CYBER LAW INDONESIA,ANTARA KEBUTUHAN ATAU PELENGKAP

Oleh : Sidik

ABSTRACT

The use of internet technology affects greatly toward its users. It is seen clearly on the increasing number of internet users in big cities in Indonesia and other parts of the world. This triggers various motives of users from good to malicious attempts for crimes. Therefore, a set of identified regulation in a form of Cyber Law and its enforcement is an urgency to take action against internet abuse done by lawbreaker users.

Penggunaan teknologi internet membawa pengaruh yang sangat pesat kepada para penggunanya. Hal ini terlihat dan semakin nyata terlihat pada para pengguna internet dikota-kota besar di negara kita Indonesia dan dibelahan dunia lain. Namun seiring dengan kondisi tersebut maka semakin banyak para pengguna internet dengan tujuan yang berbeda, dari kondisi yang baik sampai dengan kondisi yang tidak baik dan cenderung mengkhawatirkan dan kejahatan-kejahatan yang kian berani dan nyata. Oleh karena itu diperlukannya perangkat hukum yang jelas dan mempunyai kepastian hukum yang jelas terhadap para pelanggar dan penyalahgunaan internet untuk hal-hal yang tidak baik dalam bentuk Cyber Law yang dapat memberikan sanksi sesuai kejahatan yang dilakukan.

I. PENDAHULUAN

1.1 Umum

Perkembangan teknologi informasi yang terjadi pada hampir setiap negara sudah merupakan ciri global yang mengakibatkan hilangnya batas-batas negara (*borderless*). Negara yang sudah mempunyai infrastruktur jaringan informasi yang lebih memadai tentu telah menikmati hasil pengembangan teknologi informasinya, negara yang sedang berkembang salah satunya Indonesia, dalam pengembangannya akan merasakan kecenderungan timbulnya neo-kolonialisme terselubung . Hal tersebut menunjukan adanya pergeseran paradigma dimana jaringan informasi merupakan infrastruktur bagi perkembangan suatu negara. Tanpa penguasaan dan pemahaman akan teknologi informasi ini akan mengakibatkan masih banyaknya masyarakat yang "GapTek" atau Gagap Teknologi. Tantangan globalisasi akan menyebabkan ketergantungan yang tinggi terhadap pihak lain dan hilangnya kesempatan untuk bersaing karena minimnya pemanfaatan teknologi informasi.

Untuk itu perlu adanya upaya-upaya khusus yang harus ditempuh agar dinegara tersebut menjadi masyarakat yang dapat mengikuti perkembangan teknologi informasi. Adalah Thomas L. Friedman seorang coloumnist asing The New York Times dalam bukunya "World is Flat: A Brief History of the Twenty-first Century" menggambarkan bagaimana peradaban dunia saat ini. Friedman menggambarkan bahwa globalisasi merupakan hal yang tidak bisa di

tolak lagi oleh setiap bangsa. Friedman memaparkan tiap tahapan-tahapan globalisasi secara rinci. Globalisasi menurut Friedman terjadi pada hampir di seluruh negara di dunia. Globalisasi yang dijabarkan termasuk didalamnya juga pengaruh besar teknologi informasi dalam aktifitas manusia.

1.2. Perkembangan Teknologi Internet

Sejarah munculnya teknologi internet dimulai pada tahun 1972 yang ditandai dengan dibuatnya jaringan pertama oleh ARPNet dengan menghubungkan beberapa titik jaringan dengan fasilitas yang diberi nama FTP (*file transfer protocol*) dan juga teknik TCP IP . Kemudian pada tahun 1973 ARPnet bekerja sama dengan salah satu lembaga riset di Amerika Serikat yaitu DARPA (*Defence Advanced Research Project Agency*). Pada waktu itu lembaga ini membangun sebuah jaringan sederhana (*interconnection networking*) yang digunakan sebagai sarana penghubung beberapa jaringan paket data diantaranya CS-Net, BIT-Net, NSF-Net. Sekitar 11 tahun kemudian, tepatnya 1983 teknologi ini dikembangkan lagi hingga sudah mulai digunakannya *host* hingga tahun 1990 baru diperkenalkan penggunaan nama domain bagi sebuah alamat internet atau yang disebut dengan DNS (*domain name server*). Sehingga sekarang kita menyebut internet dengan nama I*nterconnection Networking*. Disadari atau tidak, bahwa perkembangan teknologi informasi yang berwujud internet, telah mengubah pola interaksi masyarakat, seperti interaksi bisnis, ekonomi, sosial, dan budaya. Internet telah memberikan kontribusi yang demikian besar bagi masyarakat, perusahaan / industri maupun pemerintah. Fitur-fitur *service* (layanan) yang disediakan dalam jaringan internet juga begitu banyak ragamnya, mulai dari *web server, File Transfer Protocol (FTP)*, layanan *E-mail*, sampai fitur-fitur yang berhubungan dengan layanan transaksi yang semakin marak di dalam jaringan internet. Layanan tersebut seperti *Electronic Commerce (E-Commerce), Electronic Banking (E-Banking), Electronic Goverment (E-Gov), Teleconference, Electronic Learning (E-Learning)* dan sebagainya. Karena internet yang begitu banyak memberikan manfaat dan bersifat publik, maka dibutuhkan suatu sistem keamanan dalam menjaga informasi yang ada di internet supaya tidak dirusak oleh pihak-pihak yang potensial melakukan pengrusakan seperti *hacker* dan *cracker*.

Hadirnya internet telah menunjang efektifitas dan efisiensi operasional setiap aktifitas manusia. Bahkan seorang Jhon Chamber, President dan CEO terkemuka di Amerika menyebutkan bahwa saat ini revolusi internet memiliki dampak cukup besar bahkan mungkin lebih besar dari revolusi industri yang pernah terjadi. Pesatnya perkembangan di bidang teknologi informasi saat ini merupakan dampak dari semakin kompleksnya kebutuhan manusia akan informasi itu sendiri. Dekatnya hubungan antara informasi dan teknologi jaringan komunikasi telah menghasilkan dunia maya yang amat luas yang biasa disebut dengan teknologi *cyberspace*. Teknologi ini berisikan kumpulan informasi yang dapat diakses oleh semua orang dalam bentuk jaringan-jaringan komputer yang disebut jaringan internet. Meskipun infrastruktur di bidang teknologi informasi di Indonesia tidak sebanyak negara-

negara lain, namun bukan berarti Indonesia lepas dari ketergantungan terhadap teknologi informasi. Ada beberapa aspek kehidupan masyarakat di Indonesia yang saat ini dipengaruhi oleh peran teknologi informasi internet seperti; pelayanan informasi, transaksi perdagangan dan bisnis, serta pelayanan jasa oleh pemerintah dan swasta.

Beberapa alasan mengapa internet memberikan dampak besar dalam segala aspek kehidupan manusia :

a) Dapat diakses selama 24 jam terus menerus
b) Biaya relatif murah bahkan bisa didapatkan dengan gratis (*hotspot*)
c) Kemudahan akses informasi dalam melakukan transaksi
d) Kemudahan membangun reasi
e) Materi di-*update* dengan mudah
f) Pengguna bisa siapa saja dan kapan saja
g) Dapat diakses diseluruh penjuru dunia

Teknologi internet atau dikenal dengan istilah dunia maya (*cyber space*) mempunyai karakteristik atau sifat yang dijelaskan oleh Dysson (1994), diantaranya :

a) Beroperasi secara kasat mata (*virtual*)
b) Selalu berubah dengan cepat
c) Tidak mengenal batas-batas teritorial negara
d) Orang-orang yang beraktifitas didalamnya tidak memerlukan identitas tertentu
e) Informasi yang didapat bersifat publik

1.3. Ketentuan Hukum Dunia Maya (*cyber space*)

Kemajuan teknologi informasi termasuk internet di dalamnya juga memberikan tantangan tersendiri bagi perkembangan hukum di Indonesia. Hukum di Indonesia di tuntut untuk dapat menyesuaikan dengan perubahan sosial yang terjadi. Seorang pakar hukum dan sosiolog, Soerjono Soekanto mengemukakan bahwa perubahan-perubahan sosial dan perubahan hukum atau sebaliknya tidak selalu berlangsung bersama-sama. Artinya pada keadaan tertentu perkembangan hukum mungkin tertinggal oleh perkembangan unsur-unsur lainnya dari masyarakat serta kebudayaannya atau mungkin hal yang sebaliknya.

Ada lima unsur yang dirumuskan oleh Soerjono Soekanto berkaitan dengan upaya penegakan hukum, diantaranya adalah :

a) Undang-undang.
b) Mentalitas aparat penegak hukum.
c) Perilaku masyarakat.
d) Sarana.
e) Kultur.

Segala sesuatu yang dilakukan oleh anggota masyarakat akan berpengaruh langsung pada proses penegakan hukum. Sehingga memaksa para aparat penegak hukum untuk dapat mengimplementasikan *law in book* menjadi *law in action*. Artinya adalah regulasi atau aturan-aturan yang sudah dibuat dalam KUHP (Kitab Undang-Undang Hukum Pidana/ Perdata) harus bisa diterapkan dalam kehidupan nyata dan tidak hanya dijadikan sebagai "pajangan" saja. Memang harus disadari bahwa Undang-undang yang mengatur permasalahan kejahatan di dunia maya belum diatur secara khusus atau spesifik dalam KUHP tersebut.

Beberapa hal yang secara khusus diatur dalam KUHP dan disusun

berdasarkan tingkat intensitas terjadinya kasus tersebut yaitu :

a) Ketentuan yang berkaitan dengan delik pencurian
b) Ketentuan yang berkaitan dengan perusakan/penghancuran barang
c) Delik tentang pornografi
d) Delik tentang penipuan
e) Ketentuan yang berkaitan dengan perbuatan memasuki atau melintasi wilayah orang lain Delik tentang penggelapan
f) Kejahatan terhadap ketertiban umum
g) Delik tentang penghinaan
h) Delik tentang pemalsuan surat
i) Ketentuan tentang pembocoran rahasia dan;
j) Delik tentang perjudian

Dibawah ini ada beberapa contoh pasal dalam KUHP yang sudah memberikan regulasi atau sangsi mengenai kejahatan-kejahatan yang dilakukan didunia maya (*cyber crime*).

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 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.

Sedangkan Jeane Nelttje Saly berpendapat bahwa perkembangan teknologi informasi yang begitu cepat menimbulkan akibat yang menguntungkan dan akibat yang merugikan bagi masyarakat. Menguntungkan masyarakat karena antara lain komunikasi yang mudah dengan menggunakan informasi elektronik. Merugikan karena hukum terkait belum cukup mampu

memfungsikan dirinya sebagai sarana ketertiban. Disinilah tampak jelas bahwa hukum di Indonesia masih tertinggal (bahkan tertinggal jauh) dengan perubahan yang ada di masyarakat. Hukum di Indonesia belum mengenal istilah internet, *carding, e-commerce* atau istilah lainnya di bidang Teknologi Informasi. Dengan kata lain *cyberlaw* di Indonesia belum benar-benar terwujud seperti yang diharapkan masyarakat. *Cyberlaw* mungkin dapat diklasifikasikan sebagai rejim hukum tersendiri, karena memiliki multi aspek; seperti aspek pidana, perdata, internasional, administrasi, dan aspek Hak Kekayaan Intelektual (HaKI).

II. PEMBAHASAN

UPAYA PENEGAKAN *CYBER LAW* DI INDONESIA

2.1. KEJAHATAN (*CYBER CRIME*) INTERNET

Semakin mudahnya akses mendapatkan fasilitas internet ditengarai sebagai faktor utama munculnya berbagai jenis kejahatan (*cyber crime*) didunia maya. Sekarang hampir disetiap sudut kota banyak bermunculan fasilitas-fasilitas pelayanan internet baik itu berupa Warnet, Café Hotspot, bahkan disekolah-sekolah dasar sudah diajarkan bagaimana mengakses internet. Disatu sisi hal itu merupakan dampak dari kemajuan teknologi yang ada di negara ini tentunya adalah yang berdampak positif dan juga ada yang berdampak negatif . Dibawah ini penulis coba menjabarkan beberapa dampak yang mungkin terjadi berkaitan dengan mudahnya akses internet diseluruh dunia.

a). Dampak positif

- Kemudahan mendapatkan informasi dari belahan dunia manapun
- Tidak memerlukan biaya yang banyak bahkan bisa gratis (*hotspot*)
- Dalam mengakses tidak perlu menunjukan identitas diri
- Informasi yang didapat *up to date*
- Dapat mencari informasi apa saja, tinggal gunakan fasilitas *search engine*

b). Dampak negatif

- Mengirim *e-mail* palsu (*spam*)
- Melakukan pembajakan
- Mencoba masuk ke sistem komputer orang lain
- Menyebarkan virus
- Membuka situs porno

Kemudahan-kemudahan yang didapat dari akses internet secara global, tentunya bukan berarti tidak terdapat sisi atau bagian yang rentan terhadap kejahatan dunia siber. Sisi yang sangat merisaukan yaitu dari sisi keamanan dari sebuah sistem. Pengamanan sistem informasi berbasis internet sekarang ini sedang menjadi pembahasan yang sangat mendesak untuk segera dicari solusi yang tepat. Ancaman terhadap suatu sistem timbul, manakala ada seseorang yang mempunyai keinginan untuk memperoleh akses ilegal ke dalam jaringan komputer orang lain, merusak jaringan, mengubah tampilan dengan tampilan lain yang dapat merugikan banyak pihak.

Cybercrime mempunyai berbagai macam pengertian, diantaranya adalah Kejahatan yang dilakukan oleh seseorang ataupun kelompok dengan menggunakan sarana komputer dan alat telekomunikasi lainnya yang terhubung ke dalam jaringan internet,

atau sering juga disebut dengan kejahatan mayantara, kejahatan siber, kejahatan komputer, kejahatan dunia maya, dan sebagainya.

Menurut Ari Juliano Gema, *cybercrime* memiliki karakteristik yang khas apabila dibandingkan dengan kejahatan konvensional lainnya, yaitu :

a. Perbuatan yang dilakukan secara ilegal, tanpa hak atau etika yang terjadi dalam ruang atau wilayah siber.
b. Dilakukan dengan manggunakan alat apapun yang terhubung kedalam jaringan internet.
c. Menyebabkan kerugian material maupun immaterial (waktu, nilai, uang, jasa, barang, harga diri, martabat dan kerahasiaan informasi) yang lebih besar daripada kejahatan konvensional.
d. Pelakunya adalah orang yang menguasai perkembangan internet dan aplikasinya.
e. Perbuatan yang sering dilakukan lintas negara (transnasional).

Sedangkan menurut Didik M. Arief Mansyur dan Alisatris Gultom, *cyber crime* memiliki ciri-ciri khusus, yaitu :

a. *Non-violence* (tanpa kekerasan)
b. Sedikit melibatkan kontak fisik
c. Menggunakan peralatan teknologi
d. Memanfaatkan jaringan telematika (telekomunikasi, media dan informatika) global.

Pada awalnya orang atau kelompok tersebut hanya sekedar "iseng" mencoba-coba untuk masuk kedalam sistem orang lain, kemudian karena adanya kemudahan dan ada orientasi mendapatkan keuntungan dalam bentuk barang maupun uang, sehingga orang atau kelompok tersebut menjadikan hal tersebut sebagai profesi. Beberapa kejahatan atau pelanggaran yang sering dilakukan oleh orang atau kelompok yang tidak bertanggung jawab dalam penggunaan teknologi *internet* diantaranya adalah sebagai berikut :

a. *Denial of Service (DoS) Attack,* suatu usaha untuk membuat suatu sumber daya pada sistem komputer tidak dapat bekerja dengan baik dan tidak dapat digunakan oleh pemakainya. *DoS Attack* ini oleh FBI disebut dengan *unprecedented.* Tujuan dari kejahatan ini adalah untuk memacetkan sistem dengan mengganggu akses dari pengguna yang sah atau *legitimate.* Secara khas targetnya adalah *high profile web server* yang bertujuan mengarahkan dan menjadikan *host* halaman web yang tidak terdaftar di internet.

Denial of Service (DoS) Attack mempunyai dua format umum :

1. Memaksa komputer korban untuk me- *reset* atau korban tidak bisa lagi menggunakan perangkat komputernya seperti semula.
2. Menghalangi media komunikasi antara pemakai dan korban sehingga mereka tidak dapat saling berkomunikasi lagi.

Cara lain dari ***Denial of Service (DoS) Attack*** untuk menyerang sistem komputer orang lain :

1. Mencoba untuk "membanjiri" suatu jaringan, dengan demikian mencegah lalu lintas jaringan yang ada.
2. Berusaha mengganggu koneksi antara dua mesin, dengan demikian mencegah akses kepada suatu *service*
3. Berusaha untuk mencegah individu tertentu dari mengakses suatu service.
4. Berusaha mengganggu *service* kepada suatu orang atau sistem secara spesifik.

b. Pembajakan atau *Piracy,* adalah kemampuan dari suatu individu

atau kelompok untuk memeliharan urusan pribadi dan hidup mereka keluar dari pandangan publik atau mengendalikan alir informasi tentang diri mereka. Pembajakan *software* aplikasi, lagu maupun video dalam format MP3, MP4, WAV, AVI dan sebagainya yang dapat dilakukan dengan cara men-*download file* tersebut secara gratis, dibuat salinannya kemudian dijual ke masyarakat umum. Hal tersebut tentunya sangat merugikan dari pihak produsen atau penciptanya.

c. ***Fraud,*** adalah sejenis memanipulasi informasi keuangan dengan tujuan mendapatkan keuntungan yang sebesar-besarnya. Contohnya adanya sebuah situs lelang fiktif dengan mengeruk uang yang masuk dari peserta lelang tetapi barangnya tidak dikirim bahkan identitas pelakunya tidak dapat dilacak.

d. ***Gambling,*** perjudian yang sudah berskala internasional sangat sulit untuk dilacak keberadaanya dan sangat sulit dijerat dengan hukum nasional suatu negara. Dari kegiatana ini uang yang didapat bisa diputar di negara yang merupakan *tax heaven* seperti *Cyman Island* yang menjadi surga bagi para "cukong" untuk melakukan *money laundring.* Ada beberapa jenis *online gambling,* diantaranya adalah :

1. ***Online Casinos***, dalam jenis judi ini orang dapat bermain *Rolet, BlackJack, Cheap* dan lain-lain.
2. ***Online Poker,*** permainan judi yang menawarkan *Texas Hold'em, Omaha, Seven Card Stud* dan permainan lainnya.
3. ***Mobile Gambling,*** merupakan jenis perjudian yang menggunakan media telekomunikasi berupa *handphone, PDA, Wareless Tabled PCs.*

e. ***Pornographi*** **dan** ***Paedophilia,*** merupakan jenis kejahatan didunia maya yang mempertontonkan bentuk tubuh tanpa busana, erotis dan kegiatan seksual lainnya dengan tujuan untuk merusak moral. Dunia *cyber* selain mendatangkan kemudahan dengan mengatasi kendala ruang dan waktu, juga telah melahirkan dunia pornografi yang mengkhawatrikan berbagai kalangan. Melalui *news group, chatroom, webcam* yang mengeksploitasi pornografi anak-anak dibawah umur. Contohnya penyebarluasan *obscene materials* termasuk *pornographi* atau biasa disebut *indecent exposure.* Pelecehan seksual melalui *e-mail, websites, chatprograms* biasa disebut dengan *cyber harrasment*

   Paedophilia merupakan kejahatan penyimpangan seksual yang lebih condong kearah anak-anak (*child pornographi*).

f. ***Data Forgery,*** merupakan kejahatan dunia maya yang dilakukan dengan tujuan memalsukan data atau memanipulasi data pada dokumen-dokumen penting perusahaan yang ada di internet. Dokumen yang dipaluskan biasanya yang dimiliki oleh instansi atau perusahaan yang memiliki situs *web database.* Dokumen yang sudah dipalsukan biasanya disimpan sebagai *scriptless document* dengan menggunakan media internet.

g. ***Insiders*** **atau** ***Internal Hackers,*** biasanya merupakan kejahatan yang dilakukan oleh orang dalan

perusahaan yang merasa kecewa terhadap perusahaan dimana orang tersebut bekerja.

h. ***Viruses,*** program pengganggu yang dapat disebarkan melalui media internet. *Virus* ini biasanya disisipkan dalam sebuah *file download, e-mail,spyware, adware* dan lain-lain.

i. ***Cyber Stalking,*** merupakan kejahatan dalam bentuk kiriman *e-mail* yang tidak dikehendaki oleh *user* atau *junk e-mail* yang sering memadati *folder* dan terkadang ada unsur pemaksaan untuk memperoleh identitas personal secara detil dari calon para korbannya.

j. ***Hate Sites,*** merupakan kejahatan yang menggunakan media situs untuk saling menyerang dan melontarkan komentar-komentar yang tidak sopan dan vulgar dan biasanya dikelola olah para ekstrimis. Isu yang sering diangkat adalah masalah SARA (Suku, Agama dan Ras).

k. ***Criminal Communications,*** media internet ternyata bisa juga dijadikan sebagai alat untuk saling berkomunikasi sesama *gangster, mavia,* sindikat obat bius, dan bahkan komunikasi antar *holigans* dalam dunia sepakbola.

2.2 MASYARAKAT *UNDER GROUND* INTERNET

Kegiatan yang dilakukan oleh para *netter* mempunyai banyak keragaman, sehingga tidak jarang mereka berkumpul menjadi sebuah komunitas. Komunitas itu dapat dibangun melalui *mailing list,* forum diskusi, *polling, blogger* dan sebagainya. Sehingga pada saat kita mengakses kedalam jaringan internet, seolah kita akan masuk kedalamsebuah komunitas yang tidak tampak secara kasat mata.

A. *HACKER*

- Seseorang yang memiliki keahlian dalan bidang komputer dan mampu membuat program komputer lebih baik dibandingkan dengan program yang dirancang bersama.
- *Hacker* menurut Eric Raymond di definisikan sebagai programmer yang pandai.
- Menurut Mansfield, *hacker* didefinisikan sebagai seseorang yang memiliki keinginan untuk melakukan eksplorasi dan penetrasi ke dalam sebuah sistem operasi atau kode pengaman lainnya, tetapi tidak melakukan pengrusakan apapun, tidak mencuri uang atau informasi.
  - Jadi sebuah *hack* yang baik adalah solusi yang cantik kepada masalah *programming* dan *hacking* adalah proses pembuatan-nya.

Karakteristik dari seorang *hacker* diantaranya adalah :

- Suka belajar detail dari bahasa pemrograman atau sistem
- Melakukan pemrograman tidak Cuma berteori saja
- Bisa menghargai, menikmati hasil *hacking* orang lain
- Dapat secara cepat belajar pemrogramman
- Ahli dalam bahasa pemrograman tertentu atau sistem tertentu, seperti "*UNIX hacker*".

Seorang *hacker* dapat dihormati dan dihargai oleh *hacker* lainnya, bukan dilihat dari umur, kekayaan, ataupun tinggi badan. Strata atau tingkatan seorang *hacker* dapat dilihat dari :

- Bukan karena umur atau senioritasnya & pengakuan dari masyarakat underground lainnya.

- Harus mampu membuat program untuk meng-eksploit kelemahan sistem, menulis tutorial (artikel) biasanya dalam format ASCII text biasa, aktif diskusi di mailing list / IRC channel para hacker, membuat situs web dsb.
- Proses memperoleh acknowledgement/pengakuan, akan memakan waktu lama bulanan bahkan tahun.

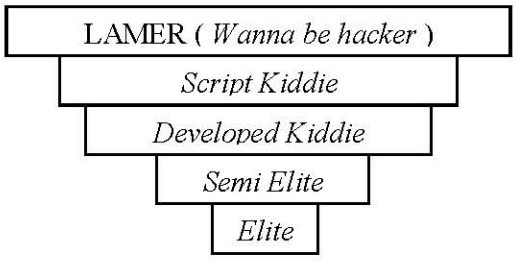
Menurut Steven Levy (1984), seorang *hacker* harus mempunyai kode etik yang harus dipatuhi. Ada 6 etika bagi seorang *hacker* yaitu :

- Akses ke computer harus dilakukan tanpa batas & totalitas. Selalu mengutamakan pengalaman lapangan!
- Semua informasi harus bebas, terbuka, transparan, tidak ada yang disembunyikan.
- Tidak pernah percaya pada otoritas, penguasa percaya pada desentralisasi.
- Seorang *hacker* hanya di nilai dari kemampuan *hacking*-nya, bukan kriteria buatan seperti gelar, umur, posisi atau suku bangsa.
- Seorang *hacker* membuat seni & keindahan di komputer.
- Komputer dapat mengubah hidup anda menuju yang lebih baik.

Selain mempunyai etika yang berlaku sesama *hacker,* masyarakat *underground* juga mempunyai aturan main yang harus dipatuhi juga oleh mereka. Ada banyak sekali aturan-aturan main yang harus diikuti bagi seseorang yang ingin menjadi *hacker,* diantaranya yaitu :

- Hormati pengetahuan dan kebebasan informasi
- Memberitahukan sistem administrator akan adanya pelanggaran keamanan / lubang di keamanan yang anda lihat.
- Jangan mengambil keuntungan yang tidak *fair* dari *hack*.
- Tidak mendistribusikan dan mengumpulkan *software* bajakan.
- Tidak pernah mengambil resiko yang bodoh – dan harus selalu mengetahui kemampuan sendiri.
- Selalu bersedia untuk secara terbuka / bebas / gratis memberitahukan & mengajarkan berbagai informasi & metoda yang diperoleh.
- Tidak pernah meng-hack sebuah sistem untuk mencuri uang.
- Tidak pernah memberikan akses ke seseorang yang akan membuat kerusakan.
- Tidak pernah secara sengaja menghapus & merusak file di komputer yang di*hack.*
- Hormati mesin yang di *hack*, dan memperlakukan dia seperti mesin sendiri.

Dalam masyarakat *underground* dalam dunia *hacker,* mereka juga mempunyai strata atau tingkatan bagi sesama anggota *hacker.* Tingkatan atau strata bagi komunitas *hacker* dapat dilihat dari gambar dibawah ini :



Gambar 2.1 Strata atau tingkatan *hacker*

- ***Elite,*** Juga dikenal sebagai 3l33t, 3l337, 31337 atau kombinasi dari itu; merupakan ujung tombak industri keamanan jaringan. Mereka mengerti sistem operasi luar dalam, sanggup mengkonfigurasi & menyambungkan jaringan secara global. Sanggup melakukan pemrograman setiap harinya. Mereka biasanya efisien & trampil menggunakan pengetahuannya dengan tepat. Mereka seperti siluman dapat memasuki sistem tanpa di ketahui, walaupun mereka tidak akan menghancurkan data-data. Karena mereka selalu mengikuti peraturan yang ada.
- ***Seni Elite,*** tingkatan h*acker* ini biasanya lebih muda daripada Elite. Mereka juga mempunyai kemampuan & pengetahuan luas tentang komputer, mengerti tentang sistem operasi (termasuk lubangnya). Biasanya dilengkapi dengan sejumlah kecil program cukup untuk mengubah program eksploit. Banyak serangan yang dipublikasi dilakukan oleh *hacker* kaliber ini, tetapi terkadang oleh para kalangan *Elite,* mereka masih sering dikategorikan sebagai *Lamer.*
- ***Developed Kiddie,*** **s**butan ini diberikan karena umur kelompok ini masih muda (ABG) dan masih sekolah. Mereka membaca tentang metoda hacking dan caranya di berbagai kesempatan. Mereka mencoba berbagai sistem sampai akhirnya berhasil dan memproklamirkan kemenangan ke lainnya. Umumnya mereka masih menggunakan *Grafik User Interface* (GUI) dan baru belajar *basic* dari UNIX, tanpa mampu menemukan lubang kelemahan baru di sistem operasi.
- ***Script Kiddie,*** kegiatan yang dilakukan hampir sama dengan tetapi mereka hanya mempunyai pengetahuan teknis *networking* yang sangat minimal. Biasanya tidak lepas dari GUI. *Hacking* dilakukan menggunakan *trojan* untuk menakuti dan menyusahkan hidup sebagian pengguna Internet.
- ***Lamer (Wanna be hacker),*** Mereka adalah orang tanpa pengalaman dan pengetahuan yang ingin menjadi *hacker (wanna-be hacker)*. Mereka biasanya membaca atau mendengar tentang *hacker* dan ingin seperti itu. Biasanya melakukan *hacking* masih menggunakan *software trojan, nuke* dan DoS. Karena banyak kekurangannya untuk mencapai *elite,* dalam perkembangannya mereka hanya akan sampai level *developed kiddie* atau *script kiddie* saja.

B. *CRACKER*

Dibawah ini ada beberapa pengertian berkenaan dengan apa yang disebut dengan *cracker* , diantaranya yaitu :

- "Seseorang yang masuk ke sistem orang lain, biasanya di jaringan komputer, mem-*bypass password* atau lisensi program komputer, atau secara sengaja melawan keamanan komputer. *Cracker* dapat mengerjakan hal ini untuk keuntungan, maksud jahat, atau karena sebab lainnya karena ada tantangan. Beberapa proses pembobolan dilakukan untuk menunjukan kelemahan keamanan sistem"
- Atau pengertian yang lainnya adalah *cracker* merupakan "sisi gelap" atau *dark side* dari *hacker* yang mempunyai maksud merusak sebuah sistem komputer, mencuri

informasi yang ada didalamnya dan bahkan bisa sampai melumpuhkan keseluruhan sistem komputer orang lain.

Penggolongan *hacker* dan *cracker* menurut NCIS Inggris adalah sebagai berikut :

1. ***Recreational Hackers,*** kejahatan yang dilakukan *netter* tingkat pemula untuk sekedar mencoba kekurang handalan sebuah sistem sekuritas (keamanan) suatu perusahaan.
2. ***Crackers atau criminal minded hackers***, pelaku kejahatan ini memiliki motivasi untuk mendapatkan keuntungan finansial, sabotase, dan penghancuran data. Tipe kejahatan ini biasanya terjadi karena ada bantuan orang dalam perusahaan tersebut atau juga berasal dari lawan bisnisnya.
3. ***Political Hackers,*** aktivis politik atau yang disebut dengan *hacktivist* dengan cara melakukan pengrusakan terhadap ratusan situs web untuk mengkampanyekan program-programnya, bahkan tidak jarang digunakan juga untuk mendiskriditkan lawan politiknya.

2.2. *CYBER LAW*

a. Definisi

Pengguna internet di Indonesia sebenarnya berjumlah cukup besar. Namun, bila angka itu dibandingkan dengan total populasi yang mencapai 207 juta jiwa, maka diperoleh angka kurang dari 2% penduduk Indonesia yang menggunakan internet. Angka nisbi itu kian kecil lagi kalau kita mau mengulas soal kepemilikan komputer dimasyarakat kita. Relatif rendahnya prosentase ini tidak berarti lantas kita tidak membutuhkan kehadiran *cyberlaw* . *Cyberlaw* sendiri merupakan pengertian umum yang mengacu pada aspek regulasi dan perundangan dari TI dalam *cyber space*. Dibawah ini terdapat beberapa pengertian dari *cyberlaw* :

1. *CyberLaw* adalah hukum yang digunakan di dunia *cyber* (dunia maya), yang umumnya diasosiasikan dengan *Internet*. *Cyberlaw* dibutuhkan karena dasar atau fondasi dari hukum di banyak negara adalah "ruang dan waktu". Sementara itu, Internet dan jaringan komputer mendobrak batas ruang dan waktu ini.
2. Hukum atau regulasi yang mengatur kejahatan-kejahatan yang dilakukan didalam dunia maya (*CyberCrime*).
3. Aturan-aturan hukum yang didalamnya memuat atau membicarakan mengenai aspek-aspek hukum yang berkaitan dengan aktivitas manusia yang berinteraksi dengan internet

Patut disyukuri sekarang, paling tidak Indonesia sudah berhasil mengatur masalah HaKI (Hak atas Kekayaan Intelektual) beberapa waktu lalu. Namun undang-undang tersebut masih berfokus pada persoalan perlindungan kekayaan intelektual saja. Ini terkait dengan persoalan tingginya kasus pembajakan piranti lunak di negeri ini. Selain itu bagi para insan musik dan perfilman di Indonesia turut bersyukur dengan adanya undang-undang HaKI ini dan diharapkan dapat mengurangi masalah pembajakan hak cipta.

b. Mengapa *Cyber Law*

Kehadiran UU mengenai HaKI tersebut, tentu tidak lepas dari desakan negara-negara produsen piranti lunak itu berasal. Terlepas dari masalah itu, sebenarnya kehadiran

cyberlaw yang langsung memfasilitasi *eCommerce*, *eGovernment* dan *cybercrime* sudah sangat diperlukan. Sebenarnya negara kita sudah merumuskan adanya undang-undang yang dapat mengatur secara spesifik mengenai kejahatan di dunia maya. Sekitar bulan Maret 2003 dua buah Rancangan Undang-Undang (RUU) sudah dibuatkan *draft* –nya, yang satu diberi nama: RUU Pemanfaatan Teknologi Informasi (RUU PTI), sementara satunya lagi bernama RUU Transaksi Elektronik (RUU TE) sudah dirancang dan sudah mulai disosialisasikan melalui seminar-seminar di perguruan tinggi di seluruh Indonesia. RUU PTI dimotori oleh Fakultas Hukum Universitas Pajajaran dan Tim Asistensi dari Institut Teknologi Bandung (ITB) dengan jalur Departemen Perhubungan (melalui Dirjen Postel), sementara RUU TE dimotori oleh Lembaga Kajian Hukum dan Teknologi dari Universitas Indonesia dengan jalur Departemen Perindustrian dan Perdagangan yang kemudian menjadi Rancangan Undang-undang Informasi dan Transaksi Elektronik (RUU ITE). Materi-materi yang dicakup dalam RUU Informasi dan Transaksi Elektronik (ITE) sudah termasuk mengenai *eCommerce*, *eGovernment* dan *cybercrime*.

Pengakomodasian ketiga materi tersebut dirasakan sudah sangat mendesak mengingat persoalan ketiganya memang sudah muncul dalam kehidupan secara nyata. Memang terkesan bahwa pemerintah terlihat sangat lamban dalam bertindak. Namun, secara mendasar memang harus dikatakan pengaturan secara legal-formal baru bisa dilakukan bila fenomena yang ada sudah muncul. Dalam membuat suatu aturan baru tentunya harus sudah merumuskan mengenai "Apa yang harus diatur, mengapa harus diatur dan bagaimana mekanisme pengaturannya". Apabila ketiga pertanyaan ini belum bisa ditemukan jawabannya, maka hasil yang akan dicapai akan jauh dari maksimal. Sebenarnya secara nyata sebelum RUU ITE dikeluarkan, dunia hukum Indonesia sudah memberikan itikad baik dalam upaya penegakan hukum dengan mempergunakan regulasi yang sudah ada.

Ada beberapa ruang lingkup *cyberlaw* yang memerlukan perhatian serius di Indonesia saat ini yakni;

1. Kriminalisasi *Cyber Crime* atau kejahatan di dunia maya. Dampak negatif dari kejahatan di dunia maya ini telah banyak terjadi di Indonesia. Namun karena perangkat aturan yang ada saat ini masih belum cukup kuat menjerat pelaku dengan sanksi tegas, kejahatan ini semakin berkembang seiring perkembangan teknologi informasi. Kejahatan sebenarnya tumbuh dan berkembang dalam masyarakat, tidak ada kejahatan tanpa masyarakat. Benar yang diucapankan Lacassagne bahwa masyarakat mempunyai penjahat sesuai dengan jasanya . Betapapun kita mengetahui banyak tentang berbagai faktor kejahatan yang ada dalam masyarakat, namun yang pasti adalah bahwa kejahatan merupakan salah satu bentuk prilaku manusia yang terus mengalami perkembangan sejajar dengan perkembangan masyarakat itu sendiri.
2. Aspek Pembuktian. Saat ini sistem pembuktian hukum di Indonesia (khususnya dalam pasal 184 KUHAP) belum mengenal istilah

bukti elektronik/digital *(digital evidence)* sebagai bukti yang sah menurut undang-undang. Masih banyak perdebatan khususnya antara akademisi dan praktisi mengenai hal ini. Untuk aspek perdata, pada dasarnya hakim dapat bahkan dituntun untuk melakukan *rechtsvinding* (penemuan hukum). Tapi untuk aspek pidana tidak demikian. Asas legalitas menetapkan bahwa tidak ada suatu perbuatan dapat dipidana jika tidak ada aturan hukum yang mengaturnya *(nullum delictum nulla poena sine previe lege poenali)* . Untuk itulah dibutuhkan adanya dalil yang cukup kuat sehingga perdebatan akademisi dan praktisi mengenai hal ini tidak perlu terjadi lagi.

3. Aspek Hak Atas Kekayaan Intelektual di *cyberspace*, termasuk didalamnya hak Cipta dan Hak Milik Industrial yang mencakup paten, merek, desain industri, rahasia dagang, sirkuit terpadu, dan lain-lain.
4. Standardisasi di bidang telematika. Penetapan standardisasi bidang telematika akan membantu masyarakat untuk mendapatkan keamanan dan kenyamanan dalam menggunakan teknologi informasi.
5. Aturan-aturan di bidang *E-Bussiness* termasuk didalamnya perlindungan konsumen dan pelaku bisnis.
6. Aturan-aturan di bidang *E-Government*. Apabila *E-Government* di Indonesia telah terintegrasi dengan baik, maka efeknya adalah pelayanan kepada masyarakat menjadi lebih baik.
7. Aturan tentang jaminan keamanan dan kerahasiaan Informasi dalam menggunakan teknologi informasi.
8. Yurisdiksi hukum, *cyberlaw* tidak akan berhasil jika aspek ini diabaikan. Karena pemetaan yang mengatur *cybespace* menyangkut juga hubungan antar kawasan, antar wilayah, dan antar negara. Sehingga penetapan yurisdiksi yang jelas mutlak diperlukan.

Upaya yang sedang dilakukan pemerintah saat ini dalam rangka menyusun payung hukum ruang *cyber* melalui usulan Rancangan Undang-undang Informasi dan Transaksi Elektronik (RUU ITE) memang patut dihargai. Rancangan Undang-undang Informasi dan Transaksi Elektronik memuat beberapa hal yakni;masalah yurisdiksi, perlindungan hak pribadi, azas perdagangan secara e-comerce, azas persaingan usaha usaha tidak sehat dan perlindungan konsumen, azas-azas hak atas kekayaan intelektual (HaKI) dan hukum Internasional serta azas *Cyber Crime* . Kendati Rancangan Undang-undang Informasi dan Transaksi Elektronik telah diusulkan dan di bahas oleh Pemerintah (melalui Depkominfo) dan DPR, namun hasil riil berupa disahkannya RUU tersebut menjadi Undang-undang belum tercapai. Menurut pemerintah, masih ada beberapa Daftar Inventaris Masalah (DIM) yang perlu dilakukan pembahasan lagi. Padahal Rancangan Undang-undang Informasi dan Transaksi Elektronik telah di susun sejak tahun 2003 yang lalu. Waktu yang terbilang cukup lama, jika dibanding dengan pesatnya perkembangan teknologi informasi.

Di tingkat Internasional Perserikatan Bangsa-Bangsa melalui komisi khususnya, *The United Nations*

Commissions on International Trade Law (UNCITRAL), telah mengeluarkan 2 *guidelines* yang terkait dengan transaksi elektronik, yaitu UNCITRAL *Model Law on Electronic Commerce with Guide to Enactment 1996* dan UNCITRAL *Model Law on Electronic Signature with Guide to Enactment 2001*. Sedangkan di Uni Eropa, dalam upaya mengantisipasi masalah-masalah pidana di *cyberspace*, Uni Eropa mengadakan *Convention on Cybercrime* yang didalamnya membahas jenis-jenis kejahatan apa saja yang dikategorikan sebagai *cyber crime*. Di bdiang perdagangan elektronik, Uni Eropa mengeluarkan *The General EU Electronic Commerce Directive, Electronic Signature Directive, dan Brussels Convention on Online Transactions.* Aturan-aturan serupa juga dikeluarkan lembaga-lembaga internasional seperti WTO, ASEAN, APEC dan OECD .

c. *Cyber Law* sudah menjadi kebutuhan

Pemberian regulasi atau aturan-aturan yang berkaitan dengan tindak kejahatan dunia maya saat ini sudah menjadi kebutuhan yang mendesak. Untuk negara-negara berkembang, Indonesia seharusnya bisa bercermin kepada negara-negara seperti India, Banglades, Srilanka Malaysia, dan Singapura yang telah memiliki perangkat hukum di bidang *cyberlaw* atau terhadap Armenia yang pada akhir tahun 2006 lalu telah meratifikasi *Convention on Cybercrime and the Additional Protocol to the Convention on Cybercrime concerning the criminalisation of acts of a racist and xenophobic nature committed through computer system.*

Survei yang dilakukan oleh Stein Schjolberg mantan hakim di Oslo terhadap 78 negara di dunia menempatkan Indonesia sama seperti Thailand, Kuwait, Uganda, dan Afrika Selatan yang belum memiliki perangkat hukum pendukung di bidang *cyberlaw*. Indonesia masih tertinggal jauh jika dibandingkan dengan Negara-negara Asia lainnya apalagi jika dibandingkan dengan negara-negara Uni Eropa yang telah memiliki perangkat hukum lengkap di bidang *cyberlaw*. Ketiadaan perangkat hukum di bidang *cyberlaw* di Indonesia mengakibatkan terjadinya kesenjangan hukum di masyarakat. Namun demikian Satjipto Rahardjo berpendapat bahwa apabila timbul kesenjangan antara hukum dengan perubahan dalam masyarakat, maka kesenjangan itu termasuk hal yang normal. Karena hukum sebetulnya sudah diperlengkapi dengan peralatan teknik untuk bisa mengatasi kesenjangan tersebut. Dalam keadaan demikian hukum tidak selalu harus di ubah secara tegas. Namun dapat dilakukan adaptasi hukum terhadap perubahan masyarakat .

Untuk membangun pijakan hukum yang kuat dalam mengatur masalah-masalah hukum di ruang *cyber* (internet) diperlukan komitmen kuat pemerintah dan DPR. Namun yang lebih penting lagi selain komitmen adalah bahwa aturan yang dibuat nantinya merupakan produk hukum yang *adaptable* terhadap berbagai perubahan khususnya di bidang teknologi informasi. Kunci dari keberhasilan pengaturan *cyberlaw* adalah riset yang komprehensif yang mampu melihat masalah cyberspace dari aspek konvergensi hukum dan teknologi. Kongkretnya pemerintah dapat membuat laboratorium dan pusat studi cyberlaw di perguruan-perguruan tinggi dan instansi-instansi pemerintah yang dianggap capable

di bidang tersebut. Laboratorium dan pusat studi *cyber law* kemudian bekerjasama dengan Badan Litbang Instansi atau Perguruan Tinggi membuat riset komprehensif tentang *cyber law* dan teknologi informasi. Riset ini tentu saja harus mengkombinasikan para ahli hukum dan ahli teknologi informasi. Hasil dari riset inilah yang kemudian dijadikan masukan dalam menyusun produk-produk cyberlaw yang berkualitas selain tentunya masukan dari pihak-pihak lain seperti swasta, masyarakat, dan komunitas cyber.

Selain hal tersebut hal paling penting lainnya adalah peningkatan kemampuan SDM aparatur hukum di bidang Teknologi Informasi mulai dari polisi, jaksa, hakim bahkan advokat khususnya yang menangani masalah-masalah ini. Penegakan hukum di bidang cyberlaw mustahil bisa terlaksana dengan baik tanpa didukung SDM aparatur yang berkualitas dan ahli di bidangnya. Teddy Sukardi, Presiden Federasi Teknologi Informasi Indonesia, mengungkapkan bahwa kehadiran RUU ITE seharusnya dipandang sebagai pembentukan platform yang bisa menyepahamkan persoalan yang dihadapi. "Selama ini tidak ada sebuah platform yang memberikan aturan main dalam masalah tersebut," akunya. Itu sebabnya ia sangat optimis dengan RUU ini, sekalipun ia mengatakan bahwa memang RUU ini bukan merupakan obat mujarab bagi semua penyakit yang ada. Teddy menunjukkan bahwa dari sebuah penelitian, Indonesia menempati urutan ke 14 dari 16 negara Asia yang disurvei. Indonesia bahkan kalah menarik sebagai tempat berinvestasi dan berbisnis dibanding Srilanka yang baru saja mengakhiri perang saudaranya.

Salah satu penyebabnya adalah Indonesia belum memiliki *cyberlaw* yang secara jelas mengatur ketentuan hukum yang berkaitan dengan pemanfaatan teknologi informasi internet, seperti negara-negara tetangga yang masih dalam satu kawasan Asia Tenggara seperti Malaysia dan Singapura. Dalam konteks perdagangan dan perekonomian global, pebisnis Indonesia, mau tidak mau dan suka tidak suka, menggunakan dan memanfaatkan *eCommerce*. Tentunya masalah ini menyangkut pula masalah transfer elektronik. Mitra dagang dan bisnis Indonesia tentu merasa tidak nyaman karena merasa tidak terlindungi akibat ketidak-adaan *cyberlaw*. Perlu diingat sejak pecahnya gelembung perekonomian nasional, sejumlah pebisnis merasakan kian sulitnya pembayaran lewat kartu kredit.

Jadi melihat bahwa dengan hadirnya RUU ITE bukan hanya bisa mengeliminir kesulitan semacam itu. Tapi juga bisa mendongkrak kepercayaan masyarakat bisnis internasional, sambil juga menumbuhkan peluang dalam memacu perekonomian nasional berlaga di pasar global.

Sebenarnya persoalan transaksi elektronik juga sudah menjadi persoalan dalam negeri. Sejak diperkenalkannya sistem pembayaran ini, boleh dibilang tidak ada satupun regulasi yang memberikan landasan hukum dan aturan main. Sejak awal tahun 90-an lalu, masyarakat kita sudah mulai mengenal transaksi secara elektronik. Ini dimulai dari dikenalkannya ATM dan *phone banking*. Menyusul, *Internet banking* (*i-banking*) dan *mobile banking* (*m-banking*). Sayangnya, transaksi semacam ini tidak diberikan aturan main yang jelas.

Padahal transaksi semacam ini terjadi karena adanya kepercayaan konsumen.

Kondisi semacam ini bisa merugikan konsumen perbankan, terutama jika masalah timbul. Kebanyakan konsumen perbankan justru berada pada posisi yang sangat lemah. Lembaga peradilan umumnya masih belum bisa menerima slip kartu ATM sebagai bukti materi yang sah menurut hukum pidana.. Itu sebabnya, dalam RUU ITE diatur bahwa informasi yang terdapat dalam slip yang diterima konsumen ATM bisa digunakan sebagai bukti yang sah dalam peradilan. Selain itu juga diatur bahwa pihak yang memberikan wewenang kepada *electronic agent*, seperti ATM dan *cellular phone* yang digunakan dalam transaksi elektronik, memiliki tanggung jawab penuh. Hal ini juga berlaku dalam Internet banking atau transaksi elektronik yang menggunakan internet sebagai mediumnya. Sebenarnya, Bank Indonesia sebagai bank sentral sudah merasakan adanya kebutuhan untuk menerbitkan regulasi yang mengatur transaksi elektronik.. Keinginan pihak BI ternyata juga memperoleh sambutan positif dari pemerintah dalam hal ini melalu Departemen Komunikasi dan Informatika.

d. Kepastian Hukum

Kepastian hukum merupakan salah satu asas yang dianut dalam RUU ITE. Asas lainnya yang terkadung dalam RUU itu adalah manfaat, sikap kehati-hatian, itikad baik, dan netralitas teknologi. Sebagaimana undang-undang layaknya, RUU ini mengatur hal-hal pokok dan aspek-aspek yang terkait dengan pemanfaatan Teknologi Informasi (TI), khususnya pengelolaan informasi elektronik dan transaksi elektronik. Karenanya, RUU ini mencakup berbagai aspek, mulai dari informasi elektronik, penyelenggaraan sistem elektronik, transaksi elektronik, tanda tangan elektronik, penyelenggara tanda tangan elektronik, akses ke sistem dan jaringan komputer, nama domain, dan perlindungan terhadap informasi dalam komputer serta sistem komputer. RUU juga mengatur aspek-aspek yang belum diatur dalam HaKI, seperti desain situs dan karya intelektual yang ada di dalamnya.

Perlindungan juga diberikan atas hak-hak pribadi (*privacy*). Sehingga penggunaan setiap informasi melalui media elektronik, yang menyangkut data tentang hak pribadi seseorang harus memperoleh persetujuan pemiliknya. Selain itu, diatur juga tentang penyelesaian sengketa. Ini mencakup gugatan perdata, tata cara melakukan gugatan itu, pengadilan yang memprosesnya, upaya hukum, arbitrase, dan penyelesaian di luar pengadilan (*Alternative Dispute Resolution – ADR*) yang bisa berupa negoisasi, mediasi dan konsiliasi. Yang baru dalam khasanah hukum di Indonesia adalah karena RUU ini menganut asas ekstra teritorial. Artinya, UU ini juga berlaku bagi setiap orang yang berada di luar Indonesia yang melakukan tindak pidana seperti yang diatur dalam RUU ini yang akibatnya merugikan untuk pihak-pihak yang berada di Indonesia.

e. Ketentuan pidana untuk pelaku *cyber crime*

Selain memuat ketentuan gugatan perdata, RUU ini juga mencakup ketentuan pidana. Ketentuan yang dimaksud meliputi kategori penyalahgunaan komputer, seperti larangan akses ke komputer dan sistem komputer tanpa hak dan berbagai aspek *cybercrime*. Permasalahan *cybercrime* yang diatur

mencakup *carding*, *spy*, *mailbomb*, *e-mail* palsu atau *junk e-mail*, penyebaran virus, *rerouting*, penyadapan informasi, perusakan dan penghancuran informasi, *hacking*, EPER serta *intruder*. Kalau bisa dicegah mulai dari adanya niatan buruk. Kita berharap bahwa bukan hanya kepastian hukum yang bisa ditumbuhkan dengan kehadiran RUU ini. Tetapi juga berharap tumbuhnya peluang bisnis baru maupun membuat kepercayaan pihak investor kembali bisa didongkrak lagi dengan adanya kepastian hukum tersebut.

Dibawah ini terdapat beberapa pasal yang menjelaskan ketentuan pidana bagi seseorang ataupun kelompok yang melakukan kejahatan siber atau *cyber crime* dan dituangkan dalam RUU ITE dalam **BAB XI** yang membahas mengenai **KETENTUAN PIDANA**

Pasal 42

(1) Setiap orang yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 26, dipidana dengan pidana penjara paling lama 3 (tiga) tahun dan pidana denda paling banyak Rp.1.000.000.000,-. (satu milyar rupiah).
(2) Setiap orang yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 27 ayat (1), dipidana dengan pidana penjara paling lama 4 (empat) tahun dan atau denda paling banyak Rp. 1.000.000.000.,- (satu milyar rupiah).

Pasal 43

Setiap orang yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 22 ayat (1), Pasal 25 dipidana dengan pidana penjara paling lama 6 (enam) bulan dan atau denda paling banyak Rp.100.000.000.,- (seratus juta rupiah).

Pasal 44

(1) Setiap orang yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 23 ayat (2), dipidana dengan pidana penjara paling lama 6 (enam) bulan dan atau denda paling banyak Rp.100.000.000,- (seratus juta rupiah).
(2) Tindak pidana sebagaimana dimaksud dalam ayat (1) hanya dapat dituntut atas pengaduan dari orang yang terkena tindak pidana.

Pasal 45

Setiap orang yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 27 ayat (3), Pasal 28, Pasal 29, Pasal 30 ayat (1), Pasal 30 ayat (2), Pasal 30 ayat (3), Pasal 30 ayat (4), Pasal 33 ayat (2), atau Pasal 34, dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan atau denda paling banyak Rp.2.000.000.000.,- (dua milyar rupiah).

Pasal 46

Setiap orang yang melanggar Pasal 27 ayat (2), dipidana dengan pidana penjara paling lama 20 (dua puluh) tahun dan atau denda paling banyak Rp.10.000.000.000,- (sepuluh milyar rupiah).

Pasal 47

Setiap orang yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 31 ayat (1), Pasal 31 ayat (2), Pasal 32, atau Pasal 33 ayat (1), pasal 35 dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan atau denda paling banyak Rp.2.000.000.000.,- (dua milyar rupiah).

Hanya saja, perjalanan dari RUU menjadi UU masih lumayan jauh. Diharapkan dalam waktu dekat ini sudah bisa dibahas oleh DPR, sehingga sekitar pertengahan tahun 2008 negara kita ini sudah memiliki UU ITE (Undang-undang Informasi dan Transaksi Elektronik).

III. KESIMPULAN

Pernah dengar kisah sebilah pisau? Pisau akan sangat bermanfaat bila ada di tangan seorang dokter bedah dibanding bila di tangan seorang bromocorah. Sekarang ini asas yang digunakan pemerintah dalam merumuskan RUU ini adalah 'netralitas teknologi'. Maksudnya adalah teknologi itu adalah *tools* dan itu akan tergantung niatan penggunanya, sejauh mana *tools* tersebut bisa digunakan secara maksimal. Karenanya pendekatan yang digunakan oleh pemerintah dalam meyusun RUU ini adalah 'Teknologi untuk Manusia' bukan kebalikannya 'Manusia untuk teknologi'. Pendekatan pertama adalah pendekatan untuk memberdayakan, mencerdaskan dan memak-murkan manusia melalui pemanfaatan teknologi. Sementara pendekatan 'Manusia untuk teknologi' adalah pendekatan yang merendahkan manusia dan menjadikannya sebagai robot.TI haruslah dipandang sebagai teknologi untuk manusia.

Namun pemanfaatan TI sebagai tools juga memiliki kisah pisau bermata dua. Di satu sisi, TI bermanfaat dalam meningkatkan efisiensi, produktivitas, dan kualitas hidup serta kemakmuran masyarakat. Di sisi lain, pemanfaatan TI dapat menimbulkan per-masalahan dengan implikasi yang beragam. Dengan kata lain, internet memungkinkan seseorang melakukan aktivitas yang dapat bersifat melawan hukum yang dapat dilakukan dengan melintasi batas negara, tanpa terhambat ruang dan waktu. Ada aspek kerawanan dalam pemanfaatan TI, dalam arti terbuka kemungkinan disalahgunakan oleh pihak-pihak tertentu untuk melakukan tindak kejahatan yang merugikan orang lain. Sejumlah tindak kejaahatan dapat dilakukan melalui komunikasi elektronik dengan internet sebagai medium. Ini mulai dari pornografi, perdagangan dan penyelundupan senjata ilegal, perjudian online, pembajakan piranti lunak, pencucian uang, kegiatan terorisme, pencurian dan manipulasi kartu kredit, pencurian rahasia dagang, transaksi narkotika, pencurian, perusakan, dan penghacuran informasi di dalam komputer atau sistem komputer. Secara langsung ini mempengaruhi lahirnya bentuk-bentuk perbuatan hukum baru, termasuk lahirnya RUU ITE.

Mengingat semakin banyaknya kejahatan ataupun pelanggaran yang dilakukan dalam jaringan internet, jadi jelas bahwa negara kita ini sudah sangat membutuhkan dengan adanya penegakan hukum yang mengatur kegiatan tersebut. *Cyber Law* sekarang ini sudah menjadi kebutuhan yang sangat mutlak dan sudah tidak dapat ditawar-tawar lagi. Jadi sebagai warga negara yang baik, kita harus mendukung secara penuh dengan adanya RUU ITE sehingga dapat segera diteruskan untuk menjadi Undang-undang, sehingga ada aturan atau regulasi yang jelas dan nyata dalam penegakan hukum didunia maya.

DAFTAR PUSTAKA

Abdul Wahid, SH, MA, Drs, Mohamad Labib, SH, Kejahatan Mayantara (*Cyber Crime*), PT. Refika Aditama, Bandung, 2005

Budi Raharjo, Memahami Teknologi Informasi, Elexmedia Komputindo, Jakarta, 2002

Bunafit Nugroho, Referensi Berinternet Bagi Pemula, Elex Media Komputindo, Jakarta, 2007

Dikdik M. Arif Mansur, SH, MH, Drs, Alisatris Gultom, SH, MH, *CyberLaw* (Aspek Hukum Teknologi Informasi), PT. Refika Aditama, Bandung, 2005

Merry Magdalena, Mas Wigrantoro Roes Setiyadi, *CyberLaw* Tidak Perlu Takut, Andi *Offset* , Yogyakarta, 2007