

ISSN 1979-5955

JURNAL HUKUM

LEGALITAS



s negeri gorontalo universitas negeri gorontalo universitas negeri gorontalo universitas negeri gorontalo universitas negeri gorontalo

Vol. 2 NO. 2. JUNI 2009



ISSN 1969-5262

Vol 2 No. 2 Bulan Juni 2009

Pelindung :

Ketua Program Studi Hukum Universitas Negeri Gorontalo

Ketua Penyunting :

Fence M Wantu, SH, MH

Wakil Ketua Penyunting

Weny Almoravid Dungga, SH, MH

Penyunting Ahli/Dewan Penyunting :

Prof. Drs. Wely Pangayouw, M.Si, Ph.D

Fenty Puluhulawa SH, MH

Johan Yasin SH, MH

Moh. Rusdyanto Puluhulawa SH, MH

Penyunting Pelaksana:

Mutia Herawaty Talib, SH, M.H

Nirwan Yunus SH, MH

Dian Ekawaty Ismail SH, MH



Desain Cover
Amirudin Y. Dako, ST

Manajemen Pengembangan/Keuangan
Halim K Malik, SPd

Penerbit :
Program Studi Ilmu Hukum Universitas Negeri Gorontalo

Sekretariat :
Program Studi Ilmu Hukum UNG
Jetis Pasiraman JT II / 587 Yogyakarta, Telp. (0274) 560413
Hunting : 085240110443 (Halim), 08124484858 (Amir), 081340315416

Email :
fence.wantu@yahoo.co.id, dan amir_dako@yahoo.com serta
maseko32@yahoo.co.id

DAFTAR ISI

Kontribusi Hukum Dalam Perkembangan Pembangunan
Ekonomi Indonesia Oleh: **Tineke Wolok**

Restrukturisasi Birokrasi Pemerintah Daerah Dalam
Mewujudkan *Good Local Governance*. Oleh: **Udin Hamim**

Membangun Otonomi Daerah Melalui Peningkatan Kinerja
Aparatur Pemerintah Provinsi Gorontalo Oleh: **Sastro M. Wantu**

Eksistensi Kode Etik Profesi Bagi Anggota Legislatif
Oleh: **Rustam Akili**

Nilai Etika Yang Harus Diwujudkan Oleh Setiap Orang
Yang Memilih Profesi Hukum Oleh: **Fence M. Wantu**

Penyelenggaraan Pesta Demokrasi Dan Komitmen
Mewujudkan Keadilan Gender Oleh: **Nurmin K. Martam**

Pemilu Sebagai Instrumen Demokrasi Menuju Tata Kelola
Pemerintahan Yang Baik (*Good Governance*)
Oleh : **Zainuddin**.....

Pengelolaan Sumber Daya Alam Danau Limboto Di Era
Otonomi Daerah Dalam Prespektif Sosiologi Hukum
Oleh: **Faried Th. Musa**

Tinjauan Hukum Pada Penerapan Teknologi Internet
Oleh: **Amirudin Y. Dako**

Perkembangan Teknologi Informasi Dan Komunikasi
(Telekomunikasi) Dilihat Dari Kajian Aspek Hukum
Oleh: **Iskandar Zulkarnaen Nasibu**

Tinjauan Hukum Pada Penerapan Teknologi Internet

Oleh: Amirudin Y. Dako

Abstract

The existing computer technology is a main requirement which cannot be overruled again in every human activity. Usage of computer technology is not forever brings positive impact, but earns is brings negativity impact. In consequence to avoid negativity impact, hence required law aspect. That's law aspect is divide into public law aspect and private law aspect.

Kata Kunci: Hukum, Penerapan, Teknologi, Komputer, Internet.

Pendahuluan

Internet (*interconnected network*) merupakan jaringan (*network*) komputer yang terdiri dari ribuan jaringan komputer independen yang dihubungkan satu dengan yang lainnya. Jaringan komputer ini dapat terdiri dari lembaga pendidikan, pemerintahan, militer, organisasi, bisnis dan organisasi lainnya. Internet atau nama pendeknya .net merupakan jaringan komputer terbesar di dunia.

Perkembangan sains dan teknologi membawa dampak yang signifikan terhadap sistem yang berlaku di Indonesia, misalnya ekonomi, politik, budaya dan lain

sebagainya. Teknologi telah membawa kontribusi terhadap sistem-sistem ekonomi, budaya, politik yang selama ini berlaku. Era ekonomi bebas yang berbasis informasi, menjadikan teknologi komputer memiliki peranan yang sangat menentukan, seperti praktik bisnis yang sangat tergantung pada informasi teknologi (Suparman, 2002).

Internet sudah menjadi bagian dari kehidupan yang dapat menghubungkan setiap apapun juga kegiatan manusia. Internet merupakan bagian dari mekanisme telekomunikasi yang bersifat global yang fungsinya menjadi jembatan

bebas hambatan informasi. Perkembangan dunia maya tersebut ternyata membuat dan menciptakan berbagai kemudahan dalam hal menjalankan transaksi, dunia pendidikan, perdagangan, perbankan, serta menciptakan jutaan kesempatan untuk menggali keuntungan ekonomis.

Jaringan komputer/internet pada awalnya digunakan hanya untuk saling tukar menukar informasi, fungsinya kemudian berubah meningkat dari sekedar media komunikasi menjadi sarana untuk melakukan kegiatan komersial seperti informasi, penjualan dan pembelian produk. Keberadaannya menjadi sebuah keharusan penting sebagaimana layaknya kepemilikan intelektual atau *intellectual property* (www.kompas.com).

Kemajuan ilmu pengetahuan dan teknologi sangat berperan dalam pertumbuhan industri. Pengembangan dasar teknologi di negara berkembang termasuk Indonesia tergantung pada berbagai kapasitas teknologi dan kemampuan memperoleh teknologi dari negara maju untuk melengkapi usaha-usaha dan riset nasional.

Perkembangan teknologi komputer dan telekomunikasi sudah sedemikian cepat sehingga merasuk dalam kehidupan manusia sehari-

hari. Tanpa disadari produk teknologi sudah menjadi kebutuhan manusia di Indonesia. Penggunaan Internet sudah bukan menjadi hal yang aneh dan baru. Internet yang tadinya hanya bisa diakses melalui komputer atau laptop, kini dengan kemajuan teknologi yang ada, bisa dihadirkan dalam genggam tangan melalui perangkat telekomunikasi yang sering disebut dengan *handheld devices* seperti HP, PDA dan sejenisnya.

Melalui media internet, saat ini anda dapat melakukan transaksi keuangan, pembayaran rekening, pemesanan dan pembelian barang, serta transaksi finansial lainnya dapat dilakukan tanpa batas waktu dan batas geografis, yang dimungkinkan dengan layanan e-commerce yang berbasis internet. Contohnya adalah aplikasi perbankan BCA on line/ www.klikbca.com, amazon.com, dan aplikasi e-commerce sejenisnya.

Aplikasi jejaring sosial seperti *facebook*, *YM*, *friendster*, *myspace*, *youtube* dan aplikasi sejenisnya juga telah merambah seluruh pelosok negeri ini, mulai dari kalangan ABG (anak baru gede) dan sampai kalangan profesional. Bahkan aplikasi berbasis internet juga telah dipergunakan dalam dunia edukasi seperti hadirnya *e-learning*, dunia

entertainment (indowebster.com, gudanglagu.com), berita (kompas.com, detik.com) bahkan sampai ke aplikasi yang khusus untuk kalangan orang dewasa (17tahun.com dan sejenisnya).

Di satu sisi penerapan teknologi internet telah mempermudah hidup manusia, namun di sisi lain juga menimbulkan permasalahan. Ada banyak aspek yang nampaknya membutuhkan telaah hukum untuk penyelesaiannya.

Masalah Hak Dan Kekayaan Intelektual (HaKI)

Masalah hak atas kekayaan intelektual dilatarbelakangi oleh kemampuan teknologi digital dalam mempermudah duplikasi materi yang dikemas dalam bentuk digital (*digitalized products*). Contoh materi yang dikemas dalam bentuk digital adalah produk musik, film (video), karya tulis (buku), dan perangkat lunak (*software*). Teknologi digital dapat digunakan untuk mengandakan atau membuat salinan dari materi tersebut dengan kualitas yang sama dengan aslinya tanpa merusak atau mengurangi sumber aslinya.

Pembajakan kaset, CD lagu (baik dalam format cd audio/CDA ataupun dalam format MP3 (www.mp3.com)) dimana dalam satu

CD dapat diisi dengan ratusan lagu), VCD, e-book, dan perangkat lunak marak dilakukan di seluruh dunia. Negara-negara di Asia termasuk Indonesia di dalamnya memiliki jumlah pembajak yang relatif besar dan menjadi sorotan di seluruh dunia. Meski demikian, teknologi untuk memproteksi seperti *watermarking*, *dongle*, *enkripsi*, dan sebagainya dicoba dikembangkan. Akan tetapi nampaknya pihak yang melakukan proteksi kalah langkah dengan pihak pembuka (*code breakers*).

Bidang HaKI lainnya adalah adanya kelompok yang tidak setuju dengan proteksi yang berlebihan sehingga mencoba mengambil pendekatan lain seperti dengan menggunakan jalan *public domain*, *copyleft*, *GNU Public License* (GPL), *open source* dan sejenisnya. Cara ini tidak memecahkan masalah yang ada, akan tetapi mencoba melihat permasalahan dari sudut pandang yang lain. (Jika sudah *public domain*, maka tidak ada masalah pencurian.)

Kasus yang cukup ramai disoroti adalah kasus perusahaan Napster (www.napster.com). Perusahaan ini memberikan layanan untuk mempermudah pengguna Internet dalam tukar menukar file MP3 (lagu). Dalam hal ini, Napster

sendiri tidak menyediakan koleksi lagu dalam format MP3 akan tetapi hanya memfasilitasi pertukaran MP3.

Situs sejenis juga banyak ditemukan di dalam negeri. Dengan memanfaatkan mesin pencari yang tersedia di internet beserta kata kunci yang sesuai, maka akan diberikan daftar situs penyedia file lagu dalam format yang beragam, yang selanjutnya dapat di *download* secara gratis.

Hal yang sama juga berlaku untuk media video. Hal ini dimungkinkan oleh teknologi yang berkembang saat ini memungkinkan *bandwidth* (lebar pita) Internet yang semakin besar sehingga pertukaran media video yang berukuran besar sudah sangat mudah untuk dilakukan. Pengguna Internet yang hanya menggunakan fasilitas dial-up melalui telepon biasa dengan kecepatan maksimum 56Kbps dapat dengan mudah mentransfer video dalam format MPEG (yang banyak digunakan di VCD) dengan waktu yang relatif singkat. Teknologi komputer dan telekomunikasi memang telah berkembang dengan sangat pesat belakangan ini.

Teknologi telekomunikasi dan komputer banyak menggunakan hak cipta/paten. Sebagai contoh adalah penggunaan algoritma enkripsi RSA

yang umum digunakan untuk mengamankan transaksi atau komunikasi di Internet. Algoritma RSA ini dipatenkan oleh penemunya. Bayangkan bahwa "kehidupan elektronik" manusia bergantung kepada paten seseorang atau sekelompok orang. Untungnya paten tersebut sudah habis dan sekarang sudah menjadi public domain. Hal yang serupa dapat terjadi kembali. (Kasus yang sama juga terjadi dengan algoritma kompresi yang digunakan dalam format GIF yang umum digunakan sebagai format gambar di Internet. Pemilik patent GIF, Unisys, pernah diisytukan meminta bayaran dari setiap gambar yang menggunakan format tersebut.)

Domain Internet

Nama domain (misalnya .com) yang digunakan sebagai alamat dan identitas di Internet juga memiliki permasalahan sendiri. Penamaan domain berkaitan erat dengan nama perusahaan dan/atau produk (servis) yang dimilikinya. Seringkali produk / service ini didaftarkan sebagai *trademark* atau *servicemark*. Bagaimana aturan penggunaan trademark milik orang lain dalam nama domain?

Masalah nama domain ini cukup pelik dikarenakan di dunia ini

ada beberapa pengelola nama domain yang independen. Ada lebih dari dua ratus pengelola domain yang berbasis teritory (yang sering disebut sebagai *Country Code Top Level Domain* atau ccTLD). Sebagai contoh diambil pengelola domain untuk Indonesia (ID). Bolehkah seseorang mendaftarkan nama domain yang sebetulnya ditrademarkkan di negara lain? Darimana pengelola domain tahu bahwa nama tersebut merupakan *trademark* yang terdaftar di negara lain?

Kasus pertikaian sudah terjadi seperti contohnya adalah kasus *mustika-ratu.com* yang diduga didaftarkan oleh kompetitor dari perusahaan Mustika Ratu. Salah satu paradigma pemrograman berbasis web yang marak beberapa tahun belakangan ini adalah *blogging*. Siapa yang tidak mengenal blog, suatu istilah keren bagi sebuah web log atau jurnal online yang bisa disimpan oleh organisasi atau perseorangan. Semakin banyaknya para *bloggers* dan semakin banyaknya aplikasi *web blog* membuat *blog* menjadi standar *defacto content web* di dunia *internet* (www.mti.ugm.ac.id/~ridi).

Bagaimana jika ada yang mendaftarkan dengan nama orang yang terkenal (seperti kasus

JuliaRoberts.com dan *John Tesh.com*)? Apa landasan hukum yang digunakan? Di Amerika Serikat ada "*Anti-Cybersquatting Consumer Protection Act*" yang ditandatangani oleh presiden Clinton yang mengatakan:

Any person who registers a domain name that consists of the name of another living person, or a name substantially and confusingly similar thereto, without that person's consent, with the specific intent to profit from such name by selling the domain name for financial gain to that person or any third party, shall be liable in a civil action by such person.

Perijinan Dari Aspek Perlindungan Konsumen Dan Anti Monopoli

Di Indonesia, untuk layanan Internet membutuhkan ijin khusus. *Internet Service Provider* (ISP) atau Penyedia Jasa Internet (PJI) harus mendapatkan lisensi dari Dirjen Postel, Departemen Perhubungan. Di negara lain, seperti di Canada, ISP tidak membutuhkan ijin khusus. Telekomunikasi di Indonesia masih dimonopoli. Pelanggaran monopoli ini melalui teknologi sudah terjadi melalui penyediaan jasa *Voice over internet protocol* (VoIP, protokol

yang digunakan di Internet untuk berkomunikasi) oleh beberapa orang dan perusahaan. Bahkan, sudah ada kasus penangkapan orang yang menyediakan jasa VoIP. (Dalam pemberitaan surat kabar bahkan disebutkan bahwa orang yang memberikan layanan VoIP tersebut seolah-olah mencuri pulsa PT Telkom.) Layanan VoIP pada prinsipnya adalah mengubah suara (*voice*) menjadi data dan mengirimkan data ini melalui saluran Internet. Penyedia layanan VoIP berargumentasi bahwa yang dia salurkan adalah data bukan *voice* oleh sebab itu dia tidak melanggar monopoli Telkom dan Indosat. Pihak pemerintah merasa bahwa yang dikirimkan asalnya berupa *voice* sehingga sebetulnya merupakan layanan suara (*voice*) juga. Ini merupakan contoh bahwa teknologi mengubah segalanya. Saat ini bukan hanya *voice* saja yang dapat dikirimkan dengan *real-time* akan tetapi juga gambar bergerak melalui fasilitas kamera yang secara *built in* telah terpasang dan memungkinkan komunikasi *video conference*. Teknologi ini sering dikenal sebagai Multimedia over IP.

VoIP hanya salah satu teknologi saja. Masih ada teknologi lain seperti *Voice over ATM* dimana protokol ATM digunakan sebagai

pengganti protokol IP. ATM di sini berbeda dengan terminal ATM yang digunakan untuk mengambil uang di bank, ATM (*Asynchronous Transfer Mode*) adalah protokol yang umum digunakan di *backbone* computer networks. Selain IP dan ATM, masih ada protokol lain seperti IPX (yang banyak digunakan oleh Novell) dan Appletalk (yang banyak digunakan oleh *Apple*). Persoalannya ialah apakah sudah ada hukum yang mengatur VoATM, VoIPX, VoAppletalk. Hukum seharusnya *technology neutral* sehingga adanya perubahan teknologi tidak harus mengubah hukum yang ada.

Seorang pengguna dapat memberikan layanan *broadcasting* melalui Internet (Radio Internet dan TV Internet), apakah perlu meminta ijin dari pemerintah? Saat ini dengan teknologi yang ada, setiap orang dapat menjadi *broadcaster*. Lagi-lagi ini masalah perijinan. Undang-undang anti monopoli diharapkan dapat mengurangi masalah yang timbul. Akan tetapi masih tetap menjadi pertanyaan dalam implementasinya. Monopoli merupakan penghambat kompetisi dan inovasi yang menguntungkan masyarakat (komunitas).

Privacy

Di Indonesia masalah *privacy* masih belum menjadi masalah yang besar. Di luar negeri, masalah *privacy* ini menjadi perhatian utama. Seringkali kita mengisi formulir yang menanyakan data-data pribadi (nama, alamat, tempat tanggal lahir, agama, status, dan sebagainya) tanpa informasi yang jelas mengenai penggunaan data-data ini. Bagaimana jika data-data ini diperjual belikan? Salah satu contoh adalah ketika kita pertama kali membuka *account* baru di Facebook. Saat pertama kita mendaftar kita diwajibkan untuk mengisi formulir identitas pribadi, alamat, pekerjaan dan lain sebagainya. Meski memang telah ditegaskan pada *terms of services*, namun bagaimana jika nanti ada penyalahgunaan atas data pribadi kita?

Keamanan Jaringan Internet

Masalah keamanan merupakan salah satu aspek penting dari sebuah aplikasi maupun sistem informasi yang berbasis internet. Informasi saat ini sudah menjadi sebuah komoditi yang sangat penting. Bahkan ada yang mengatakan bahwa kita sudah berada di sebuah "*information-based society*". Kemampuan untuk mengakses dan menyediakan informasi secara cepat

dan akurat menjadi sangat esensial bagi sebuah organisasi, baik yang berupa organisasi komersial (perusahaan), perguruan tinggi, lembaga pemerintahan, maupun individual (pribadi). Hal ini dimungkinkan dengan perkembangan pesat di bidang teknologi komputer dan telekomunikasi.

Pentingnya nilai sebuah informasi menyebabkan seringkali informasi diinginkan hanya boleh diakses oleh orang-orang tertentu. Jatuhnya informasi ke tangan pihak lain (misalnya pihak lawan bisnis) dapat menimbulkan kerugian bagi pemilik informasi. Sebagai contoh, banyak informasi dalam sebuah perusahaan yang hanya diperbolehkan diketahui oleh orang-orang tertentu di dalam perusahaan tersebut, seperti misalnya informasi tentang produk yang sedang dalam *development*, algoritma-algoritma dan teknik-teknik yang digunakan untuk menghasilkan produk tersebut. Untuk itu keamanan dari sistem informasi yang digunakan harus terjamin dalam batas yang dapat diterima.

Jaringan komputer, seperti LAN dan Internet, memungkinkan untuk menyediakan informasi secara cepat. Ini salah satu alasan perusahaan atau organisasi mulai berbondong-bondong membuat LAN

untuk sistem informasinya dan menghubungkan LAN tersebut ke Internet. Terhubungnya LAN atau komputer ke Internet membuka potensi adanya lubang keamanan (*security hole*). Hal ini sesuai dengan pendapat bahwa kemudahan (kenyamanan) mengakses informasi berbanding terbalik dengan tingkat keamanan sistem informasi itu sendiri. Semakin tinggi tingkat keamanan, semakin sulit (tidak nyaman) untuk mengakses informasi.

Berikut ini adalah beberapa kejadian yang berhubungan dengan jebolnya keamanan pada aplikasi berbasis internet. Data-data yang ditampilkan umumnya bersifat konservatif mengingat banyak perusahaan yang tidak ingin diketahui telah mengalami "*security breach*" dikarenakan informasi ini dapat menyebabkan "*negative publicity*". Perusahaan-perusahaan tersebut memilih untuk diam dan mencoba menangani sendiri masalah keamanannya tanpa publikasi.

Tahun 1996, *U.S. Federal Computer Incident Response Capability* (FedCIRC) melaporkan bahwa lebih dari 2500 "insiden" di sistem komputer atau jaringan komputer yang disebabkan oleh gagalnya sistem keamanan atau adanya usaha untuk membobol

sistem keamanan, dan pada tahun yang sama *FBI National Computer Crimes Squad*, Washington D.C., memperkirakan kejahatan komputer yang terdeteksi kurang dari 15%, dan hanya 10% dari angka itu yang dilaporkan (Icove, 1996).

Selanjutnya penelitian di tahun 1997 yang dilakukan oleh perusahaan *Deloitte Touch Tohmatsu* menunjukkan bahwa dari 300 perusahaan di Australia, 37% (dua diantara lima) pernah mengalami masalah keamanan sistem komputernya, kemudian Penelitian di tahun 1996 oleh *American Bar Association* menunjukkan bahwa dari 1000 perusahaan, 48% telah mengalami "*computer fraud*" dalam kurun lima tahun terakhir (Jhonson, 1998).

Ada beberapa contoh akibat dari jebolnya sistem keamanan yakni, sebagai berikut: *Pertama*, pada tahun 1988, Keamanan sistem *mail sendmail* dieksploitasi oleh Robert Tapan Morris sehingga melumpuhkan sistem Internet. Kegiatan ini dapat diklasifikasikan sebagai "*denial of service attack*". Diperkirakan biaya yang digunakan untuk memperbaiki dan hal-hal lain yang hilang adalah sekitar \$100 juta. Di tahun 1990 Morris dihukum (*convicted*) dan hanya didenda \$10.000. *Kedua*, pada tanggal 10

Maret 1997, Seorang *hacker* dari Massachusetts berhasil mematikan sistem telekomunikasi di sebuah bandara lokal (Worcester, Massachusetts) sehingga mematikan komunikasi di *control tower* dan menghalau pesawat yang hendak mendarat. Dia juga mengacaukan sistem telepon di Rutland, Massachusetts (www.news.com)

Menurut David Icove (1997), keamanan pada aplikasi internet diklasifikasikan menjadi empat, yaitu: *Pertama*, Keamanan yang bersifat fisik (*physical security*): termasuk akses orang ke gedung, peralatan, dan media yang digunakan. *Kedua*, lubang keamanan dari implementasi protokol TCP/IP yang dikenal dengan istilah *Syn Flood Attack*, dimana sistem (*host*) yang dituju dibanjiri oleh permintaan sehingga dia menjadi terlalu sibuk dan bahkan dapat berakibat macetnya sistem (*hang*). *Ketiga*, Keamanan yang berhubungan dengan orang (personel); termasuk identifikasi, dan profil resiko dari orang yang mempunyai akses (pekerja). Seringkali kelemahan keamanan sistem informasi bergantung kepada manusia (pemakai dan pengelola). Ada sebuah teknik yang dikenal dengan istilah "*social engineering*" yang sering digunakan oleh kriminal

untuk berpura-pura sebagai orang yang berhak mengakses informasi. Misalnya kriminal ini berpura-pura sebagai pemakai yang lupa passwordnya dan minta agar diganti menjadi kata lain. *Keeempat*, Keamanan dari data dan media serta teknik komunikasi (*communications*). Seorang kriminal dapat memasang virus atau trojan horse sehingga dapat mengumpulkan informasi (seperti *password*) yang semestinya tidak berhak diakses. *Kelima*, Keamanan dalam operasi: termasuk prosedur yang digunakan untuk mengatur dan mengelola sistem keamanan, dan juga termasuk prosedur setelah serangan (*post attack recovery*).

Keamanan di Internet sebetulnya sudah pada tahap yang dapat diterima. Hanya hal ini perlu mendapat pengesahan dari pemerintah sehingga pelaku bisnis mendapatkan kepastian hukum. Identitas seseorang dapat diberikan dengan menggunakan *digital signature* yang dikelola oleh *Certification Authority* (CA). Masalahnya tanda tangan digital ini belum dapat dianggap sebagai bukti yang sah meskipun sebetulnya tingkat keamanannya cukup tinggi. Di beberapa negara, hal ini sudah diakomodasi dalam bentuk "*Digital Signature Act*".

Kejahatan yang ditimbulkan dengan teknologi komputer dan telekomunikasi perlu diantisipasi. Istilah *hacker*, *cracker*, *cybercrime* mulai sering didengar. Kejahatan *cyber* umumnya dapat ditelusuri (*trace*) dengan bantuan catatan (*logfile*) yang ada di *server internet service provider/ISP* yang digunakan oleh *cracker*. Akan tetapi seringkali ISP tidak melakukan pencatatan (*logging*) atau hanya menyimpan *log* dalam kurun waktu yang singkat (dikarenakan besarnya jumlah data yang harus dicatat). *Logfile* ini sebetulnya dapat menjadi bukti adanya akses *cracker* tersebut. Namun *logfile* ini (jika ada) belum tentu dapat menjadi bukti yang sah di pengadilan. Penyidikan kejahatan *cyber* ini juga membutuhkan keahlian khusus. Pihak penegak hukum harus lebih cepat tanggap dalam menguasai teknologi baru ini.

Kebijakan Penanganan Kejahatan Komputer

Dunia teknologi informasi yang berkembang sedemikian cepat sungguh diluar dugaan, tetapi perkembangan ini diikuti pula dengan kejahatan teknologi informasi. Dan karena kejahatan ini pula menyebabkan banyak orang harus membayar mahal untuk

mencegahnya dan menaati hukum yang ada.

Internet menghilangkan batas tempat dan waktu, dua asas yang cukup esensial di bidang hukum. Terhubungnya sebuah sistem informasi dengan Internet membuka peluang adanya kejahatan melalui jaringan komputer. Hal ini menimbulkan tantangan bagi penegak hukum. Hukum dari sebagian besar negara di dunia belum menjangkau daerah *cyberspace*. Saat ini hampir semua negara di dunia berlomba-lomba untuk menyiapkan landasan hukum bagi Internet.

Tentunya banyak hal yang dapat dibahas, akan tetapi dalam tulisan ini hanya dibahas beberapa masalah hukum pada penerapan teknologi yang berhubungan dengan internet.

Berikut ini beberapa kebijakan yang dapat digunakan untuk mencegah kejahatan yakni sebagai berikut: *Pertama*, Memperkuat peraturan perundang-undangan. Dengan kehadiran peraturan perundang-undangan, maka setiap orang tidak seenaknya lagi melanggar hukum, karena bisa-bisa digiring sampai ke kantor polisi. Organisasi industri seperti *Software Publishers Association (SPA)* segera dibentuk setelah maraknya

pembajakan perangkat lunak dalam skala besar maupun kecil. (Pembajakan perangkat lunak komersial sekarang merupakan tindak pidana berat, bisa dipenjarakan maksimal 5 tahun dan didenda hingga 250.000 dollar bagi siapa saja yang terbukti memakai perangkat bajakan). Dengan memperkuat hukum ini minimal akan mengurangi resiko kejahatan teknologi informasi. Kehadiran peraturan perundang-undangan seperti Undang-Undang Informasi Dan Teknologi kiranya masih kurang efektif untuk mengakomodasi tuntutan hukum yang dapat mengatur kemajuan jaringan internet. *Kedua*, kebijakan CERT : Computer Emergency response Team. Hal ini dapat dilihat seperti pada tahun 1988, setelah internet tersebar luas, Departemen pertahanan AS membentuk CERT. Meskipun lembaga ini tidak mempunyai wewenang untuk menahan atau mengadili, CERT menyediakan informasi internasional dan layanan seputar keamanan bagi para pengguna internet. CERT hadir sebagai pendamping pihak yang diserang, membantu mengatasi gangguan, dan mengevaluasi sistem yang telah mengalami serangan untuk melindunginya dari gangguan dimasa yang akan datang. *Ketiga*, kebijakan

Alat pendeteksi kecurangan perangkat lunak deteksi berbasis aturan. Dalam teknik ini pengguna, semisal pedagang membuat file negatif yang memuat kriteria yang harus dipenuhi oleh setiap transaksi. Kriteria ini meliputi nomor kartu kredit yang dicuri dan juga batas harganya, kecocokan alamat rekening pemegang kartu dan alamat pengiriman, dan peringatan jika satu item dipesan dalam jumlah besar. *Keempat*, kebijakan Perangkat Lunak Manajemen Internet Pegawai (EIM). Hal ini seperti program yang dibuat oleh Websense, SurfControl, dan Smartfilter yang digunakan untuk memantau berapa banyak waktu yang dihabiskan pemakai komputer untuk berinteraksi dengan internet dan untuk memblokir akses ke situs judi atau porno. Selanjutnya beberapa perusahaan menggunakan perangkat lunak penyaring/filter khusus untuk memblokir akses ke pornografi, download music *bootleg*, dan situs Internet lain yang tidak dikehendaki dengan menggunakan berbagai jenis pengawas elektronik yang menyertakan teknologi pemantau audio dan visual, membaca email dan blog, dan merekam *keystroke*. *Kelima*, kesadaran masyarakat. Aspek yang ditawarkan di atas kiranya masih kurang lengkap sekiranya kesadaran

masyarakat terhadap pemanfaatan teknologi internet secara positif sama sekali tidak ada. Kesadaran masyarakat terhadap berbagai peraturan perundang-undangan yang dilahirkan oleh pemerintah juga penting dalam rangka mengantisipasi kejahatan dan perbuatan yang bertentangan dengan hukum di bidang jaringan internet.

Dengan berbagai kebijakan pencegahan di atas memang akan mengurangi kejahatan di dunia maya, namun semuanya itu kembali kepada kita sebagai pengguna teknologi informasi khususnya internet, selama kita semua masih memakai cara-cara dan etika yang benar, perkembangan IT akan terus bergerak ke arah yang positif. Dan sampai sekarang metode pencegahan

masih terus dikembangkan dengan beraneka ragam dan akan terus berkembang sesuai dengan tingkat perkembangan teknologi informasi.

PENUTUP

Tulisan singkat ini tentunya belum mencakup seluruh permasalahan hukum yang timbul dengan adanya kemajuan teknologi. Meskipun demikian tulisan ini diharapkan minimal dapat memberikan wawasan permasalahan yang ada.

Untuk mengatasi dan mengantisipasi masalah yang akan terjadi maka sebaiknya ada dialog yang berkelanjutan antara pihak yang mengerti teknologi dan pihak yang mengerti hukum serta penegak hukum. Dengan demikian, hukum tidak menjadi bumerang bagi komunitas itu sendiri.

Daftar Pustaka

A. Buku dan Jurnal

- Ade Maman Suparman, 2002, *Aspek Hukum Dalam Ekonomi Global*
- David J. Icové, 1997. "Collaring the cybercrook: an investigator's view," *IEEE Spectrum*.
- Simson Garfinkel, and Gene Spafford, 1996. 2nd edition. "Practical UNIX & Internet Security," O'Reilly & Associates, Inc.
- William Stallings, 1995. "Network and Internetwork Security," Prentice Hall

B. Internet.

- Anna Johnson, 1998. "Companies Losing Millions over Rising Computer Crime," *Shake Security Journal*, March, http://www.shake.net/crime_march98.htm

www.mp3.com, diakses tanggal 9 mei 2005. www.napster.com, diakses tanggal 9 Juli 2005.

Kompas, *Konflik Kepentingan Di Dunia Cyber*, <http://>

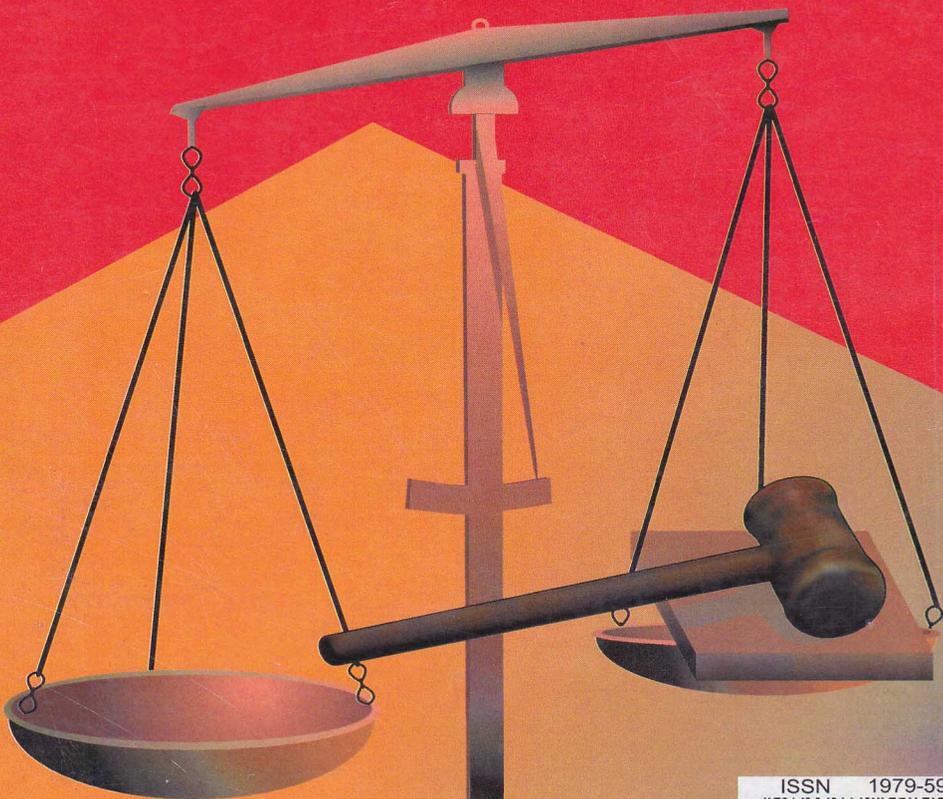
R.M. Roy Suryo. *Pentingnya Hukum Di Jagad Maya Internet*, <http://kontan-online.com>, diakses tanggal 9 Juni 2007.

Indra Safitri. *Commerce Dalam Prespektif Hukum*, <http://>. Bussines.com, diakses pada bulan Pebruari 2008.

www.beritanet.com/Technology/Berita-IT/kejahatan-teknologi-informasi.html, diakses tanggal 8 mei 2008.

www.mti.ugm.ac.id/~ridi, ASP.NET Blog Engine – *Sebuah Jurnal Kehidupan di Era Digital*.pdf, Kompas.com, diakses tanggal 2 Pebruari 2007. Diakses tanggal 2 Januari 2009.

www.news.com/News/Item/Textonly/0,25,20278,00.html?pfv, diakses tanggal 4 Pebruari 2009. www.news.com/News/Item/0,4,20226,00.html, diakses tanggal 4 Maret 2009 cv.



ISSN 1979-5955



9 771979 595521

LEGALITAS