**Etika Hukum**

Cyber crime merupakan fenomena sosial yang membuka cakrawala keilmuan dalam dunia hukum, cyber crime merupakan suatu kejahatan yang sangat dahsyat efeknya yang dilakukan hanya dari depan komputer tanpa perlu kemana-mana. Tindak pidana cyber crime merupakan sisi gelap dari kemajuan teknologi komunikasi dan informasi yang mengakibatkan efek yang sangat luas disemua lini kehidupan karena sangat berkaitan dengan economic crime dan organized crime.

Problematika cyber crime merupakan suatu problematika besar yang berdampak negatif disamping berpengaruh positif, oleh karena itu diperlukan hukum / perundang-undangan untuk dapat memberi ketertiban kepastian dan keadilan hukum yang berbeda ukuran dan isinya dalam menangani kejahatan yang timbul akibat penyalah gunaan media teknologi dan informasi.

Cyber crime adalah kejahatan yang menggunakan teknologi informasi dan merupakan salah satu bentuk kejahatan lintas Negara (transnational crime) tidak mengenal batas wilayah (borderless), tanpa kekerasan (non violence), tidak ada kontak fisik (no physically contact) dan tanpa nama Karakteristik Cyber crime tersebut membuat pelaku Cyber Crime sangat sulit dilacak dan unsur-unsur pidananya sulit dibuktikan, apalagi adanya keterbatasan regulasi.

Perlindungan terhadap korban kejahatan cyber memerlukan keseriusan dan kepiawaian yang tinggi dari aparat penegak hukum, diperlukan aparat hukum yang menguasai teknologi tinggi dibidang teknologi informatika baik aparat kepolisian, kejaksaan maupun kehakiman dikarenakan eksistensi dunia maya yang bersifat tanpa batas wilayah negara (border state less), selain itu diperlukan suatu kerjasama yang baik dan terukur antar negara baik yang bersifat regional maupun global dalam rangka mencegah dan menanggulangi terjadinya kejahatan transnasional seperti ciber crime.

Oleh karena banyaknya kasus kejahatan di dunia yang tanpa batas (borderles) diperlukan suatu aturan hukum serta implementasinya di lapangan, kerjasama antar instansi yang terkait baik dalam skala nasional, regional maupun internasional dalam rangka menanggulangi, mencegah dan memberantas semua pelaku kejahatan yang terjadi di dunia maya

Dengan melakukan upaya penyelidikan, pembuktian dan penyidikan terhadap semua pelaku kejahatan cyber guna melindungi para pengguna cyberspace (netizen) dari para hacker hitam (cracker).

**Konsep Cyber Crime**

Cyber crime merupakan kejahatan yang melintas batas Negara, tidak terbatas yurisdiksi, tanpa kekerasan, tidak ada kontak fisik, yang bisa menimbulkan korban bagi siapa saja pengguna internet sehingga memerlukan upaya perlindungan hukum dari pemerintah terhadap masyarakat yang menjadi korban tindak pidana cyber crime baik melalui tindakan preventif maupun represif melalui pendekatan teknologi, pendekatan sosial budaya, dan pendekatan hukum.

Secara umum ada beberapa hal yang perlu diperhatikan dalam menanggulangi dampak perkembangan cyber crime yaitu:

a. Pendekatan penal ( menggunakan sistem peradilan pidana):

1) Merumuskan sistem peradilan pidana yang tepat, mulai dari Kriminalisasi yang rasional sampai dengan merumuskan elementelement hukum acara yang kondusif; sebagai contoh adalah pengaturan yurisdiksi sebagaimana tercantum dalam council of Europe convention yang disamping penerapan asas teritorialitas. juga menerapkan yurisdiksi terhadap warga Negara yang melakukan tindak pidana di tempat dimana perbuatan tersebut juga diancam dan di luar territorial Negara dan juga sama sekali diluar di luar territorial Negara lain. Disingapura bahkan berlaku berlaku bagi mereka yang dari luar singapura melakukan perbuatan yang merugikan komputer singapura dan pelaku dari singapura yang merugikan komputer Negara lain.

2) Sejauh mungkin dihindari kemungkinan terjadinya Over criminalization

3) Perumusan kriminalisasi harus dilakukan secara komprehensif sehingga menggambarkan approximasi hukum pidana sebagai safeguard yang sesuai dengan standart antar bangsa;

4) Dalam kriminalisasi harus diperhitungkan keselarasan antar HAM dan kewajiban asasi;

5) Perlu diatur tentang corporate criminal responsibility dan perluasan yurisdiksi.

b. Pendekatan non penal ( prevention without punishment)

1) Perlu dirumuskan terlebih dahulu umbrella act yang mengatur kebijakan tentang komunikasi massa, baik yang bersifat cetak, penyiaran maupun cyber.

2) Perlu dirumuskan secara professional penyusunan kode etik, code of conduct and code of practice tentang penggunaan teknologi informatika;

3) Perlu kerjasama antar segala pihak yang terkait termasuk kalangan industry untuk mengembangkan preventive technology menghadapi cyber crime sebagai contoh adalah dikembangkannya cyber patrol software yang dapat digunakan oleh internet service provider (ISP) atau internet conten provider (ICP) untuk menyaring atau memblok akses ke situs tertentu secara otomatik apabila situs tersebut telah masuk black list. Internet memang bukan jaringan yang aman.

**Perlindungan Hukum Terhadap Korban Tindak Pidana Cyber Crime dalam Sistem Hukum Pidana Indonesia**

Penegakan hukum terhadap pelaku tindak pidana mayantara merupakan suatu upaya perlindungan terhadap pengguna cyberspace (internet) dari para cracker yang menggunakan media internet dalam melakukan aksi kejahatannya . Meskipun belum terbentuknya hukum khusus siber (cyber law) di Indonesia yang berorientasi kepada kepentingan korban tapi diperlukan adanya upaya hukum melindungi kepentingan penduduk dunia maya (netizen) berikut privasinya dengan menggunakan hukum yang sudah ada sebelumnya meliputi perundang-undangan, yurisprudensi maupun konvensikonvensi Internasional yang sudah diratifikasi oleh Indonesia.

Penanggulangan kejahatan tindak pidana internet dapat dilakukan dengan berbagai upaya diantaranya penanggulangan secara preemtif, preventif dan represif. Upaya preemtif dilakukan dengan meratifikasi konvensi-konvensi cyber crime internasional kedalam sistem perundang-undangan Indonesia. Konvensi Dewan Eropa merupakan salah satu bentuk konvensi internasional yang sudah diratifikasi sebagian isi kovenannya kedalam sistem perundang-udangan Indonesia Penanggulangan cyber crime secara preventif dapat dilakukan dengan meningkatkan pengamanan, meningkatkan daya guna perangkat komputer, keahlian serta kedisplinan dalam menggunakan perangkat saat berselancar di dunia maya. Kegiatan tersebut dapat berupa tindakantindakan yang bisa dilakukan baik secara perorangan (pribadi), kebijakan nasional maupun global. Sedangkan Penanggulangan cyber crime secara represif dilakukan dengan menangkap para pelaku tindak pidana untuk diproses sesuai dengan hukum yang berorentasi kepentingan korban melalui pemberian restitusi, kompensasi maupun asistensi yang menjadi tanggung jawab pelaku dengan Negara sebagai fasilitatornya.

Upaya perlindungan terhadap korban tindak pidana merupakan upaya pemulihan kerugian yang telah di dapatkan oleh korban. Hal tersebut akan lebih termaknai apabila korban dilibatkan langsung dalam proses penyelesaian perkara pidana. Penegakan hukum merupakan upaya pembangunan yang berkesinambungan yang bertujuan mewujudkan kehidupan berbangsa dan bernegara yang aman, tentram tertib serta dinamis dalam lingkungan pergaulan dunia yang independen. Penegakan hukum pidana dimasa mendatang sebaiknya lebih bertumpu kepada sistem Restorative Justice atau keadilan restoratif yang merupakan suatu penyelesaian secara adil yang melibatkan pelaku, korban, keluarga mereka, dan pihak lain yang terkait dalam suatu tindak pidana secara bersama-sama mencari penyelesaian terhadap tindak pidana tersebut dan implikasinya dengan menekankan pemulihan kembali pada keadaan semula sebagaimana diatur dalam surat keputusan bersama antara ketua Mahkamah Agung RI, Menteri Hukum dan HAM, Menteri Sosial, Menteri Pemberdayaan Perempuan dan Perlindungan Anak Republik Indonesia.

Secara konseptual perlindungan korban merupakan suatu upaya melindungi orang/badan hukum, yang telah mendapatkan kerugian baik kerugian fisik, mental emosional, kehilangan harta benda atau perusakan terhadap hak-hak mereka melalui tindakan ataupun pembiaran yang telah diatur dalam hukum pidana akibat suatu perbuatan jahat yang tidak dapat dibiarkan berlangsung ditengah-tengah masyarakat, yang memperkosa skala nilai sosial dan perasaan hukum yang hidup dalam masyarakat yang diakibatkan oleh para pelaku tindak pidana.

Pelaksanaan perlindungan hukum terhadap korban menurut Muladi merupakan bagian perlindungan kepada masyarakat yang dapat diwujudkan dalam berbagai bentuk seperti: pemberian restitusi dan kompensasi, pelayanan medis dan bantuan hukum.

Dalam penanganan perkara pidana kepentingan korban sudah saatnya untuk diberikan perhatian khusus, selain sebagai saksi yang mengetahui terjadinya suatu kejahatan juga karena kedudukan korban sebagai subjek hukum yang memiliki kedudukan sederajat di depan hukum (equality before the law). Perhatian kepada korban dalam penanganan perkara pidana hendaknya dilakukan atas dasar belas kasihan dan hormat atas martabat korban.. (Muladi, 1995:107).

Perlindungan hukum bagi masyarakat sangatlah penting karena masyarakat baik kelompok maupun perorangan, dapat menjadi korban atau bahkan sebagai pelaku kejahatan. Perlindungan hukum korban kejahatan sebagai bagian dari perlindungan kepada masyarakat, seperti melalui pemberian restitusi dan kompensasi, pelayanan medis, dan bantuan hukum (Dikdik M. Arief Mansur& Elisatris Gultom, 2007: 31).

Agus Raharjo, Cyber Crime, Pemahaman dan UpayaPencegahan Berteknologi, PT Citra Aditya  
Bakti, Bandung, 2002.

Ahmad M. Ramli, Cyber Law dan Haki Dalam SistemHukum Indonesia, Refika Aditama, Cet 2,  
Bandung, 2006.

Andi Hamzah, Hukum Acara Pidana indonesia, Sinar  
Grafika, Jakarta, Edisi Revisi, 2004.

Danrivanto Budhijanto, Hukum Telekomunikasi,Penyiaran, dan Tekhnologi Informasi Regulasidan Konfegensi, PT Refika Aditama, 2010.

Dikdik M. Arief Mansur dan Elisatris Gultom, UrgensiPerlindungan Korban Kejahatan Antara Norma

**Perlindungan Hukum Terhadap Korban Kejahatan cybercrime di Indonesia.**

Kejahatan dunia maya atau cybercrime adalah istilah yang mengacu kepada aktivitas kajahatan dengan komputer atau jaringan komputer yang menjadi alat, sasaran atau tempat terjadinya kejahatan.7 Hukum pada prinsipnya merupakan pengaturan terhadap sikap tindak (perilaku) seseorang dan masyarakat yang terhadap pelanggarnya diberikan sanksi oleh negara. Meskipun dunia cyber adalah dunia virtual, hukum tetap diperlukan untuk mengatur sikap tindak masyarakat, setidaknya ada dua hal yakni: Pertama masyarakat yang ada didunia maya adalah masyarakat yang ada di dunia nyata, masyarakat memiliki nilai dan kepentingan baik secara sendiri-sendiri maupun bersama-sama harus dilindungi. Kedua, walaupun terjadi di dunia maya, transaksi yang dilakukan oleh masyarakat memiliki pengaruh dalam dunia nyata, baik secara ekonomis maupun non ekonomis.8 Saat ini regulasi yang dipergunakan sebagai dasar hukum atas kasus-kasus cybercrime adalah Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE). Dengan adanya UU ITE ini diharapkan dapat melindungi masyarakat pengguna teknologi informasi di Indonesia, hal ini penting mengingat jumlah pengguna teknologi internet yang semakin meningkat dari tahun ke tahun. Meningkatnya penggunaan internet di satu sisi memberikan banyak kemudahan bagi manusia dalam melakukan aktivitasnya, disisi lain memudahkan bagi pihak-pihak tertentu untuk melakukan suatu perbuatan tindak pidana, kemajuan teknologi ini juga mempengaruhi gaya hidup dan pola pikir manusia faktanya saat ini banyak terjadi kejahatan dengan menggunakan teknologi informasi. Fenomena cybercrime yang berkembang dengan pesat yang tidak mengenal batas teritorial ini memang harus diwaspadai karena kejahatan ini agak berbeda dengan kejahatan lain pada umumnya. Pemanfaatan Teknologi Informasi berperan penting dalam perdagangan dan pertumbuhan perekonomian nasional untuk mewujudkan kesejahteraan masyarakat, bahwa pemerintah perlu mendukung pengembangan Teknologi Informasi melalui infrastruktur hukum dan pengaturannya sehingga pemanfaatan Teknologi Informasi dilakukan secara aman untuk mencegah penyalahgunaannya dengan memperhatikan nilai-nilai agama dan sosial budaya masyarakat Indonesia. Di dalam ketentuan Pasal 4 ayat (2) UU ITE disebutkan bahwa Pemerintah melindungi kepentingan umum dari segala jenis gangguan sebagai akibat penyalahgunaan Informasi Elektronik dan Transaksi Elektronik yang mengganggu ketertiban umum, sesuai dengan ketentuan Peraturan Perundang-undangan. Penyalahgunaan teknologi informasi ini yang dapat merugikan orang lain, bangsa dan negara yang menggunakan sarana komputer yang memiliki fasilitas internet yang dilakukan oleh hacker atau sekelompok cracker dari rumah atau tempat tertentu tanpa diketahui oleh pihak korban yang dapat menimbulkan kerugian moril, materil maupun waktu akibat dari perusakan data yang dilakukan oleh hacker. Untuk mengatasi kejahatan cybercrime dibutuhkan aparat penegak hukum yang memahami dan menguasai teknologi, kendala yang dihadapi oleh korban adalah dikarnakan ketidaktahuan, pengetahuan komputer dan internet sehingga apabila dirugikan tidak dapat melaporkaan segala peristiwa pidana yang dialami tentunya ini menjadi permaslahan kita bersama. Asas dan tujuan undang-undang ini adalah pemanfaatan Teknologi Informasi dan Transaksi Elektronik dilaksanakan berdasarkan asas kepastian hukum, manfaat, kehati-hatian, iktikad baik, dan kebebasan memilih teknologi atau netral teknologi. Jadi dapat diartikan bahwa pengunaan teknologi informasi dan Transaksi elektronik diharapkan dijamin dengan kepastian hukum, memiliki manfaat, penuh kehati-hatian, beritikad baik, dan adanya kebebasan memilih teknologi dan netral. Menjawab tuntutan dan tantangan komunikasi global lewat Internet, Undang-Undang diharapkan mampu untuk menjawab semua permasalahan hukum terhadap perkembangan global teknologi serta antisipatif terhadap semua permasalahan yang ada, termasuk dampak negatif penyalahgunaan internet yang pada akhirnya akan menimbulkan kerugian bagi penggunanya. Terdapat beberapa hukum positif lain yang berlaku umum dan dapat dikenakan bagi para pelaku cybercrime terutama untuk kasus-kasus yang menggunakan komputer sebagai sarana, antara lain:

a. KUHP

b. Undang-Undang Nomor 11 tahun 2008 tentang ITE

c. Undang-Undang Nomor 44 tahun 2008 tentang Pornografi

d. Undang-Undang Nomor 36 tahun 1999 tentang Telekomunikasi.

e. Undang-Undang Nomor 5 tahun 1999 tentang Larangan Praktek Monopoli dan Persaingan Usaha Tidak Sehat.

f. Undang-Undang Nomor 8 tahun 1999 tentang Perlindungan Konsumen.

g. Undang-Undang Nomor 19 tahun 2002 tentang Hak Cipta.

h. Undang-Undang Nomor 8 Tahun 1997 tentang Dokumen Perusahaan

i. Undang-Undang Nomor 25 Tahun 2003 tentang Perubahan atas UndangUndang Nomor 15 Tahun 2002 tentang Tindak Pidana Pencucian Uang

j. Undang-Undang Nomor 15 Tahun 2003 tentang Pemberantasan Terorisme Dalam menjaga dan melindungi masyarakat pengguna teknologi dibutuhkan kerjasama dan keseriusan semua pihak mengingat teknologi informasi khususnya internet telah dijadikan sebagai sarana untuk membangun masyarakat yang berbudaya informasi. Keberadaan undang-undang yang mengatur cybercrime diharapkan dapat melindungi dan memberikan rasa aman bagi mereka yang menggunakan teknologi sebagai wadah untuk melalukan transaksi maupun melakukan kegiatan ekonomi. Dalam melakukan penindakan bagi mereka yang menyalahgunakan perkembangan teknologi dibutuhkan sumberdaya manusia yang berkualitas yang memiliki kemampuan dan keahlian dibidang teknologi. Dalam penegakan hukum setidaknya dipengaruhi beberapa faktor yakni aturan hukum itu sendiri atau undang-undang, aparat pelaksana dari aturan tersebut yakni aparat penegak hukum dan budaya hukum itu sendiri yakni masyarakat itu sendiri yang menjadi sasaran dari undang-undang. Undang-undang informasi dan transaksi elektronik (UU ITE) atau yang disebut dengan cyberlaw, digunakan untuk mengatur berbagai perlindungan hukum atas kegiatan yang memanfaatkan internet sebagai medianya,baik transaksi maupun pemanfaatan informasinya. Pada UU ITE ini juga diatur berbagai macam hukuman bagi kejahatan melalui internet. UU ITE mengakomodir kebutuhan para pelaku bisnis di internet dan masyarakat pada umumnya untuk mendapat kepastian hukum dengan diakuinya bukti elektronik dan tanda tangan elektronik digital sebagai bukti yang sah dipengadilan.UU ITE sendiri baru ada di Indonesia dan telah disahkan oleh DPR pada tanggal 25 Maret 2008. UU ITE terdiri dari 13 Bab dan 54 Pasal yang mengupas secara mendetail bagaimana aturan hidup di dunia maya dan transaksi yang terjadi di dalamnya. Dengan adanya undang-undang ITE tersebut diharapkan dapat memberikan rasa aman dan dapat melindungi bagi mereka yang menggunakan teknologi. Disamping itu, dalam keadaan tertentu dan membahayakan bagi mereka yang menjadi korban kejahatan teknologi juga berhak mendapatkan perlindungan hukum hal ini tercantum dalam Undang-undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban (UU PSK). Di dalam ketentuan Pasal 5 UU PSK menyatakan bahwa :

1) Seorang saksi dan korban berhak:

a. Memperoleh perlindungan atas keamanan pribadi, keluarga, dan harta bendanya, serta bebas dari ancaman yang berkenaan dengan kesaksian yang akan, sedang, atau telah diberikannya;

b. Ikut serta dalam proses memilih dan menentukan bentuk perlindungan dan dukungan keamanan;

c. Memberikan keterangan tanpa tekanan;

d. Mendapat penerjemah;

e. Bebas dari pertanyaan yang menjerat;

f. Mendapatkan informasi mengenai perkembangan kasus;

g. Mendapat informasi mengenai putusan pengadilan;

h. Mengetahui dalam hal terpidana dibebaskan;

i. Mendapatkan identitas baru;

j. Mendapatkan tempat kediaman baru;

k. Memperoleh penggantian biaya transportasi sesuai dengan kebutuhan;

l. Mendapat nasehat hukum dan/atau;

m. Memperoleh bantuan biaya hidup sementara sampai batas waktu perlindungan berakhir.

2) Hak sebagaimana dimaksud dalam ayat

(1) diberikan kepada Saksi dan/atau Korban tindak pidana dalam kasus-kasus tertentu sesuai dengan keputusan LPSK. Selanjutnya dalam ketentuan Pasal 1 ayat (2) UU PSK menyebutkan “korban adalah seseorang yang mengalami penderitaan fisik, mental dan/atau kerugian ekonomi yang diakibatkan oleh suatu tindak pidana”. Korban dalam hal ini adalah mereka yang telah dirugikan baik secara materi maupun non materi akibat dari kejahatan cybercrime. Dalam perlindungan hukum terhadap korban cybercrime secara mendasar ada dua model yaitu model hak-hak prosedural dan model pelayanan9 :

1). Model Hak-hak Prosedural (The Procedural Rights Model) Pada model hak prosedural, korban kejahatan cybercrime diberikan hak untuk melakukan tuntutan pidana atau membantu jaksa, atau hak untuk dihadirkan pada setiap tingkatan peradilan diamana keterangannya dibutuhkan, secara implisit dalam model ini korban diberikan kesempatan untuk “membalas” pelaku kejahatan yang telah merugikannya. Dalam model prosedural itu korban juga diminta lebih aktif membantu aparat penegak hukum dalam menangani kasusnya apalagi berkaitan dengan kejahatan yang modern cybercrime. Dengan adanya hak prosedural juga dapat menimbulkan kembali kepercayaan korban setelah dirinya dirugikan oleh mereka yang tidak bertanggungjawab (terdakwa), disamping itu hal ini juga dapat menjadi pertimbangan bagi jaksa dalam hal apabila jaksa membuat tuntutan yang terlalu ringan.

2). Model Pelayanan (The Service Model) Model pelayanan ini bertitik berat terletak pada perlunya diciptakan standarstandar baku bagi pembinaan korban kejahatan cybercrime. Model ini melihat korban sebagai sosok yang harus dilayani oleh Polisi dan aparat penegak hukum yang lain, pelayanan terhadap korban cybercrime oleh aparat penegak hukum apabila dilakuakan dengan baik akan membawa dampak positif bagi penegakan hukum ksususnya cybercrime, dengan demikian korban perkembangan teknologi ini akan lebih percaya institusi penegak hukum dengan adanya pelayanan terhadap korban, dengan demikian maka korban akan merasa haknya dilindungi dan dijamin kembali kepentingannya. Pada proses persidangan, terutama yang berkenaan dengan pembuktian kejahatan dunia maya, banyak kasus yang terjadi akibat perkembangan teknologi informasi hal ini mengharuskan aparat penegak hukum menyiapkan sumber daya manusia yang handal dan mengerti dab paham dengan teknologi., mengingat kejahatan cybercrime merupakan kejahatan modern yang harus mendapat perhatian yang serius dari pemerintah, karena kejahatan di dunia maya akan berimbas pada dunia yata. Dengan adanya Undang-undang Nomor 11 Tahun 2008 diharapkan dapat membantu aparat penegak hukum dalam melindungi masyarakat yang menggunakan teknologi. Dalam memberikan perlindungan hukum terhadap korban cybercrime aparat penegak hukum khususnya pihak kepolisian telah melakukan berbagai cara dalam mengatasi maraknya kejahatan yang terjadi di dunia maya salah satunya sosialisasi kepada masyarakat pengguna teknologi dan bagi masyarakat yang pernah menjadi korban cybercrime dapat melaporkan penipuan yang dialami dengan mengirim laporan ke alamat surel yakni cybercrime@polri.go.id10 . Dengan menyertakan nomor rekening dan telpon pelaku dalam laporan, agar segera dilacak. seperti, penipuan dan penjualan online yang semakin marak, untuk mengatasi maraknya kejahatan semacam ini. Polri menyediakan email khusus untuk menerima laporan kasus-kasus terkait cybercrime. Pentingnya perlindungan hukum bagi korban kejahatan cyber, selain dalam kerangka mewujudkan negara hukum, hal ini penting dilakukan sebagai suatu tindakan preventif yang dilakukan oleh aparat penegak hukum dalam mengurangi ataupun mencegah terjadinya korban kejahatan dunia maya dan tentunya bukan hanya sebagai penampung laporan akan tetapi yang diharapkan adalah adanya tindakan nyata dari aparat penegak hukum sehingga masyarakat pengguna teknologi benar-benar merasa aman dalam melakaukan aktifitasnya di dunia maya.

Andi Hamzah, 1990, Aspek-aspek Pidana di Bidang Komputer, Sinar Grafika, Jakarta.

Arif Gosita, 2004, Masalah Korban Kejahata, PT Bhuana Ilmu Populer, Jakarta

Barda Nawawi Arief, 2000, Perlindungan HAM dan Korban dalam Pembaharuan Hukum, Citra Aditya Bakti, Bandung.

Dikdik M Arief Mansyur dan Elisatris Gultom, 2008, Urgensi Perlindungan Korban Kejahatan, PT Raja Grafindo Persada, Jakarta.

J.E Sahetapy, 1987, Viktimologi Sebuah Bunga Rampai, cet.I, Pustaka Sinar Harapan, Jakarta.

Josua Sitompul, 2012, Cyberspace, cybercrime, cyberlaw, Tinjauan Aspek Hukum Pidana, PT. Tatanusa, Jakarta.

Muladi dan Barda Nawawi Arif, 1992, Bunga Rampai Hukum Pidana, Alumni, Bandung.

**CONTOH**

**PERLINDUNGAN HUKUM BAGI KORBAN PENCURIAN INFORMASI PRIBADI MELALUI DUNIA CYBER DITINJAU DARI UU ITE**

Saat ini belum adanya perhatian terhadap korban kejahatan di dalam masyarakat yang merupakan tanda belum adanya keadilan dan kesejahteraan dari keadaan masyarakat tersebut. Dalam hal ini korban kejahatan diartikan sebagai seseorang yang telah menderita kerugian sebagai akibat suatu kejahatan dan atau rasa keadilannya secara langsung telah terganggu sebagai akibat pengalamannya sebagai target (sasaran) kejahatan. 5 Sebagai korban kejahatan, korban berhak mendapatkan perlindungan hukum, dalam memberikan perlindungan hukum ini harus secara maksimal khususnya korban-korban yang bergolongan lemah ekonomi. Perlindungan hukum yang dimaksud dapat berupa kompensasi, restitusi dan bantuan hukum yang diatur dalam Peraturan Pemerintah No.44 Tahun 2008 Tentang Pemberian Kompensasi, Restitusi, Dan, Bantuan Kepada Saksi Dan Korban. Dalam hal kejahatan dunia cyber, korban lebih tepat mendapatkan Restitusi. Menurut Pasal 1 angka 5 "Restitusi adalah ganti kerugian yang diberikan kepada Korban atau Keluarganya oleh pelaku atau pihak ketiga, dapat berupa pengembalian harta milik, pembayaran ganti kerugian untuk kehilangan atau penderitaan, atau penggantian biaya untuk tindakan tertentu". Pencurian informasi pribadi merupakan salah satu ancaman kejahatan paling lazim saat ini, yang dilakukan dengan cara mencuri data penting orang lain. Data penting dalam hal ini tentu saja mulai dari data pribadi (nama, alamat, email, nomor handphone dll), lalu data terkait dengan keuangan antara lain data bank(nomor rekening), data ATM, serta data kartu kredit. Pelaku pencurian informasi pribadi dapat dikenakan sanksi pasal 30 ayat (2) Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, yang berbunyi "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". Dengan melihat pasal tersebut pelaku pencurian informasi telah memenuhi unsur-unsur pasal 30 ayat(2) UU ITE, cara apa pun yang dimaksud disini adalah dengan menyusup sistem keamanan komputer baik dengan menggunakan software tertentu ataupun tidak yang bertujuan untuk mencuri data atau informasi seseorang. Sesuai dengan ketentuan Pasal 46 ayat (2) pelaku dapat dikenakan sanksi pidana penjara paling lama 7(tujuh) tahun dan/atau denda paling banyak Rp. 700.000.000,00 (tujuh ratus juta rupiah). Permasalahan lainnya terdapat pada belum adanya pengaturan mengenai bentuk perlindungan hukum kepada korban dalam Undang-Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Pelaku tindak pidana pencurian melalui dunia cyber ini seharusnya berkewajiban untuk memberikan restitusi kepada korbannya sebagai bentuk pertanggungjawabannya, besar dan jenis bentuk restitusi yang diterima korban dapat ditentukan oleh Hakim dalam amar putusannya. Bentuk restitusi dapat berupa pengembalian harta kekayaan (materi). Perlunya dibuat suatu kebijakan pidana dalam rangka pembaharuan Undang-Undang ITE yang menyangkut bentuk perlindungan korban, khususnya perlindungan korban pencurian informasi pribadi melalui media dunia cyber.