BAB IV

ANALISIS HUKUM TENTANG PENYADAPAN DATA PRIBADI PENGGUNA INTERNET MELALUI MONITORING AKTIVITAS KOMPUTER DIHUBUNGKAN DENGAN UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK

A. Ketentuan Hukum Mengenai Penyadapan Data Pribadi Pengguna Internet Melalui Monitoring Aktivitas Komputer Berdasarkan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

Perkembangan teknologi informasi yang sangat pesat di Indonesia, menuntut masyarakat untuk dapat menyesuaikan diri dengan perubahan-perubahan yang terjadi sebagai dampak dari kemajuan teknologi informasi tersebut. Teknologi informasi dan komunikasi telah mengubah perilaku dan pola hidup masyarakat secara global, perkembangan teknologi informasi telah pula menyebabkan dunia menjadi tanpa batas (bordeless) dan menyebabkan perubahan sosial budaya, ekonomi dan pola penegakan hukum yang secara signifikan berlangsung demikian cepat. Teknologi informasi saat ini menjadi pedang bermata dua karena disalah satu sisi teknologi informasi tersebut telah memberikan kontribusi bagi peningkatan kesejahteraan kemajuan dan peradaban manusia, sedangkan disisi lainnya

teknologi informasi juga menjadi sarana yang sangat efektif untuk melakukan perbuatan melawan hukum.

Banyaknya penyedia internet dan semakin terjangkaunya biaya untuk mengakses internet pada saat ini menimbulkan banyak terjadi penyalahgunaan sarana internet oleh seseorang yang tidak bertanggung jawab dimana internet dijadikan sebagai sarana untuk menguntungkan diri sendiri tanpa menghiraukan batas-batas hak orang lain. Salah satu penyalahgunaan yang terjadi yaitu penyadapan data pribadi pengguna internet melalui monitoring aktivitas komputer. Penyadapan data pribadi pengguna internet dengan menggunakan program monitoring aktivitas komputer itu sendiri adalah perbuatan seseorang dengan menggunakan software khusus yang diaplikasikan pada komputer yang terhubung dengan internet, sehingga komputer itu dapat memantau aktivitas seseorang yang sedang menggunakan internet, dengan tujuan untuk mendapatkan data pribadi pengguna internet diantaranya username dan password dari akun pribadi seseorang dalam internet.

Pada dasarnya setiap kegiatan atau aktivitas manusia dapat diatur oleh hukum. Hukum dipersempit pengertiannya menjadi peraturan perundang-undangan yang dibuat oleh negara, begitu pula aktivitas kejahatan mayantara yang menjadikan internet sebagai sarana utamanya. Dalam kaitan dengan teknologi informasi khususnya dunia maya, peran hukum adalah melindungi pihak-pihak yang lemah terhadap eksploitasi dari pihak yang kuat atau berniat jahat, disamping itu hukum dapat pula mencegah dampak negatif dari ditemukannya suatu teknologi baru.

Kekhawatiran akan kejahatan mayantara di dunia sebetulnya telah dibahas secara khusus dalam suatu lokakarya yang diorganisir oleh United Nations Asia and Far East Institute (UNAFEI) pada kongres PBB X/2000, dengan tema workshop on crimes to computer networks. Adapun kesimpulan dari lokakarya tersebut adalah sebagai berikut :

a. *CRC (computer related crime) harus di kriminalisasikan,*
b. *Diperlukan hukum acara yang tepat untuk melakukan penyidikan dan penuntutan terhadap penjahat siber (Cybercrimes),*
c. *Harus ada kerjasama antara pemerintah dan industri terhadap tujuan umum pencegahan dan penaggulangan kejahatan komputer agar internet menjadi tempat yang aman,*
d. *Diperlukan kerja sama internasional untuk menelusuri atau mencari para penjahat di internet,*
e. *PBB harus mengambil langkah serta tindak lanjut yang berhubungan dengan bantuan dan kerjasama teknis dalam penanggulangan CRC.*

Berdasarkan uraian di atas diketahui bahwa sebenarnya cybercrime khususnya kejahatan hacking adalah sebuah isu hukum internasional. Perbedaannya adalah di beberapa negara anggota PBB sudah meratifikasi hasil kongres internasional mengenai kejahatan ini dalam sebuah regulasi peraturan perundang-undangan secara khusus, sedangkan di Indonesia pengaturan khusus mengenai kejahatan tersebut telah ditetapkan menjadi undang-undang pada tanggal 25 Maret 2008 yaitu Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE).

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik itu sendiri disusun sedemikian rupa sebagai upaya pemerintah dalam pengakuan transaksi elektronik dan dokumen elektronik dalam kerangka hukum perikatan dan hukum pembuktian, sehingga kepastian hukum transaksi elektronik dapat terjamin, kemudian sebagai bentuk dari upaya penegakan hukum menyangkut tindakan-tindakan yang termasuk kualifikasi pelanggaran hukum terkait penyalahgunaan teknologi informasi disertai sanksi pidananya termasuk untuk tindakan carding, hacking dan cracking.

Pengaturan yang menyangkut intersepsi atau penyadapan tertuang dalam Pasal 31 ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) tersebut, yaitu :

> *"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."*

Pasal tersebut diatas merupakan landasan hukum atau perlindungan hukum bagi para pengguna internet dari tindakan penyadapan yang dilakukan oleh seseorang yang dengan sengaja dan tanpa hak untuk mengakses masuk terhadap informasi elektronik atau dokumen elektronik pribadi milik orang lain secara melawan hukum. Dalam aksinya, pelaku mempunyai tujuan tertentu contohnya yaitu untuk mendapatkan informasi rahasia pengguna internet seperti username dan password akun pengguna internet.

Terdapat beberapa unsur yang terkandung dalam Pasal 31 ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) tersebut diantaranya yaitu :

1. *Setiap orang*
2. *Dengan sengaja*
3. *Tanpa hak atau melawan hukum atau (wederrechtelijk).*
4. *Melakukan intersepsi atau penyadapan*
5. *Atas informasi elektronik dan/atau dokumen elektronik dalam satu komputer dan/atau sistem elektronik tertentu milik orang lain.*

Penyadapan data pribadi pengguna internet yang dilakukan seseorang yang biasa disebut dengan sniffer merupakan suatu kesengajaan dari seseorang yang tidak mempunyai hak dengan maksud untuk menguntungkan diri sendiri. Kata dengan maksud atau met het oogmerk itu harus diartikan sebagai maksud dari pelaku untuk menguntungkan diri sendiri atau orang lain secara melawan hukum atau wederrechtelijk. Unsur menguntungkan diri sendiri atau orang lain secara melawan hukum mengandung arti bahwa keuntungan yang diperoleh dan cara memperoleh keuntungan tersebut bersifat bertentangan dengan kepatutan dalam pergaulan masyarakat.

Unsur lain dari tindakan penyadapan data pribadi pengguna internet adalah setiap orang, kata setiap orang menunjukkan siapa saja orang yang apabila orang tersebut memenuhi semua unsur dari tindakan penyadapan secara sengaja dan tanpa hak, maka ia dapat disebut pelaku penyadapan atau sniffer.

Selain itu, unsur yang juga terdapat dalam pasal penyadapan yaitu melakukan intersepsi atau penyadapan. Yang dimaksud dengan intersepsi atau penyadapan adalah kegiatan untuk mendengarkan, merekam, membelokkan, mengubah, menghambat, dan/atau mencatat transmisi Informasi elektronik dan/atau dokumen elektronik yang tidak bersifat publik, baik menggunakan jaringan kabel komunikasi maupun jaringan nirkabel, seperti pancaran elektromagnetis atau radio frekuensi.

Dalam penyadapan data pribadi pengguna internet yang dilakukan dengan menggunakan program monitoring aktivitas komputer pelaku atau sniffer melakukan penyadapan dengan cara membelokkan transmisi informasi elektronik dan/atau dokumen elektronik.

Unsur yang juga terdapat didalam pasal penyadapan antara lain informasi elektronik dan/atau dokumen elektronik dalam satu komputer dan/atau sistem elektronik tertentu milik orang lain, yaitu satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, electronic data interchange (EDI), surat elektronik (electronic mail), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.

Umumnya pelaku penyadapan atau sniffer melakukan penyadapan untuk memperoleh data pribadi pengguna internet seperti username dan password berupa kode PIN (personal identification number) pengguna internet yang kemudian untuk seterusnya username dan password tersebut digunakan untuk mengakses masuk akun pribadi pengguna internet dalam

suatu situs tertentu dalam internet. Username dan password tersebut merupakan suatu bentuk dari informasi elektronik atau dokumen elektronik dimana username dan password berbentuk suatu tulisan terdiri dari huruf, tanda, angka, atau kode akses yang telah diolah dan memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.

Berdasarkan rumusan unsur-unsur diatas, maka perbuatan yang dilakukan oleh sniffer sudah memenuhi unsur obyektif dan unsur subjektif sebagaimana yang terdapat dalam pasal 31 ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE). Dengan demikian, pasal 31 ayat (1) Undang-Undang nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) dapat diterapkan terhadap tindak pidana penyadapan data pribadi pengguna internet melalui monitoring aktivitas komputer.

Selanjutnya dalam Pasal 31 ayat (2) Undang-Undang nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik ditegaskan :

> *“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."*

Pasal 31 ayat (2) tersebut menegaskan untuk melarang siapa saja yang secara sengaja dan tanpa hak untuk melakukan intersepsi atau penyadapan atas transmisi informasi elektronik atau dokumen elektronik yang tidak bersifat publik. Tidak bersifat publik disini mengandung arti yaitu

pribadi dalam arti informasi elektronik atau dokumen elektronik tersebut milik pribadi orang lain.

Intersepsi yang dilakukan baik menyebabkan adanya perubahan, penghilangan maupun penghentian informasi atau dokumen elektronik yang sedang ditransmisikan, mempunyai maksud yaitu, menegaskan bahwa intersepsi atau penyadapan yang dilakukan dalam bentuk apapun maka intersepsi atau penyadapan tersebut sudah bertentangan dengan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, khususnya pasal 31 ayat (2) yang selanjutnya bagi pelaku akan dikenakan sanksi pidana sesuai dengan ketentuan pidana yang telah di atur dalam Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik tersebut.

Sanksi pidana yang berkaitan dengan Intersepsi atau penyadapan, diatur dalam BAB XI Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik mengenai ketentuan pidana yaitu pasal 47, yang menyatakan :

> *"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)."*

Seseorang yang telah melakukan intersepsi atau penyadapan, dalam hal ini penyadapan data pribadi pengguna internet dengan menggunakan program monitoring aktivitas komputer yang merupakan perbuatan seseorang dengan tanpa hak dan secara melawan hukum karena telah

melewati batas-batas wilayah pribadi orang lain untuk memperoleh data pribadi orang lain seperti password dan username akun seseorang dalam suatu situs internet maka sangat relevan untuk dikenakan sanksi sesuai dengan sanksi pidana yang telah tercantum dalam BAB XI Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik mengenai ketentuan pidana khususnya pada pasal 47 tersebut.

Korban yang mengalami kerugian atas tindakan penyadapan khususnya penyadapan data pribadi pengguna internet dengan menggunakan program monitoring aktivitas komputer yang umumnya merupakan pengguna internet dapat pula melakukan tindakan hukum terhadap pelaku penyadapan atau sniffer tersebut dengan menempuh proses hukum melalui lembaga peradilan umum secara perdata, yaitu berdasarkan pada Pasal 1365 BW dimana penyadapan data pribadi pengguna internet dengan menggunakan program monitoring aktivitas komputer tersebut merupakan perbuatan yang dapat dikategorikan sebagai Perbuatan Melawan Hukum (Onrechtmatigedaad) sebagaimana ditentukan dalam Pasal 1365 BW yang menyatakan bahwa:

> *"Tiap perbuatan melanggar hukum, yang membawa kerugian kepada seorang lain, mewajibkan orang yang karena salahnya menerbitkan kerugian itu, mengganti kerugian tersebut."*

Berdasarkan isi pasal diatas, suatu perbuatan dapat dianggap perbuatan melawan hukum bilamana memenuhi unsur-unsurnya, dimana unsur-unsur tersebut yaitu :

1. *Perbuatan melanggar hukum,*

2. *Unsur kesalahan (ada sebuah niat);*
3. *Adanya kerugian (kerugian materil),*
4. *Hubungan sebab akibat/kausal antara point 1,2 dan 3.*

Berdasarkan Pasal 1365 BW tersebut, dalam kegiatan yang terjadi di dunia internet, perbuatan melawan hukum mungkin dapat terjadi selama memenuhi unsur-unsur yang terdapat dalam pasal diatas. Jadi, selama unsur-unsur tersebut tidak terpenuhi, maka suatu perbuatan tidak dapat dikategorikan sebagai perbuatan melawan hukum. Dimana dalam hal ini pelaku penyadapan atau sniffer tersebut telah memenuhi unsur-unsur tersebut.

Penerapan ketentuan pasal 1365 termaksud dilakukan dengan cara melakukan penafsiran hukum ekstensif yaitu memperluas arti kata perbuatan melawan hukum itu sendiri, tidak hanya yang terjadi dalam dunia nyata, tetapi juga dimungkinkan perbuatan melawan hukum yang terjadi di dunia maya, dalam hal ini intersepsi atau penyadapan data pribadi pengguna internet dengan menggunakan program monitoring aktivitas komputer. Selain itu, dapat pula diterapkan Pasal 1365 BW dengan melakukan konstruksi hukum analogi yaitu dengan cara membandingkan antara perbuatan melawan hukum yang dilakukan di dunia nyata dengan dunia maya, sehingga pada akhirnya unsur-unsur perbuatan melawan hukum sebagaimana disyaratkan tetap dapat terpenuhi. Walaupun pada prakteknya muncul kesulitan-kesulitan dalam penerapannya, namun tetap diharapkan perbuatan melawan hukum yang terjadi harus tetap mendapat sanksi secara hukum sehingga tidak ada kekosongan hukum.

Suatu perbuatan dapat dikatakan perbuatan melawan hukum apabila perbuatan tersebut memang melanggar peraturan perundang-undangan, bertentangan dengan kesusilaan dan ketertiban umum. Meskipun demikian, suatu perbuatan yang telah dikategorikan sebagai perbuatan melawan hukum ini harus dapat dipertanggungjawabkan apakah mengandung unsur kesalahan atau tidak.

Pasal 1365 BW tidak membedakan kesalahan dalam bentuk kesengajaan (opzet-dolus) dan kesalahan dalam bentuk kurang hati-hati (culpa), dengan demikian hakim harus dapat menilai dan mempertimbangkan berat ringannya kesalahan yang dilakukan sesorang dalam hubungannnya dengan perbuatan melawan hukum ini, sehingga dapat ditentukan ganti kerugian yang seadil-adilnya.

Adapun perbuatan yang dianggap sebagai perbuatan melawan hukum, namun tidak dapat dituntut sebagai perbuatan melawan hukum, yaitu apabila perbuatan tersebut dilakukan dalam keadaan darurat, keadaan memaksa (overmacht), karena perintah kepegawaian atau salah sangka yang dapat dimaafkan. Namun dalam hal ini, pengecualian tersebut tidak berlaku bagi pelaku karena pelaku melakukannya dengan sengaja untuk mencari keuntungan. Apabila unsur kesalahan dalam suatu perbuatan melawan hukum dapat dibuktikan, maka ia bertanggung jawab atas kerugian yang disebabkan perbuatannya tersebut.

Perbuatan melawan hukum sebagaimana diatur dalam Pasal 1365 BW ini dapat digunakan sebagai dasar untuk mengajukan ganti kerugian atas perbuatan yang dianggap melawan hukum karena telah menyebabkan

kerugian kepada pengguna internet baik kerugian secara materiil maupun immaterial.

B. Kendala-Kendala Yang Dihadapi Dalam Proses Penegakan Hukum Atas Penyadapan Data Pribadi Pengguna Internet Melalui Monitoring Aktivitas Komputer

Semakin tingginya kejahatan dengan menggunakan media internet sebagai sarananya pada saat ini yang meliputi berbagai jenis kejahatan contohnya yaitu penipuan kartu kredit, penipuan perbankan, defacing, cracking, transaksi seks, judi online dan terorisme dengan korban yang sudah melintasi batas-batas teritorial dari suatu wilayah negara pada saat ini, merupakan salah satu permasalahan yang cukup rumit yang harus dihadapi oleh aparat penegak hukum dalam suatu wilayah negara.

Salah satu upaya pemerintah dalam menekan tingkat kejahatan dunia maya atau cybercrime tersebut yaitu dengan menyusun dan mengesahkan suatu peraturan perundang-undangan yang secara khusus mengatur mengenai kejahatan dunia maya atau cybercrime yang termasuk di dalamnya membahas mengenai intersepsi atau penyadapan, dalam hal ini penyadapan data pribadi pengguna internet melalui monitoring aktivitas komputer yang merupakan salah satu bentuk dari cybercrime.

Indoneisa sendiri yang merupakan salah satu negara dengan tingkat cybercrime yang cukup tinggi telah mengesahkan suatu peraturan perundang-undangan yang secara khusus mengatur mengenai seluruh kegiatan dalam dunia maya khususnya bagi permasalahan yang menyangkut cybercrime yaitu Undang-Undang Nomor 11 Tahun 2008 tentang Informasi

dan Transaksi Elektronik. Meskipun tidak mencakup semua aktivitas di dunia maya, namun dengan adanya Undang-Undang Informasi dan Transaksi Elektronik dirasa membawa angin segar bagi para penegak hukum khususnya Polri dalam menghadang laju kejahatan yang dilakukan para cracker yang semakin banyak muncul di dunia siber (cyberspace).

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik ini mempunyai 13 (tiga belas) bab dan 54 (lima puluh empat) pasal di dalamnya yang mengatur berbagai kegiatan dunia siber serta menerapkan azas-azas diantaranya yaitu Azas Ekstra Teritorial, Azas Kepasatian Hukum, Azas Manfaat, Azas Kehati-hatian, Azas Itikad Baik dan Azas Netral Teknologi. Tetapi, Lahirnya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik ini belum didukung dengan peraturan yang mengatur tentang hukum formilnya.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik mengacu pada prinsip pengaturan dengan metode sintesis hukum materiil dan lex informatica. Yaitu strategi pembentukan pengaturan dalam Undang-Undang Informasi dan Transaksi Elektronik tersebut dilakukan dengan cara menetapkan prinsip-prinsip pembentukan dan pengembangan teknologi informasi, yang isinya antara lain sebagai berikut:

1. *Mengikuti keunikan cyberspace;*
2. *Melibatkan unsur-unsur masyarakat, pemerintah, swasta dan profesional serta perguruan tinggi;*
3. *Mendorong peran sektor swasta;*

4. *Mendorong peran masyarakat, swasta, pemerintah, kelompok profesi dan perguruan tinggi;*
5. *Peran dan tanggung jawab pemerintah terhadap kepentingan publik;*
6. *Aturan hukum yang bersifat preventif, direktif dan futuristik yang tidak bersifat restriktif;*
7. *Mendorong harmonisasi dan uniformitas hukum regional dan internasional; dan*
8. *Melakukan pengkajian terhadap peraturan yang berkaitan langsung atau tidak langsung dengan munculnya persoalan-persoalan hukum akibat perkembangan teknologi informasi.*

Dalam upaya pelaksanaan penegakan hukum menyangkut permasalahan cybercrime yang mengacu pada Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, diserahkan kepada institusi Polri sebagai pihak yang berwenang dalam proses penyidikan.

Dalam proses beracara, aparat penegak hukum yang berwenang untuk melaksanakan pengadilan masih banyak menemui kendala dalam mengajukan pelaku kejahatan cybercrime karena peraturan perundang-undangan mengenai proses beracara masih mengacu pada hukum formil lama yang berlaku di Indonesia yaitu mengacu pada KUHAP. Salah satu jalan yang ditempuh oleh aparat penegak hukum dalam melaksanakan pengadilan yang menyangkut cybercrime adalah dengan mengakomodir undang-undang yang ada dengan melakukan perluasan makna yang tercantum dalam pasal-pasal perundang-undangan yang ada yaitu dengan

Undang-Undang Nomor 8 Tahun 1981 tentang Kitab Undang-Undang Hukum Acara Pidana.

Pasal 183 KUHAP menyatakan bahwa hakim tidak boleh menjatuhkan pidana kepada seseorang kecuali dengan sekurang-kurangnya dua alat bukti yang sah sehingga hakim memperoleh keyakinan bahwa suatu tindak pidana benar-benar terjadi dan bahwa terdakwalah yang bersalah melakukannya. Berdasarkan Pasal 183 KUHAP tersebut dapat diketahui bahwa peradilan di Indonesia menuntut sekurang-kurangnya harus ada dua alat bukti yang sah untuk menjatuhkan pidana terhadap seseorang yang terkait dalam suatu kasus. sedangkan alat bukti yang dimaksud adalah alat bukti sebagaimana diatur dalam pasal 184 Kitab Undang-Undang Hukum Acara Pidana (KUHAP) yaitu terdiri dari :

1. *Keterangan saksi, dalam Pasal 185 ayat (1) KUHAP disebutkan bahwa keterangan saksi sebagai alat bukti ialah apa yang saksi nyatakan dalam persidangan. Berdasarkan penjelasan KUHAP dinyatakan bahwa dalam keterangan saksi tidak termasuk keterangan yang diperoleh dari orang lain. Pasal 1 angka 27 KUHAP menyatakan bahwa keterangan saksi adalah salah satu alat bukti dalam perkara pidana berupa keterangan dari saksi mengenai suatu peristiwa pidana yang ia lihat sendiri dan dialami sendiri dengan menyebut alasan dari pengetahuannya itu.*
2. *Keterangan ahli, Pasal 186 KUHAP menyatakan bahwa keterangan seorang ahli ialah apa yang seorang ahli nyatakan di sidang pengadilan. Selanjutnya penjelasan Pasal 186 KUHAP menyatakan bahwa keterangan ahli ini dapat juga telah diberikan*

pada waktu pemeriksaan oleh penyidik atau penuntut umum yang dituangkan dalam suatu bentuk laporan dan dibuat dengan mengingat sumpah pada waktu ia menerima jabatan atau pekerjaan. Menurut teori hukum pidana yang dimaksud dengan keterangan ahli adalah keterangan yang diberikan seseorang berdasarkan ilmu dan pengetahuan yang dikuasainya.

3. *Surat, sebagai alat bukti diatur dalam Pasal 187 KUHAP. Menurut komentar KUHAP yang disusun oleh M. Karjadi dan R. Soesilo, Pasal 187 membedakan atas empat macam surat, yaitu :*

    a. *Berita acara dan surat lain dalam bentuk resmi yang dibuat oleh pejabat umum yang berwenang atau yang dibuat dihadapannya, didengar, dilihat atau dialaminya sendiri, disertai dengan alasan tentang keterangan itu;*
    b. *Surat yang dibuat menurut peraturan undang-undang atau surat yang dibuat oleh pejabat mengenai hal yang termasuk dalam tata laksana yang menjadi tanggung jawabnya dan yang diperuntukan bagi pembuktian sesuatu hal atau keadaan;*
    c. *Surat keterangan dari seorang ahli yang memuat pendapat berdasarkan keahliannya mengenai suatu hal atau keadaan yang diminta secara resmi dari padanya; dan*
    d. *Surat lain yang hanya dapat berlaku jika ada hubungannya dengan isi dari alat pembuktian yang lain.*

4. *Petunjuk, Pasal 188 ayat (1) KUHAP memberi definisi petunjuk sebagai perbuatan, kejadian atau keadaan, yang karena penyesuaiannya, baik antara yang satu dengan yang lain, maupun*

dengan tindak pidana itu sendiri, menandakan bahwa telah terjadi suatu tindak pidana dan siapa pelakunya. Selanjutnya Pasal 188 ayat (3) KUHAP dinyatakan bahwa penilaian atas kekuatan pembuktian dari suatu petunjuk dalam setiap keadaan tertentu dilakukan oleh hakim dengan arif dan bijaksana, setelah ia mengadakan pemeriksaan dengan penuh kecermatan dan keseksamaan berdasarkan hati nuraninya.

5. *Keterangan terdakwa, menurut Pasal 189 ayat (1) KUHAP adalah apa yang terdakwa nyatakan di sidang tentang perbuatan yang ia lakukan atau yang ia ketahui sendiri dan alami sendiri. Keterangan terdakwa tidak perlu sama dengan pengakuan, karena pengakuan sebagai alat bukti mempunyai syarat, yaitu :*
   a. *Mengaku ia yang melakukan delik yang didakwakan; dan*
   b. *Mengaku ia bersalah*

Di antara kelima jenis alat bukti tersebut, yang sering dipermasalahkan adalah keterangan ahli. Keterangan ahli yang dimaksud adalah ahli komputer, masalahnya adalah hingga sampai saat ini Indonesia masih belum ada organisasi yang mewadahi profesi di bidang komputer, sehingga persoalannya adalah apakah setiap orang yang mahir mengoperasikan komputer dapat dikategorikan sebagai ahli komputer. Dalam KUHAP sendiri tidak terdapat penjelasan mengenai apakah yang dimaksud dengan keterangan ahli dan siapakah yang dimaksud dengan ahli. Padahal keterangan saksi ahli (expert testimony) merupakan salah satu ciri peradilan modern.

Mengantisipasi kendala-kendala yang menyangkut alat bukti yang sah yang merupakan salah satu unsur yang harus ada dalam persidangan, maka masalah pembuktian dalam tindak pidana siber (cybercrime) dalam hal ini penyadapan data pribadi pengguna internet melalui monitoring aktivitas komputer menunjuk pada Pasal 5 ayat (1) dan ayat (2) Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi elektronik. Pasal 5 ayat (1) Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik menyatakan bahwa :

> *"Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti yang sah."*

Berdasarkan ketentuan Pasal 5 ayat (1) Undang-Undang Nomor11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik diatas, bahwa dokumen elektronik dan/atau hasil cetaknya merupakan alat bukti yang sah. Dalam pengertiannya, Informasi Elektronik adalah salah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, surat elektronik, telegram, teleks, huruf, tanda, angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yag mampu memahaminya. Sedangkan dokumen elektronik adalah setiap informasi elektronik yang dibuat, diteruskan, dikirimkan, diterima atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui komputer atau sistem elektronik, termasuk tapi tidak terbatas pada tulisan, suara, gambar, peta rancangan, foto atau sejenisnya, huruf, tanda,angka, kode akses, simbol atau

perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya. Kemudian Pasal 5 ayat (2) menyebutkan :

> *"Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya sebagaimana dimaksud pada Ayat (1) merupakan perluasan dari alat bukti yang sah sesuai dengan hukum acara yang berlaku di indonesia".*
>
> *Berdasarkan ketentuan Pasal 5 ayat (2) diatas, bahwa informasi elektronik dan/atau hasil cetaknya sebagaimana yang dimaksud pada ayat (1) merupakan perluasan dari alat bukti yang sah yang dapat diungkapkan pada persidangan yang berlaku dalam hukum acara di Indonesia. Berdasarkan Pasal 5 ayat (1) dan (2) diatas, maka untuk kendala dalam proses pembuktian di persidangan menyangkut kejahatan siber (cybercrime), dalam hal ini penyadapan data pribadi pengguna internet melalui monitoring aktivitas komputer, Pasal 5 ayat (1) dan ayat (2) Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik yang merupakan perluasan dari pasal 184 Kitab Undang-Undang Hukum Acara Pidana sudah sangat relevan untuk dijadikan dasar hukum menyangkut alat bukti yang sah dalam persdangan yang menyangkut kejahatan siber (cybercrime) dalam hal ini penyadapan data pribadi pengguna internet melalui monitoring aktivitas komputer yang bertentangan dengan Pasal 31 ayat (1) dan ayat (2) Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik*

Cybercrime yang pada prosesnya menggunakan teknologi tinggi (hi-tech), jangkauannya sangat luas serta pelaku rata-rata mempunyai intelektualitas yang tinggi dan mempunyai komunitas tersendiri, sehingga untuk pembuktiannya memerlukan penyidik yang mengerti bidang tersebut. Sementara dari pihak penyidik itu sendiri masih sangat membutuhkan orang-orang yang mengerti betul akan bidang tersebut guna melaksanakan proses penyidikan yang berkaitan dengan cybercrime. Banyak faktor yang mempengaruhi kurangnya anggota penyidik yang menguasai bidang komputer secara mendalam, namun dari beberapa faktor tersebut ada yang sangat berpengaruh (determinan), diantaranya sebagai berikut :

1. *Kurangnya pengetahuan tentang komputer dan sebagaian dari mereka sangat jarang menggunakan komputer.*
2. *Pengetahuan dan pengalaman para penyidik dalam menangani kasus-kasus cyber crime masih terbatas. Mereka belum mampu memahami teknik hacking, modus modus operandi para hacker.*
3. *Faktor sistem pembuktian yang menyulitkan para penyidik, karena Jaksa Penuntut Umum (JPU) masih meminta keterangan saksi dalam bentuk Berita Acara Pemeriksaan (BAP) formal. Sehingga diperlukan pemanggilan saksi/korban yang berada di luar negeri untuk dibuatkan berita acaranya di Indonesia, belum dapat menerima pernyataan korban atau saksi dalam bentuk faksimili atau email sebagai alat bukti.*

Kemudian kendala lainnya yang sangat mempengaruhi dalam mengatasi permaslahan yang berkaitan dengan penyadapan data prbadi pengguna internet melalui monitoring aktivitas komputer yang merupakan

salah satu bentuk dari cybercrime yaitu fasilitas komputer forensik. Untuk membuktikan jejak-jejak para hacker dan cracker dalam melakukan aksinya terutama yang berhubungan dengan program-program dan data-data komputer, sarana Polri belum cukup memadai karena fasilitas komputer forensik yang masih sangat terbatas dalam instansi tersebut. Fasilitas komputer forensik ini sangat dibutuhkan sebagai upaya untuk mengungkap data-data digital serta merekam dan menyimpan bukti-bukti berupa softcopy image, program, dan lain sebagainya.