

PERLINDUNGAN KORBAN TINDAK PIDANA CYBER CRIME DALAM SISTEM HUKUM PIDANA INDONESIA

Tanthawi¹, Dahlan Ali², Suhaimi³

¹⁾ Magister Ilmu Hukum Program Pascasarjana Universitas Syiah Kuala Banda Aceh
email t.tanthawi@yahoo.com

^{2,3)} Staff Pengajar Ilmu Hukum Universitas Syiah Kuala

Abstract: *Cyber Crime has become a trend of crime these days in which its range is always expanding from day to day. The nature of Cyber Crime that is timeless and not bound with any place or any boundaries of particular countries has made cyber crime as a global crime that cause huge losses from its victims. Crimes committed only from the computers has made this type of crime very difficult to be investigated and identified. The method used in this study is a normative juridical approach and done to assess, test and examine aspects of the law, especially criminal law relating to cyber crime by conducting research on secondary data in the field of law; type of data obtained from the research literature (library research), court decisions (cases) and from other data (eg print media, seminar, etc.) associated with the title. The intent and purpose of the study was to determine how to analyze and understand the arrangement of cyber crime in the Indonesian criminal justice system, analyze and understand how the law enforcement against criminal of cyber crime in Indonesia as well as to find out and get the formulation of legal protection for victims of cyber crime in the system of Indonesian criminal law. Based on the results of this study, it is concluded that the regulation on prevention and protection of cyber crime victims in Indonesia is regulated in legislation outside the Criminal Code Bill and in the Criminal Code. Indonesian criminal justice system has not made many contributions to the protection of victims of cyber crime but is more concerned on the crime doer. This study suggests that the regulation of cyber crime prevention set in special cyberlaw legislation accomodating the interests of victims and providing restitution to the losses of victims in both material and immaterial.*

Keywords: *cyber crime, protection of victims, restitution, trend.*

Abstrak: *cyber crime* sudah menjadi trend kejahatan masa kini yang bertambah luas jangkauannya. Sifat *cyber crime* yang tidak terbatas waktu, tempat maupun batas-batas wilayah suatu Negara telah menjadikan *cyber crime* sebagai suatu kejahatan global yang menimbulkan kerugian besar dari korbannya. Kejahatan yang dilakukan hanya dari komputer membuat pelacakan dan penyelidikan terhadap jenis kejahatan ini sangat sulit diidentifikasi. Metode yang dilakukan dalam penelitian ini adalah pendekatan yuridis normatif, dengan mengkaji, menguji dan menelaah aspek hukum, khususnya hukum pidana yang berkaitan dengan tindak pidana dunia maya dengan cara mengadakan penelitian terhadap data sekunder di bidang hukum yaitu; jenis data yang diperoleh dari riset kepustakaan (*library research*), putusan pengadilan (kasus) serta dari data-data lain (misalnya: media cetak, hasil seminar, dan sebagainya) yang berhubungan dengan judul penelitian. Maksud dan tujuan penelitian adalah mengetahui menganalisis dan memahami bagaimana pengaturan *cyber crime* dalam sistem hukum pidana Indonesia, menganalisis dan memahami bagaimana penegakan hukum terhadap pelaku tindak pidana *cyber crime* di Indonesia serta untuk mengetahui dan mendapatkan rumusan tentang perlindungan hukum terhadap korban tindak pidana *cyber crime* dalam sistem hukum pidana Indonesia. Berdasarkan hasil penelitian dapat disimpulkan bahwa pengaturan tentang penanggulangan dan perlindungan korban *cyber crime* di Indonesia diatur dalam perundang-undangan di luar KUHP pun didalam RUU KUHP. Sistem hukum pidana Indonesia belum memberikan banyak kontribusi dalam perlindungan terhadap korban tindak pidana akan tetapi lebih banyak mengatur tentang pelaku kejahatan. saran dari penelitian ini agar pengaturan tentang penanggulangan *cyber crime* diatur dalam perundangan khusus *cyberlaw* yang mengakomodir kepentingan korban dengan mewajibkan pelaku memberikan restitusi terhadap kerugian yang dialami korban baik materi maupun immateri.

Kata kunci : *cyber crime, perlindungan korban, restitusi, bentuk.*

PENDAHULUAN

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 penyalahgunaan 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*).

KAJIAN KEPUSTAKAAN

Teori Perlindungan korban

Pengertian Perlindungan Hukum Korban Kejahatan

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).

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 element-element 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 memblokir akses ke situs tertentu secara otomatis apabila situs tersebut telah masuk

black list. Internet memang bukan jaringan yang aman.

Teori Yurisdiksi

Yurisdiksi dapat dimaknai; kedaulatan suatu negara yang dilaksanakan dalam batas batas wilayah negara tersebut dan merupakan eksistensi dari sebuah negara yang berdaulat serta mendapat pengakuan dari dunia internasional baik dalam membuat hukum, melaksanakan hukum, maupun menuntut dan mengadili apabila ada yang melakukan pelanggaran hukum dalam wilayah negara tersebut.

Prinsip utama dalam hukum teknologi informasi meletakkan prinsip yurisdiksi sebagai dasar acuannya. Perihal yurisdiksi berlaku untuk setiap orang yang melakukan perbuatan melawan hukum, baik yang berada di wilayah hukum Indonesia maupun yang berada di luar wilayah hukum Indonesia, yang memiliki akibat hukum di wilayah Indonesia dan/atau di luar wilayah hukum Indonesia yang merugikan 5-
1. ingan Indonesia (Danrivanto Budhijanto, 2010:136).

Dunia maya (*cyberspace*) merupakan dunia yang bersifat lintas negara tanpa dibatasi oleh waktu, tempat maupun yurisdiksi (batas-batas teritorial negara). Sejalan dengan prinsip yang berlaku dalam penegakan hukum *cyber crime* yakni prinsip yurisdiksi. Keberlakuan prinsip ini dikarenakan tidak serta merta dapat diterapkannya yurisdiksi teretorial dari suatu negara dalam kegiatan di *cyberspace* yang merupakan

kegiatan tanpa dibatasi oleh waktu maupun batasan-batasan yurisdiksi wilayah suatu Negara (Yudha Bakti, 2003: 96).

Diperlukan pendekatan prinsip yurisdiksi *extra territorial* dalam penegakan hukum di dunia maya, serta diperlukan kerjasama antar semua elemen terkait, baik dalam lingkup nasional, regional maupun internasional. Lebih lanjut diperlukan adanya perjanjian ekstradisi antar negara terhadap pelaku kejahatan *cyber* dan juga diperlukan penyelarasan makna dari pada tindak pidana *cyber crime* dalam perundang-undangan antar semua negara guna memudahkan penegakan hukum dalam penanggulangan *cyber crime*.

Dimungkinkannya penerapan hukum teknologi informasi oleh karena Undang-Undang Informasi dan Transaksi Elektronik memiliki jangkauan yurisdiksi tidak hanya untuk perbuatan hukum yang berlaku di Indonesia dan/atau dilakukan oleh WNI tetapi juga berlaku untuk perbuatan hukum yang dilakukan diluar wilayah hukum (yurisdiksi) Indonesia baik oleh WNI maupun WNA maupun badan hukum asing yang memiliki akibat hukum di Indonesia mengingat pemamfaatan teknologi informasi untuk informasi elektronik dan transaksi elektronik dapat bersifat lintas teretorial atau universal (Danrivanto Budhiyanto, 2010: 136).

METODE PENELITIAN

Metode pendekatan yang dilakukan dalam penelitian ini adalah metode pendekatan yuridis normatif dengan mengkaji menguji dan menelaah aspek hukum khususnya hukum pidana yang berkaitan dengan tindak pidana *cyber crime* dengan cara mengadakan penelitian terhadap data sekunder dibidang hukum yaitu; jenis data yang diperoleh dari riset kepustakaan (*library research*), putusan pengadilan (kasus) serta dari data-data lain (misalnya: media cetak, hasil seminar, dsb.) yang berhubungan dengan judul penelitian.

Teknik pengumpulan data yang digunakan oleh peneliti dalam penelitian ini bersumber dari studi pustaka (*library research*) yaitu memperoleh data sekunder dengan cara mengumpulkan berbagai literatur dan data serta informasi yang relevan dengan penelitian Mengingat penelitian ini merupakan penelitian hukum normatif, maka data yang di butuhkan dalam penelitian ini adalah data sekunder, yang akan diperoleh dari bahan-bahan hukum primer (ketentuan-ketentuan perundang-undangan yang mengatur tentang tindak pidana *cyber*), bahan-bahan hukum sekunder berupa putusan pengadilan (kasus) serta dari data-data lain (misalnya: media cetak, hasil seminar, dsb.) yang berhubungan dengan penelitian yang akan di teliti.

HASIL PEMBAHASAN

Pengaturan *Cyber Crime* dalam sistem Hukum Pidana Indonesia

Sistem hukum Indonesia belum secara khusus mengatur tentang *cyber law* (*cyber crime*) namun beberapa Perundang-undangan telah mengatur tentang penanggulangan tindak pidana *Cyber Crime* seperti Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi, Undang-Undang Nomor 19 Tahun 2002 tentang Hak Cipta, Undang-Undang Nomor 15 Tahun 2003 tentang Penanggulangan Terorisme, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Peraturan perundangan tersebut telah mengkrim -6 jenis-jenis tindak pidana *cyber crime* berikut ancaman hukuman bagi setiap pelanggarnya.

Kebijakan kriminalisasi yang termasuk kategori tindak pidana siber telah dirumuskan dalam Rancangan Kitab Undang-Undang Hukum Pidana (RKUHP) sebagaimana dirumuskan dalam buku kedua: Tindak Pidana, Bab VIII : Tindak Pidana yang membahayakan keamanan Umum Bagi Orang, Barang, Lingkungan Hidup, Bagian Kelima: Tindak Pidana terhadap Informatika dan Telematika Pasal 373-Pasal 379, yang mengatur tindak pidana *illegal access*, *illegal interception*, *data interference* dan *system interference*, penyalahgunaan nama domain, dan pornografi anak.

Dalam wacana pembangunan hukum pidana yang akan datang penanggulangan terhadap *cyber crime* perlu di imbangi dengan pembenahan dan pembangunan sistem hukum pidana secara menyeluruh,

yakni meliputi pembangunan struktur, kultur, dan substansi hukum pidana. Dalam hal ini kebijakan hukum pidana menduduki posisi yang strategis dalam pengembangan hukum pidana modern (id.yhs4.search.yahoo.com diakses 26 Juli 2013) Kebijakan hukum pidana bertujuan untuk mewujudkan kemakmuran dan kesejahteraan rakyat secara menyeluruh.

Penegakan Hukum Terhadap Pelaku Tindak Pidana *Cyber Crime* di Indonesia

Penegakan hukum terhadap pelaku tindak pidana *cyber* masih punya kendala Meskipun sudah disahkannya Rancangan Undang-Undang ITE menjadi Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang memperluas alat bukti *cyber crime* yang sebelumnya tidak di atur dalam KUHP seperti substansi yang terkandung dalam Pasal 5 tentang perluasan alat bukti baru, diterimanya Informasi Elektronik dan/ Data Elektronik atau hasil cetakannya sebagai alat bukti yang sah sesuai dengan hukum acara yang berlaku di Indonesia. Penegakan hukum terhadap pelaku tindak pidana *cyber crime* masih terkendala beberapa hal yaitu; masih rendahnya *skill*/ kualitas yang dimiliki oleh aparat penegak hukum dalam memberantas para *cracker* didunia maya, keterbatasan sarana prasarana *up to date* yang dimiliki Kepolisian seperti laboratorium *cyber crime* seharusnya ada disetiap Polda guna mempercepat deteksi dan antisipasi keberadaan para

cracker saat beraksi akan tetapi hanya Mabes Polri dan beberapa Kepolisian Kota Besar yang memiliki *Lab Cyber* sehingga terjadi kendala keterlambatan serta biaya tinggi dalam setiap prose penyelidikan kasus *cyber crime* di Indonesia, serta adanya keengganan para korban tindak pidana untuk melaporkan kejahatan yang menimpa dirinya oleh karena alasan privasi, ekonomis maupun ketidakpercayaan korban terhadap kemampuan dan dedikasi aparat Kepolisian dalam mengungkap kasus.

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 konvensi-konvensi 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 kedisiplinan dalam menggunakan perangkat saat berselancar di dunia maya. Kegiatan tersebut dapat berupa tindakan-tindakan 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 berorientasi 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.

KESIMPULAN DAN SARAN

Berdasarkan uraian diatas, maka dapat disimpulkan dan disarankan hal-hal sebagaimana berikut:

Kesimpulan

1. Pengaturan *cyber crime* dalam sistem hukum pidana Indonesia belum diatur dalam ranah hukum *cyberlaw* khusus akan tetapi disusun dalam beberapa perundang-undangan yaitu Undang-Undang No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-Undang No 36 Tahun 1999 tentang Telekomunikasi, Undang-

Undang No 15 Tahun 2003 tentang Terorisme, Undang-undang No 19 Tahun 2002 tentang Hak Cipta, kriminalisasi terhadap *cyber crime* juga diatur dalam RKUHP baru yang sedang dipersiapkan.

2. Secara umum Upaya Penegakan hukum terhadap pelaku tindak pidana *cyber crime* di Indonesia belum mencapai target masih banyak kasus-kasus *cyber crime* tersebar di seluruh yurisdiksi hukum Indonesia masih lambat dalam penanganannya. Begitupun dengan Penyelidikan, penyidikan maupun identifikasi terhadap pelakunya, dikarenakan masih minimnya perangkat Teknologi Informasi yang dimiliki instansi penegak hukum dalam mendeteksi pelaku tindak pidana yang tidak terbatas waktu, tempat, wilayah dan Negara. Meskipun demikian beberapa kasus besar yang mensabotase situs-situs Negara dan kepentingan orang banyak sudah ditangani dan diselesaikan dengan baik.

Belum ada pengaturan dalam perundang-undangan tentang *cyber crime* yang membahas tentang perlindungan terhadap korban *cyber crime* baik membahas tentang pemberian restitusi, kompensasi maupun asistensi terhadap korban, pengembalian hak-hak korban hanya diatur dalam undang-undang tentang perlindungan saksi dan korban tentang kewajiban pemberian restitusi oleh pelaku terhadap korban yang ditentukan oleh putusan hakim artinya apabila hakim

memerintahkan untuk membayar restitusi maka pelaku membayar restitusi namun tidak ada sanksi apa-apa diatur dalam perundang-undangan apabila pelaku tidak membayar restitusi dikemudian hari. Tetapi apabila hakim tidak memvonis pelaku membayar restitusi, korban tidak mendapatkan apa-apa atas kerugiannya meskipun pelaku dipidana atas kesalahan-kesalahannya.

Saran

1. Dalam rancangan penyempurnaan Undang-Undang *Cyber* kedepan baik Rancangan KUHP baru maupun perundang-undangan diluar KUHP agar berorientasi terhadap kepentingan korban dengan mewajibkan pelaku untuk memeberikan restitusi terhadap korban didalam Pasal perundang-undangan penanggulangan *cyber crime*. Hal ini selain wujud perlindungan terhadap korban juga akan membuat penjahat berfikir panjang sebelum melakukan suatu tindak pidana.

DAFTAR KEPUSTAKAAN

Buku

- Agus Raharjo, *Cyber Crime, Pemahaman dan Upaya Pencegahan Berteknologi*, PT Citra Aditya Bakti, Bandung, 2002.
- Ahmad M. Ramli, *Cyber Law dan Haki Dalam Sistem Hukum 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 Teknologi Informasi Regulasi dan Konfegensi*, PT Refika Aditama, 2010.
- Dikdik M. Arief Mansur dan Elisatris Gultom, *Urgensi Perlindungan Korban Kejahatan Antara Norma*

dan Realita, Jakarta, Raja Grafindo Persada, 2007.

Muladi, *Kapita Selekta Sistem Peradilan Pidana*, Universitas Diponegoro, Semarang, 1995.

Sigid Suseno, *Yurisdiksi Tindak Pidana Siber*, PT Refika Aditama, Cet. Ke , 2012.

Yudha Bakti, *Hukum Internasional*, Alumni, Bandung, Cet ke 1, 2003.

Web

id.yhs4.search.yahoo.com diakses 26 Juli 2013