CYBER CRIME DALAM SISTEM HUKUM INDONESIA

CYBER CRIME IN INDONESIA LAW SYSTEM

Fiorida Mathilda
(Staf Pengajar UP MKU Politeknik Negeri Bandung)

ABSTRAK

Penggunaan teknologi komputer, telekomunikasi, dan informasi mendorong berkembangnya transaksi melalui internet, elektronik, atau *on line*. Hal ini menyebabkan timbulnya istilah *e-banking, e-commerse, e-trade, and e-business*. Dalam perkembangannya, pemanfaatan jasa internet bisa berdampak buruk yaitu pelanggaran hukum. *Cyber crime* adalah bentuk kejahatan virtual dengan memanfaatkan media komputer yang terhubung dengan internet. Hukum seharusnya memberikan perlindungan kepada pengguna internet yang beritikad baik dan memberikan tindakan yang tegas kepada pelaku *cyber crime*. Akan tetapi, sistem hukum belum mengakomodasi seluruh kejahatan komputer melalui media internet. Begitu pula dalam hal penyidikan, banyak hambatan yang berkaitan dengan perangkat hukum, kemampuan penyidik, alat bukti, dan fasilitas komputer forensik. Hal ini yang menyebabkan penegakan hukum *cyber crime* masih lemah.

Kata Kunci: *cyber crime*, sistem hukum, penegakan hukum di Indonesia.

ABSTRACT

The use of computer, telecommunication and information technologies have pushed the advance of transactions made through internet, electronic or on line. This leads to the emergence of the e-banking, e-commerce, e-trade, and e-business terminations. In the development of internet, the utilization of internet service can emerge bad effects to the jurisdiction. This mischief against national jurisdiction through ICT is called "cyber crime". Cyber crime is a kind of infamy by using computation media through internet. The government should give internet users who have good willing a strong protection against cyber crime. The government should also give decisive punishment for all criminals who use internet media as the tool to do their crime. Unfortunately, legal system in Indonesia can't control all kinds of cyber crime. Hence in the investigation system there are so many obstacles with justice tools which make the cybercrime law is difficult to be applied.

Keywords: *cyber crime, legal system, rule of law in Indonesia.*

PENDAHULUAN

Teknologi informasi pada saat ini sudah semakin berkembang. Perkembangan ini menyebabkan terjadinya perubahan perilaku dan peradaban manusia yang ditandai dengan semakin banyaknya kegiatan yang dilakukan melalui internet. Kegiatan tersebut meliputi kegiatan pembelajaran (*e-education*), kegiatan pemerintahan (*e-government*), kegiatan perbankan (*e-banking*), dan lainnya.

Perkembangan internet semakin hari semakin meningkat baik teknologi maupun penggunaannya. Teknologi informasi saat ini dapat menjadi pedang bermata dua. Teknologi informasi dapat memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia, tetapi dapat juga menjadi sarana efektif perbuatan melawan hukum (*onrecht matigedaad*).

Dalam hal ini, hukum seharusnya memberikan perlindungan kepada pengguna internet yang beritikad baik dan menindak tegas kepada pelaku kejahatan internet yang menimbulkan banyak kerugian orang lain.

PERBUATAN MELAWAN HUKUM

Perbuatan melawan hukum diatur pada pasal 1365 KUHP yang mengandung unsur-unsur sebagai berikut

1. Adanya perbuatan
2. Perbuatan tersebut melawan hukum
3. Adanya kesalahan dari pihak pelaku
4. Adanya kerugian bagi korban
5. Adanya hubungan kausal antara perbuatan dengan kerugian.

Perbuatan melawan hukum dalam bidang teknologi informasi disebut juga *cyber crime*. (Hamzah, 1989)

Cyber crime adalah perbuatan melanggar hukum/kejahatan virtual (tidak nyata) yang memanfaatkan media komputer yang terhubung ke internet dan mengeksploitasi komputer lain yang terhubung dengan internet.

Karakteristik unik dari kejahatan di dunia maya tersebut antara lain menyangkut lima hal

1. Ruang lingkup kejahatan
2. Sifat kejahatan
3. Modus kejahatan
4. Pelaku kejahatan
5. Kerugian yang ditimbulkan

1. Ruang Lingkup Kejahatan

Selama ini, dalam kejahatan konvensional dikenal adanya dua jenis kejahatan (Ramli, 2004)

a. Kejahatan kerah biru atau *blue color crime*
Kejahatan ini merupakan tindak kriminal yang dilakukan secara konvensional seperti perampokan, pencurian, pembunuhan.

b. Kejahatan kerah putih atau *white color crime*
Kejahatan ini merupakan tindak kriminal yang dilakukan secara kelompok atau terorganisasi. Kejahatan ini terbagi dalam empat kelompok, yakni kejahatan korporasi, kejahatan birokrat, malpraktek, dan kejahatan individu.

Cyber crime sendiri merupakan suatu kejahatan yang muncul akibat adanya komunitas dunia maya di

internet. Pola kejahatan ini termasuk wilayah "abu-abu". (Ramli, 2004).

2. Sifat Kejahatan

Sifat kejahatan *cyber crime* dapat digolongkan sebagai berikut

a. *Cyber crime* sebagai tindakan kriminal

Cyber crime sebagai tindakan kriminal merupakan kejahatan yang dilakukan dengan motif kriminalitas yangmenggunakan internet sebagai sarana kejahatan seperti pencurian nomor pin ATM dan *carding*, yaitu pencurian nomor kartu kredit milik orang lain untuk digunakan dalam transaksi perdagangan di internet; dan pemanfaatan media internet (*webserver, mailing list*) untuk menyebarkan material bajakan. Pengirim *e-mail anonym* yang berisi promosi (*spamming*) juga dapat dimasukkan dalam contoh kejahatan yang menggunakan internet sebagai sarana. Di beberapa negara maju, pelaku *spamming* dapat dituntut dengan tuduhan pelanggaran privasi.

b. *Cyber crime* sebagai kejahatan "abu-abu"

Jenis kejahatan di internet masuk ke dalam wilayah "abu-abu". Oleh sebab itu, sulit menentukan apakah tindakan ini merupakan tindak kriminal atau bukan mengingat motif kegiatannya terkadang bukan untuk kejahatan. Salah satu contohnya adalah *probing* atau *portscanning*. Ini adalah sebutan untuk tindakan pengintaian terhadap sistem milik orang lain dengan cara mengumpulkan informasi sebanyak-banyaknya dari sistem tersebut untuk disalahgunakan. (Ramli, 2004).

3. Modus Kejahatan

Berdasarkan modus kejahatan internet, kejahatan yang berhubungan erat dengan penggunaan teknologi yang berbasis komputer dan jaringan telekomunikasi ini dikelompokkan dalam beberapa bentuk, antara lain : (Golose, 2006).

a. Unauthorized Acces to Computer System and Service

Kejahatan ini terjadi saat seseorang menyusup ke dalam suatu sistem jaringan komputer milik orang lain secara tidak sah, tanpa izin, atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. *Probing* dan *port* merupakan contoh kejahatan ini.

b. Illegal Contents

Kejahatan dengan memasukkan data atau informasi ke internet tentang suatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum. Salah satu contoh kejahatan ini adalah memuat berita bohong atau fitnah yang menghancurkan martabat atau harga diri pihak lain, hal-hal yang berhubungan dengan pornografi, atau memuat informasi yang merupakan rahasia negara.

c. Data Forgery

Kejahatan ini dilakukan dengan tujuan memalsukan data pada dokumen-dokumen penting yang ada di internet. Dokumen-dokumen ini biasanya dimiliki oleh institusi atau lembaga yang memiliki situs berbasis *web data base*.

d. Cyber Espionage, Sabotage, and Extortion

Kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata pada pihak lain. Kejahatan ini dilakukan dengan memasuki sistem jaringan komputer pihak sasaran. *Sabotage* dan *extortion* merupakan jenis kejahatan yang dilakukan dengan membuat gangguan kerusakan atau penghancuran terhadap suatu data, program komputer, atau sistem jaringan komputer yang terhubung dengan internet.

e. Data Theft
Kejahatan yang mengambil data komputer milik orang lain secara tidak sah, baik untuk digunakan sendiri atau digunakan untuk orang lain. *Identity theft* merupakan salah satu kejahatan yang diikuti dengan penipuan.

f. Infringements of Privacy
Kejahatan ini biasanya ditujukan kepada keterangan pribadi seseorang pada formulir data pribadi yang tersimpan secara *computerized*. Apabila diketahui orang lain, data ini dapat merugikan korban secara materil maupun immaterial, seperti nomor kartu kredit, nomor PIN ATM.

g. Cyber Terorism
Cyber terorism adalah suatu tindakan *cyber crime* yang mengancam pemerintah atau warga negara, termasuk *cracking* ke situs pemerintah atau militer. Contohnya, kasus Ramzi Yousef, dalang penyerangan pertama ke gedung WTC. Ramzi diketahui menyimpan detail seragam dalam file yang dienkripsi di laptopnya.

4. Pelaku Kejahatan

Pelaku kejahatan dalam *cyber crime* disebut *hacker* dan *cracker*. Contoh perbuatan yang dilakukan oleh *hacker* dan *cracker*, antara lain (Golose, 2006).

a. pencurian dan penggunaan *account* internet milik orang lain
b. pengubahan halaman web yang dikenal dengan istilah *deface*.
c. pembajakan dapat dilakukan dengan mengeksploitasi lubang keamanan. Salah satu langkah yang dilakukan *cracker* sebelum masuk ke server yang ditargetkan adalah melakukan pengintaian. Cara yang dilakukan adalah dengan melakukan *portscanning* atau *probing* untuk melihat servis-servis apa yang saja yang tersedia di server target. Contoh hasil *scanning* dapat menunjukkan bahwa *server* target menjalankan program *web server Apache, mail server Sendmail*, dan seterusnya.
d. penyebaran virus ke komputer. Penyebaran dilakukan dengan menggunakan *e-mail*, seringkali orang yang sistem *e-mail*-nya terkena virus tidak sadar akan hal itu. Virus ini dikirimkan ke tempat lain melalui *e-mail*-nya. Kasus virus ini sudah cukup banyak seperti virus *Mellisa, I Love You*, dan *SirCam*.
e. *DoS attack* merupakan serangan yang bertujuan untuk melumpuhkan target (*hang, crash*) sehingga tidak dapat memberikan layanan. Serangan ini tidak melakukan pencurian,

penyadapan, ataupun pemalsuan data, tetapi dengan hilangnya layanan, target tidak dapat memberikan servis sehingga ada kerugian finansial.

f. Kejahatan yang berhubungan dengan nama *domain*. Nama *domain* digunakan untuk mengidentifikasikan perusahaan dan merk dagang. Banyak orang mencoba menarik kentungan dengan mendaftarkan *domain* nama perusahaan orang lain kemudian berusaha menjualnya dengan harga yang lebih mahal. Istilah yang sering digunakan adalah *cybersquatting*.

Sasaran kejahatan *cyber crime* dapat dikelompokkan menjadi katagori sebagai berikut (Hinea, 2005)

a. *Cyber crime* yang menyerang individu (*Against Person*)

Sasaran jenis kejahatan ini ditujukan kepada perorangan atau individu yang memiliki sifat atau kriteria tertentu sesuai tujuan penyerangan tersebut. Salah satu contoh kejahatan ini adalah pornografi yang merupakan kegiatan yang dilakukan dengan membuat, memasang, mendistribusikan, dan menyebarkan material yang berbau pornografi, cabul serta mengekspos hal-hal yang tidak pantas (Hinea, 2005).

b. *Cyberstalking*

Kegiatan yang dilakukan untuk mengganggu atau melecehkan seseorang dengan memanfaatkan komputer, misalnya dengan menggunakan *e-mail* yang dilakukan secara berulang-ulang seperti halnya teror di dunia *cyber*. Gangguan tersebut bisa saja berbau seksual, religius, dan lain-lain.

c. *Cyber-Tresspass*

Kegiatan yang dilakukan melanggar area privasi orang lain seperti misalnya *web hacking, breaking* ke PC, *probing, port scanning.*

d. *Cyber crime* menyerang hak milik (*Against Property*)

Cyber crime yang dilakukan untuk mengganggu atau menyerang hak milik orang lain. Beberapa contoh kejahatan jenis ini misalnya pengaksesan komputer secara tidak sah melalui dunia *cyber*, pemilikan informasi elektronik secara tidak sah/pencurian informasi, *carding, cybersquating, hijacking,* data *forgery* dan segala kegiatan yang bersifat merugikan hak milik orang lain.

e. *Cyber crime* menyerang pemerintah (*Against Goverment*)

Cyber crime Against Government dilakukan dengan tujuan khusus penyerangan terhadap pemerintah. Kegiatan tersebut misalnya *cyber terrorism* sebagai tindakan yang mengancam pemerintah termasuk juga *cracking* ke situs resmi pemerintah atau situs militer.

5. Jenis Kerugian yang Ditimbulkan

Hacking atau *cracking* adalah istilah yang diberikan kepada orang yang melakukan kejahatan internet yang dampaknya merugikan para pengguna jasa internet. Para korban menganggap bahwa *cracker* adalah penjahat. Dampak kerugian yang ditimbulkan oleh *cracker* adalah materil dan nonmateril. Contoh

kerugian materil adalah penyalahgunaan nomor pin ATM, kartu kredit, dan lain-lain. Contoh kerugian nonmateril adalah pornografi, pencemaran nama baik, dan lainnya.

UNDANG-UNDANG DAN PENEGAKAN HUKUM *CYBER CRIME*

Untuk menjawab tuntutan dan tantangan komunikasi global melalui internet, undang-undang yang diharapkan adalah perangkat hukum yang akomodatif terhadap perkembangan serta antisipatif terhadap permasalahan termasuk dampak negatif penyalahgunaan internet dengan berbagai motivasi yang dapat menimbulkan kerugian materi dan nonmateri bagi pengguna jasa internet.

Saat ini, Indonesia belum memiliki undang-undang khusus yang mengatur *cyber crime* walaupun rancangan undang-undang tersebut sudah ada sejak tahun 2000 tetapi mendapat penolakan dari DPR. Namun, terdapat beberapa hukum positif yang berlaku umum dan dapat dikenakan kepada para pelaku *cyber crime* terutama untuk kasus-kasus yang menggunakan komputer sebagai sarana.

- **Kitab Undang-Undang Hukum Pidana**

  Dalam upaya menangani kasus-kasus yang terjadi, para penyidik melakukan analogi atau perumpamaan dan persamaan terhadap pasal-pasal yang ada dalam KUHP. Pasal-pasal di dalam KUHP biasanya digunakan lebih dari satu pasal karena melibatkan beberapa perbuatan sekaligus. Pasal-pasal yang dapat dikenakan dalam KUHP pada *cyber crime* antara lain :

1) Pasal 362 KUHP yang dikenakan untuk kasus *carding;* pelaku mencari nomor kartu kredit milik orang lain walaupun tidak secara fisik karena hanya nomor kartunya yang diambil dengan menggunakan *software card generator* di internet untuk melakukan transaksi di *e-commerce*. Setelah dilakukan transaksi dan barang dikirimkan, 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. Pada kenyataannya, barang tersebut tidak ada. Hal tersebut diketahui setelah uang dikirimkan dan barang yang dipesankan tidak datang sehingga pembeli tersebut 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. Jika tidak dilaksanakan, akan membawa dampak yang membahayakan. Hal ini 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 *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. Walaupun berbahasa Indonesia, sangat sulit untuk menindak pelakunya karena mereka melakukan pendaftaran *domain* tersebut di luar negeri di mana pornografi yang menampilkan orang dewasa bukan merupakan hal yang ilegal.
7) Pasal 282 dan 311 KUHP dapat dikenakan untuk kasus penyebaran foto atau film pribadi seseorang secara vulgar di internet , misalnya kasus-kasus video porno para mahasiswa.
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 padahal 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 tidak dapat digunakan sebagaimana mestinya.

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

  Menurut pasal 1 angka 8 Undang-Undang Nomor 19 Tahun 2002 tentang Hak Cipta, program komputer adalah sekumpulan instruksi 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 instruksi-instruksi tersebut. Hak cipta untuk program komputer berlaku selama 50 tahun. Berikut isi dari pasal 30.

  (1) Hak Cipta atas Ciptaan:
      a. program komputer;
      b. sinematografi;
      c. fotografi;
      d. *database*; dan
      e. karya hasil pengalihwujudan yang berlaku selama 50 (lima puluh) tahun sejak pertama kali diumumkan.
  (2) Hak Cipta atas perwajahan karya tulis yang diterbitkan berlaku selama 50 (lima puluh) tahun sejak pertama kali diterbitkan.
  (3) Hak Cipta atas Ciptaan sebagaimana dimaksud pada ayat (1) dan ayat (2) pasal ini serta Pasal 29 ayat (1) yang dimiliki atau dipegang oleh suatu badan hukum berlaku

selama 50 (lima puluh) tahun sejak pertama kali diumumkan.

- **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, 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, terutama para *hacker*, dapat dikenakan sanksi dengan menggunakan Undang- Undang ini, 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, seseorang 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)"

- **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. Berikut isi Pasal 12.

  (1) Dokumen perusahaan dapat dialihkan ke dalam mikrofilm atau media lainnya.
  (2) Pengalihan dokumen perusahaan ke dalam mikrofilm atau media lainnya sebagaimana dalam ayat (1) dapat dilakukan sejak dokumen tersebut dibuat atau diterima oleh perusahaan yang bersangkutan.
  (3) Dalam mengalihkan dokumen perusahaan yang dimaksud dalam ayat (1), pimpinan perusahaan wajib mempertimbangkan kegunaan naskah asli dokumen yang perlu tetap

disimpan karena mengandung nilai tertentu demi kepentingan perusahaan atau kepentingan nasional.

(4) Dalam hal dokumen perusahaan yang dialihkan ke dalam mikrofilm atau media lainnya adalah naskah asli yang mempunyai kekuatan pembuktian otentik dan masih mengandung kepentingan hukum tertentu, pimpinan perusahaan wajib tetap menyimpan naskah asli tersebut.

Pengalihan dari *paper based* ke *paper less* juga harus diharmonisasikan dengan RUU ITE agar dokumen yang dialihkan memiliki kekuatan hukum yang sama dengan dokumen elektronik lainnya.

- **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, dalam proses tersebut 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 penyelidikan terhadap pelaku. Data yang diberikan oleh pihak bank berbentuk aplikasi pendaftaran, jumlah rekening masuk dan keluar serta kapan dan di mana dilakukan transaksi sehingga penyidik dapat menelusuri keberadaan pelaku berdasarkan data– data tersebut. Undang-undang ini juga mengatur 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.

- **Undang-Undang No. 10 Tahun 1998 tentang Perbankan**

Pasal 40 menyatakan bahwa bank wajib merahasiakan keterangan mengenai keterangan nasabah penyimpan dan simpanannya. Perlindungan privasi dalam kegiatan perbankan, termasuk dalam kegiatan *internet banking* dan *electronics banking*. Pengeualian terhadap perlindungan privasi dimungkinkan untuk kepentingan perpajakan, peradilan,

dan tukar menukar informasi antarbank.

Berikut isi Pasal 6 huruf e, f, g:
Usaha Bank Umum yang meliputi

- pemindahan uang baik untuk kepentingan sendiri maupun unutk kepentingan nasabah
- penempatan dana pada, pemindahan dana dari, atau peminjaman dana kepada bank lain, baik dengan menggunakan surat, sarana telekomunikasi maupun dengan wesel unjuk, cek, atau sarana lainnya
- penerimaan pembayaran dari tagihan atas surat berharga dan melakukan perhitungan dengan atau antarpihak ketiga.

Perlu regulasi tentang transfer dana, yang sangat erat kaitannya dengan penggunaan sarana teknologi informasi, harmonisasi penerapan sanksi dalam RUU Transfer dana dan RUU ITE. Juga, implementasi regulasi lebih lanjut tentang *internet banking* sebagai salah satu bentuk pelayanan perbankan.

- **Undang-Undang No 15 Tahun 2003 tentang Pemberantasan Terorisme**

Selain Undang-Undang No. 25 Tahun 2003, undang-undang ini mengatur 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. Saat ini, komunikasi antara para pelaku di lapangan dengan pimpinan atau aktor intelektualnya dilakukan dengan memanfaatkan fasilitas internet untuk menerima perintah atau menyampaikan kondisi di lapangan. Para pelaku mengetahui pelacakan terhadap internet lebih sulit dibandingkan pelacakan melalui *handphon**e***. **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*.**

Sistem perundang-undangan di Indonesia belum mengatur secara khusus kejahatan komputer melalui media internet, beberapa peraturan yang ada di dalam KUHP maupun di luar KUHP untuk sementara dapat diterapkan terhadap beberapa kejahatan, tetapi ada juga kejahatan yang tidak dapat diantisipasi oleh undang-undang yang saat ini berlaku.

Selain dari undang-undang, penegakan hukum, dalam masalah *cyber crime* ditemui banyak hambatan yang berkaitan dengan kemampuan penyidik, alat bukti, dan fasilitas komputer forensik. Upaya-upaya yang dapat dilakukan untuk mengatasi hambatan yang ditemukan di dalam melakukan penyelidikan terhadap *cyber crime* antara lain penyempurnaan perangkap hukum, misalnya dengan membuat undang-undang tentang *cyber crime* yang dibuat secara khusus sebagai ekspesialis untuk memudahkan

penegakan hukum terhadap kejahatan tersebut. Kualifikasi perbuatan yang berkaitan dengan *cyber crime* harus dibuat secara jelas agar tercipta kepastian hukum bagi masyarakat khususnya pengguna jasa internet. Mendidik para penyidik untuk lebih paham dengan masalah *cyber crime*, memberikan wewenang khusus kepada penyidik dalam melakukan beberapa tindakan yang diperlukan dalam rangka penyidikan kasus *cyber crime*, membangun fasilitas komputer forensik, meningkatkan upaya penyidikan dan kerja sama internasional, serta melakukan upaya penanggulangan pencegahan.

SIMPULAN

Cyber crime merupakan perbuatan yang merugikan pengguna jasa internet. Para korban menganggap bahwa pelaku *cyber crime* adalah penjahat. Modus operandi *cyber crime* sangat beragam dan terus berkembang sejalan dengan perkembangan teknologi. Kejahatan *cyber crime* berbeda dengan kejahatan konvensional karena kejahatan *cyber crime* menggunakan komputer dalam pelaksanaannya. Penegakan hukum bagi tindak kejahatan *cyber crime* mengalami kendala baik dari segi perangkat hukumnya, kemampuan penyidik, alat bukti, dan fasilitas komputer forensik.

SARAN

1. Undang-undang *cyber crime* perlu dibuat secara khusus untuk memudahkan penegakan hukum terhadap kejahatan tersebut
2. Kualifikasi perbuatan yang berkaitan dengan *cyber crime* agar pengguna jasa internet mengerti batasan perbuatan melanggar hukum dalam penggunaan jasa internet.
3. Perlu hukum acara khusus yang dapat mengatur jenis-jenis alat bukti yang sah dalam kasus *cyber crime*, dan pemberian wewenang khusus pada penyidik dalam melakukan beberapa tindakan penyidikan kasus *cyber crime*.

DAFTAR PUSTAKA

Golose, Petrus Reinhard. 2006. "Perkembangan *Cyber crime* dan Upaya Penanganannya di Indonesia oleh POLRI", *Buletin Hukum Perbankan dan Kebanksentralan, Vol. 4, No. 2,* 29-42.

Hamzah, Andi. 1989. *Aspek-Aspek Pidana di Bidang Komputer*.

Hinca. 2005. *Membangun Cyber Law di Indonesia yang Demokratis*. Jakarta.

Ramli, Ahmad M. 2004. *Cyberlaw dan HAKI dalam Sistem Hukum Indonesia*. Bandung: PT. Refika Aditama.

Undang-Undang Hukum Pidana.

Undang-Undang No. 36 Tahun 1999 tentang Telekomunikasi.

Undang-Undang No. 15 tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme.

Undang-Undang No. 25 tahun 2003 tentang Tindak Pidana Pencucian Uang.

Undang-Undang No. 8 tahun 1997 tentang Dokumen Perusahaan.