

# PERLUNYA *CYBERLAW* DALAM RANGKA MENGHADAPI DAN MENANGGULANGI KEJAHATAN DUNIA MAYA

Oleh: Cahyana Ahmadjayadi<sup>\*)</sup>

## Latar Belakang

Teknologi informasi dan komunikasi (TIK) telah menjadi bagian hidup manusia yang tidak dapat dipisahkan. Keberadaan TIK membuat hidup kita menjadi lebih mudah dan menyenangkan. Aktivitas yang terkait dengan pekerjaan, pendidikan, hingga hiburan terkait erat dengan pemanfaatan TIK. Menyusun dokumen elektronik, melakukan penghitungan, mengirim dan membaca *e-mail*, berselancar di internet, *chatting* merupakan aktivitas sehari-hari yang memanfaatkan TIK. Tidak ada satupun organisasi atau perusahaan yang tidak menggunakan peralatan TIK dalam kegiatannya, bahkan bagi sebagian mereka, TIK sudah menjadi bagian utama pelaksanaan kegiatan.

Layaknya dunia nyata, dalam dunia TIK selain hal-hal baik yang diperoleh, ada juga hal-hal buruk yang mengintai, antara lain seperti penyebaran virus komputer dan

spam, aktivitas *cracking* dan *sniffing*, dan sebagainya. Kita harus menerima kenyataan bahwa ada orang yang bermaksud tidak baik diluar sana.

Setiap pengguna komputer pernah mengalami serangan virus, spam, atau bentuk kejahatan TIK lainnya pada satu ketika dalam hidupnya. Siapa yang tidak kenal "Brontok", *worm made in Indonesia*, yang dapat menginfeksi suatu komputer dan menyebar dengan sangat cepat melalui *USB Flash Disk* dan jaringan. Banyak komputer yang terinfeksi dengan parah tidak dapat dipergunakan hingga mereka dibersihkan atau diformat ulang. Dapat dibayangkan berapa kerugian dari segi waktu, produktifitas kerja, serta biaya yang harus dikeluarkan untuk membersihkan virus tersebut. Karakteristik serangan virus yang dapat menyebar luas dengan cepat juga dapat mengancam keberlangsungan operasional suatu organisasi atau perusahaan yang menggantungkan segala aktivitasnya pada TIK.

Sejalan dengan perkembangan teknologi, kejahatan dalam dunia TIK juga berkembang sangat cepat. Kita tidak akan mungkin dapat

---

<sup>\*)</sup> Dirjen Aplikasi dan Telematika,  
Departemen Komunikasi dan Informatika

menuntaskan semua potensi serangan kejahatan TIK tersebut sekaligus. Namun demikian ada langkah-langkah reaktif maupun preventif yang dapat dilaksanakan guna mengatasi permasalahan tersebut diatas. Salah satunya melalui penegakan hukum dunia maya atau *cyberlaw*.

### **Potensi Kejahatan Dunia Maya**

Kejahatan dalam bidang teknologi informasi dengan melakukan serangan elektronik berpotensi menimbulkan kerugian pada bidang politik, ekonomi, sosial budaya, yang lebih besar dampaknya dibandingkan dengan kejahatan yang berintensitas tinggi lainnya. Di masa datang, serangan elektronik dapat mengganggu perekonomian nasional melalui jaringan yang berbasis teknologi informasi seperti perbankan, telekomunikasi satelit, listrik dan lalu lintas penerbangan. Hal ini dipicu oleh beberapa permasalahan yang ada dalam konvergensi teknologi, misalnya internet membawa dampak negatif dalam bentuk munculnya jenis kejahatan baru, seperti *hacker* yang membobol komputer milik bank dan memindahkan dana serta merubah data secara melawan hukum. Teroris menggunakan internet untuk merancang dan melaksanakan serangan, penipu menggunakan kartu kredit milik orang lain untuk berbelanja melalui

internet. Perkembangan TI di era globalisasi akan diwarnai oleh manfaat dari adanya *e-commerce*, *e-government*, *foreign direct investment*, industri penyedia informasi dan pengembangan UKM.

Dapat dibayangkan, bagaimana jika sebuah infrastruktur teknologi informasi yang bersentuhan dengan hajat hidup orang banyak tidak dilindungi dengan sistem keamanan. Misalnya jaringan perbankan, dikacau balaukan atau dirusak data-datanya oleh pihak yang tidak bertanggung jawab, sehingga informasi yang ada di dalamnya juga kacau dan rusak. Dengan demikian masyarakat yang bersentuhan hanyalah sederetan tulisan, akan tetapi angka-angka dalam sebuah data dan informasi perbankan merupakan hal yang sensitif. Kacaunya atau rusaknya angka-angka tersebut dapat merugikan masyarakat dan bahkan dapat merusak lalu lintas perekonomian dan keuangan serta dapat berdampak pada keamanan, ketentraman dan ketertiban dalam masyarakat. Demikian pula, infrastruktur TI lainnya seperti Penerbangan, Pertahanan, Migas, PLN dan lain-lainnya, dapat dijadikan sebagai sarana teror bagi teroris. Di masa depan, bukan tidak mungkin teroris akan menjadikan jaringan teknologi informasi sebagai

sarana untuk membuat kacau dan teror dalam masyarakat.

Motivasi untuk melakukan kejahatan dunia maya meningkat secara eksponensial. Ditambah lagi dengan potensi yang dihasilkan dari kejahatan dunia maya. Pada kejahatan perampokan bank, rata-rata dihasilkan US\$ 14,000, sedangkan dalam kejahatan berbasis teknologi informasi kerugian yang dihasilkan rata-rata mencapai US\$ 2 juta. Berapa besar kerugian yang sebenarnya terjadi akibat *cyber crime* tidak dapat dinilai secara pasti, karena sangat sedikit perusahaan atau organisasi yang melaporkannya. Hal ini terjadi karena mereka takut akan adanya kepanikan yang dapat mengakibatkan kerugian yang lebih besar lagi.

Pemerintah memberikan perhatian serius pula terhadap masalah keamanan informasi. Departemen Kominfo telah membentuk **ID-SIRTI (Indonesian Security Incident Response Team on Information Infrastructure)**, POLRI juga membentuk **Cyber Task Force Center**, disamping itu juga ada **ID-CERT** sebagai institusi independen yang bertujuan melakukan sistem keamanan teknologi informasi. Pembentukan ID-SIRTI dalam jajaran Departemen Kominfo bukan berarti mengambil alih tugas dan fungsi institusi

sekuriti lainnya. Bahkan tanpa *task force* yang ada di Departemen Kominfo peran dan fungsi Kepolisian dan Kejaksaanpun tetap akan berjalan wajar, demikian pula ID-CERT dan lembaga lainnya yang dibentuk oleh masyarakat TI tetap berfungsi dan berjalan normal.

Pada era global sekarang ini, keamanan sistem informasi berbasis internet menjadi suatu "Keharusan" untuk diperhatikan, karena jaringan komputer internet yang sifatnya publik dan global pada dasarnya tidak aman. Pada saat data terkirim dari suatu komputer ke komputer yang lain dalam internet, data itu akan melewati sejumlah komputer yang lain yang berarti akan memberi kesempatan pada user internet lainnya untuk menyadap atau mengubah data tersebut. Dalam perjalanan data tersebut, memungkinkan orang lain untuk ikut serta "mendengarkan" melalui alat bantu yang lazim disebut dengan "*sniffer*". Ini bisa dianalogikan bahwa seseorang memberi informasi ke pak RT lewat beberapa tetangga. Dalam dunia komunikasi data global yang senantiasa berubah, dan cepatnya perkembangan *software*, keamanan senantiasa menjadi isu yang penting. Untuk itulah diperlukan adanya keamanan sistem informasi data global yang sifatnya komperhensif.

Masih segar dalam ingatan kita, sebuah peristiwa hacking pada tabulasi data pemilu 2004 pada situs <http://tnp.kpu.go.id>, dimana telah terjadi perubahan tampilan pada situs tersebut dengan merubah nama-nama partai peserta pemilu, dengan tehnik serangan *Cross Site Scripting (XSS) dan SQL Injection (Structure Query Language)*. Sang hacker cukup cerdas melakukan serangan dengan jenis "web hacking" yang dikombinasikan dengan proses "spoofing", yakni dengan menggunakan "Anonymous Proxy" tertentu dan dari *proxy list* diambil *proxy* yang berada di Thailand dengan IP tertentu.

Kemudian sang *hacker* melakukan update daftar nama-nama partai dengan tehnik *SQL Injection* melalui IP Thailand (IP.208.147.1.1)

Terkadang kita meremehkan orang lain dan telah menganggap sistem yang kita bangun sudah aman 100%. Padahal, sampai detik ini, tidak ada suatu sistem yang bisa aman 100%. Peristiwa yang menimpa situs KPU merupakan bencana bagi dunia IT, sekecil apapun akibat yang ditimbulkannya, pasti akan ada bentuk-bentuk kerugian yang dialami. Jika bukan kerugian materi, bisa juga berdampak pada kerugian sosial politik. Jika saja sang *hacker* tidak segera tertangkap, tentunya dia

akan memiliki waktu lebih banyak untuk melakukan uji cobanya terhadap kehandalan situs KPU. Dampak yang paling kita tidak harapkan adalah jika terjadi perubahan pada perolehan suara, dimana dapat membuat Negara ini **chaos** dan pemilu bisa gagal atau batal dibuatnya, rakyat protes dan demo akan ada dimana-mana secara besar-besaran.

### **Perlunya Undang-undang Dunia Maya (Cyber Law)**

Dari sekian banyak pernik-pernik sistem keamanan penyusun kebijakan sistem keamanan merupakan hal yang sangat penting untuk diperhatikan. Keijakan keamanan menyediakan kerangka-kerangka untuk membuat keputusan yang spesifik, misalnya mekanisme apa yang akan digunakan untuk melindungi jaringan dan bagaimana mengkonfigurasi servis-servis. Kebijakan keamanan juga merupakan dasar untuk mengembangkan petunjuk pemrograman yang aman untuk diikuti user maupun bagi administrator sistem.

Kebijakan keamanan sistem informasi yang paling penting ada pada tatanan hukum nasional dalam bentuk Undang-undang Dunia Maya (*Cyber Law*) yang mengatur aktivitas dunia maya termasuk

pemberian sanksi pada aktivitas jahat dan merugikan

Pengaturan hukum dalam internet masih relatif baru dan terus berkembang, ada dorongan pengaturan yang bersifat global, namun kedaulatan hukum menjadikannya tidak mudah terlaksana. Hal ini menjadi salah satu kelemahan dari penegakkan *cyber law*, terutama jika menyangkut perkara kejahatan yang dilakukan oleh individu atau teroris dan entitas bisnis yang berada di negara lain. Konstitusi suatu negara tidak dapat dipaksakan kepada Negara lain, karena dapat bertentangan dengan kedaulatan dan konstitusi negara lain, oleh karena itu hanya berlaku di negara yang bersangkutan saja. Oleh karena itu, masyarakat peduli keamanan teknologi informasi sangat menaruh perhatian dan kerjasama global dalam menyikapi kejahatan-kejahatan TI yang sudah terjadi, sedang terjadi dan akan terjadi, seperti misalnya *Convention on Cybercrime 2001* yang digagas oleh Uni Eropa pada tanggal 23 November 2001 di Budapest, Hongaria. Substansi konvensi mencakup area yang cukup luas, bahkan mengandung kebijakan kriminal yang bertujuan untuk melindungi masyarakat dari *cybercrime* baik melalui undang-undang maupun kerjasama

international. Dalam konvensi ini telah dicakup adanya "ekstradisi otomatis", artinya, walau tidak ada perjanjian ekstradisi dengan negara tertentu, cukup dengan meratifikasi konvensi ini atau ikut dalam konvensi ini, maka telah dianggap adanya perjanjian ekstradisi dengan negara-negara peserta konvensi, guna mempersempit ruang yurisdiksi suatu negara terhadap negara lainnya khususnya dalam menegakkan hukum cyber secara global.

Kejahatan *cyber* dapat dipicu oleh adanya transisi dari *single vendor* ke multi vendor. Banyak jenis perangkat dari berbagai vendor yang harus dipelajari, misalnya untuk router Cisco, Bay Networks, Nortel, 3Com, Juiper, Linux-Based router dan sebagainya. Dan untuk server seperti Solaris, Windowa NT/2000/XP, SCO Unix, Linux, BSD, AIX, HP-UX dan sebagainya. Untuk mencari satu orang yang menguasai semuanya sangatlah sulit. Apalagi jika dibutuhkan sumber daya manusia (SDM) yang lebih banyak. Disamping itu, kesulitan penegak hukum untuk mengejar kemajuan dunia telekomunikasi dan komputer, *cyber law* masih dalam proses pembuatan, tingkat *awareness* masih rendah, *technical capability* juga masih rendah, dan potensi lubang-lubang keamanan semakin besar, karena

meningkatnya kompleksitas sistem, program menjadi semakin besar, dari megabytes menjadi gigabytes, ketergantungan komputer dan jumlah komputer yang digunakan semakin bertambah, nilai informasi semakin berharga/tinggi, jumlah operator komputer semakin bertambah, jaringan sistem semakin luas, hukum kurang menjangkau kejahatan teknologi informasi, belum ada manajemen yang melakukan aksi preventive yang pro-aktif, pola bisnis berubah, *partners, alliance, inhouse development, outsource* dan sebagainya. Untuk itu, tanggung jawab TI security merupakan tanggung jawab kita bersama. Sebagai tanggung jawab kita bersama, maka kita perlu untuk melakukan pencegahan dan penanggulangan, khususnya dalam

jajaran pemerintah dengan instansinya yang terkait dan bersinergi dengan pihak non pemerintah. Hal ini perlu dilakukan, mengingat adanya **"Lack of Law"**, dimana KUHP tidak mengatur secara khusus kejahatan berbasis TI, walaupun beberapa kasus dapat dipakai pada pasal-pasal tertentu. UU No: 36 Tahun 1999 tentang Telekomunikasi lebih fokus pada *pipeline issues*. Kurang memadai untuk menganggulangi masalah-masalah yang terkait dengan ICT, dan di lain sisi adanya **Procedure versus protecting privacy, Lack of Cybercrime Expertise, Jurisdiction versus Internet is borderless World**, dan kurangnya kerjasama antara pihak-pihak terkait.