PENANGGULANGAN KEJAHATAN INTERNET DI INDONESIA

Nuria Siswi Enggarani

Fakultas Hukum
Universitas Muhammadiyah Surakarta
nurinasaku@gmail.com

Abstract

Straightening of the law of Cybercrime have to be supported by three aspect which is related to enforcer punishment aspect, that is : 1. law instrumental aspect, 2. enforcer government officer and its application in field. Law Instrumental Aspect could be happen with the existence of various law of. Thats including Information And Technological Law (ITE) which it can minimize the effect of the badness of the cybercrime, with the attended Of Information and Technological Law, that will give some benefit, that is : guarantying rule of law to society [doing/conducting] electronic transaction, pushing economic growth, preventing the happening of badness base on information technology and protect service user society by exploiting information technology. As for important breakthrough which owned it, thats first. An electronical signature confessed to have the power of law which is equal to conventional signature. Both, electronic evidence appliance confessed like an other evidence appliance which arranged in KUHAP. Third, Information and Technological Law could be applying to each and everyone who can do or conducting in deed of law, both for residing in Indonesia region and also outside Indonesia owning legal consequences in Indonesia.

Key words: *cyber crime, cyber police*

PENDAHULUAN

Perkembangan teknologi khususnya di bidang telekomunikasi dan transportasi dianggap sebagai lokomotif dan turut mempercepat proses globalisasi

di pelbagai aspek kehidupan[1]Perkembangan yang pesat dari teknologi telekomunikasi dan teknologi komputer menghasilkan internet yang multifungsi. Perkembangan ini membawa kita ke ambang revolusi keempat dalam sejarah pemikiran manusia bila ditinjau dari konstruksi pengetahuan umat manusia yang dicirikan dengan cara berfikir yang tanpa batas (*borderless way of thinking*).[2]Internet membuat globe dunia, seolah-olah menjadi seperti hanya "selebar daun kelor".

Perkembangan ini membawa perubahan yang besar dan mendasar pada tatanan sosial dan budaya pada skala global.Namun dibalik kemudahan layanan internet, terdapat ancaman dari sisi keamanannya.Perkembangan teknologi informasi menghasikan internet yang multi-fungsi dan dampak positif maupun negatif pada kehidupan manusia.Internet ialah jaringan global antar komputer untuk berkomunikasi dari satu lokasi kelokasi lainnya dibelahan dunia (seperti sekolah, universitas, institusi riset, museum, bank, perusahaan bisnis, perorangan, stasiun TV ataupun radio).

Pengamanan sistem informasi berbasis internet perlu diperhatikan, karena jaringan internet yang bersifat publik dan global sangat rentan dari berbagai kejahatan.Ancaman timbul manakala seseorang mempunyai keinginan memperoleh akses *illegal* ke dalam jaringan komputer, merusak jaringan, mencuri data dengan memanfaatkan teknologi canggih tersebut untuk mencapai tujuan dengan melakukan kejahatan yang merugikan banyak pihak.Kejahatan ini dikenal sebagai kejahatan dunia maya atau *cyber crime*.

Pada saat ini kebutuhan adanya internet didominasi para kalangan pelajar mulai dari sekolah dasar (SD) sampai dengan SMU dan Mahasiswa, dewasa bahkan sampai dengan orangtua.Internet memang ibarat pisau bermata dua. Disatu sisi, teknologi ini bisa bermanfaat apabila digunakan untuk melakukan hal-hal yang baik dan bermanfaat, seperti: mencari bahan-bahan pelajaran sekolah, diskusi mata pelajaran, mencari program beasiswa, belajar jarak jauh, dan mencari metode-metode pengajaran berbasis multimedia. Sedangkan dampak negative dari internet misalnya banyaknya situs-situs pornografi, pornoaksi, perjudian, kekerasan dan lain-lain, yang mengakibatkan maraknya tindakan-tindakan perkosaan, pelecehan sexual, yang disebabkan para remaja yang gemar membuka situs-situs terlarang di internet, selain itu maraknya tindakan-tindakan

[1] Muhammad Aulia Adnan, Tinjauan Hukum dalam E Business Olyx76@Yahoo.com

[2] Steven Harnad, *Post-Gutenberg Galaxy: The Fourth Revolution in the Means of Production of Knowledge*, Public-Access Computer System Review 2 (1): 39-53, versi elektronik dapat dibaca pada http://cogprints.org/1580/00/harnad91.postgutenberg.html.

kejahatan didunia maya seperti carding, Hacking, membobol pasword orang lain, facebook, yang merupakan situs jejaring pertemanan. Penculikan para remaja melalui facebook, yang merupakan situs jejaring pertemanan sampai pada kasus terakhir yang pernah menggegerkan public yaitu kasus Prita mulyasari versus RS Omni Internasional terkait dengan kasus tindakan pencemaran nama baik lewat email pribadi Prita mulyasari yang berkaitan dengan pelayanan RS Omni Internasional, merupakan serangkaian kasus yang terjadi di dunia maya. Sehingga dapat disimpulkan bahwa globalisasi teknologi juga dibarengi oleh globalisasi kejahatan.

Dampak perkembangan teknologi informasi selain menyangkut aspek ekonomi dan sosial budaya juga menyangkut aspek hukum, karena ICT pada akhirnya memunculkan sisi hitam dalam kehidupan umat manusia, yaitu adanya segelintir orang yang memanfaatkan teknologi untuk kepentingan pribadi dengan merugikan pihak lain *(cyber crime)* sehingga memerlukan penanganan hukum tersendiri *(cyberlaw)*. contoh kasus: Penipuan terhadap institusi keuangan, termasuk dalam kategori ini antara lain penipuan dengan modus menggunakan alat pembayaran seperti kartu kredit dan atau kartu debit dengan cara berbelanja melalui Internet. Penipuan dengan kedok penawaran transaksi bisnis, penipuan kategori ini dapat dilakukan oleh dua belah pihak; pengusaha dan individu. umumnya dalam bentuk penawaran investasi atau jual beli barang / jasa. Penipuan terhadap instansi pemerintah,termasuk dalam kategori ini adalah penipuan pajak, penipuan dalam proses e-procurement dan layanan e-government, baik yang dilakukan oleh anggota masyarakat kepada pemerintah ataupun oleh aparat birokrasi kepada rakyat.

Fenomena kejahatan *cyber crime*sendiri di Indonesia semakin lama semakin meningkat dengan berbagai kasus yang bervariasi seperti kasus pemakaian nama domain Mustika Ratu. com, YKCI vs Indosat (Royalti 'ring back tone'), Kasus lain adalah perusakan fasilitas internet banking BCA dengan membuat situs tiruan www.klikbca.com oleh seorang hacker seperti kilkbca.com, www.klickbca.com, klickbca.com, clickbca.com, Contoh lain pernah terjadi di beberapa kota besar seperti di yogyakarta, bandung, semarang yaitu dengan ditangkapnya beberapa pemuda yang melakukan kejahatan cyber crime dengan modus *carding* (kejahatan internet dengan membobol kartu kredit orang lain untuk bertransaksi) yang membuat Indonesia menjadi salah satu Negara terkenal dalam cybercrime dan modus *hacking* (perusakan jaringan komputer pihak lain). Kasus yang menghebohkan lagi adalah hacker bernama Dani Hermansyah, pada tanggal 17 April 2004 melakukan *deface* dengan mengubah nama-nama

partai yang ada dengan nama-nama buah dalam website www.kpu.go.id yang mengakibatkan berkurangnya kepercayaan masyarakat terhadap pemilu yang sedang berlangsung pada saat itu. Di kota Surakarta sendiri kasus *cybercrime* belum pernah mencuat, akan tetapi yang terbaru adalah adanya kasus pembobolan data melalui email yang dilakukan warga pasarkliwon.

Dalam penggunaannya sendiri salah satu contoh situs di internet yaitu facebook bisa dikatakan dapat memberikan dampak positif dan negatif bagi seseorang.Dampak positif yang dirasakan oleh para pengguna facebook selain untuk sarana bersosialisasi, komunikasi, rekreasi, chatting, berkomunikasi dengan teman lama, facebook pun berfungsi untuk sarana berdiskusi bahkan sampai bisa digunakan untuk mengumpulkan bantuan untuk kegiatan social seperti koin untuk prita, koin untuk bilqis dsb.Sedangkan dampak negative dari penggunaan facebook yaitu membuat orang menjadi malas belajar, hanya membuang-buang waktu bahkan memicu adanya tindak kejahatan berupa penipuan, pelecehan, sampai terjadinya penculikan dan para korban penculikan rata-rata dialami oleh perempuan yang kebanyakan masih berstatus sebagai pelajar.

Budaya global tersebut secara positif memiliki muatan ilmu pengetahuan, teknologi, politik, sosial dan kebudayaan, tetapi juga memiliki dampak negative manakala disalahgunakan.Ancaman atau bahaya yang datang dari internet bagi anak-anak dan remaja menjadi perhatian serius bagi masyarakat Indonesia.Dalam makalah ini, penulis membahas tentang penanggulangan kejahatan internet di Indonesia.

Masyarakat khususnya para remaja yang sekarang sedang digandrungi oleh situs-situs di internet dan paham betul tentang penggunaan internet, perlu dibekali berbagai informasi, dalam rangka untuk mengetahui tentang dampak negatif perkembangan teknologi informasi seperti internet dan tentang penanggulangan kejahatan cybercrime dari aspek hukum, maka diberikan penyuluhan dan pengertian seputar dampak dari perkembangan teknologi informasi, kemudian peraturan yang berkaitan dengan perkembangan teknologi informasi seperti UU ITE No 11 Tahun 2008 yang didalamnya mengatur tentang perbuatan-perbuatan yang dilarang yang berkaitan dengan pencurian, penipuan, perjudian, pencemaran nama baik dst.

PEMBAHASAN

Tinjauan Umum Cyber Crime

Menurut Andi Hamzah, memandang kejahatan komputer bukanlah sebagai kejahatan baru melainkan menganggap kejahatan biasa (tradisionil), kare-

na masih memungkinkan diselesaikan melalui KUHP.[3]. Demikian juga suatu studi dari Kongres Amerika Serikat, menyimpulkan bahwa ada tiga kategori dari tindak pidana di bidang komputer, yakni: pemakaian data yang tidak benar ke dalam komputer, mengubah atau merusak informasi atau arsip dan pencurian, apakah secara elektronis atau cara-cara lain: uang, denda, benda, fasilitas-fasili-tas atau data yang berharga.[4]

Cyber crime atau kejahatan dunia maya adalah kejahatan yang dilakukan oleh seseorang maupun kelompok yang menguasai dan mampu mengoperasikan komputer dan alat telekomunikasi lainnya. Cara-cara yang biasa yang dilakukan dengan merusak data, mencuri data dan menggunakannya secara *ilegall*. Menurut Abdul Wahib dan Mohammad Labib[5], *cyber crime* merupakan salah satu jenis kejahatan yang membahayakan individu, masyarakat dan negara.Jenis kejahatan ini *(cyber crime)* tidak tepat jika disebut sebagai '*crime without victim'*, tetapi dapat dikategorikan sebagai kejahatan yang dapat menimbulkan korban berlapis-lapis baik secara privat maupun publik.Hak privat dapat terancam, terganggu, bahkan rusak atau hilang akibat ulah segelintir orang atau beberapa orang yang memanfaatkan kelebihan ilmunya dan teknologi dengan modus operandi yang tergolong dalam *cyber crime*.

Indra Safitri mengatakan bahwa cybercrime sebagai kejahatan dunia maya yaitu jenis kejahatan yang berkaitan dengan pemanfaatan sebuah teknologi informasi tanpa batas serta memiliki karakteristik yang kuat dengan sebuah rekayasa teknologi yang mengandalkan kepada tingkat keamanan yang tinggi dan kredibilitas dari sebuah informasi yang disampaikan dan diakses oleh pelanggan internet.[6]John Spiropoulos mengungkapkan bahwa *cybercrime* memiliki sifat efisien dan cepat serta sangat menyulitkan bagi pihak penyidik dalam melakukan penangkapan terhadap pelakunya.[7]

Cyber crime yang menggunakan media komunikasi dan komputer, kendati berada di dunia lain dalam bentuk maya tetapi memiliki dampak yang sa-

---

[3] Andi Hamzah, *Hukum Pidana Yang Berkaitan Dengan Komputer*, Sinar Grafika, Jakarta, 1993, Hal 9.

[4] Widyo Pramono, *Kejahatan di Bidang Komputer, Pustaka Sinar Harapan*, Jakarta, 1994, Hal 32.

[5] Abdul Wahib dan Mohammad Labib, *Kejahatan Mayantara (Cyber crime)*, Refika Aditama, Bandung, 2005, Hal 15

[6]Indra Safitri, "Tindak Pidana di Dunia Cyber" dalam Insider, Legal Journal From Indonesian Capital & Investmen Market. Dapat dijumpai di Internet: http://business.fortunecity.com/buffett/842/art180199_tindakpidana.htm.

[7]Jhon Sipropoulus, 1999, "*Cyber Crime Fighting*, The Law Enforcement Officer's Guide to Online Crime", The Natinal Cybercrime Training Partnership, Introduction.

ngat nyata. Penyimpangan dan kerugian besar telah terjadi dan berdampak luas kepada sektor-sektor ekonomi, perbankan, moneter, budaya bahkan dapat mengancam pertahanan dan keamanan negara.Supaya tidak dikucilkan dalam pergaulan global, Indonesia harus mengantisipasi dan melakukan langkah konkrit dalam penanggulangan kejahatan internet.

Kualifikasi kejahatan dunia maya *(cyber crime),* sebagaimana dikutip Barda Nawawi Arief, adalah kualifikasi *cybercrime* menurut *Convention on Cybercrime* 2001 di Bunapest Hongaria, yaitu:[8] (1) *Illegal access*: 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 computer; (4) *System interference*: yaitu sengaja melakukan gangguan atau rintangan serius tanpa hak terhadap berfungsinya sistem computer; (5) *Misuse of Devices*: penyalahgunaan perlengkapan komputer, termasuk program komputer, 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 autenti); (7) *Computer related Fraud*: Penipuan (dengan sengaja dan tanpa hak menyebabkan hilangnya barang/kekayaan orang lain dengan cara memasukkan, mengubah, menghapus data computer atau dengan mengganggu berfungsinya komputer/sistem computer, dengan tujuan untuk memperoleh keuntungan ekonomi bagi dirinya sendiri atau orang lain).

Untuk mencegah merajalelanya tindakan yang termasuk kategori *cyber crime*, pemerintah bersama aparatur penegak hukum perlu segera melakukan tindakan-tindakan penanggulangan dan penegakan hukum yaitu dengan mensosialisasikan, merealisasikan dan mengimplementasikan berbagai peraturan dan perundang-undangan yang telah ada seperti dalam KUHP dan UU ITE untuk menjerat para pelaku kejahatan *cyber crime*.

Sebelum munculnya UU ITE No 11 Tahun 2008, untuk menjerat pelaku *cyber crime,* dipakai undang-undang yang bersifat khusus dan ketentuan-ke-

---

[8] Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*, Jakarta: Kencana Predana Media Group, 2007) , hlm. 246-247.

tentuan yang bersifat umum, seperti: Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi; Undang-Undang Nomor 5 Tahun 1999 tentang Lara-ngan Praktek Monopoli dan Persaingan Usaha yang Tidak Sehat, Undang-Un-dang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, Undang-Undang Nomor 19 Tahun 2002 tentang Hak Cipta, Undang-Undang Nomor 14 Tahun 2001 tentang Hak Paten; Undang-Undang Nomor 15 Tahun 2001 tentang Merk, dan KUHP. Dalam prakteknya, yang sering dipakai adalah Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi dan KUHP.

Undang-Undang No 19 Tahun 2002 tentang Hak Cipta

Tindakan pembajakan program computer tersebut merupakan tindak pidana sebagaimana diatur dalam Pasal 72 ayat (3) yaitu "Barang siapa dengan sengaja dan tanpa hak memperbanyak penggunaan untuk kepentingan komersial suatu program computer dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau denda paling banyak Rp. 500.000.000,00 (lima ratus juta rupiah)".

Undang-Undang No 36 Tahun 1999 tentang Telekomunikasi

Penyalahgunaan Internet yang mengganggu ketertiban umum atau pribadi dapat dikenakan sanksi dalam Undang-Undang ini, terutama bagi para hacker yang masuk kepada sistem jaringan milik orang lain *(illegal acces)* yaitu akses secara tidak sah terhadap system computer, Sebagaimana diatur dalam Pasal 22, yaitu setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah, atau memanipulasi: (a) Akses ke jaringan telekomunikasi; (b) Akses ke jasa telekomunikasi; (c) Akses ke jaringan telekomunikasi khusus.Apabila anda melakukan hal tersebut seperti yang pernah terjadi pada website KPU www.kpu.go.id, maka dapat dikenakan Pasal 50 yang berbunyi "Barang siapa yang melanggar ketentuan sebagaimana di maksud dalam Pasal 22, dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp. 600.000.000,00 (enam ratus juta rupiah).[9]

[9] Petrus Reinhard Golose, *Perkembangan Cyber Crime dan Upaya Penanggulangannya di Indonesia Oleh Polri*, Jakarta: Buliten Hukum Perbankan dan Kebanksentralan, Volume 4 Nomor 2, Agustus, 2006 , hlm. 40

Undang-Undang No 15 Tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme

Undang-undang ini mengatur mengenai alat bukti elektronik sesuai dengan Pasal 27 huruf b Digital evidence atau alat bukti elektronik sangatlah berperan dalam penyelidikan kasus terorisme, karena saat ini komunikasi antara para pelaku di lapangan dengan pimpinan atau aktor intelektualnya dilakukan dengan memanfaatkan fasilitas di Internet.

UU Nomor 20 Tahun 2001 jo UU Nomor 31 Tahun 1999 tentang Tindak Pidana

Pemberantasan Korupsi yaitu dengan memasukkan alat bukti elektronik sebagai alat bukti yang sah, dalam bentuk 'petunjuk', yang diatur dalam Pasal 26 A yang menyatakan sebagai berikut: "Alat bukti yang sah dalam bentuk petunjuk sebagaimana dimaksud dalam Pasal 188 ayat (2) Undang-undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana, khusus untuk tindak pidana korupsi juga dapat diperoleh dari: Alat bukti yang berupa informasi yang diucapkan, dikirim, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu; dan Dokumen.

Para pelaku *cyber crime* dikenakan pasal-pasal dalam KUHP seperti penipuan, pengrusakan server KPU, penggelapan dan pasal pidana lain diluar KUHP seperti UU telekomunikasi dan UU lain yang memiliki sangsi pidana. Untuk KUHP yang sering digunakan adalah: (1) Pasal 362 KUHP dapat dikenakan untuk kasus carding dimana pelaku mencuri nomor kartu kredit milik orang lain. (2) Pasal 378 KUHP dapat dikenakan untuk penipuan dengan seolah-olah menawarkan dan menjual suatu produk atau barang dengan memasang iklan, tetapi, pada kenyataannya ,barang tersebut tidak ada. Hal tersebut dike-tahui setelah uang dikirimkan dan barang yang dipesan tidak datang sehingga pembeli tersebut merasa tertipu. (3) Pasal 335 KUHP dapat dikenakan untuk kasus pengancaman dan pemerasan yang dilakukan melalui e-mail yang dikirimkan oleh pelaku untuk memaksa korban melakukan sesuatu sesuai dengan apa yang diinginkan oleh pelaku dan jika tidak dilaksanakan akan membawa dampak yang membahayakan. Hal ini biasanya dilakukan karena pelaku biasanya mengetahui rahasia korban. (4) Pasal 311 KUHP dapat dikenakan untuk kasus pencemaran nama baik dengan menggunakan media Internet. Modusnya adalah pelaku menyebarkan *e-mail* kepada teman-teman korban tentang suatu cerita yang tidak benar atau mengirimkan *e-mail* kesuatu mailing list sehingga banyak orang mengetahui cerita tidak benar tersebut. (5) Pasal 303 KUHP dapat dikenakan untuk menjerat permainan judi yang dilakukan secara online di

Internet dengan penyelenggara dari Indonesia. (6) Pasal 282 KUHP dapat dikenakan untuk penyebaran pornografi maupun website porno yang banyak beredar dan mudah diakses di Internet. Walaupun berbahasa Indonesia, sangat sulit sekali untuk menindak pelakunya karena mereka melakukan pendaftaran domain tersebut di luar negeri dimana pornografi yang menampilkan orang dewasa bukan merupakan hal yang ilegal. (8) Pasal 406 KUHP dapat dikenakan pada kasus deface atau *hacking* yang membuat system milik orang lain, seperti website atau program menjadi tidak berfungsi atau dapat digunakan sebagaimana mestinya.

Dalam UU ITE beberapa pasal-pasal yang penting adalah: (1) Pasal 30 ayat (1) yang menyebutkan: "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apapun, dipidana dengan pidana penjara paling lama 12 tahun / denda paling banyak Rp. 600 Juta. (2) Pasal 46, ayat (2) "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apapun dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen elektronik, dipidana dengan pidana penjara paling lama 7 tahun dan / denda paling banyak Rp. 700 Juta. Sedangkan ayat (3) "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/ atau sistem elektronik dengan cara apapun dengan melanggar, menerobos, melampaui atau menjebol sistem pengamanan, dipidana dengan pidana penjara paling lama 8 tahun dan / atau denda paling banyak Rp. 800 Juta. (3) Kemudian Pasal 31 sampai dengan pasal 37. Gugatan kelompok atau biasa dikenal dengan *class action,* dinaungi oleh Pasal 38 ayat 2. Di dalam UU tersebut juga dinyatakan bahwa masyarakat dapat mengajukan gugatan perwakilan terhadap pihak yang menyelenggarakan sistem elektronik yang berakibat merugikan masyarakat.

Sebelum UU ITE lahir perkembangan teknologi informasi telah diakomodasi ke dalam UU Nomor 20 Tahun 2001 jo UU Nomor 31 Tahun 1999 tentang Tindak Pidana Pemberantasan Korupsi yaitu dengan memasukkan alat bukti elektronik sebagai alat bukti yang sah, dalam bentuk 'petunjuk', yang diatur dalam Pasal 26 A yang menyatakan sebagai berikut: "Alat bukti yang sah dalam bentuk petunjuk sebagaimana dimaksud dalam Pasal 188 ayat (2) Undang-undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana, khusus untuk tindak pidana korupsi juga dapat diperoleh dari: (1) Alat bukti yang berupa informasi yang diucapkan, dikirim, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu; dan (2) Dokumen, yakni setiap rekaman data atau informasi yang dapat dilihat, dibaca, dan atau didengar yang dapat dikeluarkan dengan atau tanpa bantuan suatu sarana, baik yang tertuang di atas kertas, benda fisik apapun selain kertas, maupun yang

terekam secara elektronik, yang berupa tulisan, suara, gambar, peta, rancangan, foto, huruf, tanda, angka, atau perforasi yang memiliki makna.

Untuk menjerat pelaku kejahatan melalui internet, Tim penyusun RUU KUHP Baru juga telah berusaha memasukkan pasal-pasal baru dan memperluas pengertian-pengertian yang terdapat di dalam Rancangan Undang-Undang KUHP yang ada yang terkait kegiatan-kegiatan cyber space. Konsep Rancangan Undang-Undang KUHP 2000, dimana konsep ini mengalami perubahan sampai dengan 2004 yaitu:

Dalam Buku I (Ketentuan Umum) Dibuat Ketentuan Mengenai: (1) Pengertian "barang" (Pasal 174/178) yang di dalamnya termasuk benda tidak berujud berupa data dan program komputer, jasa telepon atau telekomunikasi atau jasa komputer. (2) Pengertian "anak kunci" (Pasal 178/182) yang di dalamnya termasuk kode rahasia, kunci masuk computer, kartu magnetic, sinyal yang telah di program untuk membuka sesuatu. Menurut Agus Raharjo, maksud dari anak kunci ini kemungkinannya adalah password atau kode-kode tertentu seperti privat atau public key infrastructure. (3) Pengertian "surat" (Pasal 188/192) termasuk data tertulis atau tersimpan dalam disket, pita magnetic, media penyimpanan komputer atau penyimpanan data elektronik lainnya. (4) Pengertian "ruang" (Pasal 189/193) termasuk bentangan atau terminal computer yang dapat diakses dengan cara-cara tertentu. Maksud dari ruang ini kemungkinan termasuk pula dunia maya atau mayantara atau cyberspace atau virtual reality. (5) Pengertian "masuk" (Pasal 190/194) termasuk mengakses komputer atau masuk ke dalam sistem computer. Pengertian masuk menurut Agus Raharjo di sini adalah masuk ke dalam sistem jaringan informasi global yang disebut internet dan kemudian baru masuk ke sebuah situs atau website yang di dalamnya berupa server dan komputer yang termasuk dalam pengelolaan situs.Jadi ada 2 pengertian masuk, yaitu masuk ke internet dan masuk ke situs. (6) Pengertian "jaringan telepon" (Pasal 191/195) termasuk jaringan komputer atau system komunikasi komputer.

Sementara dalam Buku II dinyatakan bahwa dengan dibuatnya ketentuan seperti di atas, maka konsep tidak atau belum membuat delik khusus untuk cyber crime atau computer-related crime. Konsep juga mengubah perumusan delik atau menambah delik-delik baru yang berkaitan dengan kemajuan teknologi., dengan harapan dapat menjaring kasus-kasus cyber crime. Untuk sementara dimasukkan dalam Bab V (Tindak Pidana Terhadap Ketertiban Umum) antara lain: (1) Menyadap pembicaraan di ruangan tertutup dengan alat bantu teknis (Pasal 263/300); (2) Memasang alat Bantu teknis untuk tujuan mendengar atau merekam pembicaraan (Pasal 264/301); (3) Merekam (memiliki atau menyiar-kan) gambar dengan alat bantu teknis di ruangan tidak untuk umum (pasal 266 /303)

Untuk sementara dimasukkan dalam Bab VIII (Tindak Pidana yang membahayakan Keamanan Umum Bagi Orang, Barang, dan Lingkungan Hidup): (1) Mengakses komputer tanpa hak (Pasal 368, Pasal 371, Pasal 372, dan Pasal 373 Konsep 2004); (2) Pornografi anak melalui sistem komputer (Pasal 374 Konsep 2004) Merusak/membuat tidak dapat dipakai bangunan untuk sarana/prasarana pelayanan umum (antara lain bangunan telekomunikasi/komunikasi lewat satelit/ komunikasi jarak jauh) Pasal 630 Konsep 2004. Sementara masalah Pencucian uang (Money Laundering) terdapat di dalam: Pasal 719-Pasal 722 Konsep 2004).

Selama ini terdapat permasalahan ketika suatu UU yang dijadikan pedoman merujuk pada KUHAP sebagai acuan dalam penyidikan, penuntutan maupun pemeriksaan di pengadilan. Hal itu disebabkan dalam KUHAP diatur bahwa alat bukti yang sah hanya meliputi: Keterangan saksi, Keterangan Ahli; Surat; Petunjuk; dan Terdakwa. Sehingga seiring dengan globalisasi KUHAP juga perlu direvisi.

Untuk kejahatan hacking sebagai contoh, bila seseorang melakukan penyadapan, kemudian menghilangkan suatu informasi elektronik, ia bisa dipidana maksimal 10 tahun dan/atau denda Rp800 juta. Hal ini ditegaskan di Pasal 31 dan Pasal 47. Tapi, kegiatan *hacking* bisa dibenarkan. Pasal 31 ayat 3 UU ini mengatakan, intersepsi atau penyadapan dibolehkan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, atau penegak hukum lainnya.

Penanggulangan *Cybercrime* di Indonesia

Pendekatan Teknologi dalamUpaya Pencegahan *Cybercrime*

Pengamanan Software Jaringan Komputer; Tindakan preventif yg dapat dilakukan dalam rangka pengamanan software jaringan komputer sbb: (1) Mengatur akses (acces control), melalui mekanisme *authentication* dengan menggunakan password. (2) Firewall, program yang merupakan sebuah perangkat yang diletakkan antara internet dengan jaringan internal yang berfungsi untuk menjaga agar akses ke dalam maupun keluar dari orang yang tidak berwenang tidak dapat dilakukan. (3) Intruder Detection System (IDS), diantaranya adalah Autobase, mendeteksi probing dengan memonitor *log file. (4) Backup* rutin, untuk cadangan manakala sistem kita berhasil dimasuki pihakn lain. *(intruder)* dll.

Pengamanan Hardware dalam Upaya Pencegahan *Cybercrime*

Langkah-langkah yang dapat dilakukan adalah:Penguncian computer, Penggunaan dial back, adalah penggunaan telepon double, antara telepon kirim dengan telepon terima, dengan cara bergantian dalam pemakaian saluran telepon.

Di Indonesia yang pernah dilakukan adalah upaya sosialisasi computer dan internet di tengah-tengah masyarakat. Upaya ini dapat ditempuh dengan jalan sebagai berikut:[10] (1) Pengenalan Komputer dan Internet Lewat Pendidikan. Penandatangan nota kesepakatan antara PT Indosat dan Depdiknas tentang pengembangan Cyber Education di Malang Jawa Timur, merupakan salah satu upaya pengenalan komputer kepada masyarakat sejak usia dini. Prinsip dasar Cyber Education cukup sederhana, yakni memanfaatkan teknologi multimedia internet untuk menyalurkan suatu materi dari satu tempat ke tempat lain. Untuk itu tempat-tempat yang bersangkutan harus tergabung dalam suatu jaringan komunikasi berbasis protokol internet. PT Indosat, melalui anak perusahaannya Indosat Multi Media, menyediakan infrastruktur sekaligus menyiapkan koneksi internet yang menghubungkan antarlokasi dalam satu jaringan. Depdiknas secara bertahap mengembangkan jaringan internet ke sekolah-sekolah di kabupaten/kota di seluruh Indonesia. Dengan dibangunnya jaringan antar sekolah tersebut maka data pendukung, referensi ataupun berbagai informasi lain yang relevan dapat diperoleh dengan cepat dan mudah. Selain itu juga dapat dilakukan diskusi dan pengajaran jarak jauh. (2) Seminar Teknologi Informasi membantu pengenalan teknologi computer kepada masyarakat. Acara-acara seminar teknologi informasi sangat membantu pengenalan teknologi computer kepada masyarakat.Seminar yang dimaksudkan di sini dalam arti luas, dimana bisa juga dalam bentuk diskusi interaktif, bedah buku teknologi informasi, seminar dan lokakarya (SEMILOKA), workshop dan sebagainya.

Sebenarnya Internet Service Provider (ISP) di Indonesia juga telah melakukan hal serupa, akan tetapi jumlah situs yang diblok belum banyak sehingga para pengakses masih leluasa untuk masuk ke dalam situs tersebut, terutama situs yang berasal dari luar negeri. Untuk itu ISP perlu bekerjasama dengan instansi terkait untuk memutakhirkan daftar situs *child pornography* yang perlu diblok.

Upaya Penegakan Hukum terhadap Cybercrime

Salah satu persoalan yang muncul terkait dengan perkembangan kejahatan transnasional adalah penegakkan hukumnya terhadap para pelaku *cyber crime*. Kejahatan transnasional dalam *cyber crime* jelas akan bersinggungan dengan masalah jurisdiksi. Dalam ruang siber pelaku pelanggaran sulit untuk ditindak oleh karena pelakunya berada di luar wilayah Indonesia.Hal inilah yang kemudian menjadi

[10] Sutarman, *Cybercrime Modus Operandinya dan Penanggulangannya*, Jogjakarta, LaksBangPRESSindo, 2007, hal 102-103.

persoalan jurisdiksi dari penegakan *cybercrime* di Indonesia. Artinya hukum mana yang akan diberlakukan dalam menangani kejahatan cybercrime tersebut.

Terkait dengan penentuan hukum yang berlaku, dikenal adanya beberapa asas yang biasa digunakan, yaitu: (a) *Asas Subjective Territoriality,* Keberlakuan hukum berdasarkan tempat perbuatan dan penyelesaian tindak pidana dilakukan di Negara lain. (b) *Asas Objective Territoriality,* Hukum yang berlaku adalah dimana akibat utama perbuatan itu terjadi dan memberikan dampak kerugian bagi Negara yang bersangkutan. (c) *Asas Nationality,* hukum berlaku berdasarkan kewarganeraan pelaku. (d) *Asas Passive Nationality,* Hukum berlaku berdasarkan kewarganeraan korban. (e) *Asas Protective Principle,* Berlakunya berdasarkan atas keinginan Negara untuk melindungi kepentingan Negara dari kejahatan yang dilakukan diluar wilayahnya. (f) *Asas Universality,* Asas ini diberlakukan untuk lintas Negara terhadap kejahatan yang dianggap sangat serius seperti pembajakan dan terorisme *(crimes against humanity)*.

Kemudian beberapa aspek yang terkait dengan upaya penegakan hukum *cyber crime*.adalah mulai dari aspek instrumen hukum, aparat hukum penegak hukum dan aplikasinya dilapangan.

Aspek Instrumen Hukum

Agar penegakkan hukum dapat terlaksana dengan baik maka harus dipenuhi empat syarat, yaitu: (1) Adanya aturan perundang-undangan khusus yang mengatur dunia *cyber*. (2) Adanya lembaga yang akan menjalankan peraturan yaitu polisi, jaksa dan hakim khusus yang khusus menangani *cyber crime. (3)* Adanya fasilitas atau sarana untuk mendukung pelaksanaan peraturan itu. (4) Kesadaran hukum dari masyarakat yang terkena peraturan.

Tujuan pembentukan undang-undang yang khusus mengatur tentang dunia maya ini adalah untuk pemberatan atas tindakan pelaku agar dapat menimbulkan efek jera dan mengatur sifat khusus dari sistem pembuktian. Dengan adanya undang-undang yang khusus mengatur *cybercrime* maka dapat mempermudah bagi aparat penegak hukum dalam penegakan hukum.

Di beberapa negara seperti Amerika Serikat, Inggris, India telah memiliki undang-undang *cybercrime*, yang berlaku bagi masing-masing negara, bahkan ada deklarasi dunia tentang *cyberspace*. Dengan demikian tidak menutup kemungkinan kita harus mendapatkan informasi atau membutuhkan pemeriksaan di negara lain karena berkembang dan berhubungan dengan kasus yang sedang ditangani di Indonesia, sehingga perlu dilakukan Kerjasama internasional untuk melakukan penegakkan hukum, mengingat kejahatan modern sudah melintasi batas-batas negara

yang dilakukan dengan teknologi dan komunikasi yang canggih. Locus delikti cyber crime melibatkan beberapa negara, sehingga perlu membuat perjanjian bilateral untuk menanggulanginya dan mengatasi setiap masalah yang melibatkan antar negara, khususnya *cyber crime*. Dalam hal ini Indonesia setidaknya telah memiliki UU ITE yang bisa digunakan untuk menjerat para pelaku cybercrime.

UU ITE pada dasarnya mengatur penggunaan informasi dan transaksi elektronik yang dilakukan dengan menggunakan komputer atau media elektronik lainnya.Yang tergolong informasi dalam UU ini tak terbatas pada tulisan, gambar atau suara, tapi juga *e-mail*, telegram dan lainnya.Jangkauan UU ini sangat luas. Sebagaimana tercantum di Pasal 2, UU ini berlaku untuk setiap orang yang melakukan perbuatan hukum, baik yang berada di wilayah Indonesia maupun di luar negeri, yang memiliki akibat hukum di wilayah Indonesia. Bahkan, tindakan yang dilakukan di luar wilayah Indonesia yang merugikan kepentingan Indonesia juga menjadi lingkup UU ini karena setiap transaksi sifatnya lintas Negara.

UU ini juga mengatur alat bukti elektronik dan UU ini memang mengaklamasikan keabsahan penggunaan alat bukti elektronik.Pasal 5 ayat 2 UU ini mengatakan, informasi elektronik merupakan perluasan dari alat bukti yang sah sesuai hukum acara di Indonesia. Tapi ketentuan itu tidak berlaku untuk surat yang menurut UU harus dibuat dalam bentuk tertulis. Selain itu juga tidak berlaku untuk surat beserta dokumennya yang menurut UU harus dibuat dalam bentuk akta notaril atau akta yang dibuat oleh pejabat pembuat akta.

UU ITE memberi ancaman berat kepada para *hacker*.UU ini merinci berbagai jenis ulah *hacker* yang bisa dikategorikan sebagai tindak pidana. Sebagai contoh, bila seseorang melakukan penyadapan, kemudian menghilangkan suatu informasi elektronik, ia bisa dipidana maksimal 10 tahun dan/atau denda Rp800 juta. Hal ini ditegaskan di Pasal 31 dan Pasal 47.Tapi, kegiatan *hacking* bisa dibenarkan.Pasal 31 ayat 3 UU ini mengatakan, intersepsi atau penyadapan dibolehkan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, atau penegak hukum lainnya.

Selain *hacker*, yang was-was dengan kehadiran UU ini adalah pelaku usaha yang menawarkan produk melalui sistem elektronik. Pasal 9 UU ini menegaskan, pelaku usaha harus menyediakan informasi yang lengkap dan benar. Informasi itu di antaranya syarat kontrak, profil produsen dan produk yang ditawarkan.Dengan demikian, pengusaha toko *online* tak bisa menjajakan dagangannya di dunia maya.UU ini juga hendak menyelenggarakan suatu sertifikasi bagi pelaku usaha *online*.Namun, pemerintah sekedar menganjurkan, bukan mewajibkan.Pasal 10 ayat

1 menyatakan, setiap pelaku usaha dapat disertifikasi oleh lembaga sertifikasi keandalan untuk menghindari memanipulasi informasi yang diancam hukuman berat. Berdasarkan Pasal 51, pelakunya bisa dijatuhi hukuman maksimal 12 tahun penjara atau denda Rp12 Miliar.

UU ini juga memperluas pengertian hak karya intelektual (HKI).Pasal 25 UU ini menyebutkan, situs internet dan karya intelektual yang ada di dalam-nya dilindungi sebagai HKI. UU ini juga hendak memerangi penyalahgunaan identitas orang lain. Misalnya, Pasal 26 menyatakan, penggunaan data pribadi seseorang mesti dilakukan atas persetujuan orang yang bersangkutan.Demikian juga terhadap pendistribusian informasi yang mengandung muatan perjudian, penghinaan dan pemerasan atau pengancaman.Larangan ini tertuang di Pasal 27. Adapun sanksinya, sebagaimana tertulis di Pasal 45, adalah pidana penjara maksimal enam bulan atau denda Rp1 Miliar.

Yang diatur dalam UU ini adalah tindak pidana khusus, maka diperlukan penyidik yang khusus pula. Pasal 43 UU ini menyatakan, selain polisi, wewenang penyidikan berada di pundak Pejabat Pegawai Negeri Sipil (PPNS) yaitu Depkominfo, UU ini menjabarkan bahwa PPNS itu berasal dari lingkungan pemerintah yang bertugas di bidang TI dan Transaksi Elektronik.

Dalam melakukan penggeledahan atau penyitaan, PPNS ini mesti mendapat izin Ketua Pengadilan Negeri setempat.Demikian juga dalam melakukan penangkapan dan penyidikan. Selain berkoordinasi dengan kepolisian, PPNS ini dapat bekerja sama dengan penyidik dari negara lain untuk berbagi informasi dan alat bukti. Salah satu wewenang PPNS, menurut isi Pasal 43 ayat 5 huruf (f), adalah meminta bantuan ahli yang diperlukan dalam penyidikan. "Ahli" yang dimaksud di sini tentu saja adalah seseorang yang memiliki keahlian khusus di bidang TI.Namun tak cuma itu.Penjelasan pasal tersebut menyatakan, pengetahuan seorang ahli itu harus bisa dipertanggungjawabkan secara akademis maupun praktis.

Dalam hal terjadi sengketa, UU ini menekankan diberlakukannya asas hukum perdata internasional.Soal kontrak elektronik lintas negara diatur dalam Pasal 18. Ditegaskan di sana, para pihak memiliki kewenangan untuk memilih hukum yang berlaku bagi transaksi yang dibuatnya. Jika para pihak tidak secara spesifik melakukan pilihan hukum, maka yang diberlakukan adalah hukum yang berazaskan hukum perdata internasional.Jika timbul sengketa, para pihak juga memiliki kewenangan menetapkan forum pengadilan, arbitrase, atau lembaga penyelesaian sengketa lainnya.Bab VIII itu mengatur mekanisme pengajuan gugatan, baik secara individual maupun perwakilan.Gugatan kelompok atau biasa dikenal dengan *class action,* dinaungi oleh Pasal 38 ayat 2.Di situ dinyatakan, masyarakat dapat

mengajukan gugatan perwakilan terhadap pihak yang menyelenggarakan sistem elektronik yang berakibat merugikan masyarakat.

Aspek Aparatur Penegak Hukum

Penegak hukum di Indonesia mengalami kesulitan dalam menghadapi merebaknya *cybercrime,* beberapa penyebab diantaranya adalah keterbatasan Sumber Daya Manusia yang dimiliki penegak hukum, yakni sangat langka yang intens terhadap kejahatan komputer, kejahatan yang menggunakan sarana komputer, kejahatan dunia maya. Sebab kejahatan ini memerlukan ketrampilan khusus bagi aparatur penegak hukum. Sehingga dalam hal penyelidikan dan penyidikan selalu mengalami jalan buntu atau tidak tuntas. Metode penyidikannya juga bersifat khusus, tidak semua penyidik dapat melakukannya. Harus ada anggota kepolisian yang bertugas di bidang internet atau biasa disebut *polisi cyber atau cyber police*.

Untuk membuktikan jejak-jejak para *hacker*, *cracker* dan *phreacker* dalam melakukan aksinya terutama yang berhubungan dengan program-program dan data-data komputer, sarana Polri belum memadai karena belum ada komputer forensik.Fasilitas ini diperlukan untuk mengungkap data-data digital serta merekam dan menyimpan bukti-bukti berupa soft copy (image, program, dsb).Dalam hal ini Polri masih belum mempunyai fasilitas forensic computing yang memadai. Fasilitas *forensic computing* yang akandidirikan Polri diharapkan akan dapat melayani tiga hal penting yaitu *evidence collection, forensic analysis, expert witness*.[11]

Aplikasi di Lapangan

Aplikasi di lapangan menunjukan bahwa pelaku cybercrime dikenakan dengan pasal-pasal dalam KUHP seperti penipuan, pengrusakan, penggelapan dan pasal pidana lain diluar KUHP seperti undang-undang telekomunikasi, undang-undang hak cipta dan yang terbaru adalah undang-undang ITE.

Fenomena kejahatan *cyber crime* di Indonesia semakin lama semakin meningkat dengan berbagai kasus yang bervariasi seperti kasus pemakaian nama domain Mustika Ratu Com pada tahun 2000. Mustika ratu melaporkan Chandra Sugiono karena melakukan persaingan usaha dengan cara pemakaian nama perusahaan / domain Mustika ratu dalam situs Chandra Sugiono. Chandra Sugiono yang pada waktu itu merupakan GM PT. Martha Tilaar di dakwa pasal 382

[11]Makalah Rusbagio Ishak (Kombes Pol/49120373), Kadit Serse Polda Jateng, pada seminar tentang Hacking yang diadakan oleh Majalah NeoTek pada bulan Agustus 2002 di Semarang.

bis KUHP dan pasal 19 Jo 48 Undang-undang Nomor 5 tahun 1999 tentang Larangan Praktek Monopoli dan Persaingan Usaha Tidak Sehat dengan tuntutan 6 bulan penjara atau denda minimal 25 milyar dan maksimal 100 milyar dan juga didakwa dengan Undang-undang Nomor 15 Tahun 2001 tentang mereka. Dalam pemeriksaan perkara tersebut, majelis hakim Pengadilan Negeri Jakarta Selatan memutuskan bahwa perbuatan yang didakwakan tersebut tidak terbukti. Oleh karena itu, Tjandra Sugijono dibebaskan dari segala dakwaan *(vrijspraak)*, akan tetapi di tingkat Mahkamah Agung di kenai dakwaan 4 bulan penjara. *Cybercrim*e membuka peluang terjadinya pelanggaran terhadap HAKI seperti hak cipta, merek dan lain-lain, misalnya terkait pemakaian nama domain perusahaan-perusahaan, merek-merek besar ataupun yang sudah terkenal tanpa izin dari pemiliknya.

Kasus yang kedua terjadi pada tahun 2001 yaitu perusakan fasilitas internet banking BCA dengan membuat situs tiruan www.klikbca.com oleh seorang hacker bernama Steven Haryanto, tiruan tersebut berupa kilkbca.com, www.klickbca.com, klickbca.com, clickbca.com. Para user yang salah melakukan login di situs klikbca secara otomatis akan memasuki situs-situs tiruan pemilik tersebut kemudian user name dan PIN juga otomatis terkirim kepada sang pemilik situs (pembuat domain tiruan). Kasus situs tiruan tersebut tidak sampai ke meja hijau karena pelaku tidak berniat melakukan pencurian rekening pelanggan BCA yang masuk ke dalam situs tiruan tersebut.

Kasus yang terbaru pada tahun 2009 ini adalah kasus prita mulyasari, dimana prita mulyasari di jerat dengan menggunakan UU ITE pasal 27 ayat 3 karena telah dianggap melakukan pencemaran nama baik kepada RS Omni Internasional Jakarta melalui surat elektronik. Berdasarkan UU ITE tersebut prita mulyasari terkena ancaman pidana penjara paling lama 6 (enam tahun) dan atau denda paling banyak satu miliar rupiah.

Sulit memang bagi penegak hukum untuk melakukan tugasnya secara maksimal, tanpa dilengkapi dengan instrument hukum yang mengatur *cyber crime*. Selain itu mekanisme ditubuh penegak hukum tentang *cyber crime* juga belumlah terbentuk dengan baik.Meskipun telah ada UU ITE yang minimal memberikan kepastian hukum terhadap kejahatan di dunia maya,namun tidak menutup kemungkinan terjadi perbedaan persepsi dalam menafsirkan pasal yang disangkakan kepada pelaku. Seperti pada kasus prita mulyasari yang sebelumnya hanya dijerat dengan KUHP Pasal 310 dan 311 tentang pasal penghinaan dengan ancaman pidana penjara paling lama 9 bulan dan paling lama 1 tahun 4 bulan jika pencemaran itu dilakukan secara tertulis. Setelah adanya UU ITE yang mengatur tentang surat elektronik, maka UU tersebut juga dapat dijadikan

dasar untuk menjerat perbuatan pencemaran nama baik yang dilakukan melalui surat elektronik.

PENUTUP

Sebelum munculnya UU ITE No 11 Tahun 2008, untuk menjerat pelaku *cyber crime*, dipakai undang-undang yang bersifat khusus dan ketentuan-ketentuan yang bersifat umum, seperti: Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi; Undang-Undang Nomor 5 Tahun 1999 tentang Lara-ngan Praktek Monopoli dan Persaingan Usaha yang Tidak Sehat, Undang-Un-dang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, Undang-Undang Nomor 19 Tahun 2002 tentang Hak Cipta, Undang-Undang Nomor 14 Tahun 2001 tentang Hak Paten; Undang-Undang Nomor 15 Tahun 2001 tentang Merk, dan KUHP.

Kejahatan di dunia *cyber*yang tidak lagi mengenal batas-batas suatu Negara sehingga menimbulkan persoalan-persoalan baru dan dampaknya telah dirasakan oleh masyarakat pengguna computer dan jaringannya. Oleh karena itu selain sudah adanya pengaturan hukum juga diperlukan strategi penanggu-langan *cyber crime*. Penanggulangan dimaksud dimulai dari upaya pencegahan kejahatan *cyber crime* yaitu pendekatan secara teknologi dengan pengamanan software, hardware, kemudian dilakukan upaya sosialisasi computer dan internet di tengah-tengah masyarakat,pendekatan kultur juga bisa dilakukan dengan cara menerapkan etika. Dalam berinteraksi dengan orang lain menggunakan internet, diliputi oleh suatu aturan tertentu yang dinamakan *Nettiquette* atau etika di internet. Meskipun belum ada ketetapan yang baku mengenai bagaimana etika berinteraksi di internet, etika dalam berinteraksi di dunia nyata *(real life*) dapat dipakai sebagai acuan Selain upaya pencegahan juga dilakukan penegakan hukum terhadap kejahatan *cyber crime*.

Dalam rangka mewujudkan penegakan hukum terhadap kejahatan Cy-bercrime harus didukung tiga aspek yang terkait dengan penegakkan hukum yaitu aspek instrumen hukum, aparat penegak hukum dan aplikasinya di lapa-ngan. *Aspek Instrumen* adalah dengan adanya berbagai undang-undang termasuk UU ITE yang dapat meminimalisir dan dapat dijadikan payung hukum terhadap penindakan kejahatan cybercrime, Dengan hadirnya UU ITE akan memberikan manfaat, yaitu : menjamin kepastian hukum bagi masyarakat yang melakukan transaksi elektronik, mendorong pertumbuhan ekonomi, mencegah terjadinya kejahatan berbasis teknologi informasi dan melindungi masyarakat pengguna jasa dengan memanfaatkan teknologi informasi. Adapun terobosan-terobosan yang penting yang dimilikinya, adalah*pertama*,tanda tangan elektronik diakui memiliki kekuatan hukum yang sama

dengan tandatangankonvensional (tinta bsah dan bermaterai). *Kedua*, alat bukti elektronik diakui seperti alat bukti lainnya yang diatur dalam KUHAP.*Ketiga*, Undang-Undang ITE, berlaku untuk setiap orangyang melakukan perbuatan hukum, baik yang berada di wilayah Indonesia maupun di luarIndonesia yang memiliki akibat hukum di Indonesia.

Aspek aparat penegak hukum; Penegak hukum di Indonesia mengalami kesulitan dalam menghadapi merebaknya *cybercrime*, beberapa penyebab diantaranya adalah keterbatasan Sumber Daya Manusia yang dimiliki penegak hukum, yakni sangat langka yang intens terhadap kejahatan komputer, kejahatan yang menggunakan sarana komputer, kejahatan dunia maya. Sebab kejahatan ini memerlukan ketrampilan khusus bagi aparatur penegak hukum. Metode penyidikannya juga bersifat khusus, tidak semua penyidik dapat melakukannya. Harus ada anggota kepolisian yang bertugas di bidang internet atau biasa disebut *polisi cyber atau cyber police*. Untuk membuktikan jejak-jejak para *hacker, cracker* dan *phreacker* dalam melakukan aksinya terutama yang berhubungan dengan program-program dan data komputer, sarana Polri belum memadai karena belum ada komputer forensik. Fasilitas ini diperlukan untuk mengungkap data-data digital serta merekam dan menyimpan bukti-bukti berupa soft copy (image, program, dsb).

*Aplikasi di lapangan;*Aplikasi di lapangan menunjukan bahwa pelaku cybercrime dikenakan dengan pasal-pasal dalam KUHP seperti penipuan, pengrusakan, penggelapan dan pasal pidana lain diluar KUHP seperti undang-undang telekomunikasi, undang-undang hak cipta dan yang terbaru adalah undang-undang ITE.

DAFTAR PUSTAKA

Andi Hamzah, 1993, *Hukum Pidana Yang Berkaitan Dengan Komputer*, Sinar Grafika, Jakarta.

Aulia Adnan, Muhammad, Tinjauan Hukum dalam E Business Olyx76@ Yahoo.com

Ishak, Rusbagio (Kombes Pol/49120373), Kadit Serse Polda Jateng, pada seminar tentang Hacking yang diadakan oleh Majalah NeoTek pada bulan Agustus 2002 di Semarang.

Nawawi Arief, Barda, 2007, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*, Jakarta: Kencana Predana Media Group.

Pramono,Widyo, 1994, *Kejahatan di Bidang Komputer*, Jakarta: Pustaka Sinar Harapan.

Reinhard Golose, Petrus,2006, *Perkembangan Cyber Crime dan Upaya Penanggulangannya di Indonesia Oleh Polri*, Jakarta: Buliten Hukum Perbankan dan Kebanksentralan, Volume 4 Nomor 2, Agustus.

Safitri, Indra, "Tindak Pidana di Dunia Cyber" dalam Insider, Legal Journal From Indonesian Capital & Investmen Market. Dapat dijumpai di Internet: http://business.fortunecity.com/buffett/842/ art 180199_ tindakpidana.htm.

Shea,Virginia, 2004, *Netiquette*, San Fransisco: Albion Book, dapat dijumpai di http://www.albion.com/nettiquette/book/

Sipropoulus, Jhon, 1999, "*Cyber Crime Fighting*, The Law Enforcement Officer's Guide to Online Crime", The Natinal Cybercrime Training Partnership, Introduction.

Steven Harnad, *Post-Gutenberg Galaxy: The Fourth Revolution in the Means of Production of Knowledge*, Public-Access Computer System Review 2 (1): 39-53, versi elektronik dapat dibaca pada http:// cogprints.org/1580/00/harnad91.postgutenberg.html.

Sutarman, 2007, *Cybercrime Modus Operandinya dan Penanggulangannya*, Jogjakarta, LaksBangPRESSindo.

Wahib¸Abdul dan Mohammad Labib, 2005, *Kejahatan Mayantara (Cyber crime)*, Bandung: Refika Aditama.