

Pernak Pernik Peraturan dan Pengaturan Cyberspace di Indonesia

*Budi Rahardjo*¹
2003

Daftar Isi

Latar Belakang.....	1
Apakah cyberspace dapat diatur?.....	2
Kejahatan dunia maya (cybercrime).....	2
Penanganan cybercrime: aspek pembuktian.....	2
HaKI / Intellectual Property Rights.....	3
Anti-IPR.....	3
Free Software Movement: Gerakan Software Bebas.....	4
HaKI di Indonesia.....	4
Digital Millennium Copyright Act (DMCA).....	4
Paten Software: perlukah? Tidak!.....	6
Privacy & confidentiality.....	6
Policy & procedure di perusahaan.....	7
Privacy & confidentiality di luar negeri.....	7
Privacy policy di situs web.....	8
Beberapa Peraturan Untuk Cyberspace.....	8
RUU IT.....	8
Pengaturan VoIP.....	8
Penutup.....	9
Daftar Bacaan.....	9

Tulisan ini bermula dari kumpulan tulisan yang membahas atau memberikan penjelasan lebih detail dari Rancangan Undang-Undang Pemanfaatan Teknologi Informasi (RUU PTI). Kebetulan saya menjadi salah satu orang yang terlibat dalam pembuatan atau pengembangan RUU tersebut, yang dimotori oleh Direktorat Jendral Pos dan Telekomunikasi, Fakultas Hukum UNPAD, dan Tim Asistensi ITB. Namun dalam perjalanannya, RUU ini kemudian dijadikan satu dengan RUU Informasi Elektronik dan Transaksi Elektronik (RUU IETE) yang dikembangkan oleh kawan-kawan di FKHT UI. Akibatnya, tulisan saya yang tadinya mencoba membahas RUU PTI secara detail tersebut menjadi tidak dapat diteruskan. Berantakan. Oleh sebab itu, saya akan membuat tulisan (buku?) yang lebih umum tentang peraturan dan pengaturan cyberspace di Indonesia ini. Jadilah tulisan ini.

Latar Belakang

Teknologi telekomunikasi, komputer, dan informasi sudah berkembang demikian canggihnya sehingga aplikasi yang berhubungan dengan teknologi tersebut sudah menjadi bagian dari kehidupan kita sehari-hari. Teknologi ini mengubah cara hidup kita. Berbagai hambatan atau batasan yang

1 Budi Rahardjo adalah dosen Teknik Elektro ITB, ketua IDNIC (pengelola domain .ID), founder & head dari ID-CERT (Indonesia Computer Emergency Response Team). Web site: <http://budi.insan.co.id>

semula menjadi kendala sangat besar menjadi hilang atau berkurang dengan adanya teknologi ini. Sebagai contoh, batas ruang dan waktu menjadi hilang atau tipis dengan adanya jaringan komputer Internet.

Pada mulanya jaringan Internet hanya dapat digunakan oleh lingkungan pendidikan (perguruan tinggi) dan lembaga penelitian. Baru pada tahun 1995 Internet dapat digunakan untuk publik. Pada tahun yang berdekatan, awal tahun 1990-an, Tim Berners-Lee mengembangkan aplikasi World Wide Web (WWW) yang memudahkan orang untuk mengakses informasi di Internet. Gabungan antara dibukanya Internet untuk keperluan publik dan WWW ini membuat munculnya aplikasi-aplikasi bisnis di Internet.

Aplikasi bisnis yang berbasis teknologi internet ini mulai menunjukkan adanya aspek finansial. Mulailah muncul kecurangan-kecurangan dan kejahatan yang berbasis kepada teknologi informasi (*cybercrime*). Ketersediaan hukum yang menangani masalah-masalah di dunia maya sudah tidak dapat dihindari.

Apakah cyberspace dapat diatur?

Kata “cyber” berasal dari kata “cybernetics”, yaitu suatu bidang ilmu yang merupakan perpaduan antara robotik, matematika, elektro, dan psikologi yang dikembangkan oleh Norbert Wiener di tahun 1948. Salah satu aplikasi dari cybernetics adalah di bidang pengendalian (robot) dari jarak jauh. Dalam hal ini tentunya diinginkan sebuah kendali yang betul-betul sempurna. *Perfect control*. Jadi agak aneh kalau kata “cyberspace” yang kata asalnya adalah “cyber” tidak dapat dikendalikan.

Cyberspace dapat diatur, meskipun cara mengaturnya membutuhkan pendekatan yang berbeda dengan cara yang digunakan untuk mengatur dunia nyata. Lawrence Lessig dalam bukunya “Code” mencoba menjabarkan hal ini dengan lebih detail. Saya menyarankan agar para pembaca membaca buku tersebut.

Kejahatan dunia maya (cybercrime)

High-tech menghasilkan high-(tech-)crime. Kejahatan terjadi di dunia maya. Sayangnya kejahatan di dunia maya tidak tinggal di dunia maya saja, akan tetapi efeknya terasa juga di dunia nyata. Banyak sudah statistik dan berita yang menunjukkan kejahatan di dunia maya ini.

<statistik cybercrime akan diletakkan di sini>

Penanganan cybercrime: aspek pembuktian

*What is the meaning of evidence in an environment where crime scenes themselves are mutable and can be altered, destroyed, or even created in milliseconds?
(Marcus J. Ranum, “Questions About the Future,” Secure Business Quarterly, volume one, issue one. www.sbj.com)*

Banyak orang yang beranggapan bahwa jika belum ada cyberlaw maka kita vakum hukum sehingga kejahatan di dunia maya dapat dilakukan. Ini anggapan yang salah. Para penegak hukum dapat menggunakan hukum-hukum yang belaku untuk menjerat para pelaku kejahatan cyber. Memang landasan hukum konvensional akan mempersulit pekerjaan penegak hukum (Polisi).

Sebagai contoh, banyak orang yang mempertanyakan bukti-bukti apa yang dapat digunakan untuk menjerat seorang tertuduh? Apakah sebuah berkas elektronik (electronic file), seperti misalnya sebuah e-mail, dapat dijadikan bukti? Bisa ya dan bisa tidak.

Pihak yang berpendapat bahwa digital file tidak dapat dijadikan bukti mengatakan bahwa file dapat

dibuat dengan mudah. Bisa saja seseorang (bahkan mungkin juga penyidik) yang membuat atau mengubah file tersebut, bukan tertuduh. Memang benar file digital mudah dibuat dan diubah. Akan tetapi ada jejak-jejak yang dibuat ketika kita membuat sebuah berkas digital. Tergantung kepada sistem operasi komputer yang digunakan, sistem komputer mencatat perubahan yang dilakukan terhadap sistem (termasuk membuat file) dalam berbagai berkas. Biasanya ini dikenal dengan istilah “log”. Selain log, ada juga tanda-tanda lain yang melekat pada berkas itu sendiri (kapan berkas dibuat, kapan terakhir diakses) atau tercatat di *file system* (misalnya di *File Allocation Table*, FAT).

Mengenai pembuktian isi berkas itu sendiri memang tidak mudah dibuktikan. Sifat yang ingin dibuktikan adalah sifat *integrity*. Sifat ini dapat terjaga dan dibuktikan jika digunakan *digital signature*² untuk mengesahkan berkas tersebut. Dengan digital signature, perubahan satu huruf saja dalam isi berkas akan dapat ditunjukkan bahwa berkas sudah berubah (meskipun tidak ditunjukkan apanya yang berubah). Tanpa digital signature akan sulit melakukan pembuktian. Namun ini bukan berarti tidak mungkin, hanya sangat sulit.

Di dalam RUU Cyberlaw Indonesia, istilah “dokumen elektronik” merujuk kepada “electronic records”. Jadi dokumen elektronik di sini tidak sekedar berkas atau file saja. Dokumen elektronik yang sah harus ditandatangani (secara digital).

Perlu diingat, secara teknis sebetulnya yang dilakukan oleh Polisi adalah investigasi konvensional. Aspek teknologi informasinya ada namun masih pola investigasi konvensional yang digunakan untuk menyidik.

HaKI / Intellectual Property Rights

Intellectual Property Rights (IPR) atau HaKI (Hak atas Kekayaan Intellectual) merupakan salah satu masalah hukum yang terkait dengan teknologi. Masalah yang muncul dengan HaKI terkait dengan mudahnya membuat duplikat lagu (CD, MP3), film (video, VCD, DVD), software (disket, CD), buku (dalam format elektronik).

Teknologi digital memungkinkan pembuatan duplikasi dengan sempurna. Lagu-lagu yang disimpan dalam format digital, seperti yang digunakan pada Compact Disc (CD), dapat diduplikasi (*di-copy*) tanpa cacat. CD duplikat (*copy-an*) tidak dapat dibedakan dengan CD aslinya. Hal ini berbeda ketika teknologi analog masih digunakan pada rekaman piringan hitam (*records, LP*) atau kaset. Hasil duplikat kaset atau piringan hitam memiliki kualitas yang lebih buruk dari aslinya sehingga orang masih mendapat nilai tambah dari membeli kaset asli. Teknologi digital ini mengubah pola bisnis, dimana biaya untuk membuat 1000 copy CD tidak jauh berbeda dengan membuat 100.000 copy. Biaya hanya bertambah di sisi medianya saja. Selain memudahkan duplikasi, teknologi digital juga memudahkan untuk mengirimkan materi tersebut melalui media elektronik seperti melalui Internet.

Mudahnya untuk membuat duplikat yang sama dengan aslinya berlaku untuk produk-produk yang dapat disimpan dalam format digital, yang bisa disebut “*digitized format*”, seperti audio, video, buku, gambar, dan software.

Anti-IPR

Masalah HaKI ini tidak berkembang dengan mulus karena ada pemikiran lain yang menentang HaKI yaitu pendapat yang beraliran “*anti intellectual property rights*”. Penganut anti-IPR ini bukan

2 Penjelasan mengenai teknis digital signature akan dibahas pada versi berikutnya dari tulisan ini. Untuk sementara ini para pembaca diharap menggunakan buku lain untuk mencari informasi yang lebih dalam mengenai digital signature ini. Juga perlu dibedakan perbedaan antara digital signature dengan tanda tangan yang di-scan. Untuk yang terakhir ini, istilah yang lebih tepat adalah “*digitized signature*”. *Digitized signature* secara teknis justru sukar dibuktikan keabsahannya. Digital signature tidak berupa gambar tangan tangan yang di-scan, akan tetapi merupakan urutan angka yang panjang.

menganjurkan pembajakan atau pelanggaran HaKI, namun mereka menganjurkan untuk mengembalikan kepemilikan kepada umat manusia seperti misalnya membuat temuan menjadi *public domain*. HaKI sudah dimonopoli oleh negara besar dan perusahaan besar sehingga manfaat bagi manusia menjadi nomor dua. Saya pribadi sepakat dengan pendapat ini.

Perlindungan HaKI dilakukan dengan alasan untuk memberikan insentif kepada penemu (inventor) dalam bentuk hak eksklusif atau monopoli. Cara ini mungkin cocok untuk waktu dulu, namun perlu dikaji kembali. Banyak yang berpendapat bahwa alasan insentif ini sudah tidak cocok lagi. Banyak penemu yang melakukan penemuan bukan semata-mata untuk mendapat popularitas dan kekayaan (fame & fortune). Alasan insentif ini tidak cocok lagi. Nanti kita tunjukkan contoh inovasi yang tidak berdasarkan kekayaan di bagian software.

Di dunia obat-obatan terjadi harga obat yang mahal dan tidak dapat dijangkau oleh orang miskin karena pabrik obat harus membayar royalty kepada penemunya (atau perusahaan yang memiliki patennya). Obat generik juga tidak dapat dibuat dengan murah karena tidak diijinkan. (Kasus AIDS, dll. Referensi?)

Free Software Movement: Gerakan Software Bebas

Di dunia software dikenal dengan gerakan *Free Software* movement yang dimotori oleh *Free Software Foundation* (FSF) yang menghasilkan software yang dikenal dengan nama GNU³, seperti GNU C compiler (gcc), GNU/Hurd (sistem operasi). Motor dari gerakan ini adalah Richard Stallman. Kata “free” dalam “free software” ini bermakna “freedom” atau bebas, bukan berarti gratis meskipun kebanyakan free software ini bisa diperoleh secara gratis. Software bebas ini bisa kita gunakan semau kita; diutak-atik, diubah-ubah, disimpan, dan bahkan dijual.

Selain gerakan free software, ada juga gerakan lain yang disebut “open source”. Gerakan ini memfokuskan kepada ketersediaan *source code* atau *program listing*. Pengguna dapat melihat code-code yang digunakan untuk membuat software tersebut. Jika dahulu source code ini dijaga kerahasiaannya, maka paradigma baru ini justru membuka source codenya. Contoh terkenal dari pendekatan open source ini adalah sistem operasi (operating system) Linux, dan web server Apache⁴.

HaKI di Indonesia

Satu hal lain yang membuat saya sering berpikir panjang tentang HaKI di Indonesia ini adalah para pendukung HaKI di Indonesia seringkali menggunakan argumentasi yang kurang kuat. Sebagai contoh, mereka sering menggunakan argumentasi tentang batik, tempe, dan seterusnya yang dieksploitasi (didaftarkan patennya) di luar negeri. Memang perlindungan terhadap hal tersebut penting. Akan tetapi saya masih belum mendapat jawaban mengapa tidak dibuat menjadi *public domain* saja?

Pendaftaran paten dan perlindungan HaKI lainnya biasanya hanya bisa dilakukan oleh perusahaan besar dari negara besar. Di Indonesia yang notabene didasari oleh Usaha Kecil Menengah (UKM), HaKI malah mungkin akan menghambat bisnis mereka karena belum apa-apa mereka sudah dihadapi dengan *barrier* paten milik orang / perusahaan lain dari luar negeri.

Digital Millennium Copyright Act (DMCA)

Business increasingly use DMCA lawsuits as a competitive tool, to slow down or hurt their rivals, Schneier and other DMCA critics point out.

3 Kata “GNU” ini merupakan singkatan dari “GNU is Not UNIX”. Jika kita perhatikan singkatan ini rekursif, karena kepanjangannya lagi ada kata GNU lagi. Informasi mengenai software GNU dapat dilihat pada situs web <http://www.gnu.org>

4 Situs Apache ada di <http://www.apache.org>

(Laurianne McLaughlin, ...)

Di Amerika Serikat ada Digital Millennium Copyright Act (DMCA) yang mencoba menangani masalah copyright di era ini. Ada banyak masalah yang terkait dengan DMCA ini.

Salah satu contoh kasus yang terkait dengan DMCA terjadi pada perusahaan software ElcomSoft. Perusahaan ini membuat sebuah program yang dapat mengubah berkas dalam format Adobe eBook menjadi Adobe Portable Document Format (PDF). Perusahaan Adobe merasa bahwa ElcomSoft melanggar pasal *anticircumvention* dari DMCA⁵ karena program tersebut memotong penyandian (enkripsi) yang ada pada eBook. Programmer dari ElcomSoft yang bernama Dmitry Sklyarov ditangkap oleh FBI ketika dia mengikuti konvensi Defcon di Las Vegas (summer 2001). ElcomSoft akhirnya diputuskan bebas oleh Federal Jury pada bulan Desember 2002.⁶

Ada sebuah catatan tentang kasus Sklyarov di atas, yaitu Dmitry Sklyarov adalah orang Rusia. Dia ditangkap ketika datang ke Las Vegas. Ini menunjukkan bahwa jangkauan hukum Amerika Serikat sangat jauh, meskipun mereka tidak melakukan penangkapan secara pro-aktif. Ide yang sama dapat diterapkan kepada hukum cyber Indonesia, dimana jika ada kejahatan (cybercrime) yang efeknya dirasakan di Indonesia (atau oleh orang / institusi Indonesia), maka pelakunya dapat ditangkap ketika dia masuk ke Indonesia. Hal ini merupakan sebuah faktor pencegahan (*deterant*) agar orang asing berpikir panjang lebar untuk melakukan kejahatan yang dampaknya dirasakan oleh orang Indonesia. Paling tidak, dia akan berpikir bahwa dia tidak dapat masuk ke Indonesia.

Ada beberapa contoh kasus lain yang terkait dengan DMCA, antara lain:

1. Perusahaan printer Lexmark memasang sebuah *microchip* pada *cartridge* tinta printernya. Microchip ini akan berbicara (*handshaking*) dengan printer untuk memberitahukan bahwa dia *cartridge* buatan Lexmark. Hal ini dilakukan agar Lexmark menguasai pasar *cartridge* printernya, karena tidak ada perusahaan lain yang memiliki *microchip* tersebut. Namun ada sebuah perusahaan, Static Control Components (North Carolina), yang membuat *microchip* seperti itu dan menjualnya secara umum. Lexmark menuntut bahwa Static Control Components melanggar pasal *anticircumvention* dari DMCA.
2. Perusahaan Chamberlain Group yang membuat perangkat pembuka garasi (*garage door opener*) menuntut Skylink Technologies karena mereka membuat *remote control* yang dapat bekerja dengan *door opener* buatan Chamberlain.
3. Profesor Edward Felten dari Princeton University diancam dengan pasal DMCA karena kelompok penelitiannya meneliti pengamanan (security) dari *digital watermarking* yang digunakan untuk memproteksi *digital music*. Tujuan penelitiannya adalah untuk meningkatkan level security. Namun dia (diancam) dituntut karena untuk melakukan penelitian tersebut dia harus melakukan "*reverse engineering*", yaitu mencari tahu desain dengan membongkar. Kasus ini membuat para peneliti menjadi berang. Bagi Amerika ini adalah ancaman karena penelitian-penelitian seperti itu nantinya harus dilakukan di luar negeri. (Mungkin bisa dibawa ke Indonesia jika di Indonesia hal tersebut diperkenankan. Keuntungan buat Indonesia.)

Karena kasus-kasus di atas, saat ini sedang ada usaha untuk membuat koreksi atas DMCA. Namun hal ini merupakan pekerjaan yang berat karena industri music dan film (yang ingin memastikan produknya tidak dibajak) akan tetap memaksakan adanya DMCA yang ketat.

5 Section 1201 dari DMCA secara eksplisit menyatakan bahwa tidak diperkenankan untuk mengembangkan teknologi yang "*circumvents technological measures*" yang didesain untuk memproteksi materi yang memiliki copyright. Juga disebutkan bahwa tools yang dapat melakukan hal tersebut tidak boleh didistribusikan.

6 Laurianne McLaughlin, "After ElcomSoft: DMCA Still Worries Developers, Researchers," *IEEE Software*, March/April 2003.

Paten Software: perlukah? Tidak!

Di Amerika Serikat ada perkembangan baru bahwa paten diperkenankan untuk software. Pada mulanya di dunia software hanya dikenal copyright, namun sekarang ditambah dengan paten. Bagian mana dari software yang dapat dipatenkan? Ternyata algoritma yang digunakan dalam software dapat dipatenkan. Di Indonesia, untungnya, hal ini tidak dikenal (dan mudah-mudahan tetap demikian).

Banyak orang yang tidak setuju dengan adanya paten terhadap software. Saya termasuk salah satunya⁷.

Pasalnya, algoritma dari software biasanya adalah rumus-rumus matematik. Bayangkan apabila “1+1” dipatenkan. Apa yang terjadi dengan ilmu pengetahuan? Perkembangan ilmu pengetahuan akan terhambat karena penelitian-penelitian dan simulasi-simulasi membutuhkan rumus-rumus matematik. Orang akan takut melakukan penelitian atau membuat perangkat lunak karena salah-salah dia bisa dituntut.

Beberapa contoh paten software, antara lain:

1. Algoritma Lempel-Ziv yang merupakan algoritma yang paling banyak digunakan untuk kompresi (mengecilkan ukuran berkas) gambar atau data-data lainnya.
2. Algoritma RSA yang digunakan untuk enkripsi data, seperti contohnya ketika kita mengetikkan nomor kartu kredit di situs web yang menggunakan SSL (biasanya ditandai dengan penggunaan HTTPS sebagai pengganti HTTP)

Pengalaman Amerika Serikat dalam paten software ini ternyata berdampak buruk bagi industri software mereka. Sebagai contoh, programmer di Amerika tidak dapat mengembangkan software yang berhubungan dengan DVD (misalnya seorang programmer ingin membuat DVD player) karena ada bagian tertentu yang dipatenkan. Sang programmer harus mendapat lisensi dahulu sebelum dia dapat membuat dan mendistribusikan softwaranya karena jika tidak maka dia akan melanggar paten tersebut. Untuk menghindari hal ini, programmer tersebut terpaksa pindah dari Amerika (mungkin ke Indonesia?). Ini yang meresahkan bagi pakar software di Amerika, seperti misalnya Donal Knuth⁸ (yang terkenal dengan software TeX dan buku “*The Art of Computer Programming*”).

Contoh kasus:

1. Perusahaan software *XyQuest* terpaksa menarik fitur “*automatic correction and abbreviation expansion*” dari software *XyWrite* buatannya karena dianggap melanggar paten yang dimiliki oleh perusahaan lain. Akibatnya pengguna software *XyWrite* tersebut tidak dapat menggunakan fitur tersebut. Pengguna yang dirugikan.

Untuk mengetahui tentang paten software ini silahkan kunjungi situs dari *League of Programming Freedom* di <http://lpf.ai.mit.edu/Patents/patents.html>

Privacy & confidentiality

Privacy terkait dengan kerahasiaan data-data pribadi, seperti nama lengkap, alamat, tempat tanggal lahir, status pernikahan, nama istri/suami, nama anak, tempat pekerjaan, nama ibu (mother's maiden name), status kesehatan (pernah mengidap penyakit apa saja), dan seterusnya. Banyak yang tidak menganggap penting untuk merahasiakan hal ini, padahal dia sangat penting untuk dirahasiakan. Sebagai contoh, jika saya tahu nama anda, tempat tanggal lahir, alamat, dan nama ibu anda, saya bisa mencoba untuk membatalkan kartu kredit anda. Saya tinggal telepon ke bank anda dimana anda memperoleh kartu kredit dan berpura-pura menjadi anda. Saya laporkan bahwa kartu kredit saya (anda dalam hal ini) hilang. Ketika ditanya nama, alamat, tempat tanggal lahir, dan nama ibu, saya bisa menjawabnya. Maka kartu kredit anda dinyatakan hilang dan diblokir. Meskipun tidak ada yang

⁷ Budi Rahardjo, “Katakan Tidak untuk Paten Peranti Lunak,” InfoLINUX, Januari 2003.

⁸ Surat Donald Knuth ke Patent Office dapat dibaca di <http://lpf.ai.mit.edu/Patents/knuth-topto.txt>

dicuri, anda akan kerepotan karena tidak bisa menggunakan kartu kredit anda. Bayangkan jika anda sangat membutuhkan kartu kredit tersebut.

Data-data pribadi yang diberikan kepada pihak lain, misalnya ke bank, disebutkan *confidential*. Pihak kedua ini (bank, dalam contoh ini) tidak boleh menggunakan data-data tersebut untuk keperluan lain. Mereka tidak boleh menjual data-data tersebut ke kartu kredit, atau ke pihak-pihak lain. Untuk itu perhatikan kesepakatan (agreement) yang ada.

Confidentiality juga terkait dengan data-data lain yang bukan data-data pribadi. Password (kata sandi untuk masuk ke sistem) dan PIN (kombinasi angka untuk mengakses account di bank melalui mesin ATM) merupakan contoh data yang harus dirahasiakan dan bersifat *confidential*. Pemahaman atas pentingnya kerahasiaan data-data ini umumnya lebih mudah diterima atau dimengerti ketimbang *privacy*. Tetapi masih ada saja orang yang tertipu sehingga data-data yang sifatnya *confidential* itu bisa bocor ke tangan orang yang tidak berhak. Pencurian password dapat dilakukan dengan menyadap data yang lalu lalang di jaringan komputer dengan menggunakan program yang dikenal dengan nama atau istilah *sniffer*. Atau, cara lain yang dapat digunakan adalah dengan memasang program "*keylogger*" yang mencatat semua yang diketikkan oleh pemakai ke dalam sebuah berkas. Hal semacam ini semestinya dapat dikategorikan sebagai cybercrime.

Policy & procedure di perusahaan

Ada situasi abu-abu (*grey area*) dimana seorang pengelola sistem (*system administrator*) di sebuah perusahaan yang mencurigai seorang penggunanya, misalnya sang pengguna diduga membocorkan rahasia perusahaan. Bolehkan sang administrator ini melakukan penyadapan (*tapping*) terhadap pengguna yang bersangkutan tanpa ijin? Apakah hal ini dapat dianggap sebagai pelanggaran terhadap *privacy*? Ada dua kubu pendapat dalam kasus ini. Kubu pertama, kebanyakan terdapat di luar negeri, mengatakan bahwa kegiatan penyadapan tanpa ijin ini merupakan pelanggaran terhadap *privacy*. Administrator tidak dapat seenaknya melakukan penyadapan. Kubu kedua berpendapat bahwa semua yang ada di kantor merupakan milik (*property*) dari kantor. Jadi, sang administrator berhak melakukan langkah-langkah untuk mengamankan aset perusahaan, termasuk melakukan penyadapan. Hal seperti ini seharusnya masuk kepada *policy & procedure* (SOP) dari perusahaan. Tanpa adanya SOP ini, interpretasi bisa berbeda-beda sehingga menimbulkan kasus. Bagaimana pendapat anda tentang hal ini? Anda berpihak kepada kubu yang mana?

Privacy & confidentiality di luar negeri

Masalah *privacy* / *confidentiality* merupakan salah satu aspek yang sangat penting di dunia Barat. Sayang sekali aspek ini kurang mendapat perhatian yang serius di Indonesia. Data-data pribadi berserakan dimana-mana tanpa diamankan. Bahkan data-data bank account dari seseorang, misalnya pejabat, bisa diketahui dan diberitakan di media masa. Walaupun pejabat itu korup, semestinya data-data bank accountnya tidak mudah diperoleh atau dibebaskan seperti itu.

Banyak negara yang sangat melindungi kerahasiaan data-data warga negaranya. Ketika sebuah negara (atau sebuah perusahaan) akan melakukan transaksi dengan (perusahaan) Indonesia, mereka akan menanyakan kebijakan yang terkait dengan masalah *privacy* ini (*privacy policy*). Jika kita tidak dapat memberikan jaminan kerahasiaan data-data warganya maka mereka tidak akan mau melakukan transaksi dengan Indonesia. Hal ini disebabkan mereka sudah bersusah payah menjaga kerahasiaan, akan tetapi dengan mudah dibocorkan di Indonesia.

Masalah privacy ini mulai muncul saat ini karena kemampuan teknologi komputer dan telekomunikasi sudah memungkinkan penyadapan dengan biaya yang murah. Jaman dahulu, penyadapan ini membutuhkan biaya yang mahal karena masalah fisik. Secara tidak langsung ada “perlindungan” dari alam. Hilangnya perlindungan inilah yang menyebabkan munculnya masalah privacy.

Privacy policy di situs web

Beberapa situs web yang utama biasanya menuliskan “privacy policy” mereka di halaman situs webnya. Mereka mengatakan secara eksplisit penggunaan data-data yang mereka kumpulkan dari situs web mereka. Sudahkah anda memiliki “privacy policy” di situs web anda?

Informasi mengenai privacy dapat diperoleh dari berbagai situs web, antara lain:

- Electronic Privacy Information Center (EPIC): <http://www.epic.org>

Beberapa Peraturan Untuk Cyberspace

Pada bagian ini, saya ingin membahas beberapa peraturan untuk cyberspace (cyberlaw) yang ada di Indonesia. Pada saat yang sama, saya ingin mencoba mensintesis beberapa ide-ide yang telah dibahas pada bagian-bagian sebelumnya.

RUU IT

... di sini nanti ada pembahasan RUU yang sudah dibuat ...

Pengaturan VoIP

Voice over IP (VoIP) merupakan sebuah istilah populer dari penggunaan Internet untuk bercakap-cakap dengan menggunakan suara. Sebetulnya istilah *generic*-nya adalah IP Telephony, dimana IP (Internet Protocol) digunakan sebagai basis untuk mengirimkan suara. Tidak mengherankan jika jaringan komputer Internet menggunakan basis protokol yang sama, dikarenakan IP telephony memang dikembangkan dari dunia Internet.

Pada mulanya kemampuan mengirimkan suara melalui Internet hanya merupakan eksperimen dari beberapa orang atau perusahaan kecil. Ini dimulai dengan perusahaan seperti *Vocaltech* dan kemudian pada akhirnya diikuti oleh *Microsoft* dengan program *Netmeeting*-nya. Pada saat itu jaringan komputer Internet masih sangat lambat. Di rumah-rumah (khususnya di Amerika) masih digunakan dial-up dengan kecepatan 36,6K. Backbone Internet pun masih kecil. Aplikasi yang bersifat menghabiskan bandwidth, seperti misalnya suara atau video, masih sangat terbatas penggunaannya di pusat penelitian yang memiliki bandwidth besar.

Pada saat ini jaringan komputer Internet sudah masuk ke rumah-rumah dengan kecepatan yang cukup besar. Leased line lebih murah dibandingkan dahulu. Alternatif lain, seperti Wireless LAN, memberikan layanan dengan pita bandwidth yang besar dengan harga yang masih terjangkau oleh perusahaan kecil. Aplikasi yang berbaur multimedia mulai dapat digelar di atas Internet. IP telephony menjadi memungkinkan dijalankan dengan menggunakan infrastruktur Internet.

IP telephony dapat dibagi menjadi dua kategori; ***Internet Telephony*** dan ***VoIP***. Perbedaan dari keduanya adalah Internet telephony menggunakan jaringan Internet yang umum (public internet), sementara VoIP menggunakan jaringan privat meskipun masih menggunakan teknologi yang sama⁹. Teknologi lain pun, seperti Asynchronous Transfer Mode (ATM) juga dapat digunakan untuk

9 Ada juga pengertian lain yaitu VoIP merupakan teknologi yang digunakan, yaitu Voice over IP. Sementara itu IP telephony terkait dengan layanan (service).

telephony. Namun biasanya aplikasinya juga masih disebut atau digolongkan kedalam IP telephony.

VoIP ini kemudian menjadi masalah karena orang mulai menyediakan layanan percakapan melalui jaringan internet dengan memotong (bypass) operator telepon. Seorang penyedia jasa VoIP cukup menyewa sebuah jaringan yang dikenal dengan istilah "E1" dan membawa *traffic* pembicaraan telepon melalui jalur E1 yang disewanya tersebut. Jadi pembicaraan telepon dari/ke luar negeri bisa dilewatkan melalui Internet kemudian ke saluran yang sudah disewanya tersebut. Harga bisa dipangkas menjadi sangat murah (dengan kualitas suara yang lebih rendah). Di banyak negara, layanan dasar telepon dimonopoli oleh pemerintah atau perusahaan tertentu. Di Indonesia layanan percakapan dalam negeri dimonopoli oleh PT Telkom, sementara layanan ke luar negeri dimonopoli oleh PT Indosat dan Satelindo (yang kemudian menjadi milik Indosat). Layanan VoIP memakan pendapatan dari operator yang memonopoli ini secara signifikan (dalam sisi finansial). Untuk itu perlu ada pengaturan layanan VoIP ini.

Ada berapa hal yang perlu mendapat perhatian dari layanan VoIP ini, antara lain:

- Pengguna mendapat layanan dengan kualitas suara yang lebih buruk akan tetapi harus membayar premium. Aspek perlindungan konsumen harus diperhatikan.
- Adanya persaingan tidak sehat dengan membanting harga sehingga pendapatan semua pihak menjadi sangat sedikit dan diatur oleh pihak luar.
- ...

Beberapa hal di atas menjadi pertimbangan dalam menentukan aturan VoIP.

Penutup

Permasalahan hukum dan teknologi menjadi sangat penting karena cepatnya perubahan teknologi. Pemahaman hukum bagi seorang *technologist* atau *engineer* (insinyur) menjadi esensial. Demikian pula pemahaman teknologi bagi pembuat dan penegak hukum juga menjadi penting agar hukum atau keputusan yang diambil tidak menjadi bahan tertawaan. Untuk itu mudah-mudahan tulisan ini dapat memberikan manfaat.

Daftar Bacaan

Bacan untuk bidang cyberlaw ini mulai banyak. Namun sayangnya masih banyak yang sulit diperoleh di Indonesia. Berikut ini daftar bahan bacaan yang saya gunakan dalam menulis tulisan ini.

1. Lawrence Lessig, "*Code: and other laws of cyberspace*", Basic Books, 1999.
2. Laurianne McLaughlin, "After ElcomSoft: DMCA Still Worries Developers, Researchers," *IEEE Software*, March/April 2003.
3. Budi Rahardjo, "Katakan Tidak untuk Paten Peranti Lunak," *InfoLINUX*, Januari 2003.