

ASPEK HUKUM PENGGUNAAN FAKE INTERNET PROTOCOL ADDRESS DALAM HUKUM TEKNOLOGI INFORMASI

Prehantoro

Fakultas Hukum Universitas Yos Soedarso
e-mail: prehantoro@gmail.com

ABSTRAK

Kemajuan teknologi informasi telah merubah hampir semua aspek kehidupan manusia, dan mulai sebagai sarana informasi, hiburan, transaksi bisnis dapat dilakukan dari rumah dengan perangkat yang terhubung dengan internet, dan pada perkembangannya kemajuan teknologi tidak hanya dipergunakan untuk manfaat yang baik saja, namun juga dipergunakan untuk kejahatan.

Salahsatu bentuknya adalah penyalahgunaan Fake IP dalam cybercrime, penyalahgunaan Fake IP dengan mengganti IP adress dengan tujuan untuk menyamarkan/mengganti IP adress yang sebenarnya, penyalahgunaan fake ip ini banyak terjadi dalam kasus- kasus email bombing, spamming, penyerangan terhadap sebuah server, carding dan lain sebagainya. Saat ini di Indonesia belum ada satupun regulasi mengenai penggunaan Fake IP baik untuk kepentingan sistem keamanan atau yang disalahgunakan dalam kasus-kasus cybercrime.

A. Pendahuluan

Perkembangan teknologi informasi telah menciptakan peradaban manusia dihadapkan pada fenomena baru yang mampu mengubah hampir setiap aspek kehidupan manusia. Pembangunan dibidang teknologi informasi (dengan segala aspek pendukungnya) diharapkan akan membawa dampak positif bagi kehidupan manusia, yang pada akhirnya akan bermuara pada terciptanya peningkatan kesejahteraan manusia.

Kemajuan dan perkembangan teknologi, khususnya telekomunikasi multimedia dan teknologi informasi pada akhirnya dapat merubah tatanan organisasi dan hubungan sosial kemasyarakatan. Hal ini tidak dapat dihindari, karena fleksibilitas dan kemampuan telematika dengan cepat memasuki berbagai

aspek kehidupan manusia.

Bagi sebagian orang munculnya fenomena ini telah mengubah perilakunya. Internet membantu manusia dalam berbagai aspek kehidupan, dengan teknologi informasi proses transaksi keuangan dapat dilakukan secara transnasional secara online selama 24 jam, transaksi perdagangan dapat dilakukan dari manapun secara online.

B. Pembahasan

Internet Protocol Adress (IP Adress) merupakan adalah deretan angka biner antar 32-bit sampai 128-bit yang dipakai sebagai alamat identifikasi untuk tiap komputer host dalam jaringan Internet¹, pengalamatan perangkat (device) dalam suatu jaringan (internet) sehingga satu perangkat atau device dapat berkomunikasi dengan perangkat lainnya.

Saat ini Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik telah mengatur mengenai keabsahan transaksi elektronik, hal ini diatur dalam Pasal 1 butir 2 bahwa Transaksi elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer, dan/atau media elektronik lainnya. Transaksi bisnis online saat ini berkembang dengan sangat pesat sehingga orang dapat melakukan transaksi perbankan melalui komputer, laptop, HP, PDA atau perangkat lainnya dengan aman, hal ini berkat adanya IP Adress.

Komunikasi antar perangkat komputer ini dimungkinkan dengan adanya IP Adress perangkat komputer (device) sehingga dapat berkomunikasi satu sama lain, setiap komunikasi Internet membutuhkan adanya konektivitas IP Adress, dan dalam setiap komunikasi tersebut semua data IP Adress akan terekam dalam data web server. Setiap koneksi dan setiap aktivitas akan terekam, sehingga akan bermanfaat apabila terjadi penyalahgunaan atau kejahatan yang terkait dalam jaringan internet (cybercrime) ini akan bermanfaat apabila terjadi sesuatu hal yang tidak diinginkan, beberapa kasus kejahatan yang terjadi di Internet dapat tercatat

¹ Wikipedia, Ensiklopedia Bebas, <http://id.wikipedia.org/wiki/AlamatIP>

dengan bantuan penelusuran IP Adress.

IP address ini mempunyai peranan yang sangat penting dalam proses penelusuran kejahatan di internet (cybercrime) dan dalam hal ini Internet Service Provider memiliki data setiap aktifitas kliennya, Internet Service Provider sudah selayaknya diberikan beban pertanggungjawaban atas data aktivitas setiap kliennya.²

Transaksi Online

Internet merupakan tempat terhubungnya berbagai mesin komputer yang mengolah informasi di dunia ini, baik berupa server, personal komputer, handphone, handheld, PDA, dan lain sebagainya. Masing-masing mesin (device) ini bekerja sesuai dengan fungsinya, baik sebagai penyedia layanan yang biasa saja disebut dengan Server maupun pengguna layanan yang biasa disebut dengan Klien. Kesemuanya terhubung baik melalui kabel, saluran telepon, saluran komunikasi handphone, satelit, fiber optik, listrik, wireless serta media lain apa saja yang dapat dialiri data.

Pada mulanya jaringan Internet hanya dapat digunakan oleh lingkungan pendidikan (Perguruan Tinggi) dan lembaga penelitian kemudian tahun 1995 Internet baru dapat digunakan untuk publik, beberapa tahun kemudian Tim Berners-Lee mengembangkan aplikasi World Wide Web yang memudahkan orang untuk mengakses informasi di Internet setelah dibukanya Internet untuk keperluan publik semakin banyak muncul aplikasi-aplikasi bisnis di Internet.³

Aplikasi bisnis yang berbasis teknologi Internet mulai menunjukkan adanya aspek finansial. Misalnya Internet dipergunakan sebagai sarana untuk memesan /reservasi tiket pesawat terbang, kereta api, hotel, pembayaran tagihan telepon, listrik dan lain sebagainya.

Hal ini mempermudah konsumen dalam menjalankan aktivitas/transaksi bisnisnya. Konsumen tidak perlu keluar rumah dan antri untuk memperoleh layanan yang diinginkan karena dapat dilakukan di dalam rumah, begitu pula

² Agus Rahardjo, Kebijakan Kriminalisasi Penanganan Cybercrime di Indonesia, <http://www.unsoed.ac.id/news>

³ Budi Raharjo, Pernak-pernik Pengaturan Cyber Space di Indonesia, 2001, http://www.budi_insan.web.id

tingkat keamanannya lebih terjaga.

Transaksi ini dapat berlangsung dengan baik karena adanya pengalamatan di Internet (IP Adress) sehingga dua atau lebih perangkat (device) dapat berkomunikasi dengan baik. Dengan IP Adress ini kita dapat mengetahui lokasi dari suatu server atau sebaliknya dari sisi server kita akan mengenali darimana suatu komunikasi atau interaksi berawal. Karena setiap aksesibilitas di Internet semuanya akan terekam dalam bentuk data elektronik

Fake IP

Fake IP adalah menyembunyikan IP Adress sebenarnya dengan menggunakan IP Adress pihak lain, secara teknis sebuah komputer server atau program komputer yang dapat bertindak sebagai komputer lainnya untuk melakukan Request terhadap Content dari Internet. Fake IP ini bertindak sebagai gateway terhadap dunia Internet untuk setiap komputer klien, proxy web server yang menerima request dari proxy server akan menginterpretasikan request-request tersebut seolah-olah request itu datang secara langsung dari komputer klien bukan dari proxy sever.

Fake IP pertama dikembangkan sebagai alasan keamanan, hal ini untuk menjaga adanya serangan hacking dari pihak yang tidak bertanggung jawab ketika kita mengunjungi server-server yang tidak jelas (web server yang bersifat jahat)

Karena sering terjadi suatu web server dibuat memang untuk suatu kejahatan, antara lain mengumpulkan data-data klien yang terhubung. Sehingga diciptakan Fake IP untuk mengantisipasi hal tersebut, Fake IP bisa mengantisipasi serangan terhadap IP klien.

Pada perkembangannya penggunaan Fake IP ini ternyata bukan hanya dilakukan untuk kepentingan positif, namun juga kadang dilakukan untuk hal-hal yang negatif, antarlain menutupi data lokasi yang sebenarnya dari klien untuk melakukan akses yang terlarang seperti pengiriman Email yang terus menerus juga menyerang data server sehingga mengalami kemacetan dll.

Penggunaan Fake IP biasanya berdasarkan adanya Proxy Server sehingga

data request seolah datang dari pihak server tidak seperti dari klien, sehingga hal ini selain menciptakan faktor keamanan juga dimanfaatkan untuk kejahatan, penggunaan Fake IP untuk kejahatan antara lain *bombing Email* (pengiriman Email secara terus menerus) yang mengakibatkan kemacetan pada server atau akun Email seseorang, Akses ilegal terhadap web server, pemalsuan identitas untuk akses ilegal.

Aspek Hukum Terkait Fake IP

Penggunaan Fake IP pada awalnya untuk melindungi klien dari serangan pihak-pihak tertentu yang bertujuan mengumpulkan data dari IP klien tertentu, penggunaan IP dengan tujuan seperti hal tersebut adalah legal karena bertujuan untuk melindungi klien penggunaan fake IP untuk kepentingan perlindungan sistem elektronik dapat dilindungi dengan Pasal 32 Ayat 1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik : "Setiap orang yang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apapun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu informasi elektronik dan/atau dokumen elektronik milik orang lain atau milik publik, Jo. Pasal 34 ayat (2) tindakan sebagaimana pada ayat (1) bukan tindak pidana jika ditujukan untuk melakukan kegiatan penelitian, pengujian sistem elektronik, untuk perlindungan sistem elektronik itu sendiri secara sah dan tidak melawan hukum.

Namun keberadaan Fake IP ini dimanfaatkan oleh pihak- pihak tertentu untuk tujuan tertentu. Antara lain ketika beberapa web server perjudian melarang transaksi dari negara lain, ketika kita menggunakan Fake IP, transaksi perjudian dapat dilakukan karena data IP klien berubah.

Penggunaan Fake IP untuk menyamarkan data akses klien ketika terhubung dengan web server, hal ini bertujuan untuk menyulitkan identifikasi siapa klien yang terhubung.

Pencurian Kartu Kredit (Carding) sering menggunakan Fake IP sehingga ketika aksinya diketahui, Fake IP ini akan mempersulit proses penelusuran pelakunya, beberapa Pasal dalam Undang-Undang Nomor 11 Tahun 2008 yang

terkait dengan penyalahgunaan fake IP antara lain dalam Pasal 30 UU 11/2008.

- (1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun.
- (2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.
- (3) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

Pasal 31 UU 11/2008

- (1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain.
- (2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan.
- (3) Kecuali intersepsi sebagaimana dimaksud pada ayat (1) dan ayat (2). intersepsi yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi penegak hukum lainnya yang ditetapkan berdasarkan undang-undang.
- (4) Ketentuan lebih lanjut mengenai tata cara intersepsi sebagaimana dimaksud pada ayat (3) diatur dengan Peraturan Pemerintah.

Pasal 32 UU 11/2008

- (1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik.
- (2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak.
- (3) Terhadap perbuatan sebagaimana dimaksud pada ayat (1) yang

Mengakibatkan terbukanya suatu Informasi Elektronik dan/atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya.

Pasal 33 UU 11/2008

Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya.

Pasal 34 UU 11/2008

- (1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki:
 - a. perangkat keras atau perangkat lunak Komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33;
 - b. sandi lewat Komputer, Kode Akses, atau hal yang sejenis dengan itu yang ditujukan agar Sistem Elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33.
- (2) Tindakan sebagaimana dimaksud pada ayat (1) bukan tindak pidana jika ditujukan untuk melakukan kegiatan penelitian, pengujian Sistem Elektronik, untuk perlindungan Sistem Elektronik itu sendiri secara sah dan tidak melawan hukum.

Beberapa pasal dalam Undang-Undang Informasi dan Transaksi Elektronik tersebut dapat menjerat pelaku tindak pidana di Internet (cyber crime) yang terkait dengan penyalahgunaan Fake IP, namun tidak satupun Pasal yang mengatur khusus mengenai Fake IP ini, baik pengaturan penyelenggaraan Fake IP maupun bentuk pengaturan mengenai penyalahgunaan Fake IP.

C. Penutup

Saat ini Undang-Undang Informasi dan Transaksi Elektronik tidak mengatur secara khusus mengenai Fake IP, padahal Fake IP ini mempunyai peranan penting baik sebagai segi perlindungan suatu sistem klien, maupun dari segi penyalahgunaan Fake IP itu sendiri, yang bermanfaat untuk menyamarkan IP adress dari cybercrime.

Diperlukan pengaturan khusus mengenai Fake IP, bentuk Fake IP yang diijinkan dan larangan penyalahgunaan Fake IP, dan perlu regulasi mengenai pengelolaan Fake IP tersebut, sehingga beberapa server yang menyediakan Fake IP dapat mencatat setiap aktivitas yang tejadi dalam sistem server mereka, sehingga mempermudah proses penyelidikan ketika terjadinya cybercrime.

DAFTAR PUSTAKA

Agus Rahardjo, Kebijakan Kriminalisasi Penanganan Cybercrime di Indonesia, <http://www.unsoed.ac.id/news> Budi Raharjo, Pemak-pemik Pengaturan Cyber Space di Indonesia, 2001, http://www.budi_insan.web.id

Wikipedia, Ensiklopedia Bebas, <http://id.wikipedia.org/wiki/AlamatIP>

Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik