BAB II

ASPEK HUKUM MENGENAI MONITORING AKTIVITAS KOMPUTER DAN TINDAK PIDANA PENYADAPAN DATA PRIBADI PENGGUNA INTERNET

A. Aspek Hukum Mengenai Monitoring Aktivitas Komputer

Kebutuhan manusia terhadap internet yang semakin tinggi memunculkan produk-produk baru berupa program-program aplikasi yang berfungsi sebagai sarana yang berguna mendukung kemajuan internet tersebut. Produk-produk yang berbentuk program aplikasi merupakan hasil dari perkembangan iptek yang dibuat sebagai sarana bagi pengguna internet untuk mengakses masuk ke dalam jaringan-jaringan publik untuk mencari data, melakukan pemindahan data, dan mencari informasi.

Banyaknya jumlah pengguna internet pada saat ini menimbulkan berbagai-permasalahan-permasalahan batu yang sangat rumit dimana kejahatan dilakukan dengan menggunakan sarana internet (cybercrime). Salah satu kejahatan yang dilakukan dengan menggunakan internet yaitu penyadapant erhadap data pribadi pengguna internet, kejahatan ini dilakukan dengan tujuan untuk mencuri informasi pengguna internet.

Penyadapan pada dasarnya hanya dibolehkan bagi petugas yang berwenang dalam suatu negara guna meningkatkan pengawasan tingkat tinggi dan dilakukan sepenuhnya untuk kepentingan keamanan negara agar mampu mempertahankan dan meningkatkan kemampuan melawan tindakan

teror. Kewenangan penuh untuk menerapkan penyadapan yang sah secara hukum tersebut dikenal dengan istilah lawful interception. Objek yang disadap terdiri dari layanan komunikasi yang menggunakan atau melintasi operator jaringan (network operator), akses oprator (access operator) dan atau layanan melalui service provider. Subjek-subjekdari penyadapan yang sah secara hukum (lawful interception) diantaranya yaitu akses internet, layanan-layanan yang menggunakan internet seperti, browsig ke World Wide Web, email groups, chat dan icq, Voice over IP, (VOIP) file transfer protocol (FTP) dan segalahal yang melintasi jaringan internet.

Tindakan penyadapan berdasarkan lawful interception harus memenuhi standarisasi internasional yaitu, megacu pada dua standar yang telah diakui oleh dunia internasional diantaranya :

1. *European Telecomunications Standards Institute (ETSI) yang berbasis di Perancis,*
2. *Communications Assistance for Law Enforcement Act (Calea) yang berbasis di Amerika Serikat.*

Definisi penyadapan yang sah secara hukum menurut European Telecommunications Standards Institute (ETSI) yaitu kegiatan penyadapan dilakukan terhadap network operator, akses provider, service provider dengan tujuan agar informasi yang ada selalu siap digunakan sebagai fasilitas kontrol pelaksanaan hukum. Persyaratan yang terperinci dalam melaksanakan penyadapan berdasarkan standarisasi Eropa maupun Amerika berbeda antara satu yuridiksi dengan yuridiksi lainnya, tetapi dalam pelaksanaan penyadapan tersebut terdapat satu persayaratan umum yang

sama yaitu sistem penyadapan yang disediakan harus melaksanakan penahanan atau pemotongan sebelum sebuah pokok materi yang berupa informasi tersebut sampai ke tempat tujuan. Pemotongan pokok materi tersebut harus dilaksanakn dengan baik hingga pengirim informasi tersebut tidak sadar atau tidak terpengaruh pada saat informasi tersebut dipotong sebelum sampai ke alamat yang dituju. Untuk mendukung lawful interception, kelompok industri dan agen pemerintah masih terus mencoba menstandarisasikan pengolahan secara teknis dibelakang pemotongan tersebut. Hal ini berlaku tidak hanya di eropa tetapi diseluruh negara. Teknik implementasi penyadapan dilakukan dengan beberapa metode diantaranya yaitu penyadapan aktif, yaitu penyadapan yang dilakukan secara langsung, penyadapan semi aktif, dan penyadapan pasif tetapi secara teknis, kebanyakan penyadapan yang dilakukan adalah dengan mengimpelementasikan penggabungan teknis aktif dan pasif[10].

Pengaturan mengenai penyadapan di Indonesia pada dasarnya telah memiliki sejarah yang cukup panjang. Pada masa Kolonial Belanda kewenangan mengenai penyadapan telah diatur yaitu, berdasarkan keputusan Raja Belanda Tanggal 25 Juli 1893 No. 36, pengaturan mengenai penyadapan informasi dibatasi yaitu hanya digunakan pada lalu lintas surat di kantor pos seluruh Indonesia (Mail Interception). Keputusan Raja Belanda Tanggal 25 Juli 1893 tersebut dapat dianggap sebagai peraturan tertua di Indonesia.

---

[10]*Handover Interface for the Lawful Interception of Telecommunication Traffic, http//www.kapanlagi.com, diakses pada taggal 25 April 2010, pukul 09:04 WIB*

Ditinjau dari perkembangannya saat ini, terkait dengan kewenangan khusus aparat negara untuk melakukan penyadapan komunikasi diatur dalam sejumlah undang-undang diantaranya yaitu Undang-Undang Pisikotropika, Undang-Undang Telekomunikasi, Undang-Undang Pemberantasan Tindak Pidana Terorisme, Undang-Undang Informasi dan Transaksi elektronik. Kemudian penerapan penyadapan yang sah secara hukumatau lawful interception di indonesia pada saat ini dilakukan oleh pemerintah dengan berdasarkan pada Peraturan Mentri Komunikasi dan Informatika Nomor 11/PERM.KOMINFO/02/2006, tanggal 22 Februari 2006 Tentang Teknis Penyadapan Terhadap Informasi.

Walaupun penyadapan telah diatur secara khusus dalam berbagai peraturan perundang-undangan, tetapi kewenangan penyadapan di indonesia pada dasarnya masih jauh dari standar yang memadai dalam hal melindungi hak asasi manusia terkait hak privasi dalam penegakan hukum karena pada intinya, penyadapan informasi adalah aktivitas yang bertentangan dengan kebebasan privasi individu.

Seiring perkembangan internet yang sangat pesat, penyadapan data pada jaringan komputer dengan cara memantau data yang bergerak keluar masuk dalam jaringan komputer tidak hanya dilakukuan oleh aparat yang berwenang, tetapi banyak pengguna internet melakukan aktivitas penyadapan dengan tujuan untuk mencuri informasi dari pengguna internet. Monitoring aktivitas komputer biasanya dilakukan oleh orang yang mengetahui dan sangat paham tentang ruang lingkup internet atau biasa disebut sebagai ahli internet.

Program aplikasi monitoring aktivitas komputer pada saat ini sangat mudah didapatkan melalui jaringan internet dengan cara men-download nya di internet. Walaupun cara menjalankan program tersebut cukup sulit bagi seseorang yang kurang paham atau awam terhadap ruang lingkup komputer, tetapi dengan kemudahan untuk mendapatkan program aplikasi tersebut akan menimbulkan dampak negatif bagi kemajuan teknologi dimana seseorang dapat mempelajari program monitoring aktivitas komputer tersebut dengan tujuan untuk menyadap data pribadi pengguna internet atau penguna komputer yang terhubung dalam suatu jaringan.

Penyadapan data dalam jaringan komputer terjadi akibat kurangnya sistem keamanan pada sebuah komputer yang terhubung dengan jaringan atau ketidaktahuan masyarakat awam mengenai ruang lingkup jaringan komputer. Biasanya korban dalam hal ini para pengguna internet tidak sadar bahwa pada saat mengakses internet ada seseorang yang sedang menyadapnya[11]*.*

Pentingnya nilai sebuah informasi menyebabkan seringkali informasi yang diinginkan hanya boleh diakses oleh orang-orang tertentu. Jatuhnya informasi ke tangan pihak lain, misalnya pihak lawan bisnis dapat menimbulkan kerugian bagi pemilik informasi tersebut[12]*. Salah satu tujuan seseorang yang tidak berkepentingan dalam menggunakan program monitoring aktivitas komputer yaitu untuk mendapatkan informasi secara melawan hukum untuk kepentingan pribadinya.*

---

[11] *Neonmap, Active Sniffing Detector (ARP Spoofing) With Artifical Neural Network Method, http//www.jasakom.com, diakses pada tanggal 08 Mei 2010, pukul 23:43 WIB*

[12] *Missa Lamsani, Op.Cit, Komunikasi Data*

Metode penyadapan data pribadi pengguna internet yang dilakukan secara melawan hukum oleh pihakl yang tidak berkepentingan atas sebuah informasi hampir sama dengan metode lawful interception yang dilakukan oleh aparat yang berwenang terdiri dari beberapa metode diantaranya :

1. *Penyadapan dengan menggunakan program monitoring aktivitas komputer pasif atau biasa disebut dengan program passive sniffing, dimana penyadapan terhadap data pribadi pengguna internet tanpa mengubah data atau paket apapun dalam suatu jaringan. Program passive sniffing tersebut hanya memantau paket data yang bergerak keluar masuk dalam jaringan.*
2. *Penyadapan dengan menggunakan program monitoring aktivitas komputer aktif atau biasa disebut juga dengan program active sniffing, yaitu dimana dengan menggunakan program active sniffing yang merupakan suatu program aktivitas monitoring komputer yang lebih canggih dari passive sniffing, penyadapan dilakukan tidak hanya memantau data yang bergerak dalam suatu jaringan tetapi program tersebut dapat membelokan data dari komputer korban ke komputer pelaku penyadapan tersebut sehingga pelaku penyadapan dapat mengetahui seluruh aktivitas yang dilakukuan oleh pengguna komputer pada suatu jaringan atau penggguna internet, kemudian dengan program active sniffing, pelaku juga dapat mengontrol komputer korban sehingga komputer korban tersebut dapat digerakan oleh pelaku*[13]*.*

[13]*Neonmap, OP.Cit, Active sniffing Detector (ARP Spoofing) With Artifical Neural Network Method*

Kenyataanya masih sedikit solusi yang dapat dilakukan dengan tepat untuk mendeteksi maupun untuk mencegah aktifitas penyadapan dengan menggunakan program monitoring aktifitas komputer ini. Pelaku biasanya melakukan penyadapan di tempat-tempat rawan, misalnya seorang karyawan melakukan penyadapan data pribadi di perusahaan tempat dia bekerja, atau seorang pengunjung warnet melakukan penyadapan untuk mencuri data pribadi seseorang yaitu untuk mencuri password dan username seseorang dalam internet bahkan pelaku juga biasanya melakukan penyadapan untuk mencuri data transaksi bank melalui kartu kredit. Akibatnya tingkat kejahatan dunia maya atau biasa disebut dengan cybercrime semakin meningkat dan merugikan banyak pihak.

Wewenang untuk melakukan penyadapan oleh aparat tertentu di negara-negara maju digunakan haya terbatas untuk mencegah dan mendeteksi kejahatan-kejahatan yang sangat serius dengan syarat :

1. *Dipergunakan karena metode investigasi kriminal lainnya telah mengalami kegagalan,*
2. *Tidak adanya cara lain yang dapat digunakan selain penyadapan untuk mendapatkan informasi yang dibutuhkan, dan*
3. *Penyadapan dilakuan dengan alasan yang cukup kuat dan diperaya bahwa dengan penyadapan maka bukti-bukti baru akan ditemukan dan dapat digunakan untuk menghukum pelaku pidana yang dituju.*

Selain itu, di beberapa negarapenyadapan dapat juga dilakukan dengan dasar yaitu menyangkut kepentingan khusus bagi keamanan negara (interest of national security) dan digunakan untuk menjaga keamanan dan stabilitas ekonomi negara. Ketentuan pembatasan penyadapan bagi aparat negara di berbagai dunia juga sudah sangat berkembang. Penyadapan hanya dapat digunakan dalam kondisi dan prasyarat yang khusus contohnya:

1. *Adanya otoritas resmi yang jelas berdasarkan Undang-Undang yang memberikan izin penyadapan 9mencakup tujuan yang jelas dan objektif),*
2. *Adanya jaminan jangka waktu yang pastidalam melakukan penyadapan,*
3. *Pembatasan penanganan materi hasil penyadapan,*
4. *Pembatasan mengenai orang yang dapat mengakses penyadapan dan pembatasan-pembatasan lainnya.*

Pembatasan-pembatasan itu sangat eperlu dilakukan karena penyadapan berbatasan langsung dengan perlindungan hak pribadi seseorang. Konvensi Hak Sipil Politik telah memberikan hak bagi setiap orang untuk dilindungi dari campur tangan seseorang dengan sewenang-wenang atau secara tidak sah dalam masalah pribadi, keluarga, rumah tangga atau surat menyuratnya (korespondensinya)..

B. Ketentuan Hukum Mengenai Tindak Pidana Penyadapan Data Pribadi Pengguna Internet

Monitoring aktivitas komputer yang merupakan suatu kegiatan untuk memantau paket data yang terdapat dalam jaringan komputer, dengan menggunakan suatu program aplikasi komputer (software), sehingga paket data yang berupa kode-kode yang bergerak keluar-masuk dalam suatu

jaringan milik seseorang pengguna internet dapat dilihat oleh seseorang yang tidak berkepentingan, kemudian kode-kode tersebut yang merupakan data pribadi seseorang pengguna internet dapat diterjemahkan kembali sehingga seseorang yang tidak berkepentingan tersebut dapat membaca data pribadi pengguna internet tersebut, maka kegiatan itu dapat dikategorikan sebagai suatu penyadapan karena data milik pengguna internet yang bersifat pribadi yang dikirimkan oleh pengguna internet melalui jaringan komputer dapat diketahui oleh pihak yang tidak berkepentingan.

Ketentuan mengenai penyadapan di Indonesia telah diatur dalam berbagai perundang-undangan. Pasal 40 Undang-Undang Nomor 36 tahun 1999 tentang Telekomunikasi menyebutkan,

> *"setiap orang dilarang melakukan kegiatan penyadapan atas informasi yang disalurkan melalui jaringan telekomunikasi dalam bentuk apapun".*

Dari penjelasan Pasal 40 Undang-Undang Nomor 36 tahun 1999 tentang Telekomunikasi tersebut telah menyatakan secara tegas mengenai pelarangan terhadap setiap orang dalam kegiatan penyadapan atas informasi yang disalurkan melalui jaringan telekomunikasi dalam bentuk apapun. Apabila dijabarkan Pasal 40 Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi tersebut memuat unsur-unsur sebagai berikut :

1. *Setiap orang*
2. *Penyadapan atas informasi*
3. *Dalam bentuk apapun*

Unsur setiap orang dalam ketentuan pasal tersebut menegaskan bahwa tidak terkecuali siapapun, setiap orang tidak diperkenankan untuk melakukan penyadapan. Unsur penyadapan atas informasi yaitu bahwa segala bentuk informasi yang terdapat dalam jaringan telekomunikasi yang meliputi data-data yang berbentuk dokumen elektronik milik orang lain yang bersifat pribadi. Kemudian unsur dalam bentuk apapun yaitu bahwa seluruh informasi melalui jaringan telekomunikasi yang meliputi data-data yang berbentuk apapun yang meliputi dokumen elektronik milik orang lain sehingga diketahui oleh seseorang yang tidak berkepentingan. Maka berdasarkan unsur dari Pasal tersebut diatas, tidak diperkenankan bagi setiap orang tidak terkecuali siapapun untuk melakukan penyadapan informasi melalui jaringan telekomunikasi sehingga informasi yang meliputi data-data yang berbentuk dokumen elektronik tersebut diketahui oleh pihak yang tidak berkepentingan dengan cara apapun.

Monitoring aktivitas komputer yang merupakan kegiatan seseorang untuk memantau data pribadi pengguna internet yang bergerak dalam suatu jaringan komputer telah memenuhi unsur-unsur dari pasal 40 Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi, dimana seseorang yang tidak berkepentingan dengan menggunakan suatu software dapat menyadap data pribadi milik pengguna internet untuk mendapatkan suatu informasi pribadi orang lain dalam hal ini informasi dari pengguna internet.

Selanjutnya dalam pasal 56 Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi menegaskan,

“Barang siapa melanggar ketentuan sebagaimana dimaksud Pasal 40, dipidana dengan pidana penjara paling lama 15 (lima belas) tahun”.

Sebagai perbuatan pidana, penyadapan dapat dipahami mengingat ketentuan dalam konstitusi yang menyatakan setiap orang berhak untuk berkomunikasi dan mendapat informasi untuk mengembangkan pribadi dan lingkungan sosialnya, serta berhak mencari, memperoleh, memiliki, menyimpan, mengolah, dan menyampaikan informasi dengan menggunakan segala jenis saluran yang ada sebagaimana diatur dalam Pasal 28F UUD 1945. Demikian pula Pasal 28G Ayat (1) UUD 1945 menyatakan, setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang ada di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi.

Dalam pengungkapan suatu tindak pidana, pada dasarnya tidak dibenarkan melakukan penyadapan. Hal ini terkait bewijsvoering dalam hukum pembuktian. Secara harfiah bewijsvoering berarti penguraian cara bagaimana menyampaikan alat-alat bukti kepada hakim di pengadilan. Bagi negara-negara yang cenderung menggunakan due process of law dalam sistem peradilan pidana, bewijsvoering atau penguraian bagaimana menyampaikan alat-alat bukti kepada hakim di pengadilan sangat mendapatkan perhatian. Dalam due process of law, negara menjunjung tinggi hak asasi manusia, dalam hal ini hak-hak tersangka sehingga sering seorang tersangka dibebaskan oleh pengadilan dalam pemeriksaan praperadilan karena alat bukti diperoleh dengan cara tidak sah atau disebut juga dengan

istilah unlawful legal evidence. Bewijsvoering lebih menitikberatkan pada hal-hal formalistis saja sehingga Konsekuensinya fakta dan kebenaran yang ada terkesampingkan. Dalam perkembangannya, terhadap bijzondere delicten atau delik-delik khusus yang diatur di luar Kitab Undang-undang Hukum Pidana, penyadapan boleh dilakukan dalam rangka mengungkap kejahatan. Pertimbangannya, aneka kejahatan itu biasanya dilakukan terorganisasi dan sulit pembuktiannya. Dari sudut konstitusi, penyadapan guna mengungkap suatu kejahatan, sebagai suatu pengecualian, dapat dibenarkan. Hal ini karena kebebasan untuk berkomunikasi dan mendapat informasi sebagaimana diatur dalam Pasal 28F dan Pasal 28G Ayat (1) UUD 1945 bukan pasal-pasal yang tak dapat disimpangi dalam keadaan apa pun. Artinya, penyadapan boleh dilakukan dalam rangka mengungkap kejahatan atas dasar ketentuan undang-undang yang bersifat khusus (lex specialis derogat legi generali)[14]*.*

Pasal 31 ayat (1) Undang-Undang nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang menyatakan bahwa :

> *"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".*

Intersepsi atau penyadapan menurut pasal 31 ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik tersebut adalah kegiatan untuk mendengarkan, merekam, membelokkan,

---

[14]*Eddy OS Hiariej, Penyadapan Dalam Hukum Pidana, http//www.antikorupsi.org, Diakses pada tanggal 7 Mei 2010 pukul 09:05 WIB*

mengubah, menghambat, dan/atau mencatat transmisi informasi elektronik dan/atau dokumen elektronik yang tidak bersifat publik. Bunyi penjelasan tersebut menegaskan bahwa kegiatan penyadapan yang dilarang itu adalah jika ditujukan bukan untuk kepentingan publik atau ditujukan untuk kepentingan pribadi atau perseorangan.

Maksud daripada penyadapan yang ditujukan untuk kepentingan pribadi menurut Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik di atas yaitu dimana seseorang dengan cara apapun melakukan pengambilan data milik orang lain untuk dimiliki tanpa seizin pemilik informasi atau dokumen tersebut, baik dengan cara mendengarkan, merekam, membelokkan, mengubah, menghambat dan/atau mencatat transmisi informasi elektronik atau dokumen elektronik dengan menggunakan sarana apapun. Sarana tersebut dapat berupa suatu alat yang berbentuk perangkat keras maupun suatu program atau perangkat lunak yang dapat memungkinkan alat tersebut untuk mengambil atau menyadap suatu informasi elektronik atau dokumen elektronik milik orang lain.

Sesuai dengan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Eleketronik BAB XI mengenai Ketentuan Pidana dalam Pasal 47 dijelaskan,

> *"Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam pasal 31 ayat (1) atau ayat (2) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp. 800.000.000,00 (delapan ratus juta rupiah)".*

Isi pasal 47 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik telah jelas menyebutkan mengenai ketentuan pidana bagi setiap orang yang melakukan penyadapan dalam bentuk apapun yang menyebabkan bocornya suatu infromasi pribadi seseorang atau tercurinya dokumen elektronik atau informasi elektronik seseorang, maka akan dipidana dengan hukuman berupa hukuman penjara paling lama 10 tahun atau hukuman berupa denda paling banyak sebesar Rp. 800.000.000,00 (delapan ratus juta rupiah).