Tinjauan Yuridis Penegakan Hukum Terhadap Kejahatan Dunia Maya (Cyber Crime)

Oleh: Santi Indriani [1]

Abstract

The development of information technology, which moves rapidly through computer media, create innovation named internet. The existence of this internet changes new paradigm for the patterns of human's life from the real characters changing into transparent reality (virtual). In one side, the existences of internet are very useful for human being but the on other side it brings the big negative effects. Within the existence of internet, in the beginning it has conventional character such as; posing a threat, robbing and deception at this time it can be done by using internet media online. Therefore the technology changing which move rapidly with crime of many kinds of motivation, it needs the law soon. This law must be suitable to guarantee of law assurance. In spite of the needed of suitable law as soon as possible, it also needs preventive method to prevent this cyber crime.

Key words: Information, technology, law maintenance, cyber crime,

Pendahuluan

Kemajuan teknologi telah merubah struktur masyarakat dari yang bersifat lokal menuju ke arah masyarakat yang berstruktur global. Perubahan ini disebabkan oleh kehadiran teknologi informasi. Perkembangan teknologi informasi itu berpadu dengan media dan komputer, yang kemudian melahirkan piranti baru yang disebut internet.(Abdul Wahid dan Muhamad Labib, 2005:103).

Dengan mengutip beberapa pendapat para ahli, yaitu menurut Keinichi Ohmae bahwa "globalisasi yang ditimbulkan oleh IPTEK telah membuat manusia berada dalam *Borderless World* (dunia tanpa batas) kehidupan manusia berada dalam keadaan" *interlinked economy, there is no such things as absolute loser and winners*" (dalam M.Yahya Harahap, 1997:43).

Selain itu menurut Jhon Naisbitt menambah ungkapan lain, meskipun sama maknanya bahwa perkembangan teknologi telah membawa kemajuan luas di bidang informasi dan ekonomi, kini dunia telah berubah menjadi *global vilage* (perkampungan global) dengan sistem single ekonomi (kesatuan ekonomi dunia) dalam keadaan " *as the world moving from trade countries to a single economy. One economy one market place* dengan mengacu pada pendapat para ahli dapat diketahui bahwa globalisasi yang diikuti dengan perkembangan IPTEK telah memberi dampak yang besar dalam bidang kehidupan, sehingga perkembangan teknologi informasi khususnya ledakan informasi dalam dunia maya (*cyberspace*) dan internet membawa perubahan ke segala aspek kehidupan manusia, mulai dari pendidikan, perdagangan, hiburan, pemerintahan dan komunikasi. (dalam Santi:2004:2).

Tentunya, tidak dapat dipungkiri bahwa teknologi Internet membawa dampak negatif yang tidak kalah banyak dengan manfaat yang ada. Internet membuat kejahatan yang semula bersifat konvensional seperti pengancaman, pencurian dan penipuan kini dapat

[1] ***Dosen FISIP Universitas Baturaja***

dilakukan dengan menggunakan media komputer secara online dengan resiko tertangkap yang sangat kecil oleh individu maupun kelompok dengan akibat kerugian yang lebih besar baik untuk masyarakat maupun negara disamping menimbulkan kejahatan-kejahatan baru.

Seperti seorang hacker dapat masuk ke dalam suatu sistem jaringan perbankan untuk mencuri informasi nasabah yang terdapat di dalam *server* mengenai *data base* rekening bank tersebut, karena dengan adanya *e-banking* jaringan tersebut dapat dikatakan terbuka serta dapat diakses oleh siapa saja. Walaupun pencurian data yang dilakukan sering tidak dapat dibuktikan secara kasat mata karena tidak ada data yang hilang tetapi dapat diketahui telah diakses secara illegal dari sistem yang dijalankan.

Apabila berbicara mengenai kejahatan berteknologi tinggi seperti cybercrime seolah-olah hukum ketinggalan dari perisytiwanya *(het recht hink achter de feiteen aan)*, Dalam konteks ini lah, perkembangan teknologi informasi memberikan dampak yang cukup signifikan dalam berkembangnya tindak kejahatan di dunia maya *cybercrime* (Edmon Makarim, 2004:386), hal inilah yang akan dikaji dan dibahas dalam tulisan ini mengingat bahwa belum adanya aturan-aturan yang secara spesifikasi mengatur mengenai tindak kejahatan di dunia maya .

Kejahatan Dunia Maya (*Cyber Crime*)

Ada Bebarapa kasus kejahatan didunia maya yang menjadi perhatian publik antara lain seorang *hacker* bernama Dani Hermansyah, pada tanggal 17 April 2004 melakukan *deface* (mengubah atau mengganti tampilan suatu *website*) dengan mengubah nama-nama partai yang ada dengan nama-nama buah dalam *website www.kpu.go.id*. Dalam Harian Tempo, seorang *hacker* yang telah berhasil merusak dan mengacaukan nama-nama partai dalam *Website* KPU seharga 152 milyar tersebut, untungnya tidak sampai mengacaukan penghitungan hasil Suara di KPU (Harian Tempo, 11 Mei 2008).

Seorang *hacker* dan jurnalis pada majalah *Master Web* asal Bandung ini, dengan sengaja membuat situs asli tapi palsu layanan *Internet banking Bank Central Asia* (BCA). Steven membeli domain-domain dengan nama mirip www.klikbca.com (situs asli internet banking BCA), yaitu domain *wwwklik-bca.com*, *kilkbca.com*, *clikbca.com*, *klickca.com*. dan *klikbac.com*.

Isi situs-situs plesetan inipun nyaris sama, kecuali tidak adanya *security* untuk bertransaksi dan adanya formulir akses (*login form*) palsu. Jika nasabah BCA salah mengetik situs BCA asli maka nasabah tersebut masuk perangkap situs plesetan yang dibuat oleh Steven sehingga identitas pengguna (*user id*) dan nomor identitas personal (PIN) dapat di ketahuinya. Diperkirakan, 130 nasabah BCA tercuri datanya. Menurut pengakuan Steven pada situs bagi para *webmaster* di Indonesia, www.webmaster.or.id.

Selain *carding*, masih banyak lagi kejahatan yang memanfaatkan internet. Dari kedua kasus tersebut dapat diketahui bahwa kejahatan di dunia maya teknik yang memanfaatkan celah sistem keamanan *server* alias *Hole Cross Server Scripting* (XXS), yang ada pada suatu situs.

XXS adalah kelemahan aplikasi di *server* yang memungkinkan user atau pengguna menyisipkan baris-baris perintah lainnya. Biasanya perintah yang disisipkan adalah *Javascript* sebagai jebakan, sehingga pembuat *hole* bisa mendapatkan informasi data pengunjung lain yang berinteraksi di situs tersebut.

Makin terkenal sebuah *website* yang mereka *deface*, makin tinggi rasa kebanggaan yang didapat. Teknik ini pulalah yang menjadi andalan saat terjadi *cyberwar* antara *hacker* Indonesia dan *hacker* Malaysia, yakni perang di dunia maya yang identik dengan perusakan *website* pihak lawan.

Pengertian *Cyber Crime*

Dalam dua dokumen Konferensi PBB mengenai *The Prevention of Crime and the reatment of Offenders* di Havana, Cuba pada tahun 1990 dan di Wina, Austria pada tahun 2000, ada dua istilah yang dikenal, yaitu *cybercrime* dan *computerrelated crime*. Dalam *back ground paper* untuk lokakarya Konferensi PBB X/2000 di Wina, Austria istilah *cybercrime* dibagi dalam dua kategori. *Pertama*, *cybercrime* dalam arti sempit disebut *computer crime*. *Kedua*, *cybercrime* dalam arti luas disebut *computer relatedcrime*. Secara gamblang dalam dokumen tersebut dinyatakan:

(a) *Cyber crime in a narrow sense (computer crime) : any legal behavior directed by means of electronic operations that targets the security of computer system and the data processed by them*;
(b) *Cyber crime in a broader sense (computer related crime): any illegal behavior committed by means on in relation to, a computer system or network, including such rime as illegal possession, offering or distributing information by means of a computer system or network*.

Dengan demikian *cybercrime*meliputi kejahatan, yaitu yang dilakukan dengan (1). menggunakan saranasarana dari sistem atau jaringan komputer (*by means of acomputer system or network*); (2). Di dalam sistem atau jaringan komputer (*in a computer system or network*); dan (3). Terhadap sistem atau jaringan komputer (*against a computer system or network*). Dari definisi tersebut, maka dalam arti sempit *cybercrime* adalah *computer crime* yang ditujukan terhadap sistem atau jaringan komputer, sedangkan dalam arti luas, *cybercrime* mencakup seluruh bentuk baru kejahatan yang ditujukan pada komputer, jaringan komputer dan penggunanya serta bentuk-bentuk kejahatan tradisional yang sekarang dilakukan dengan menggunakan atau dengan bantuan peralatan komputer (*computer related crime)*, (Tim Perundang-Undangan dan Pengkajian Hukum Bank Indonesia, 2006).

Andi Hamzah memberikan batasan dan definisi dari kejahatan komputer tidak jauh berbeda yang dikemukakan oleh NPA: bahwa kejahatan di bidang komputer secara keseluruhan dapat diartikan sebagai penggunaan komputer secara illegal (Andi Hamzah,1989:3). Semua perumusan atau batasan yang diberikan mengenai kejahatan computer (*computer crime)*, atau penyalahgunaan komputer (*computer misuse)* tersebut secara umum dapat disimpulkan bahwa perbuatan atau tindakan yang dilakukan dengan menggunakan Komputer sebagai alat/sarana untuk melakukan tindak pidana atau komputer itu sendiri sebagai objek tindak pidana.

Tinjauan Yuridis Penegakan Hukum Terhadap Kejahatan Didunia Maya

Dalam membicarakan pengaturan teknologi informasi yang juga penting untuk diperhatikan adalah masalah penegakan hukum (*law enforcement)*. Penegakan hukum merupakan isu yang penting dalam konteks pembuatan peraturan perundang-undangan. Hal ini karena penyelesaian masalah hukum terhadap sesuatu yang baru tidak hanya cukup berhenti dengan dibentuknya Undang-Undang.

Menjawab tuntutan dan tantangan komunikasi global lewat internet, undang-undang yang diharapkan (*ius konstituendum*), adalah perangkat hukum yang akomodatif terhadap perkembangan serta antisipatif terhadap permasalahan, termasuk dampak negatif penyalahgunaan internet dengan berbagai motivasi yang dapat menimbulkan korban-korban seperti kerugian materi dan non materi. Saat ini, Indonesia belum memiliki undang-undang khusus/*cyber law* yang mengatur mengenai *cyber crime* walaupun rancangan

undang-undang tersebut sudah ada sejak tahun 2000 dan revisi terakhir dari rancangan undang-undang tindak pidana di bidang teknologi informasi sejak tahun 2004 sudah dikirimkan ke Sekretariat Negara RI oleh Departemen Komunikasi dan Informasi serta dikirimkan ke DPR namun dikembalikan kembali ke Departemen Komunikasi dan Informasi untuk diperbaiki.

Selain ketidak adaan peraturan perundang-undangan yang mengatur secara khusus mengenai *cyber crime* adalah ketiadaan konsep mengenai apa yang perlu diatur dalam peraturan tersebut. Ketiadaan dasar konstruksi hukum mengenai apa yang perlu diatur (apa yang perlu dibuat, diamandemen ataupun dihapus), secara praktis akan berdampak pada kebijakan penyusunan regulasi. Tetapi, terdapat beberapa hukum positif lain yang berlaku umum dan dapat dikenakan bagi para pelaku *cyber crime* terutama untuk kasus-kasus yang menggunakan komputer sebagai sarana, antara lain adalah;

(1) Kitab Undang Undang Hukum Pidana; dalam upaya menangani kasus-kasus yang terjadi, para penyidik melakukan analogi atau perumpamaan dan persamaaan terhadap pasal-pasal yang ada dalam KUHP. Pasal-pasal didalam KUHP biasanya digunakan lebih dari satu Pasal karena melibatkan beberapa perbuatan sekaligus pasal-pasal yang dapat dikenakan dalam KUHP pada *cyber crime* antara lain;
   a) Pasal 362 KUHP yang dikenakan untuk kasus carding dimana pelaku mencuri nomor 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*. Setelah dilakukan transaksi dan barang dikirimkan, kemudian penjual yang ingin mencairkan uangnya di bank ternyata ditolak karena pemilik kartu bukanlah orang yang melakukan transaksi;
   b) Pasal 378 KUHP dapat dikenakan 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. Tetapi, pada kenyataannya, barang tersebut tidak ada. Hal tersebut diketahui setelah uang dikirimkan dan barang yang dipesankan tidak datang sehingga pembeli tersebut menjadi tertipu;
   c) 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;
   d) 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* ke suatu mailing list sehingga banyak orang mengetahui cerita tersebut;
   e) Pasal 303 KUHP dapat dikenakan untuk menjerat permainan judi yang dilakukan secara online 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. Walaupun berbahasa Indonesia, sangat sulit sekali untuk menindak pelakunya karena mereka melakukan pendaftaran domain tersebut di luar negeri di mana pornografi yang menampilkan orang dewasa bukan merupakan hal yang ilegal;
   g) Pasal 282 dan 311 KUHP dapat dikenakan untuk kasus penyebaran foto atau film pribadi seseorang yang vulgar di internet, misalnya kasus Sukma Ayu-Bjah;

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 kreditnya yang nomor kartu kreditnya merupakan curian, dan;
i) Pasal 406 KUHP dapat dikenakan pada kasus deface atau hacking yang membuat sistem milik orang lain, seperti *website* atau program menjadi tidak berfungsi atau dapat digunakan sebagaimana mestinya.

(2) Undang-Undang No 19 Tahun 2002 Tentang Hak Cipta; perubahan-perubahan pada teknologi musik, perbukuan, perfileman dan teknologi penyebarluasan informasi melalui *cybernet*, akan menyebabkan berubah pada pola bisnis. Oleh sebab itu bentuk kejahatan atau tindak pidana juga berubah (Oka Saidin, 2003:115). Apabila di kaji dari ketentuan undang-undang hak cipta, maka ada beberapa ketentuan yang dapat digunakan untuk mengantisipasi pelanggaran hak cipta di internet. Menurut pasal 1 angka (8) Undang-Undang No 19 Tahun 2002 tentang Hak Cipta, program komputer adalah sekumpulan intruksi yang diwujudkan dalam bentuk bahasa, kode, skema ataupun bentuk lain yang apabila digabungkan dengan media yang dapat dibaca dengan komputer akan mampu membuat komputer bekerja untuk melakukan fungsi-fungsi khusus atau untuk mencapai hasil yang khusus, termasuk persiapan dalam merancang intruksi-intruksi tersebut. Hak cipta untuk program komputer berlaku selama 50 tahun (pasal 30).Harga program komputer/*software* yang sangat mahal bagi warga negara Indonesia merupakan peluang yang cukup menjanjikan bagi para pelaku bisnis guna menggandakan serta menjual software bajakan dengan harga yang sangat murah. Misalnya, program anti virus seharga $ 50 dapat dibeli dengan harga Rp15.000,00. Penjualan dengan harga sangat murah dibandingkan dengan *software* asli tersebut menghasilkan keuntungan yang sangat besar bagi pelaku sebab modal yang dikeluarkan tidak lebih dari Rp 5.000,00 perkeping. Maraknya pembajakan *software* di Indonesia yang terkesan "dimaklumi" tentunya sangat merugikan pemilik hak cipta. Tindakan pembajakan program komputer tersebut juga 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 komputer dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau denda paling banyak Rp500.000.000,00 (lima ratus juta rupiah) ".

(3) Undang-Undang No 36 Tahun 1999 Tentang Telekomunikasi; menurut pasal 1 angka (1) Undang-Undang No 36 Tahun 1999, Telekomunikasi adalah setiap pemancaran, pengiriman, dan/atau penerimaan dan setiap informasi dalam bentuk tanda-tanda, isyarat, tulisan, gambar, suara, dan bunyi melalui sistem kawat, optik, radio, atau sistem elektromagnetik lainnya. Dari definisi tersebut, maka internet dan segala fasilitas yang dimilikinya merupakan salah satu bentuk alat komunikasi karena dapat mengirimkan dan menerima setiap informasi dalam bentuk gambar, suara maupun film dengan sistem elektromagnetik. Penyalahgunaan internet yang mengganggu ketertiban umum atau pribadi dapat dikenakan sanksi dengan menggunakan undang-undang ini, terutama bagi para *hacker* yang masuk ke sistem jaringan milik orang lain sebagaimana diatur pada Pasal 22, yaitu; setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah, atau memanipulasi: (a). Akses ke jaringan telekomunikasi; (b). Akses ke jasa telekomunikasi, dan; Akses ke jaringan telekomunikasi khusus. Apabila seseorang 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 dimaksud dalam pasal 22, dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp600.000.000,00 (enam ratus juta rupiah).

(4) Undang-Undang No 8 Tahun 1997 Tentang Dokumen Perusahaan; dengan dikeluarkannya Undang-Undang No. 8 Tahun 1997 tanggal 24 Maret 1997 tentang Dokumen Perusahaan, pemerintah berusaha untuk mengatur pengakuan atas mikrofilm dan media lainnya (alat penyimpan informasi yang bukan kertas dan mempunyai tingkat pengamanan yang dapat menjamin keaslian dokumen yang dialihkan atau ditransformasikan). Misalnya *Compact Disk-Read Only Memory* (CD -ROM), dan *Write-Once Read-Many* (WORM), yang diatur dalam Pasal 12 Undang-Undang tersebut sebagai alat bukti yang sah.

(5) Undang-Undang No 25 Tahun 2003 Tentang Perubahan atas Undang-Undang No. 15 Tahun 2002 Tentang Tindak Pidana Pencucian Uang; undang-undang ini merupakan undang-undang yang paling ampuh bagi seorang penyidik untuk mendapatkan informasi mengenai tersangka yang melakukan penipuan melalui internet, karena tidak memerlukan prosedur birokrasi yang panjang dan memakan waktu yang lama, sebab penipuan merupakan salah satu jenis tindak pidana yang termasuk dalam pencucian uang (Pasal 2 Ayat (1) Huruf q). Penyidik dapat meminta kepada bank yang menerima transfer untuk memberikan identitas dan data perbankan yang dimiliki oleh tersangka tanpa harus mengikuti peraturan sesuai dengan yang diatur dalam Undang-Undang Perbankan. Dalam Undang-Undang Pencucian Uang, proses tersebut lebih cepat karena Kapolda cukup mengirimkan surat kepada Pemimpin Bank Indonesia di daerah tersebut dengan tembusan kepada Kapolri dan Gubernur Bank Indonesia, sehingga data dan informasi yang dibutuhkan lebih cepat didapat dan memudahkan proses penyelidikan terhadap pelaku, karena data yang diberikan oleh pihak bank, berbentuk: aplikasi pendaftaran, jumlah rekening masuk dan keluar serta kapan dan dimana dilakukan transaksi maka penyidik dapat menelusuri keberadaan pelaku berdasarkan data-data tersebut. Undang-Undang ini juga mengatur mengenai alat bukti elektronik atau digital evidence sesuai dengan Pasal 38 huruf b yaitu alat bukti lain berupa informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu.

(6) Undang-Undang No 15 Tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme Selain Undang-Undang No. 25 Tahun 2003; undang-undang ini mengatur mengenai alat bukti elektronik sesuai dengan Pasal 27 huruf b yaitu alat bukti lain berupa informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu. *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 untuk menerima perintah atau menyampaikan kondisi di lapangan karena para pelaku mengetahui pelacakan terhadap internet lebih sulit dibandingkan pelacakan melalui *handphone*. Fasilitas yang sering digunakan adalah *e-mail* dan chat room selain mencari informasi dengan menggunakan *search engine* serta melakukan propaganda melalui *bulletin* board atau *mailing list*.

Penutup

Dari uraian di atas dapat disimpulkan bahwa kehidupan manusia tidak dapat dilepaskan dari kemajuan teknologi (Hikmanto Juwana: 2001:48). Sepanjang sejarah hidup manusia selalu menciptakan teknologi untuk keperluan hidupnya. Namun terhadap kemajuan teknologi yang tidak diimbangi dengan kesadara hukum masyarakat serta kurangnya penegakan hukum akan menjadi kendala timbulnya kejahatan yang menggunakan teknologi khususnya kejahatan di dunia maya.

Belum adanya ketentuan yang mengatur secara spesifikasi permasalahan kejahatan di dunia maya merupakan salah satu faktor yang mempengaruhi lemahnya penegakan hukum, akan tetapi dengan tetap menggunakan aturan-aturan yang bersifat umum diharapkan dapat memberikan efek jera bagi pelaku tindak kejahatan didunia maya. Perlunya pengaturan mengenai pembentukan peraturan perundang-undangan dibidang teknologi Informasi hendaknya nanti mampu mengakomodir seluruh kepentingan masyarakat, sehingga penegakan hukum dapat berjalan sebagaimana mestinya.

Daftar Pustaka

.

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

Harahap, Yahya, M. 1997. *Beberapa Tinjauan Tentang Permasalahan Hukum, Dampak Kemajuan IPTEK dan Globalisasi Terhadap Perkembangan* Kejahatan. Bandung: Citra Aditya Bakti.

Indriani, Santi. 2004. *Perlindungan Hukum Terhadap Pendesain Homepage di Indonesia*, Skripsi S1 Studi Hukum dan Bisnis Fakultas Hukum Universitas Sriwijaya (tidak dipublikasikan). Palembang: FH Unsri.

Makarim Emon, 2003. *Kompilasi Hukum Telematika*, Raja Grafindo Persada, Jakarta

Saidin Oka, 2003, *Aspek Hukum Kekayaan Intelektual (Intelectual Propherty Rights)*, Jakarta. Raja Grafindo Persada.

Tim Perundang-Undangan Dan Pengkajian Hukum Direktorat Hukum Bank Indonesia. *Urgensi Cyberlaw Di IndonesiaDalam Rangka Penanganan Cyber Crime di Sektor* Perbankan. Dalam Buletin Hukum Perbankan Dan Kebanksentralan Volume 4 Nomor 2, Agustus 2006. Jakarta: Bank Indonesia.

Juwana, Hikmahanto. 2001. *Aspek Penting Pembentukan Hukum Teknologi Informasi Di Indonesia*. Jurnal Hukum Bisnis, Volume 16, Nopember 2001. Jakarta: Yayasan Pengembangan Hukum Bisnis.

ahid, Abdul dan Mohammad Labib. 2005. *Kejahatan Mayantara (Cyber Crime*). Jakarta: Refika Aditama.

Undang-Undang

Kitab Undang-Undang Hukum Pidana;
Undang-Undang No 8 Tahun 1997 tentang Dokumen Perusahaan;
Undang-Undang No 36 Tahun 1999 tentang Telekomunikasi;
Undang-Undang No.19 Tahun 2002 Tentang Hak cipta;
Undang-Undang No 25 Tahun 2003 tentang Perubahan atas Undang-Undang No. 15 Tahun 2002 tentang Tindak Pidana Pencucian Uang, dan;
Undang-Undang No 15 Tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme

Suratkabar

Harian Tempo, Edisi 11 Mei 2004.