dengan penggunaan teknologi informasi yang berbasis utama komputer dan jaringa teknologi informasi, dalam beberapa literatur dan praktiknya menurut Mas Wigantoro dikelompokkan dalam beberapa bentuk antara lain:[25]

1. *Unauthorized Access to computer system and service*
   Kejahatan yang dilakukan dengan memasuki/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya
2. *Illegal Contents*
   Merupakan kejahatan dengan memasukan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum
3. *Data Forgery*
   Merupakan kejahatan dengan memalsukan data pada dokumen-dkumen penting yang tersimpan sebagai *scriptless document* melalui *internet*
4. *Cyber Espionage*
   Merupakan kejahatan yang memanfaatkan jaringan *internet* untuk melakukan kegiatan mata-mata pihak lain, dengan memasuki sistem jaringan komputer (*computer network system*) pihak sasaran
5. *Cyber Sabotage and Extortion*
   Kejahatan ini dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan *internet*
6. *Offence Against Intellectual Property*
   Kejahatan ini ditujukan terhadap hak atas kekayaan intelektual yang dimiliki pihak lain di *internet*. Sebagai contoh adalah peniruan tampilan pada web page suatu situs milik orang lain secara illegal, penyiaran suatu informasi di *internet* yang ternyata merupakan rahasia dengan orang lain dan sebagainya
7. *Infringements of Privacy*

---

[25]Naskah Akademik RUU Tindak Pidana di Bidang Teknologi Informasi disusun oleh Mas Wigantoro Roes Setiyadi, *Op. Cit*, hlm. 25-26

Kejahatan ini ditujukan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia. Kejahatan ini biasanya ditujukan terhadap keterangan seseorang pada formulir data pribadi yang tersimpan secara computerized, yang apabiladiketahui oleh orang lain akan dapat merugikan korban secara materil maupun immaterial, seperti nomor kartu kredit, nomor PIN ATM, cacat atau penyakit tersembunyi dan sebagainya.

Selain kejahatan di atas sebetulnya masih banyak jenis-jenis kejahatan yang masuk dalam katagori *cybercrime* seperti yang diungkapkan oleh M. Arief Mansur dan Alistaris Gultom, jens-jenis *cybercrime* diantaranya:[26]

1. *Cyber-terorism*
   National Police Agency of Japan (NPA) mendefenisikan *cyesber terrorism* sebagai *electronic attack through critical computer networks against critical infrastructure that have potential critical effects on social and economic activites of the nation*
2. *Cyber-Pornography*, penyebarluasan *obscene materials* termasuk *pornography*, *indecent exposure*, dan *child pornography*
3. *Cyber-harassment*, pelecehan seksual melalui *e-mail*, *website*, atau *chat pornograms*
4. *Cyber-stalking*: *crimes of stalking* melalui penggunaan komputer dan *internet*
5. *Hacking*: penggunaan *programming abilities* dengan maksud yang bertentangan dengan hukum
6. *Carding* (*credit-card fraud*) melibatkan berbagai macam aktifitas yang melibatkan kartu kredit. *Carding* muncul ketika seseorang yang bukan pemilik kartu redit menggunakan kartu kredit tersebut secara melawan hukum.

Berdasarkan beberapa tindak pidana yang berkaitan dengan teknologi informasi diatas, menurut RM Roy Suryo kasus-kasus *cybercrime* yang banyak terjadi di Indonesia setidaknya ada tiga jenis berdasarkan modusnya, yaitu:[27]

1. Mencuri Nomor Kredit
   Penyalahgunaan kartu kredit milik orang lain di *internet* merupakan kasus *cybercrime* terbesar yang berkaitan dengan dunia bsnis internet di Indonesia. Penyalahgunaan kartu kredit milik orang lain memang tidak rumit dan bias dilakukan secara fisik atau *on-line*. Nama dan kartu kredit orang lain yang diperoleh di berbagai tempat (restoran, hotel, atau segala

---

[26]M. Arief Mansur dan Alistaris Gultom, *Op. Cit*, hlm. 26
[27]Majalah Warta Ekonomi, No.9, 5 Maret 2008, hlm. 12

tempat yang melakukan transaksi pembayaran dengan kartu kredit) dimasukkan di aplikasi pembelian barang di *internet*

2. Memasuki, memodifikasi, atau merusak *Homepage* (*Hacking*)
   Tindakan *Hacker* Indonesia belum separah aksi di luar negeri. Prilaku hacker Indonesia baru sebatas masuk ke situs komputer orang lain yang ternyata rentan penyusupan dan memberitahukan kepada pemiliknya untuk berhati-hati. Di luar negeri *hacker* sudah memasuki sistem perbankan dan merusak data *base* bank
3. Penyerangan situs atau *e-mail* melalui virus atau *spamming*. Modus yang paling sering terjadi adalah mengirim virus melalui *e-mail*. Menurut RM Roy Suryo, di luar negeri kejahatan seperti ini sudah diberi hukuman yang cukup berat. Berbeda dengan di Indonesia yang sulit diatasi karena peraturan yang ada belum menjangkaunya.

Dengan memperhatikan jenis-jenis kejahatan sebagaimana dikemukakan di atas dapat digambarkan bahwa *cybercrime* memiliki ciri-ciri khusus, yaitu:

1. *Non-Violance* (tanpa kekerasan)
2. Sedikit melibatkan kontak fisik
3. Menggunakan peralatan dan teknologi
4. Memanfaatkan jaringan telematika (telekomunikasi, media dan informatika) global.[28]

Apabila memperhatikan ciri ke-3 da ke-4 yaitu menggunakan peralatan dan teknologi serta memanfaatkan jaringan telematika global, nampak jelas bahwa *cybercrime* dapat dilakukan dimana saja, kapan saja serta berdampak kemana saja, seakan-akan tanpa batas (*borderless*). Keadaan ini mengakibatkan pelaku kejahatan, korban, tempat terjadinya perbuatan pidana (*locus delicti*) serta akibat yang ditimbulkannya dapat teradi pada beberapa Negara. Oleh karena itu dalam memberantas kejahatan dalam dunia maya ini diperlukan penanganan yang serius serta melibatkan kerjasama\internasional baik yang bersifat regional maupun multilateral.

---

[28]Romli Atmasasmita, *Ruang Lingkup Berlakunya Hukum Pidana Terhadap Kejahatan Transnasional Terorganisasi*, Artikel dalam Padjadajaran Jilid XXIV No.2 tahun 1996, hlm. 90

C. Jurisdiksi Hukum Pidana Dalam Tindak Pidana Teknologi Informasi

Jurisdiksi merupakan hal yang sangat *crucial* sekaligus kompleks khususnya berkenaan dengan pengungkapan kejahatan-kejahatan di dunia maya yang bersifat internasional (*international cybercrime*). Dengan adanya kepastian jurisdiksi maka suatu negara memperoleh pengakuan dan kedaulatan penuh untuk berbagai aturan dan kebijaksanaannya secara penuh. Kekuasaan demikian harus dihormati pula oleh setiap negara lainnya sebagaimana kekuasaan yang dimiliki oleh negara-negara lain.[29]

Menurut Kamus Bahasa Indonesia, jurisdiksi adalah:[30]

a. Kekuasaan mengabdi lingkup kuasa kehakiman; peradilan
b. Lingkup hak dan kewajiban serta tanggungjawab di suatu wilayah atau lingkungan tertentu, kekuasaan hukum.

Jurisdiksi menurut hukum pidana internasional adalah kekuasaan atau kompetensi hukum negara terhadap orang, badan atau peristiwa (hukum). Jurisdiksi ini merupakan refleksi dari prinsip dasar kedaulatan Negara, kesamaan derajat negara dan prinsip tidak campur tanga. Jurisdiksi uga merupakan suatu bentuk kedaulatan yang vital dan sentral yang dapat mengubah, menciptakan atau kewajiban suatu hubungan atau kewajiban hukum.

Jurisdiksi suatu negara yang diakui oleh hukum internasional dalam pengertian konvensional, didasarkan pada batas-batas geografi, sementara komunikasi multimedia bersifat internasional, multi jurisdiksi, tanpa batas,

---

[29]Yudha Bhakti Ardhiwisastra, *Imunitas Kedaulatan Negara di Forum Pengadilan Asing*, Alumni, Bandung, 1999, hlm. 14

[30]Departemen Pendidikan dan Kebudayaan, *Kamus Bahasa Indonesia*, Cet II, Balai Pustaka, Jakarta, 1997, hlm. 1134

sehingga sampai saat ini belum dapat dipastikan bagaimana jurisdiksi auatu negaradapat diberlakukan terhadap komunikasi multimedia sebagai salah satu pemanfaatan tenologi informasi.[31]

Dalam kaitannya dengan penentuan hukum yang berlaku, dikenal beberapa asas yang biasa dilakukan, yaitu:

1. *Subjective territoriality*, yang menekankan bahwa keberlakuan hukum ditentukan berdasarkan tempat perbuatan dilakukan dan penyelesaian tindak pidananya dilakukan di negara lain
2. *Objective territoriality*, yang menyatakan bahwa hukum yang berlaku adalah hukum dimana akibat utama perbuatan itu terjadi dan memberikan dampak yang sangat merugikan bagi negara yang bersangkutan
3. *Nationality* yang menentukan bahwa negara mempunyai jurisdiksi untuk menentukan hukum berdasarkan kewarganegaraan pelaku
4. *Passive nationality* yang menekankan jurisdiksi berdasarkan kewarga negaraan korban
5. *Protective principle* yang menyatakan berlakunya hukum didasarkan atas keinginan negara ntuk melindungi kepentigan negara dari kejahatan yang dilakukan di luar wilayahnya, yang umumnya digunakan apabila korban adalah negara atau pemerintah
6. *Universality*, asas *Universality* selayaknya memperoleh perhatian khusus terkait dengan penanganan hukum kasus-kasus cyber. Asas ini disebut juga sebagai "*universal interest jurisdiction*". [32]

Pada mulanya asas *universality* menentukan bahwa setiap warga Negara berhak untuk menangkap dan menghukum para pelaku pembajakan. Asas ini kemudian diperluas sehingga mencakup pula kejahatan terhadap kemanusiaan (*crime against humanity*), misalnya penyiksaan, genosida, pembajakan udara dan lain-lain. Meskipun dimasa mendatang asas jurisdiksi niversal ini mungkin dikembangkan untuk *internet piracy*, seperti *computer*, *cracking*, *carding*, *hacking*

---

[31]Tien S. Saefulah, *Jurisdiksi Sebagai upaya Penegakan Hukum Dalam Kegiatan Cyberspace*, artikel dalam *Cyberlaw*: Suatu Pengantar, Pusat Studi *Cyberlaw* Fakultas Hukum UNPAD, ELIPS, 2002, hlm. 96

[32]Ahmad M. Ramli, *Perkembangan Cyberlaw Global dan Implikasinya Bagi Bangsa Indonesaia*, Makalah Seminar The Impormantance of Imformation System Scurity in E-Government, Tim Koordinasi Telematika Indonesia, Jakarta, 28 Juli 2004, hlm. 5-6

and viruses, namun perlu dipertimbangkan bahwa penggunaan asas ini hanya diberlakukan untuk kejahatan sangat serius berdasarkan perkembangan dalam hukum internasional.

Harus diakui bahwa menerapkan jurisdiksi yang tepat dalam kejahatan-kejahatan di dunia maya (cybercrime) bukan merupakan pekerjaan yang mudah, karena jenis kejahatannya bersifat internasional sehingga banyak bersinggung dengan kedaulatan banyak Negara (sistem hukum Negara lain). Berkenaan dengan jurisdiksi tersebut maka pertanyaan penting yang harus dikemukakan adalah sampai sejauh mana suatu negara memberikan kewenangannya kepada pengadilan untuk mengadili dan menghukum pelaku tindak pidana.

Terkait tindak pidana mayantara (*cyberspace*). Darrel Menthe, menyatakan jurisdiksi di *cyberspace* membutuhkan prinsip-prinsip yang jelas yang berakar dari hukum internasional. Selanjutnya Menthe menyatakan denga diakuinya prinsip-prinsip jurisdiksi yang berlaku dalam hukum internasional dalam kegiatan *cyberspace* oleh setiap negara, maka akan mudah bagi negara-negara untuk mengadakan kerjasama dalam rangka harmonisasi ketentuan-ketentuan pidana untuk menangulangi *cybercrime*.[33]

Pendapat menthe ini dapat ditafsirkan bahwa dengan diakuinya prinsip-prinsip jurisdiksi yang berlaku dalam hukum internasional dalam kegiatan *cyberspace* oleh setiap negara, maka akan mudah bagi negara-negara untuk mengadakan kerjasama dalam rangka harmonisasi ketentuan-ketentuan pidana untuk menanggulangi *cybercrime*.

---

[33]Darrel Menthe, "*Jurisdiction in Cyberspace: A Theory of International Sraces*" , htt://www.mtlr.org/volfour/menthe, html, hlm. 2, diakses tanggal 2 November 2013

Ada tiga lingkup jurisdiksi di ruang maya (*cyberspace*) menurut Masaki Hamano, sebagai mana dikutip oelh Barda Nawawi rief yang dimiliki suatu Negara berkenaan dengan penetapan dan pelaksanaan pengawasan terhadap setiap peristiwa, setiap orang dan setiap benda. Ketiga katagori jurisdiksi tersebut, yaitu: [34]

1. Jurisdiksi Legislatif (*legislatif jurisdiction atau jurisdiction to prescribe*)
2. Jurisdiksi Yudisial (*judicial jurisdiction atau jurisdiction to adjudicate*)
3. Jurisdiksi Ekeskutif (*exsecutive jurisdiction atau jurisdiction to enforce*).

Jurisdiksi di atas berkaitan dengan batas-batas kewenangan negara di tiga bidang penegakan hukum, *pertama* kewenangan pembuat hukum substantif (oleh karena itu disebut jurisdiksi legislatif, atau dapat juga disebut jurisdiksi formulatif). *Kedua* kewenangan mengadili atau menerapkan hukum (oleh karena itu disebut jurisdiksi judicial atau aplikatif). *Ketiga* kewenangan melaksanakan/memaksakan kepatuhan hukum yang dibuatnya (oleh karena itu disebut jurisdikasi eksekutif)[35]

Menurut Barda Nawawi Arief, problem jurisdiksi yang menonjol adalah masalah jurisdiksi judicial (kewenangan mengadili atau menerapkan hukum) dan jurisdiksi eksekutif (kewenangan melaksanakan putusan) dari pada masalah jurisdiksi legislaif (kewenangan pembuat hukum). Dikatakan demikian karena

---

[34]Barda Nawawi Aief, Tindak Pidana Mayantara, *Op. Cit*, hlm. 27-28

[35]Barda Nawawi Arief, *Kapita Selekta Hukum Pidana*, Citra Aditya Bakti, Bandung, 2003, hlm. 247

masalah jurisdiksi judicial/adjudikasi dan jurisdiksi eksekutif sangat terkait dengan kedaulatan wilayah dan kedaulatan hukum masing-masing negara.[36]

Menurut Hikmahanto Juwono dalam konteks hukum Internasonal, terdapat beberapa prinsip yang digunakan untuk menegaskan siapa yang memiliki kewenangan untuk mengadili, dikatakannya ada beberapa prinsip yang diterapkan, antara lain territorial, personalitas, nasionalitas, dan universal. Masing-masing prinsip memliki karakter yang berbeda satu sama lain. Misalkan prinsip territorial yang mendasarkan pada wilayah dimana tindak pidana itu terjadi. Di samping itu juga bias dilihat dari munculnya akibat. Kemudian perinsip personalitas dan universalitas. Tiap-tiap prinsip memiliki karakter yang berbeda antara satu dengan yang lain. Prinsip territorial mendasarkan pada wilayah dimana tindak pidana itu terjadi, bias juga dari tempat munculnya akibat tindak pidana.

Prinsip personalitas menekankan pada kewarganegaraan dari si pelaku. Misalnya jika pelaku adalah warga negara Indonesia, maka si pelaku bias disidangkan di pengadilan Indnesia. Pada prinsipnya nasionalitas yang ditekankan adalah kepentingan dari negara tempat terjadinya tindak pidana. Prinsip terakhir yaitu prnsip universal yang lebih menekankan kejahatan internasional. Setiap negara yang berkepentingan bias menerapkan dimana saja, kapan saja, dan bag siapa saja sepanjang kejahatan tersebut tergolong sebagai kejahatan internasonal.

Negara-negara yang tergabung dalam Uni Eropa (*Council of Europe*) pada tanggal 23 November 2001 di kota Budapest, Hongaria tela membuat dan menyepakati *Convention on Cybercrime* yang kemudian dimasukkan kedalam

---

[36]Barda Nawawi Arief, *Sari Kuliah: Perbandingan Hukum Pidana*, Raja Grafindo Persada, Jakarta, 2006, hlm. 280

European Treaty Series dengan Nomor 185. Tujuan konvensi tersebut adalah untuk melindngi masyarakat dari *cybercrime*, baik melalui undang-undang maupun kerjasama internasional. Hal ini dmaksudkan untuk mengatasi kejahatan *cyber*, tanpa mengurangi kesempatan setiap individu untuk tetap dapat mengembangkan kreativitasnya dalam pengembangan teknologi informasi.

Masalah jurisdiksi berkaitan dengan kecakapan dari suatu forum tertentu untu mengadili kasus (*adjudicate jurisdiction*). Jurisdiksi dalam *cyberspace* dapat menggunakan teori:

a. *The theory of uploader and downloader*. *Uploader* adalah pemberi informasi dan *downloader* adalah penerima transaksi elektronik
b. *The law of the server*. Jurisdiksi ditentukan dengan menggunakan atau memperlakukan *server* dimana *webpages* secara fisik berlokasi, yaitu dimana mereka dicatat sebagai data elektronik
c. *The theory of internasional spaces,* ada usulan bahwa *internet* dijadikan ruang tersendiri, menjadi ruang ke empat setelah air, darat, dan udara.

Pengaturan mengenai masalah jurisdiksi merupakan hal penting dan dalam pembentukan undang-undang khusus mengenai *cybercrime* perlu dipikirkan bentuk jurisdiksi yang mampu menjangkau kejahatan di dunia siber mengingat kejahatan ini punya karakter yang khas dan sifatnya lintas negara (*tansborder*). Dengan demikian penerapan asas universal (asas ubikuitas) dapat digunakan disamping juga diperlukan kerjasama dengan negara-negara lain.

Undang-undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) telah mengatur masalah jurisdiksi yang didalamnya sudah menerapkan asas universal. Hal ini dapat dilihat dari Pasal 2 dan penjelasannya.

Pasal 2 UU ITE

Undang-undang ini berlaku untuk setiap orang yang melakukan perbuatan hukum sebagaimana diatur dalam undang-undang ini, baik yang berada di wilayah hukum Indonesiamaupun di luar wilayah hukum Indonesia, yang memiliki akibat hukum di wilayah hukum Indonesia dan/atau di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia.

Penjelasan Pasal 2 UU ITE

Undang-undang ini memiliki jangkauan jurisdiksi tidak semata-mata untuk perbuatan hukum yang berlaku di Indoesia dan/atau dilakukan oleh warga negara Indonesia, tetapi juga berlaku untuk perbuatan hukum yang dilakukan diluar wilayah hukum (jurisdiksi) Indonesia baik oleh warga negara Indonesia maupun warga negara asing atau badan hukum Indonesia maupun badan hukum asing yang memiliki akibat hukum di Indonesia, mengingat pemanfaatan teknologi informasi untuk informasi elektronik da transaksi elektronik dapat bersifat lintas territorial atau universal. Yang dimaksud dengan "merugikan kepentingan Indonesia" adalah meliputi tetapi tidak tebatas pada merugikan kepentingan ekonomi nasional, perlindungan data strategis, harkat dan martabat bangsa,

pertahanan dan keamanan negara, kedaulatan negara, warga negara, serta bada hukum Indonesia.

BAB. III

PEMBAHASAN

A. Kebijakar: Formulasi Hukum Pidana Terhadap Tindak Pidana Teknologi Infomasi

Globalisasi teknologi informasi yang telah mengubah dunia ke era *cyber* dengan sarana internet yang menghadirkan *cyberspace* dengan realitas virtualnya menawarkan kepada manusia berbagai harapan dan kemudahan. Akan tetapi di balik itu, timbul persoalan berupa kejahatan yang dinamakan *cybercrime*, baik sistem jaringan komputernya itu sendiri yang menjad sasaran maupun komputer itu sendiri yang menjadi sarana untuk melakukan kejahatan. Tentunya jika kita melihat bahwa informasi itu sendiri telah menjadi komditi maka upaya untuk melindungi aset tersebut sangat diperlukan.

Kebijkan sebagai upaya untuk melindungi informasi membutuhkan suatu pengkajian yang sangat mendalam, menyangkut aspek sosiologis, filosofis, yuridis, dan sebagainya. Teknologi informasi sekarang ini sangat strategis dan berdampak luas terhadap aktifitas kehidupan manusia oleh karena tu dibutuhkan pengaturan secara khusus dengan bentuknya suatu undang-undang yang dapat menanggulangi kejahatan terhadap teknologi informasi.

Peraturan terhadap teknologi informasiagar diterima masyarakat harus mempertimbangkan semua aspirasi (suprastruktur, infrastruktur, kepakaran dan aspirasi internasional) dan perlbagai kepetingan harus diselaraskan dan diserasikan. Persoalan komunikasi massa menempati posisi yang strategis dalam

kehidupan demokrasi, dan ini akan bersentuhan secara langsung tidak hanya dengan persoalan supremasi hukum yang bersifat *"top down"*, misalnya untuk kepentingan keamanan negara, perstuan dan kesatua nasional, tetapi juga sebaliknya *"bottom up"*, sebab orang cenderung akan melemparkan banyak pertanyaan kritis.[37]

Kebijakan hukum pidana (tataran aplikatif) sangat dipengaruhi sistem hukum yang berlaku saat ini. Hukum pidana Indonesia yang ada saat ini dan pengembangan kedepan dipengaruhi oleh tradisi hukum *civil law*. Politik hukum yang cenderung mengarah pada tradisi *civil law* mengandung kosekuensi sebagai berikut:

1. Peraturan perundang-undangan harus dirumuskan secara teliti dan lengkap sehingga diharapkan mampu menjangkau semua permasalahan yang timbul.
2. Asas legalitas ditempatkan sebagai landasan yang bersifat fundamental dan dalam pelaksanaannya harus dijunjung tinggi tanpa kecuali.
3. Operasionalisasi peraturan perundang-undangan diupayakan seoptinal mungkin untuk menangani berbagai kasus yang bervariasi dengan pendaatan penafsiran (interprestasi).

Instrumen hukum memberikan landasan atau pedoman bagi para penegak hukum yang akan diterapkan kepada para pelaku *cybercrime*. Sebagai hukum positif, pembuatannya tentu melalui mekanisme pembuatan perundang-undangan dan sekaligus melakat sifat *ius constitutum*, yakni menjadi hukum positif yang

---

[37]Muladi, Demokrasi, *Hak Asasi Manusia dan Reformasi Hukum di Indonesia*, The Hbibis Center , Jakarta, 2002, hlm. 201

memberikan sanksi bagi peristiwa atau perbuatan kriminal yang menggunakan komuter.

Pembentukan peraturan perundang-undangan di dunia *cyber* pun, berpangkal pada keinginan masyarakat untuk mendapatkan jaminan keamanan, keadilan dan kepastian hukum. Sebagai norma hukum *cyber* atau *cyber law* akan bersifat mengikat bagi tiap-tiap individu-individu untuk tuntk dan mengikuti segala kaidah-kaidah yang terkandung didalamnya.

Sebelum diundangkan Undang-undang Nomor 11 tahun 2008 tetang Informasi dan Transaksi Elektronik (UU ITE) yang mengatur secara khusus tentang pemanfaatan teknologi informasi, sebenarnya Indonesia dalam persoalan cybercrime tidak ada kekosongan hukum, ini terjadi jika digunakan metode penafsiran yang dikenal dalam ilmu hukum dan ini yang mestinya dipegang oleh aparat penegak hukum dalam menghadapi perbuatan-perbuatan yang berdimensi baru yang secara khusus belum diatur dalam undang-udang.[38]

Upaya menafsirkan cybercrime ke dalam perundang-undangan KUHP dan khususnya undang-undang yang terkait dengan perkembanganteknologi informasi tela dilakukan oleh penegak hukum dalam menangani *cybercrime* selama ini. Sebelum UU ITE diundangkan ada beberapa ketentuan hukum positif yang dapat diterapkan dengan kebenranian untuk melakukan terobosan dengan penafsiran hukum yang berkaitan dengan teknologi informasi khususnya kejahatan yang berkaitan denga internet. Penafsiranhukum dapat dilakukan melalui penafsiran eksentif dan analogi.

---

[38]Badan Pembinaan Hukum Nasional, *Perkembangan Pembangunan Hukum Nasional Tentang Hukum Teknologi dan Informasi*, BPHN Departemen Kehakiman RI, 1995/1996, hlm. 32-34

Metode penafsiran hukum yang dilakukan oleh aparat penegak hukum menjadi hal yang logis untuk menghindari kekosongan hukum terhadap tindak pidana teknologi informasi. Penerapan ketentuan-ketentuan hukum positif sebelum adanya UU ITE tidaklah sedrhana karena karakterstik *cybercrime* yang bersifat khas dari kejahatan konvensional/di dunia biasa. Sebelum disyahkannya UU ITE terdapat beberapa peraturan perundang-undangan yang dapat digunakan untuk menanggulangi tindak pidana di dunia maya.

Dalam upaya menanngani kasus kejahatan dunia maya, terdapat beberapa pasal dalam KUHP yang mengkriminalisasi *cybercrime* dengan menggunakan metode interprestasi ekstensif (perumpamaan dan persaaan) terhadap pasal-pasal yang terdapat dalam KUHP. Adapun pasal-pasal yang dapat dikenakan dalam KUHP yang mengkriminalisasi terhadap kejahatan dunia maya, sebagaimana dikatakan oleh Petrus Reinhard Golose diantaranya adalah:[39]

a. Pasal 362 KUHP untuk kasus *Carding* dimana pelaku mencuri kartu kredit milik orang lain walaupun tidak secara fisik karena hanya nomor kartunya saja yang diambil dengan menggunakan *software card generator* di internet untuk melakukan transaksi di *E-Commerce*.
b. Pasal 378 KUHP untuk penipuan dengan seolah-olah menawarkan dan menjual suatu produk atau barang dengan memasang iklan di salah satu *website* sehingga orang tertarik untuk membelinya lalu mengirimkan uang kepada pemasang iklan.

---

[39]Petrus Reinhard Golose, *Perkembangan Cybercrime dan Upaya Penanggulangannya di Indonesia Oleh Polri*, Buletin Hukum Perbankan dan Kebanksentralan, Volume 4 Nomor 2, Jakarta, Agusntus 2006, hm. 38-39

c. Pasal 335 KUHP dapat dikenakan untuk kasus pengancaman dan pemerasan yang dilakukan melalui *e-mail*.

d. Pasal 331 KUHP dapat dikenakan untuk kasus pencemaran nama baik dengan menggunakan metode internet. Modusnya adalah pelaku menyebarkan *e-mail* kepada teman-teman korban tentang suatu cerita yang tidak benaratau mengirimkan *e-mail* secara berantai melalui *mailing list* (*millis*) tentang berita yang tidak benar.

e. Pasal 303 KUHP dapat dikenakan untu menjerat permainan judi yang dilakukan secara *on-line* di internet dengan penyelenggara dari Indonesia.

f. Pasal 282 KUHP dapat dikenakan untuk penyebaran pornografi maupun *website* porno yang banyak beredar dan mudah diakses di internet.

g. Pasal 282 dan 311 KUHP dapat dikenakan untuk penyebaran foto atau film pribadi seseorang yang vulgar di internet.

h. Pasal 378 dan 262 KUHP dapat dikenakan pada kasus *carding*, karena pelaku melakukan penipuan seolah-olah ingin membeli suatu barang dan membayar dengan kartu kredit yang nomor kartu kreditnya merupakan hasil curian.

i. Pasal 406 KUHP dapat dikenakan pada kasus *deface* suatu *website*, karena pelaku setelah berhasil memasuki *website* korban,

selanjutnya melakukan pengrusakan dengan cara mengganti tampilan asli dari *website* tersebut.

Terhadap perbuatan dalam ketentuan-ketentuan pasal di atas, masalah yang timbul adalah interpretasi terhadap unsur-unsur pasal karena rumusan pasal-pasal tersebut tidak disebutkan data komputer atau informasi yang dihasilkan komputer. Perkembangan teknologi informasi seiring berkembangnya sistem jaringan komputer telah mengubah pandangan konvensional terhadap unsure barang atau benda sebagai alat buktimenjadi digital *evidence* atau alat bukti elektronik baik sebagai media seperti *disket*, *tape storage*, *disk storage*, *compact disk*, *hard disk*, *USB*, *flash disk* dan hasil cetakan bukti elektronis tersebut.

Jaringan komputer yang menghasilkan *cyberspace* ada komunitas virtualnya berkembang seiring dengan berkembangnya kejahatan yang menghasikan tindak pidana yang dianggap dahulu tidak mungkin pada saat sekarang ini menjadi mungkin dampaknya dapat dirasakan diluar tempat/wilayah negara. Oleh karena itu penerapan pasal-pasal KUHP sudah tidak relevan dalam penanggulangan tinda pidana tenologi informasi.

Negara Indonesia telah membuat kebijakan yang berhubungan dengan hukum teknologi informasi (*law of information technology*) setelah diundangkannya Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) pada Tanggal 21 April 2008 oleh Menteri Hukum dan Hak Asasi Manusia. Produk hukum yang berkaitan dengan ruang siber (*cyber space*) atau maysntara ini dianggap oleh pemerintah perlu untuk memberikan

keamanan dan kepastian hukum dalam pemanfaatan teknologi informasi, media, dan komunikasi agar dapat berkembang secara optimal.

Kritik masyarakat bagi dari akademisi, aparat penegak hukum, para *bloggers* terutama hacker pada saat disyahkannya UU ITE adalah hal yang wajar di era demokratisasi seperti saat ini. Karena dalam merumuskan peraturan hukum dewasa ini harus mempertimbangkan secara komprehensif beraga dimensi persoalan. Di sini orang akan mempersoalkan hak-hak warga seperti kebebasan berekspresi, kebebasan media, dan masalah-masalh HAM seperti: persoalan privasi, hak untuk memperoleh informasi, dan sebagainya yang saat ini sangat diperhatikan dalam legislasi positif nasional. Disinilah relevansi persoalan hak dan kewajiban menjadi penting.

Penanggulangan kejahatan di dunia maya tidak terlepas dari kebijakan penanggulangan kejahatan atau yang biasa dikenal dengan istilah "politik kriminal" menurut Sudarto politik kriminal merupakan suatu usaha ang rasional dari masyarakat dalam menanggulangi kejahatan".[40] Oleh karena itu tujuan pembuatan UU ITE tidak terlepas dari tujuan politik criminal yaitu sebagai upaya untuk kesejahteraan sosial (*social welfare*) dan untuk perlindungan masyarakat (*social defence*).

Evaluasai terhadap kebijakan di dunia mayantara tetap diperlukan sekiranya ada kelemahan kebijakan formulasi dalam perundang-undangan tersebut. Menurut Barda Nawawi Arief evaluasai atau kajian ulang perlu dilakukan, karena ada keterkaitan erat antara kebijakan formulasi perundang-

---

[40]Sudarto, Hukum dan Hukum Pidana, *Op. Cit*, hlm. 38

undangan (*legaslative policy*) dengan kebijakan penegakan hukum (*law enforcement policy*) dan kebijakan pemberantasan/penangulangan kejahantan (*criminal policy*). Kelemahan kebijakan formulasi hukum pidana, akan berpengaruh pada kebijakan penegakan hukum pidana dan kebijakan penanggulangan kejahatan.[41]

Dilihat dari persfektif hukum pidana maka kebijakan formulasi harus memperhatikan harmonisasi internal dengan sistem hukum pidana atau aturan pemidanaan umum yang berlaku saat ini. Tidaklah dapat dikatakan terjadi harmonisasi/sinkronisasi apabila kebijakan formulasi berada di luar sistem hukum pidana yang berlaku saat ini.

Penanggulangan kejahatan dengan sistem hukum pidana pada tahapan formulasi pada intinya menurut Nils Jareborg mencakup tiga masalah pokok struktur sistem hukum pidana, yaitu masalah:

1. Perumusan tindak pidana/kriminalisasi dan pidana yang diancamkan (*criminalization and threatened punishment*)
2. Pemidanaan (*adjudication of punishment sentencing*)
3. Pelaksanaan pidana (*execution of punishment*).[42]

---

[41]Barda Nawawi Areif, Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan, *Op. Cit*, hlm. 214-215

[42]*Ibid*, hlm. 215

B. Kebijakan Penegakan Hukum Dalam Upaya Penanggulangan Tindak Pidana Teknologi Informasi

Kebijakan penegakan hukum ini meliputi proses apa yang dinamakan sebagai kebijakan kriminal atau *criminal policy*. Konsep dari kebijakan penegakan hukum inilah yang nantinya akan diaplikasikan melalui tataran institusional melalui suatu sistem yang dinamakan *Criminal Justice System*. (Sistem Peradilan Pidana), karenanya ada suatu keterkaitan antara kebijakan penegakan hukum dengan Sistem Peradilan Pidana, yaitu sub siste dari Sistem Peradilan Pidana inilah yang nantinya akan melaksanakan kebijakan penegakan hukum berupa pencegahan dan penanggulangan terjadinya suatu kejahatan dimana peran-peran dari sub sistem ini akan menjadi lebih *acceptable* bersama-sama denga peran masyarakatnya. Tanpa peran masyarakat, kebijakan penegakan hukum akan menjadi tidak optimalistis sifatnya.[43]

Perkembangan teknologi informasi di era globalisasi yang semakin berkembang, dibarengi dengan pembentukan hukum teknologi informasi dewasa ini hendaknya diikuti dengan langkah-langkah antisipatif oleh aparat penegak hukum untu mencapai keseimbangan dan tata pergaulan di tengah-tengah kehidupan kelompok, golongan, ras dan suku, serta masyarakat, di dalam suatu negara maupun dalam hubungan dengan pergaulan di kawasan regional dan internasional.

Masalah pokok penegakan hukum sebenarnya terletak pada factor-faktor yang mungkin mempengaruhinya. Menurut Soerjono Sekanto yang

---

[43]Indriyanto Seno Adji, *Korupsi Sistematik dan Kendala Penegak Hukum di Indonesia*, Jurnal Sudi Kepolisian Perguruan Tinggi Ilmu Kepolisian, Restu Agung, 2005, hlm. 9

mempengaruhi penegakan hukum tersebut mempunyai arti yang netral, sehingga dampak positif atau negatifnya terletak pada isi faktor-faktor tersebut. Faktor-faktor tersebut adalah:[44]

1. Faktor hukumnya sendiri (undang-undang)
2. Faktor penegak hukum yakni pihak yang membentuk maupun menerapkan hukum
3. Faktor sarana atau fasilitas yang mendukung penegakan hukum
4. Faktor masyarakat, yakni lingkungan dimana hukum tersebut berlaku atau diterapkan
5. Faktor kebudayaan, yakni sebagai hasil karya, cipta, dan rasa yang didasarkan pada karsa manusia dalam pergaulaan hidup.

Berdasarkan ke 5 (lima) faktor di atas, menurut Sutarman dalam menjamin keamanan, keadilan dan kepastian hukum dalam penegakan hukum (*law inforcement*) di dunia *cyber* dapat terlaksana dengan baik maka harus dipenuhi 4 (empat) syarat yaitu:[45]

1. Adanya aturan perundang-undangan khusus yang mengatur dunia *cyber*
2. Adanya lembaga yang akan menjalankan peraturan yaitu polisi, jaksa dan hakim khusus menangani *cybercrime*
3. Adanya fasilitas atau sarana untuk mendukung pelaksanaan peraturan itu
4. Kesadara hukum dari masyarakat yang terkena peraturan.

Selain ke 4 (empat) syarat tersebut penegakan hukum di dunia maya juga sangat tergantung dari pembuktian dan yurisdiksi yang ditentukan oleh undang-undang.

Saat ini Indonesia memiliki *cyber law* untuk mengatur dunia maya berikut sanksi bila terjadi *cybercrime* baik di wilayah Indnesia maupun di luar wilayah

---

[44]Soerjono Soekanto, *Faktor-faktor Yang Mempengaruhi Penegakan Hukum*, Raja GrafindoPersada, Jakarta, 2005, hlm. 8

[45]Sutarman, *Cybercrime: Modus Operandi dan Penanggulangannya*, Laksbang Pressindo, Yogyakarta, 2007, hlm. 108-109

hukum Indonesia yang akibatnya dirasakan di Indonesia. *Cybercrime* terus berkembang seiring dengan revolusi teknologi informasi yang membalikkan paradigma lama terhadap kejahatan konvensional kearah kejahatan virtual dengan memanfaatkan instrument elektronik tetapi akibatnya dapat dirasakan secara nyata.

Penanggulangan *cybercrime* oleh aparat penegak hukum sangat dipengaruhi oleh adanya peraturan perundang-undangan. Penegakan hukum *cybercrime* dilakukan dengan menafsirkan *cybercrime* ke dalam perundang-ujdangan KUHP dan khususnya undang-undang yang terkait dengan perkembangan teknologi informasi seperti:

1. Undang-undang Nomor 36 tahun 1999 tentang Telekomunikasi
2. Undang-undang Nomor 19 tahun 2002 tentang Hak Cipta
3. Undang-undang Nomor 25 tahun 2003 tentang Perubahan atas Undang-undang Nomor 15 tahun 2002 tentang Tindak Pidana Pencucian Uang
4. Undang-undang Nomor 15 tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme.

Penafsiran tersebut dapat dilakukan oleh aparat penegak hukum melalui metode penafsiran ekstensif bukan analogi. Moeljatno memberikan batasan pengertian terhadap penafsiran ekstensif dan analogi. Penafsiran ekstensif adalah perkataan yang diberi arti menurut makna yang hidup dalam masyarakat sekarang dan tetap berpegang pada aturan yang ada. Sedangkan dalam penafsiran analogi,

perbuatan yang menjadi soal itu tidak bias dimasukkaan dalam aturan yang ada, berpegang pada ratio.[46]

Penafsiran hukum melalui analogi menurut Sudarto artinya memperluas berlakunya suatu peraturan dengan mengabstraksikannya menjadi aturan hukum yang menjadi dasar dari peraturan itu (*ratio legis*) dan kemudian menarapkan aturan yang bersifat umum ini kepada perbuatan konkrit yang tidak diatur dalam undang-undang.[47]

Penerapan hukum positif tersebut tidaklah sederhana mengingat karakteristik *cybercrime* yang bersifat khas. Metode penafsiran secara analogi bagaimanapun juga tidak diperbolehkan. Namun penafsiran ekstensif diperbolehkan, agar tidak terjadi penafsiran aalogi, maka kebijakan penanggulangan tinda pidana teknologi informasi melalui UU ITE dapat menjadi solusi dalam melindungi internet dan penggunanya

Instrumen hukum *cyber* dengan keluarnya UU ITE memberikan landasan atau pedoman bagi para penegak hukum yang akan diterapkan pada para pelaku *cybercrime*. UU ITEdiharapkan sebagai kekuatan pengendali dan penegak ketertiban bagi kegiatan pemanfaatan analogi informasi tidak hanya terbatas pada kegiatan internet, tetapi semua kegiatan yang memanfaatkan perangkat komputer, dan instruken elektronik lainnya.

Penegak hukum di Indonesia mengalami kesulitan dalam menghadapi merebaknya *cybercrime*. Hal ini dilatarbelakangi masih sedikitnya aparat penegak hukum yang memahami seluk beluk teknologi informasi (*internet*), disamping itu

---

[46]Moeljatno, *Asas-asas Hukum Pidana*, Cetakan VI, Rineka Cipta, Jakarta, 2000, hlm. 28
[47]Sudarto, *Hukum Pidana. I*, Yayasan Sudarto, Semarang, 1990, hlm. 23

aparat penegak hukum di daerah pun belum siap dalam mengantisipasi maraknya kejahatan ini karena masih banyak aparat penegak hukum yang gagap teknologi "gaptek" hal ini disebabkan oleh masih banyaknya institusi-institusi penegak hukum di daerah yang belum didukung dengan jaringan intsernet.

Faktor yang mempengaruhi penegak hukum selanjutnya adalah sarana dan fasilitas, tanpa adanya sarana atau fasilitas, maka tidak mungkin penegakan hukum akan berlangsung dengan lancer. Sarana atau fasilitas tersebut antara lain, mencakup tenaga manusia yang berpendidikan dan terampil, organisasi yang baik, peralatan yang memadai, keuangan yang cukup, dan seterusnya. Kalau hal-hal itu tidak terpenuhi, maka mustahil penegakan hukum akan mencapa tujuan.

Sarana atau fasilitas komputer hampir dimiliki oleh semua kesatuan aparat penegak hukum, namun masih sebatas untuk keperluan mengetik. Alat ini akan sangat membantu manakala dilengkapi dengan akses internet. Kirangnya sarana dan perasarana dalam penagakan hukum *cybercrime*, sangat berpengaruh terhadap kinerja aparat penegak hukum dalam menghadapi *high-tech crimes*. Aparat penegak hukum perlu informasi yang dapat diakses melalui jaringan internet.

Faktor penegakan hukum selanjutnya adalah keasadaran masyarakat. Dalam konsep keamanan masyarakat modern, sistem keamanan bukan lagi tanggung jawab penegak hukum semata, namun menjadi tanggung jawab bersama seluruh elemen masyarakat. Dalam pandangan konsep ini, masyarakat di samping sebagai objek juga sebagai subjek. Sebagai subjek, masyarakat adalah pelaku aktivitas komunikasi antara yang satu dengan yang lain, serta pengguna jasa

kegiatan internet dan media lainnya. Sebagai objek, masyarakat dijadikan sasaran dan korban kejahatan bagi segenap aktivitas kriminalisasi internet.

Tanggung jawab bersama atas keamanan dan ketertiban di tengah masyarakat dalam konsep modern disebut *community policing*. Salah satu model pengamanan dan penegakan hukum yang professional di negara-negara maju. Semua elemen masyarakat dengan kesadaran penuh terpanggil dan bertanggung jawab atas keamanan dan ketertiban.

Dilibatkannya masyarakat dalam strategi pencegahan kejahatan mempunyai 2 (dua) tujuan pokok, menurut Mohammad Kemal Dermawan, adalah:

1. Mengeliminir faktor-faktor kriminigen yang ada dalam masyarakat
2. menggerakkan potensi masyarakat dalam hal mencegah dan mengurangi kejahatan.[48]

Sampai saat ini, kesadaran hukum masyarakat untuk melakukan pengamanan dan merespon aktivitas *cybercrime* masih dirasakan kurang. Hal ini disebabkan antara lain oleh kurangnya pemahaman dan pengetahuan (*lack of information*) masyarakat terhadap jenis kejahatan *cybercrime*. *Lack of information* ini menyebabkan upaya penanggulangan *cybercrime* mengalami kendala, dalam hal ini kendala yang berkenaan dengan penataan hukum dan proses pengawasan (*controlling*) masyarakat terhadap setiap aktivitas yang diduga berkaitan dengan *cybercrime*.

---

[48]Mohammde Kemal Dermawan, *Strategi Pencegahan Kejahatan*, Citra Aditya Bhakti, Bandung, 1994, hlm. 10

Melalui pemahaman yang komprehensif mengenai *cybercrime*, peran masyarakat menjadi sangat penting dalam upaya pengawasan, ketika masyarakat mengalami *lack of information*, peran mereka akan menjad mandul. Sebaliknya ketika masyarakat memahami bahwa *cybercrime* merupakan tindak pidana yang harus ditanggulangi, masyarakat akan mengantisipasinya atau melaporkannya kepada aparat kepolisian setempat.

BAB. IV

P E N U T U P

Dari apa yang telah diuraikan dalam bab-bab terdahulu, terutama yang ada sangkut pautnya dengan permasalahan, maka dapat ditarik kesimpulan dan saran-saran sebagai berikut.

A. Kesimpulan

1. Kebijakan formulasi hukum pidana terhadap tindak pidana teknologi informasi adalah: harus memperhatikan harmonisasi internal dengan sistem hukum pidana atau aturan pemidanaan umum yang berlaku saat ini. Tidaklah dapat dikatakan terjadi harmonisasi/sinkronisasi apabila kebijakan formulasi berada diluar sistem hukum pidana yang berlaku saat ini.
2. Kebijakan penegakan hukum dalam upaya penanggulangan tindak pidana teknologi informasi adalah:
    a. Adanya aturan perundang-undangan khusus yang mengatur dunia *cyber*
    b. Adanya lembaga yang akan menjalankan peraturan yaitu polisi, jaksa dan hakim khusus mengenai *cybercrime*
    c. Adanya fasilitas atau sarana untuk mendukung pelaksanaan peraturan itu
    d. Kesadaran hukum dari masyarakat yang terkena peraturan.

B. Saran-saran

1. Hendaknya harmonisasi internal dengan sistem hukum pidana atau aturan umum yang berlaku benar-benar diperhatikan agar kebijakan formulasi hukum pidana terhadap tindak pidana teknologi informasi saat ini benar-benar dapat dilaksanakan.
2. Perlu dilakukan penyuluhan kepada masyarakat mengenai penegakan hukum informasi, agar masyarakat mengetahuinya sehinga terjamin keamanan, keadilan dan kepastian hukumnya.

DAFTAR PUSTAKA

Buku-buku:

Abdul Wahib dan Mohammad Labib, *Kejahatan Mayantara (Cybercrime)*, Rafika Aditama, Bandung, 2005

Agus Rahardjo, *Cybercrime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, Citra Aditya Bakti, Bandung, 2002

Andi Hamzah, *Aspek-aspek Pidana di Bidang Komputer*, Raja Grafindo Persada, Jakarta, 1998

Bambang Sunggono, *Metode Penelitian Hukum*, Raja Grafindo Persada, Jakarta, 1997

Barda Nawawi Arief, *Masalah Peegakan Hukum dan Kebijakan Hukum Pidana Dalam Menanggulangi Kejahatan*, Kencana Media Group, Jakarta, 2007

----------, *Bunga Rampai Kebijakan Hukum Pidana*, Raja Grafindo Persada, Jakarta, 2006

----------, *Sari Kuliah Perbandingan Hukum Pidana*, Raja Grafindo Persada, Jakarta, 2006

----------, *Kapita Selekta Hukum Pidana*, Citra Aditya Bakti, Bandung, 2003

Departemen Pendidikan dan Kebudayaan, *Kamus Bahasa Indonesia*, Balai Pustaka, Jakarta, 1997

Freddy Haris, *Cybercrime dari Perspektif Akademis*, Lembaga Kajian Hukum dan Teknologi FH UI, Jakarta

Henry Cambell Black, *Black's Law Dictionary*, Seventh Edition, St Paulimin West Publicing. Co, 1999

Muladi, Demokrasi, *Hak zasi Manusia dan Reformasi Hukum di Indonesia*, The Habibis Center, Jakarta, 2002

Muljatno, *Azas-azas Hukum Pidana*, Rineka Cipta, Jakarta, 2000

Nyoman Sarikat Putra Jaya, *Beberapa Pemikiran Kearah Pengembangan Hukum Pidana*, Citra Aditya Bakti, Bandung 2008

Satjipto Rahardjo, *Hukum dan Masyarakat*, Angkasa, Bandung, 1980

Sudarto, *Hukum dan Hukum Pidana*, Alumni, Bandung, 1977

Sutarman, *Cybercrime: Modus perandi dan Penanggulangannya*, Laksbang Pressindo, Yogyakarta, 2007

Soerjono Soekanto, *Faktor-faktor Yang Mempengaruhi Penegakan Hukum*, Raja Grafindo Persada, Jakarta, 2005

Utanto, dkk, *Cybercrime-motif dan Penindakan*, Pensil 324, Jakarta

Wisnusubroto, *Kebijakan Hukum Pidana Dalam Penanggulangan Penyalahgunaan Komputer*, Universitas Atmajaya, Yogyakarta, 1999

Yudha Bhakti Ardhiwisastra, *Imunitas Kedaulatan Negara di Forum Pengadilan Asing*, Alumni, Bandung, 1999

Makalah dan Artkel:

Ahmad M Ramli, *Perkembangan Cyberlaw Gobal da Implikasinya Bagi Bangsa Indonesia, Makalah Seminar The Impormantance of Information System Scurity in E-Government*, Tim Koordinasi Telematika Indonesia, Jakarta, 28 Juli 2004

Barda Nawawi Arief, *Antisipasi Penanggulangan "cybersrime" Dengan Hukum Pidana*, Makalah Seminar Nasional Mengenai "cybersrime", di STHB Bandung, Hotel Grand quila, 9 April 2001

Romli Atmasasmita, *Ruang Lingkup Berlakunya Hukum Pidana Terhadap Kejahatan Transnasional Terorganisasi*, Artikel dalam Padjadjaran Jilid XXIV No 2 Tahun 1996

Tiens Saefullah, *Jurisdiksi Sebagai Upaya Penegakan Hukum Dalam Kegiatan Cybercrime*, Artikel dalam Cyberlaw. Suatu Pengantar, Pusat Studi Cyberlaw FH UNPAD, ELIPs, 2002

UNIVERSITAS MUHAMMADIYAH PALEMBANG
FAKULTAS HUKUM

KARTU AKTIVITAS BIMBINGAN SKRIPSI

Nama Mahasiswa	: Rahmat Hidayat
NOMOR POKOK	: 50 2011 376
JURUSAN	: Ilmu Hukum
PROG. KEKHUSUSAN	: Hukum Pidana

Pembimbing:
Reny Okprianti, SH., M.Hum

JUDUL SKRIPSI : KEBIJAKAN FORMULASI HUKUM PIDANA TERHADAP TINDAK PIDANA TEKNOLOGI INFORMASI

KONSULTASI KE-	MATERI YANG DIBIMBINGKAN	PARAF PEMBIMBING	KET.
I 5/9-17	Konsul Out line		
II 12/9-17	Acc Out line, lanjut Bab I		
III 19/9-17	Konsul Bab I		
IV 26/9-17	Konsul & Acc Bab I lanjut ujian Proposal		
25/10-17	Konsul Bab II		
1/11-17	Acc Bab II, lanjut Bab III & IV		

KONSULTASI KE-	MATERI YANG DIBIMBINGKAN	PARAF PEMBIMBING	KET.
5/12-14	Koreksi Bab III s/d IV		
01/01-15	Acc Bab III s/d IV		
07/02-15	Koreksi keseluruhan		
15/02-15	Acc cetak		

CATATAN:
MOHON DIBERI WAKTU
MENYELESAIKAN SKRIPSI
..... BLN SEJAK TGL.
DIKELUARKAN / DITETAPKAN

DIKELUARKAN : DI PALEMBANG
PADA TANGGAL :
Ketua Bagian Hukum Pidana,

LUIL MAKNUN, SH., MH

SURAT PERNYATAAN

Yang bertanda tangan dibawah ini:

Nama : RAHMAT HIDAYAT

NIM : 50 2011 376

Program Study : Ilmu Hukum

Program Kekhususan : Hukum Pidana

Menyatakan bahwa skripsi yang berjudul:

"KEBIJAKAN FORMULASI HUKUM PIDANA TERHADAP TINDAK PIDANA TEKNOLOGI INFORMASI"

Adalah bukan merupakan karya tulis orang lain, kecuali dalam bentuk kutipan yang telah saya sebutkan sumbernya. Apabila pernyataan ini tidak benar maka saya bersedia mendapatkan sanksi akademik.

Demikianlah pernyataan ini saya buat dengan sebenar-benarnya.

Palembang, Pebruari 2015

Yang menyatakan,

RAHMAT HIDAYAT

UNIVERSITAS MUHAMMADIYAH PALEMBANG
FAKULTAS HUKUM

Lampiran : Outline Skripsi
Perihal : Penelitian Hukum dan Penulisan Skripsi
Kepada : Yth. Ibu. Halisah Hayatuddin, SH., M.Hum
Pembimbing Akademik Fakultas Hukum UMP
di-
Palembang.

Assalamu'alaikum Wr. Wb.

Saya yang bertanda tangan dibawah ini:
Nama : Rahmat Hidayat
Nim : 50 2011 376
Program Kekhususan : Hukum Pidana

Pada semester Ganjil tahun kuliah 2014/2015 sudah menyelesaikan beban study yang meliputi MPK, MKKK, MKB, MPB, MBB (130 sks).

Dengan ini mengajukan permohonan untuk Penelitian Hukum dan Penulisan Skripsi dengan judul: "Kebijakan formulasi hukum pidana terhadap tindak pidana teknologi informasi"

Demikianlah atas perkenannya diucapkan terima kasih.
Wassalam.

Palembang, September 2014
Pemohon

Rahmat Hidayat

Rekomendasi PA, Ybs:

Pembimbing Akademik

Halisah Hayatuddin, SH., M.Hum

UNIVERSITAS MUHAMMADIYAH PALEMBANG
FAKULTAS HUKUM

REKOMENDASI DAN PEMBIMBING SKRIPSI

Nama	: Rahmat Hidayat
Nim	: 50 2011 376
Program Study	: Ilmu Hukum
Program Kekhususan	: Hukum Pidana
Judul Skripsi	: Kebijakan formulasi hukum pidana terhadap tindak pidana teknologi informasi

I. Rekomendasi Ketua Bagian : Hukum Pidana

a. Rekomendasi : Judul dpt disempurnakan

b. Usulan Pembimbing : 1. Reny Okprianti, SH. MH.

2. .....

Palembang, September 2014
Ketua Bagian,

Luil Maknun, SH., MH

II. Penetapan Pembimbing Skripsi Oleh Wakil Dekan I

1. Reni Okprianti, SH. MH.

2. .....

Palembang, September 2014
Wakil Dekan I,

Dr. Hj. Sri Sulastri, SH.,M.Hum