PENEGAKAN HUKUM CYBER CRIME DITINJAU DARI HUKUM POSITIF DAN HUKUM ISLAM

H Sofwan Jannah &M. Naufal
Dosen Fakultas Ilmu Agama Islam UII Yogyakarta

Abstract:

This articlewillexplainaboutcybercrime, effortsto overcome, focus, punishment andthe viewof Islami claw and positive law against cyber crime behavior. Cyber Crimeis a criminal activity using computer facilitiesor computer network without permission and against the law. According toIslamic shariathe punishment for cyber crime is ta'zirby difference method, such as imprisonment, exile, whips, and death penalty. The punishment (ta'zir) based on Islamic Law is very importance because Our country hasn't yet aspecial regulation governing cyber crime, exceptsomepositive law generally. Witha discussion of cyber crimein Islamic law, it became one of the alternatives and the way for controll ingthis criminal acts.

Keywords:*Cyber Crime, Hukum Positif, dan Hukum Islam***.**

A. Pendahuluan

Cybercrime dewasa ini muncul ketika penyalahgunaan internet sudah di luar batas sehingga menjadi suatu kejahatan. Pengertian kejahatan komputer pada umumnya sebagai kejahatan melalui pengetahuan khusus tentang teknologi komputer. Hukum terlalu lambat untuk mengikuti perkembangan teknologi computer, kemudian bereaksi terhadap perubahan dan perkembangan teknologi yang demikian cepat. Bahkan undang-undang yang sekarang ini tidak mampu untuk menangani kejahatan dunia maya secara tuntas.Internet sebagai hasil rekayasa teknologi bukan hanya menggunakan kecanggihan teknologi komputer tapi juga melibatkan teknologi telekomunikasi di dalam pengoperasiannya.

Keunggulan komputer berupa kecepatan dan ketelitiannya dalam menyelesaikan suatu pekerjaan dapat menekan jumlah tenaga kerja, biaya, serta dapat memperkecil kemungkinan melakukan kesalahan. akibatnnya masyarakat

semakin mengalami ketergantungan terhadap komputer. Dampak negatif dapat timbul ketika terjadi kesalahan yang ditimbulkan oleh piranti komputer yang akan mengakibatkan kerugian besar bagi pengguna atau pihak-pihak yang berkepentingan. Kesalahan yang disengaja tersebut mengarah kepada penyalahgunaan komputer.[1]

Negara RepublikIndonesia sampai saat ini belum memiliki Undang-Undang khusus yang mengatur cybercrime, kecuali beberapa hukum positif yang berlaku umum terutama bagi para pelaku cybercrime untuk kasus-kasus yang menggunakan komputer sebagai sarana. Pertanyaannya adalah: Apa dasar hukum Islam untuk kejahatan komputer? Bagaimana hukum Islam menangani isu-isu teknologi baru dan memberikan hukum yang sesuai untuk kejahatan computer?

B. Pengertian Cyber Crime

Cybercrime berasal dari kata cyber yang berarti dunia maya atau internet dan crime yang berarti kejahatan.[2] Dengan kata lain,*cybercrime*adalah segala bentuk kejahatan yang terjadi di dunia maya atau internet. Cybercrime merupakan tindakkriminal yang dilakukan dengan menggunakan teknologi komputer sebagai alat kejahatan utama.[3]*Cybercrime*yaitu kejahatan yang memanfaatkan perkembangan teknologi komputer khususnya internet. *Cybercrime* didefinisikan sebagai perbuatan melanggar hukum yang memanfaatkan teknologi komputer yang berbasis pada kecanggihan perkembangan teknologi internet.[4]

Dalam beberapa literatur, *cybercrime* sering diidentikkan sebagai *computer crime.* Andi Hamzah dalam buku Aspek-aspek Pidana di Bidang Komputer (1989) mengartikan: "*kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara illegal.*" Cybercrime adalah perbuatan kriminal yang dilakukan dengan menggunakan teknologi computer sebagai alat kejahatan utama. Dengan kata lain, Cybercrime yaitu kejahatan yang memanfaatkan perkembangan teknologi computer khususnya internet.Dengan demikian Cybercrime didefinisikan sebagai perbuatan melanggar hukum yang memanfaatkan teknologi komputer berbasasis pada kecanggihan dan perkembangan teknologi internet.

---

[1] Andi Hamzah,*Aspek-Aspek Pidana di Bidang Komputer,* (Jakarta*:* Sinar Grafika, 1990),hlm 23-24

[2] Agus Rahardjo, *Cybercrime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, (Bandung: PT Citra Aditya Bakti, 2002).

[3] *Ibid*

[4] Budi Raharjo, *Memahami Teknologi Informasi.* (Jakarta: Elexmedia Komputindo, 2002). hlm 23

Dari beberapa pengertian di atas, *computer crime* dirumuskan sebagai perbuatan melawan hukum yang dilakukan dengan memakai komputer sebagai sarana/alat atau komputer sebagai objek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain. Secara ringkas *computer crime* didefinisikan sebagai perbuatan melawan hukum yang dilakukan dengan menggunakan teknologi komputer yang canggih.

Aktivitas cyber yaitu kegiatan virtual yang berdampak sangat nyata, meskipun alat buktinya bersifat elektronik. Dengan demikian, subyek pelakunya harus dikualifikasi sebagai orang yang melakukan perbuatan hukum secara nyata. [5]Polri dalam hal ini unit cybercrime menggunakan parameter berdasarkan dokumen kongres PBB:*The Prevention of Crime and The Treatment of Offlenderes* di Havana, Cuba pada tahun 1999 dan di Wina, Austria tahun 2000, menyebutkan ada 2 istilah Cyber Crime: [6]*pertama*, *cyber crime in a narrow sense* (dalam arti sempit) disebut *computer crime: any illegal behaviour directed by means of electronic operation that target the security of computer system and the data processed by them.Kedua, cyber crime in a broader sense* (dalam arti luas)disebut *computer related crime: any illegal behaviour committed by means on relation to, a computer system offering or system or network, including such crime as illegal possession in, offering or distributing information by means of computer system or network.*

C. Bentuk *Cybercrime*

1. *Unauthorized Access to Computer System and Service*

Kejahatan yang dilakukan dengan memasuki atau menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. Biasanya pelaku kejahatan (*hacker*) melakukannya dengan maksud sabotase ataupun pencurian informasi penting dan rahasia. Namun begitu, ada juga yang melakukan hanya karena merasa tertantang untuk mencoba keahliannya menembus suatu sistem yang memiliki tingkat proteksi tinggi. Kejahatan ini semakin marak dengan berkembangnya teknologi internet/intranet.

Misalnya pada saat masalah Timor Timur sedang hangat-hangatnya dibicarakan di tingkat internasional, beberapa *website* milik pemerintah RI dirusak oleh *hacker* (Kompas, 11/08/1999). Beberapa waktu lalu, *hacker*[7] juga telah berhasil

---

[5] Pasal 5 Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE), Kementerian Komunikasi dan Informasi RI

[6] Eoghan Casey, *Digital Evidence and Komputer Crime*, (London : A Harcourt Science and Technology Company, 2001). page 16

[7] *Hacker* adalah seseorang yang dapat memasuki sistem jaringan komputer orang lain tanpa ijin.

menembus masuk ke dalam *database* berisi data para pengguna jasa America Online (AOL), sebuah perusahaan Amerika Serikat yang bergerak di bidang*e-commerce,* yang memiliki tingkat kerahasiaan tinggi (Indonesian Observer, 26/06/2000). Situs Federal Bureau of Investigation (FBI) pun tidak luput dari serangan para *hacker*, yang berakibat tidak berfungsinya situs ini dalam beberapa waktu lamanya.[8]

2. *Illegal Contents*

Merupakan kejahatan dengan memasukkan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum. Misalnya pemuatan suatu berita bohong atau fitnah yang mendiskreditkanmartabat atau harga diri pihak lain, hal-hal yang berhubungan dengan pornografi atau pemuatan suatu informasi yang merupakan rahasia negara, agitasi dan propaganda untuk melawan pemerintahan yang sah, dan lain sebagainya.

3. *Data Forgery*

Merupakan kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai *scriptless document* melalui internet. Kejahatan ini biasanya ditujukan pada dokumen-dokumen *e-commerce* dengan membuat seolah-olah terjadi "salah ketik" yang pada akhirnya akan menguntungkan pelaku.

4. *Cyber Espionage*

Merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (*computer network system*) pihak sasaran. Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen ataupun data-data pentingnya tersimpan dalam suatu sistem yang *computerized*.

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. Biasanya kejahatan ini dilakukan dengan menyusupkan suatu *logic bomb*, virus komputer ataupun suatu program tertentu, sehingga data, program komputer atau sistem jaringan komputer tidak dapat digunakan, tidak berjalan sebagaimana mestinya, atau berjalan sebagaimana yang dikehendaki oleh pelaku. Dalam beberapa kasus setelah hal tersebut terjadi, maka pelaku kejahatan tersebut menawarkan diri kepada korban untuk

[8] http://www.fbi.org, *Kejahatan Cyber Crime*, diakses pada tanggal 12 Februari 2012 pada jam 10.00 WIB.

memperbaiki data, program komputer atau sistem jaringan komputer yang telah disabotase tersebut, tentunya dengan bayaran tertentu. Kejahatan ini sering disebut sebagai *cyber-terrorism*.

6. *Offense 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 ilegal, penyiaran suatu informasi di internet yang ternyata merupakan rahasia dagang orang lain.

7. *Infringementsof Privacy*

Kejahatan ini ditujukan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia. Kejahatan ini biasanya ditujukan terhadap keterangan pribadi seseorang yang tersimpan pada formulir data pribadi yang tersimpan secara *computerized*, yang apabila diketahui oleh orang lain maka dapat merugikan korban secara materiil maupun immateriil, seperti nomor kartu kredit, nomor PIN ATM, informasi penyakit yang dirahasiakan dan sebagainya.

Cybercrime memiliki karakter yang khas dibandingkan kejahatan konvensional, antara lain:[9]

a. Perbuatan yang dilakukan secara ilegal, tanpa hak atau tidak etis tersebut terjadi di ruang/wilayah maya (*cyberspace*), sehingga tidak dapat dipastikan yurisdiksi hukum negara mana yang berlaku terhadapnya
b. Perbuatan tersebut dilakukan dengan menggunakan peralatan apapun yang bisa terhubung dengan internet
c. Perbuatan tersebut mengakibatkan kerugian materiil maupun immateriil (waktu, nilai, jasa, uang, barang, harga diri, martabat, kerahasiaan informasi) yang cenderung lebih besar dibandingkan kejahatan konvensional
d. Pelakunya adalah orang yang menguasai penggunaan internet beserta aplikasinya. Perbuatan tersebut seringkali dilakukan secara transnasional/ melintasi batas negara

D. Pengaturan Cyber Crime di Indonesia

Indonesia belum memiliki Undang-Undang khusus/cyber law yang mengatur mengenai cybercrime Tetapi, terdapat beberapa hukum positif lain yang berlaku

[9] Deris Setiawan, *Sistem Keamanan Komputer*, (Jakarta: PT Elex Media Komputindo, 2005),.hlm. 40

umum dan dapat dikenakan bagi para pelaku cybercrime terutama untuk kasus-kasus yang menggunakan komputer sebagai sarana, diantaranya:[10]

a. Kitab Undang-Undang Hukum Pidana

Pasal-pasal didalam KUHP biasanya digunakan lebih dari satu Pasal karena melibatkan beberapa perbuatan sekaligus pasal-pasal yang dapat dikenakan dalam KUHP pada cybercrime yaitu:

1. 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.
2. 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.
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 mengetahui rahasia korban.
4. Pasal 311 KUHP dapat dikenakan untuk kasus pencemaran nama baik dengan menggunakan media Internet. Modusnya adalah pelaku menyebarkan email kepada teman-teman korban tentang suatu cerita yang tidak benar atau mengirimkan email ke suatu mailing list sehingga banyak orang mengetahui cerita 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.

[10] *Ibid*, hlm. 70-77

Walaupun berbahasa Indonesia, sangat sulit sekali untuk menindak pelakunya karena mereka melakukan pendaftaran domain tersebut di luarnegeri dimana pornografi yang menampilkan orang dewasa bukan merupakan hal yang terlarang atau illegal.

7. Pasal 282 dan 311 KUHP dapat dikenakan untuk kasus penyebaran foto atau film pribadi seseorang yang vulgar di Internet , misalnya kasus-kasus video porno para mahasiswa, pekerja atau pejabat publik.
8. 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.
9. 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.

b. Undang-Undang No 19 Tahun 2002 tentang Hak Cipta

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 Rp 20.000,00. 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 per keping. 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)."

c. Undang-Undang No 36 Tahun 1999 tentang Telekomunikasi atau Undang-Undang Nomor 11 Tahun 2008 Tentang Internet & Transaksi Elektronik.

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:

1. Akses ke jaringan telekomunikasi
2. Akses ke jasa telekomunikasi
3. Akses ke jaringan telekomunikasi khusus

Apabila anda melakukan hal tersebut seperti yang pernah terjadi pada website KPU www.kpu.go.id,[11] 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)"

d. Undang Nomor 15 Tahun 2002 tentang Tindak Pidana Pencucian Uang

Undang-Undang Nomor 15 Tahun 2002 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 Perbankan identitas dan data perbankan merupakan bagian dari kerahasiaan bank sehingga apabila penyidik membutuhkan informasi dan data tersebut, prosedur yang harus dilakukan adalah mengirimkan surat dari Kapolda ke Kapolri untuk diteruskan ke Gubernur Bank

[11] Suara Merdeka , 27 April 2004 dengan judul "Polisi tangkap *Hacker* KPU"

Indonesia. Prosedur tersebut memakan waktu yang cukup lama untuk mendapatkan data dan informasi yang diinginkan.[12]

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.

Dengan semakin pesatnya perkembangan teknologi informasi, maka perlu kiranya diperhatikan upaya penyempurnaan dan perbaikan Kitab Undang-Undang Hukum Pidana Nasional, yaitu:[13]

1. Semakin maraknya kejahatan-kejahatan baru yang timbul sebagai akibat dari kemajuan teknologi informasi (cyber crime), maka alat bukti yang diperlukan harus sesuai dengan perkembangan IPTEK, baik dengan penambahan alat bukti lain yang berbasis teknologi, seperti alat bukti berupa surat elektronik (electronic mail) dan rekaman elektronik.
2. Salah satu ciri kejahatan di dunia maya (cyber crime) adalah memanfaatkan jaringan telematika (telekomunikasi, media dan informatika) global. Aspek global menimbulkan kondisi seakan-akan dunia tidak ada batasnya (borderless) keadaan ini mengakibatkan pelaku, korban serta tempat dilakukannya tindak pidana (locus delicti) terjadi dinegara yang berbeda-beda. Oleh karena itu, untuk mengantisipasi hal tersebut maka pemberlakuan Kitab Undang-Undang Hukum Pidana harus diperluas, sehingga tidak hanya mengacu pada asas/ prinsip yang selama ini di anut dalam pasal 2-pasal 9 Kitab Undang-Undang Hukum Pidana yaitu asas personal, asas territorial, dan asas universal.
3. Untuk merumuskan dan menentukan perbuatan-perbuatan yang dapat dikenai sanksi pidana dalam dunia yang relative baru dan bergerak cepat, tentu bukan merupakan pekerjaan yang mudah. Oleh karena itu, untuk

---

[12] Buletin Hukum Perbankan Dan KeBanksentralan Volume 4 Nomor 2, Agustus 2006

[13] Hinca IP Panjaitan dkk,2005,*Membangun Cyber Law Indonesia yang demokratis,* Jakarta : IMLPC. Hlm 56-58

menjerat pelaku yang melakukan kejahatan-kejahatan di dunia maya (cyber crime), dapat digunakan lembaga penafsiran hukum (interpretasi). Hal ini dimaksudkan untuk menghindarkan timbulnya kekosongan hukum.

Ahmad P Ramli (2005: 55-56) menjelaskan penentuan hukum yang berlaku, dikenal adanya beberapa asas yang dapat digunakan, yaitu :

a. Subjective territoriality, yang menekankan bahwa keberlakuan hukum pidana ditentukan berdasarkan tempat perbuatan dilakukan dan penyelesaian tindak pidananya dilakukan di negara lain.
b. Objective territoriality, yang menyatakan bahwa hukum yang berlaku adalah akibat utamanya perbuatan itu terjadi dan memberikan dampak yang sangat merugikan bagi negara yang bersangkutan.
c. Nationality, yang menentukan bahwa negara mempunyai yurisdiksi untuk menentukan hukum berdasarkan kewarganegaraan pelaku tindak pidana.
d. Passive nationality, yang menekankan yurisdiksi berdasarkan kewarganegaraan dari korban kejahatan.
e. Protective principle, yang menyatakan bahwa berlakunya hukum didasarkan atas keinginan negara untuk melindungi kepentingan negara dari kejahatan yang dilakukan diluar wilayahnya. Azas ini pada umumnya diterapkan apabila korbannya adalah negara atau pemerintah.
f. Universality, bahwa setiap negara berhak untuk menangkap dan menghukum pelaku kejahatan.

Munculnya kejahatan cyber crime merupakan suatu fenomena yang membutuhkan penanggulangan secara cepat dan akurat.Perubahan terhadap beberapa ketentuan yang terdapat dalam Kitab Undang-Undang Hukum Pidana merupakan salah satu cara yang dapat dipergunakan untuk mengatasi jenis kejahatan baru tersebut. Diharapkan dengan dilakukannya berbagai perubahan dalam Kitab Undang Hukum Pidana Nasional sebagai akibat dari timbulnya berbagai perubahan.

Contoh Kasus *Cyber Crime*di Indonesia:[14]

a. **Pencuriandan penggunaan account Internet milik orang lain.**Diantara kesulitan dari sebuah ISP (Internet Service Provider) adalah adanya account pelanggan mereka yang "dicuri" dan digunakan secara tidak sah. Berbeda dengan pencurian yang dilakukan secara fisik, "pencurian" account cukup menangkap "userid" dan "password" saja. Hanya informasi yang dicuri. Sementara orang yang kecurian tidak

[14] http://www.gatra.com/2004-10-13/. *Cybercrime di Era Digital*. Diakses 10Februari 2012, pukul 09.03.

merasakan hilangnya "benda" yang dicuri. Pencurian baru terasa efeknya jika informasi ini digunakan oleh yang tidak berhak. Akibat dari pencurian ini, penggunaan dibebani biaya penggunaan account tersebut. Kasus ini banyak terjadi di ISP. Namun yang pernah diangkat adalah penggunaan account curian oleh dua Warnet di Bandung.

b. **Membajak situs web.** Salah satu kegiatan yang sering dilakukan oleh cracker adalah mengubah halaman web, yang dikenal dengan istilah deface. Pembajakan dapat dilakukan dengan mengeksploitasi lubang keamanan. Sekitar 4 bulan yang lalu, statistik di Indonesia menunjukkan satu (1) situs web dibajak setiap harinya.

c. **Probing dan port scanning.** Salah satu langkah yang dilakukan cracker sebelum masuk ke server target yaitu melakukan pengintaian, dengan cara melakukan "port scanning" atau "probing" untuk melihat servis-servis apa saja yang tersedia di server target. Misalnya, hasil scanning dapat menunjukkan bahwa server target menjalankan program web server Apache, mail server sendmail, dan seterusnya. Analogi hal ini dengan dunia nyata yaitu dengan melihat-lihat apakah pintu rumah target terkunci, merek kunci yang digunakan, jendela mana yang terbuka, apakah pagar terkunci (menggunakan *firewall* atau tidak) dan seterusnya. Yang bersangkutan memang belum melakukan kegiatan pencurian atau penyerangan, akan tetapi kegiatan yang dilakukan sudah mencurigakan.

d. **Virus.** Seperti halnya di tempat lain, virus komputer pun menyebar di Indonesia . Penyebaran umumnya dilakukan dengan menggunakan email. Seringkali sistem email seseorang yang terkena virus tidak sadar akan hal ini. Virus ini kemudian dikirimkan ke tempat lain melalui emailnya. Kasus virus ini sudah cukup banyak seperti virus Mellisa, I love you, dan SirCam. Untuk orang yang terkena virus, kemungkinan tidak banyak yang dapat dilakukan.

e. **Denial of Service (DoS) dan Distributed DoS (DDos) attack.** DoS attack merupakan serangan yang bertujuan untuk melumpuhkan target (hang, crash) sehingga dia tidak dapat memberikan layanan. Aktifitas serangannya tidak melakukan pencurian, penyadapan, ataupun pemalsuan data. Akan tetapi dengan hilangnya layanan maka target tidak dapat memberikan servis sehingga ada kerugian finansial. Bagaimana status dari DoS attack ini? Bayangkan bila seseorang dapat membuat ATM bank menjadi tidak berfungsi. Akibatnya nasabah bank tidak dapat melakukan transaksi dan bank termasuk nasabah dapat mengalami kerugian finansial. DoS attack dapat ditujukan kepada server (komputer) dan juga dapat

ditargetkan kepada jaringan (menghabiskan bandwidth). Tools untuk melakukan hal ini banyak tersebar di Internet. DDoS attack meningkatkan serangan ini dengan melakukannya dari beberapa (puluhan, ratusan, dan bahkan ribuan) komputer secara serentak. Efek yang dihasilkan lebih dahsyat dari DoS attack saja.

f. **Kejahatan yang berhubungan dengan nama domain** (domain name) digunakan untuk mengidentifikasi perusahaan dan merek dagang. Namun banyak orang mencoba menarik keuntungan dengan mendaftarkan domain nama perusahaan orang lain dan kemudian berusaha menjualnya dengan harga yang lebih mahal. Pekerjaan ini mirip dengan calo karcis. Istilah yang sering digunakan adalah cybersquatting. Masalah lain adalah menggunakan nama domain saingan perusahaan untuk merugikan perusahaan lain. (Kasus: mustika-ratu.com) Kejahatan lain yang berhubungan dengan nama domain adalah membuat "domain plesetan", yaitu domain yang mirip dengan nama domain orang lain. (Seperti kasus klikbca.com) Istilah yang digunakan saat ini adalah typosquatting.

g. **IDCERT (Indonesia Computer Emergency Response Team)**. Salah satu cara untuk mempermudah penanganan masalah keamanan dengan membuat sebuah unit untuk melaporkan kasus keamanan. Masalah keamanan ini di luar negeri mulai dikenali dengan munculnya "*sendmail worm*" (sekitar tahun 1988) yang menghentikan sistem email Internet kala itu. Kemudian dibentuk sebuah *Computer Emergency Response Team* (CERT). Semenjak itu di negara lain mulai juga dibentuk CERT untuk menjadi *point of contact* bagi orang untuk melaporkan masalah keamanan. IDCERT merupakan CERT Indonesia .

h. **Sertifikasi perangkat security**. Perangkat yang digunakan untuk menanggulangi keamanan semestinya memiliki peringkat kualitas. Perangkat yang digunakan untuk keperluan pribadi tentunya berbeda dengan perangkat yang digunakan untuk keperluan militer. Namun sampai saat ini belum ada institusi yang menangani masalah evaluasi perangkat keamanan di Indonesia.

Mengingat kejahatan *e-commerce* merupakan salah satu kejahatan baru dan canggih, maka wajar dalam penegakan hukumnya masih mengalami beberapa kendala yang harus segera ditangani agar peluang pelaku kejahatan bisnis canggih dapat diatasi dan tidak dapat mengembangkan bakatkejahatannya di dunia maya khususnya kejahatan *e-commerce*. Meskipun demikian, ada kendala yang harus dipecahkan atau dicarikan solusinya diantaranya:

a. Pembuktian (bukti elektrik)
   Persoalan yang muncul, yaitu belum adanya kebulatan penafsiran terhadap kepastian dari alat bukti elektrik, dikarenakan alat bukti ini mudah sekali untuk di copy, digandakan atau bahkan dipalsukan, dihapus atau dipindahkan. Walaupun mengacu pada Pasal 5 Undang-Undang ITE telah jelas menyebutkan mengenai alat bukti ini, namun masih saja aparat penegak hukum mengalami kesulitan untuk mendapatkan alat bukti yang otentik.
b. Perbedaan Persepsi
   Perbedaan persepsi yang dimaksud yaitu bahwa terjadinya perbedaan antara penegak hukum dalam menafsirkan kejahatan yang terjadi dengan penerapan pasal-pasal dalam hukum positif yang berlaku sehingga menimbulkan ketidakpastian hukum bagi pencari keadilan.
c. Lemahnya penguasaan komputer
   Kurangnya kemampuan dan keterampilan aparat penegak hukum di bidang komputer yang mengakibatkan taktis, teknis penyelidikan, penuntutan dan pemeriksaan di pengadilan tidak dikuasai karena menyangkut sistem yang ada didalam komputer.
d. Sarana dan prasarana
   Fasilitas komputer mungkin memang ada di setiap kantor-kantor para penegak hukum, namun hanya berfungsi sebatasuntuk administrati, seperti mengetik saja, sedangkan kejahatan *e-commerce* ini dilakukan dengan menggunakan komputer yang berjaringan dan berkapasitas teknologi yang lumayan maju sehingga pihak aparat sulit untuk mengimbangi kegiatan para pelaku kejahatan tersebut.
e. Kesulitan Menghadirkan korban
   Terhadap kejahatan yang korbannya berasal dari luar negeri umumnya sangat sulit untuk melakukan pemeriksaan yang mana keterangan saksi korban sangat dibutuhkan untuk membuat sebuah berita acara pemeriksaan.

Cybercrime membutuhkan *global action* dalam penanggulangannya mengingat kejahatan tersebut seringkali bersifat transnasional. Adapun langkah penting yang harus dilakukan setiap negara dalam penanggulangan cybercrime adalah:[15]

a. Melakukan modernisasi hukum pidana nasional beserta hukum acaranya, yang diselaraskan dengan konvensi internasional yang terkait dengan kejahatan tersebut

[15] http://budi.insan.co.id. *Keamanan Sistem Informasi Berbasis Internet*. Diakses 09Februari 2012, pukul 06.30 WIB.

b. Meningkatkan sistem pengamanan jaringan komputer nasional sesuai standar internasional
c. Meningkatkan pemahaman serta keahlian aparatur penegak hukum mengenai upaya pencegahan, investigasi dan penuntutan perkara-perkara yang berhubungan dengan cybercrime
d. Meningkatkan kesadaran warga negara mengenai masalah cybercrime serta pentingnya upaya pencegahan kejahatan agar tidak mudah terjadi.
e. Meningkatkan kerjasama antar negara, baik bilateral, regional maupun multilateral, dalam upaya penanganan cybercrime, antara lain melalui perjanjian ekstradisi dan mutual assistance treaties

Terdapat tiga pendekatan untuk mempertahankan keamanan di *cyberspace*, pertama adalah pendekatan teknologi, kedua pendekatan sosial budaya-etika dan ketiga pendekatan hukum. Untuk mengatasi keamanan gangguan pendekatan teknologi sifatnya mutlak dilakukan, sebab tanpa suatu pengamanan jaringan akan sangat mudah disusupi, diintersepsi atau diakses secara ilegal dan tanpa hak.[16]

E. Cyber Crime Ditinajau dari Hukum Islam

Dipahami dari pengertian dan jenis–jenis cyber crime tersebut di atas, *cybercrime* merupakan bentuk kejahatan yang muncul di era modern sekarang ini. Dengan demikian, perbuatan kejahatan *cyber crime* menurut analisa hukum Islam (jinayat) dapat dihukum dengan ta'zir. Ta'zîr menurut pengertian bahasa berarti pencegahan (*al-man'u*). adapun menurut istilah ta'zîr merupakan hukuman edukatif (*ta'dîb*) dalam arti mengantisipasi dengan cara menakut-nakuti (*tankîf*). Adapun secara syar'î, ta'zîr dimaksudkan sebagai sanksi yang dijatuhkan atas dasar kemaksiatan, karena secara tegas tidak termasuk kejahatan yang termaktub dalam Al Quran da Hadis, sebagaimana had, Qisas, atau kafârat.

Hukuman *Ta'zîr*macamnya dapat berupa sangsi dalam bentuk:

(1) hukuman mati;
(2) jilid atau cambuk tidak melebihi 10 kali;
(3) pengasingan, pemboikotan,atau penjara;
(4) salib;
(5) ganti rugi (*ghuramah*) atau dengan cara penyitaan;
(6) peringatan atau nasihat
(7) pencabutan sebagian hak kekayaan (*hurmân*);

---

[16] AhmadRamli*Prinsip-prinsip Cyber Law Dan Kendala Hukum Positif Dalam Menanggulangi Cyber Crime*, (Bandung: Fakultas Hukum Universitas Padjajaran, 2004), hlm. 2.

(8) pencelaan (*taubîkh*);
(9) pewartaan (*tasyhîr*).

Bentuk sanksi ta'zîr hanya terbatas pada bentuk-bentuk tersebut. Khalifah atau yang mewakilinya yaitu *qâdhî* (hakim) diberikan hak oleh syariat untuk memilih di antara bentuk-bentuk sanksi tersebut dan menentukan kadarnya; ia tidak boleh menjatuhkan sanksi di luar itu.

Kasus ta'zîr secara umum terbagi menjadi:[17]

(1) pelanggaran terhadap kehormatan;
(2) pelanggaran terhadap kemuliaan;
(3) perbuatan yang merusak akal;
(4) pelanggaran terhadap harta
(5) gangguan keamanan;
(6) subversi;
(7) pelanggaran yang berhubungan dengan agama.

F. Simpulan

Cyber Crime merupakanaktivitas kejahatan dengan menggunakan fasilitas computer atau jaringan computer tanpa ijin dan melawan hokum, baik cara mengubahnya atau tanpa perubahan (kerusakan) pada fasilitas komputer yang dimasuki atau digunakan, atau kejahatan yang dengan menggunakan sarana media elektronik internet karena dikategorikan sebagai kejahatan dunia maya, atau kejahatan di bidang komputer dengan cara illegal, Dapat pula dikategorikan sebagai kejahatan komputer yang ditujukan kepada sistem atau jaringan komputer, yang mencakup segala bentuk baru kejahatan yang menggunakan bantuan sarana media elektronik internet.Sangsi bagi para pelaku cybercrime menurut syari'at Islam adalah Ta'zir melalui proses peradilan dengan vonis Hakim dengan ancaman hukuman berupa kurungan penjara, pengasingan, cambuk, sampai pada hukuman mati sesuai dengan tingkat mudharat yang telah dilakukannya.

Referensi

Agus Rahardjo, Cybercrime pemahaman dan upaya pencegahan kejahatan berteknologi, Bandung: PT Citra Aditya Bakti , 2002

AhmadRamli, 2004, Prinsip-prinsip Cyber Law Dan Kendala Hukum Positif Dalam Menanggulangi Cyber Crime*, Fakultas Hukum Universitas Padjajaran, Bandung.*

[17] http://id.answers.yahoo.com/question/index?qid=20081120042435AABH0vg

Andi Hamzah, 1990, Aspek-Aspek Pidana di Bidang Komputer, *Sinar Grafika, Jakarta.*

Budi Raharjo, 2002. Memahami Teknologi Informasi. *Jakarta: Elexmedia Komputindo*

Buletin Hukum Perbankan Dan KeBanksentralan Volume 4 Nomor 2, Agustus 2006

Deris Setiawan,2005, Sistem Keamanan Komputer*, Jakarta: PT Elex Media Komputindo.*

Eoghan Casey,2001, Digital Evidence and Komputer Crime*, London : A Harcourt Science and Technology Company.*

Hinca IP Panjaitan dkk, Membangun Cyber Law Indonesia yang demokratis, *Jakarta : IMLPC, 2005*

http://budi.insan.co.id. Keamanan Sistem Informasi Berbasis Internet. *Diakses 09Februari 2012, pukul 06.30 WIB*

http://www.fbi.org

http://www.gatra.com/2004-10-13/. Cybercrime di Era Digital. *Diakses 10Februari 2012, pukul 09.03 WIB*

Sinar Harapan, 10 April 2005 dengan judul Cyber War *Indonesia–Malaysia agar dihentikan*

Suara Merdeka , 27 April 2004 dengan judul "Polisi tangkap Hacker *KPU"*