

**EKSISTENSI PROTOKOL INTERNET
SEBAGAI ALAT BUKTI DALAM PEMBUKTIAN PERKARA
CYBER CRIME (CYBER CRIME)**

Oleh

**Liliana Tedjosaputro
Fakultas Hukum UNTAG Semarang**

ABSTRAK

Dewasa ini banyak sekali kejahatan di dunia maya, baik yang terjadi secara disengaja maupun tidak, semakin canggihnya teknologi menyebabkan aparat kepolisian merasa kesulitan untuk mencegah hal ini. Peraturan yang ada kurang dapat mengakomodir hal ini karena dasar hukum penggunaan protocol internet dapat digunakan sebagai alat bukti dalam perkara pidana kejahatan dunia maya, baik pencemaran nama baik atau juga cracking, hacker dan juga peneipuan, dalam prakteknya telah digunakan, sepanjang perbuatannya melanggar Undang-Undang tentang informasi dan Transaksi Elektronik, namun demikian aparat penegak hukum belum ada kesatuan pendapat mengenai hal ini, apakah dapat digunakan sebagai alat bukti surat, atau petunjuk. Oleh karenanya Protokol Internet ini membutuhkan penelaahan karena posisinya yang cukup penting.

Kata Kunci : Protokol Internet, Alat Bukti, Tindak Pidana Kejahatan Dunia Maya.

ABSTRACT

Recently that has been many occurrences of cyber crimes, either the crime which is done intentionally or unintentionally, the technology improvement makes the police is having troubles in preventing thereof. The prevailing, regulations are unable to cover because the legal basis of internet protocol usage as proof is not yet provided clearly in the applicable laws. The existence of internet protocol can be used as proof in the cyber crime case, either defamation or cracking, hacker and also computer fraud, wich practically it has been used, to the extent of violation to Act of Electronic Information and Tranaction, but the law enforcer does not have the same idea on this matters, whether it can be used as letter proof, or guiding proof. Therefore the Internet Protocol requires for review because the importance of it's position.

Keywords : Internet protocol, Proof, Cyber Crime.

A. Pendahuluan

Pengertian Protokol Internet, menurut Wikipedia adalah Sebagai sekelompok protocol yang mengatur komunikasi data dalam proses tukar-menukar data dari satu computer ke

computer lain di dalam jaringan internet yang akan memastikan pengiriman data ke alamat yang dituju. Protokol ini tidaklah dapat berdiri sendiri, karena memang protocol ini berupa kumpulan protocol (protocol suite). Protokol ini

mampu bekerja dan diimplementasikan pada lintas perangkat lunak (*software*) di berbagai system operasi istilah yang diberikan kepada perangkat lunak ini adalah TCP/IP (*Transmission Control Protocol?Internet Protocol*).¹

Protokol TCP/IP dikembangkan pada akhir decade 1970-an hingga awal 1980-an sebagai sebuah protocol standar untuk menghubungkan komputer-komputer dan jaringan untuk membentuk sebuah jaringan yang luas (WAN/Wide Area Network). TCP/IP merupakan sebuah standar jaringanb gterbuka yang bersifat independen terhadap mekanisme transpot jaringan fisik yang digunakan, sehingga dapat digunakan di mana saja. Protokol ini menggunakan skema pengalaman yang sederhana yang disebut sebagai alamat IP (IP Address) yang mengizinkan hingga beberapa ratus juta computer untuk saling berhubunga satu sama lainnya di Internet. Protokol ini cocok untuk menghubungkan system-sistem berbeda (seperti *Microsoft Windows* dan keluarga *UNIX/Multiplexed Information and computing servise*) untuk membentuk jaringan yang heterogen. Protokol TCP/IP selalu berevolusi

seiring dengan waktu, mengingat semakin banyaknya kebutuhan terhadap jaringan computer dan internet. Pengembangan ini dilakukan oleh beberapa badan, seperti halnya *Internet Society (ISOC)*, *Internet Engineering Task Force (IETF)*. Macam-macam protocol yang berjalan di atas TCP/IP didefinisikan dalam dokumen yang disebut sebagai *Request Comment (RFC)* yangb dikeluarkan oleh IETF.²

Protokol Internet menjadi cukup sering terdengar akhir-akhir ini, dikarenakan link antara pelaku kejahatan dunia maya dan korban adalah hanya dapat dibuktikan dengan protocol internet. Seseorang yang melakukan tindak pidana kejahatan baik cracking, hacking, seringkali menggunakan piranti ini untuk lolos dari jeratan hukum. Kesulitan yang sering ditemui adalah para pelaku sering menggunakan anonym (nama samara). Dimana adalah sangat sulit membuktikan missal : pelaku dengan nama abc@gmail.com, pengguna ini kemudian melakukan tindak pidana pemalsuan bahkan mungkin penipuan dengan modus yang beraneka ragam dapat menawarkan produk elektronik yang tidak berfungsi, atau juga

¹ https://id.wikipedia.org/wiki/Protokol_Internet (akses 18 Maret 2016)

²Ibid

menawarkan produk yang kurang dijaga mutunya atau juga tidak ada garansinya, produk yang merupakan produk black market, produk yang tidak sesuai dengan janjinya sampai terburuk adalah menawarkan sesuatu dan tidak memberikan sesuatu apapun bahkan korbanya telah memberikan sesuatu uang sebagai pengganti produk yang tidak sesuai tersebut. Korban lapor kepada aparat tersebut pada gilirannya akan dikecewakan karena tentunya pengguna tersebut akan sulit sekali dilacak, karena nama yang digunakan saja palsu, alamatnya tidak sebenarnya bahkan pelaku sudah beralih rupa menjadi orang lain yang sulit dibuktikan keterkaitannya dengan pelaku.

Satu-satunya cara untuk membuktikan adalah dengan meneliti alamat protocol internet dari pelaku. Setiap komputer yang terhubung dengan internet atau dunia maya mempunyai kode khusus atau alamat khusus, dalam hal ini adalah suatu protocol dengan nomor tertentu dan aturan tertentu sehingga dengan nomor yang sekaligus sebagai alamat tersebut maka seseorang akan memiliki akses dan dapat melakukan penjelajahan (browsing) di dunia maya. Untuk Indonesia misalnya mereka mempunyai

kode sendiri, jadi sebetulnyakalau dalam dunia maya protocol ini sangat penting karena menentukan kedudukan seseorang dan posisi letak dari seseorang ketika mengakses komputer yang terhubung dengan dunia maya. Sebenarnya hal ini masih mengundang pertanyaan apakah computer tersebut benar dipergunakan oleh orang A. Hal ini berbeda dengan peristiwa hukum yang diatur dalam KUHP Pidana, ketika seseorang melakukan suatu perbuatan hukum kemudian menimbulkan adanya peristiwa hukum, ada hubungan sebab akibat sehingga dalam Pengadilan seseorang yang melakukan suatu kejahatan dapat dengan mudah dibuktikan dari kartu tanda pengenal, saksi dan juga identitas lainnya. Sehingga pembuktian mengenai diri seseorang adalah absolut dan tidak dapat disangkal oleh tindak pelaku tindak pidana. Sebaliknya jika dipersamakan dengan apa yang terjadi dalam dunia maya maka hal ini menjadi sulit, seseorang masih memerlukan pembuktian yang lebih dalam, Misal : pelaku A apakah benar orang tersebut yang didepan protokol Internet tersebut adalah benar yang melakukan tindak kejahatan tersebut. Saksi sangatlah sulit untuk diperoleh, masih ditambah

dengan jika pengguna tersebut sering berpindah tempat. Bahkan sekarang ada juga piranti lunak yang dapat mengelabui protokol ini dengan menggunakan protokol dari Negara lain maka mereka dapat berupaya untuk melakukan tindak kejahatan dengan lokasi yang tidak terlacak.

Indonesia belum memiliki undang-undang yang mengatur mengenai protokol internet serta interkoneksi berbasis jaringan circuit switch. Jadi bilamana ingi ada pengaturan yang menyangkut penomoran protokol internet, maka Undang-undang mengenai Telekomunikasi harus dilakukan revisi, tidaklah mengherankan kalau setiap kasus tindak pidana kejahatan dunia maya mengundang kontroversi dan terus menerus menyebabkan pelaku tindak pidana dalam dunia maya bebas untuk melakukan tindakan pidana dengan orang lainnya hanya berbeda media yang digunakan.

Pihak kepolisian hanya memperoleh ruang untuk meneliti suatu tindak pidana kejahatan jika protokol internet telah diketahui, tetapi sebenarnya protokol ini sendiri baru merupakan petunjuk dan bukan merupakan dasar yang dapat

membuktikan seseorang melakukan tindak pidana, baru merupakan bukti permuiulaan akan tetapi protokol internet sebenarnya adalah kunci pembuktian dari tindakan pidana itu sendiri, akan tetapi kita tidak akan membahas kedudukan protokol internet dalam alat bukti, dan apakah hal ini dapat menjadi alat bukti yang sah.

B. Permasalahan

Bagaimana eksistensi protocol internet sebagai alat bukti dalam hukum Indonesia dan apakah protokol internet dapat dianggap sebagai alat bukti utama atau hanyalah sebagai alat bukti yang fungsinya memperkuat alat bukti lain ?

C. Pembahasan

1. Protokol Internet Sebagai Alat Bukti

Sebelum membahas mengenai eksistensi protokol internet sebagai alat bukti dalam system hukum pidana dan perdata maka akan lebih baik kalau kita melihat definisi dunia maya atau dunia siber, tindak pidana kejahatan siber, alat bukti baik menurut KUH Perdata dan Pidana.

Dunia Siber/Dunia Maya

Menurut Wikipedia dunia siber (*cyberspace*) adalah :

Media elektronik dalam jaringan computer yang banyak dipakai untuk keperluan komunikasi satu arah maupun timbal-balik secara online (terhubung langsung). Dunia maya ini merupakan integrasi dari berbagai peralatan teknologi komunikasi dan jaringan computer (sensor, transduser, koneksi, transmisi, prosesor, signal, kontroler) yang dapat menghubungkan peralatan komunikasi (computer, telepon genggam, instrumentasi elektronok, dan lain-lain) yang tersebar diseluruh dunia secara interaktif.

Kata "cyberspace" (dari cybernetics dan space) berasal dan pertama kali diperkenalkan oleh penulis novel fiksi ilmiah, William Gibson dalam buku ceritanya, "Burning Chrome" 1982 dan menjadi populer pada novel berikutnya, Neuromancer, A consensual hallucination experienced daily billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of every

computer in the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding.

Cyber Crime (Kejahatan Siber)

Secara terminologis, kejahatan yang berbasis pada teknologi informasi dengan menggunakan media komputer sebagaimana terjadi saat ini, dapat disebut dengan beberapa istilah yaitu computer misuse, computer abuse, computer fraud, computer related-crime. Computer assisted crime, computer related crime. Menurut Barda Nawawi Arief, pengertian computer related crime sama dengan cyber crime. Tb. Ronny R. Nitibaskara berpendapat bahwa kejahatan yang terjadi melalui atau pada jaringan computer di dalam internet disebut cyber crime. Kejahatan ini juga dapat disebut kejahatan yang berhubungan dengan komputer (computer related crime yang mencakup 2 kategori kejahatan, yaitu kejahatan yang menggunakan komputer sebagai sarana atau alat dan menjadikan

komputer sebagai sasaran atau objek kejahatan.³

Telaah Alat Bukti

Hukum Perdata

Pasal 1866 KUH Perdata

Alat pembuktian meliputi, bukti tertulis, bukti saksi, persangkaan, pengakuan, sumpah.

Alat Bukti Tertulis atau surat ialah segala sesuatu yang memuat tanda-tanda bacaan yang dimaksudkan untuk mencurahkan isi hati atau untuk menyampaikan buah pikiran seseorang dan dipergunakan sebagai pembuktian.

Alat bukti Saksi adalah kepastian yang diberikan kepada hakim di persidangan tentang peristiwa yang dipersengketakan dengan jalan pemberitahuan secara lisan dan pribadi oleh orang yang bukan salah satu pihak dalam perkara, yang dipanggil di persidangan.

Persangkaan adalah kesimpulan-kesimpulan yang oleh Undang-undang atau hakim ditarik dari suatu peristiwa yang terang nyata kearah peristiwa lain yang belum terang kenyataannya.

Pengakuan adalah keterangan sepihak baik tertulis maupun lisan yang tegas dan dinyatakan oleh salah satu pihak dalam perkara di persidangan, yang membenarkan baik seluruhnya atau sebagian dari suatu peristiwa, hak atau hubungan hukum yang diajukan oleh lawannya yang mengakibatkan pemeriksaan lebih lanjut oleh hakim tidak perlu lagi.

Hukum Pidana

Teori Pembuktian

Dalam ilmu pengetahuan terdapat beberapa teori tentang beban pembuktian yang menjadi pedoman bagi hakim, antara lain:

Teori pembuktian yang bersifat menguatkan belaka (bloot affirmatief)

Menurut teori ini siapa yang mengemukakan sesuatu harus membuktikannya dan bukan yang mengingkari atau yang menyangkalnya. Teori ini telah ditinggalkan.

Teori hukum obyektif

Menurut teori ini, mengajukan gugatan hak atau gugatan berarti bahwa penggugat minta kepada hakim agar hakim menerapkan ketentuan-ketentuan hukum obyektif terhadap peristiwa yang diajukan. Oleh karena itu penggugat harus membuktikan kebenaran daripada

³Widodo, Sistem Pidana dalam Cyber Crime, CV.Aswaja Pressindo, Yogyakarta, 2009,hal.23

peristiwa yang diajukan dan kemudian mencari hukum obyektifnya untuk diterapkan pada peristiwa itu.

Teori hukum public

Menurut teori ini maka mencari kebenaran suatu peristiwa dalam peradilan merupakan kepentingan public. Oleh karena itu hakim harus diberi wewenang yang lebih besar untuk mencari kebenaran. Disamping itu para pihak ada kewajiban yang sifatnya hukum public. Untuk membuktikan dengan segala macam alat bukti. Kewajiban ini harus disertai sanksi pidana.

Teori hukum acara

Asas audi et alteram partem atau juga asas kedudukan prosesuil yang sama daripada para pihak dimuka hakim merupakan asas pembagian beban pembuktian menurut teori ini.⁴

Pasal 184-189 KUH Pidana

1. Keterangan Saksi

Pasal 1 butir 27 KUHP, ditentukan :*“Keterangan saksi adalah salah satu alat bukti perkara pidana yang berupa keterangan dari saksi mengenai suatu peristiwa pidana yang*

ia dengar sendiri, ia lihat sendiri dan ia alami sendiri dengan menyebut alasan dari pengetahuannya itu”:

Pasal 1 butir 26 KUHP ditentukan :*“Saksi adalah orang yang dapat memberikan keterangan guna kepentingan penyelidikan, penuntutan dan peradilan tentang suatu perkara pidana yang ia dengar sendiri, ia lihat sendiri dan ia alami sendiri”*.

2. Keterangan ahli

Pasal 1 butir 28 KUHP, ditentukan :*“Keterangan ahli adalah keterangan yang diberikan oleh seorang yang memiliki keahlian khusus tentang hal yang diperlukan untuk membuat terang suatu perkara pidana guna kepentingan pemeriksaan”*.

Pasal 186 KUHP ditentukan :*“Keterangan ahli ialah apa yang seorang ahli nyatakan di sidang Pengadilan”*.

3. Alat Bukti Surat

Surat merupakan alat bukti yang menduduki urutan ketiga dari alat-alat bukti lain sebagaimana tersebut kedalam Pasal 184 ayat (1) KUHP.

Alat Bukti yang sah adalah :

- a. Keterangan saksi;
- b. Keterangan ahli;

⁴M. Yahya Harahap, Hukum Acara Perdata tentang Gugatan, Persidangan, Penyitaan, Pembuktian, dan Putusan pengadilan, Sinar Grafika, Jakarta, 2004, hal 522

- c. Surat;
- d. Petunjuk;
- e. Keterangan terdakwa;

Pasal 187 KUHP menyatakan bahwa surat dibuat atas sumpah jabatan atau dikuatkan dengan sumpah, adalah :

- a. Berita Acara dan surat-surat lain dalam bentuk resmi yang dibuat oleh pejabat umum yang berwenang atau yang dibuat dihadapannya, yang memuat tentang keterangan tentang kejadian atau keadaan yang didengar, dilihat atau dialami sendiri, disertai dengan alasan yang jelas dan tegas tentang keterangannya;
- b. Surat yang dibuat berdasarkan ketentuan peraturan perundang-undangan atau surat yang dibuat oleh pejabat mengenai hal yang termasuk dalam tata laksana yang menjadi tanggung jawabnya dan diperuntukan bagi pembuktian sesuatu hal atau sesuatu keadaan;
- c. Surat keterangan dari seorang ahli yang memuat pendapat berdasarkan keahliannya mengenai sesuatu hal atau sesuatu keadaan yang diminta secara resmi kepadanya;

- d. Surat lain yang hanya dapat berlaku jika ada hubungannya dengan isi dari alat pembuktian lain;

4. Alat Bukti Petunjuk

Alat bukti petunjuk diatur dalam pasal 188 ayat (1) KUHP, menyatakan :

- a. Petunjuk perbuatan, kejadian atau keadaan, yang karena persesuaiannya, baik antara satu dengan yang lain, mauoun dengan tindak pidana itu sendiri, meandakan bahwa telah terjadi suatu tindak pidana dan siapa pelakunya.
- b. Petunjuk sebagaimana diatur ayat 1 hanya dapat diperoleh dari :
 - 1. Keterangan saksi
 - 2. Surat
 - 3. Keterangan terdakwa
- c. Penilaian atas kekuatan pembuktian dari suatu petunjuk dalam setiap keadaan tertentu dilalukan oleh hakim dengan arif lagi bijaksana setelah ia mengadakan pemeriksaan dengan penuh kecermatan dan keseksamaan berdasarkan hati nuraninya.

Pemegang peran dalam penentuan alat bukti petunjuk berdasarkan pada penilaian oleh hakim.

5. Keterangan Terdakwa

Pengertian keterangan terdakwa diatur pasal 189 ayat (1) KUHP :

“keterangan terdakwa ialah apa yang terdakwa nyatakan disidang tentang perbuatan yang ia lakukan atau yang ia ketahui sendiri atau alami sendiri”

Undang-Undang Nomor : 11/2008 tentang Informasi dan Transaksi Elektronik

Pasal 5 ayat (1) UU Nomor 11 Tahun 2008

Informasi Elektronik dan atau Dokumen Elektronik dan atau hasil cetaknya merupakan alat bukti yang sah.

Pasal 1 ayat 1 Undang-Undang Nomor 11 Tahun 2008

Yang dimaksud dengan Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, gambar, peta, rancangan,

foto, electronic (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.

Pasal 1 ayat 4 Undang-Undang Nomor 11 Tahun 2008

Sedangkan yang dimaksud dengan 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 tetapi 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.

Pasal 5 ayat 2 UU Nomor 11 Tahun 2008

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.

Protokol internet dilihat dari semua alat bukti tersebut adalah sangat sulit untuk dimasukkan kedalam klasifikasi perundang-undangan baik perdata maupun pidana serta juga Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Permasalahan yang dijumpai adalah protokol internet hanyalah sekumpulan angka yang dikenal internet dan tidak dalam bentuk tertulis sehingga Undang-Undang Nomor :

11 Tahun 2008 juga tidak mengatur tentang protokol internet. Dilihat dari segi hukum pidana dan perdata protokol internet tidak dapat diklasifikasikan sebagai surat karena bukanlah berbentuk tertulis dan tidak dapat dibuktikan secara fisik, protokol ini hanya dapat dibuktikan jika jejak (trace) pengguna terlihat di jejaring yang telah digunakan oleh pengguna tersebut.

Persangkaan dan juga keterangan saksi serta ahli, juga tidak masuk klasifikasi protokol internet. Sementara yang paling mungkin adalah petunjuk tetapi kalau kita melihat dari pasal 188 KUHP, Petunjuk hanya dapat diperoleh dari keterangan saksi, terdakwa dan surat. Apakah protokol internet dapat diperoleh dari ketiga hal ini. Hal ini tentunya sangat sulit karena protokol internet ini tidak ada sertifikasi secara tertulis, sangat berbeda dengan ketika seseorang memperoleh KTP atau yang sekarang lebih dikenal dengan E-KTP, mereka tidak serta merta memperoleh E-KTP dengan otomatis, ada proses dimana seseorang melakukan permohonan ke Kantor Kecamatan dan akhirnya dengan pengantar dari Ketua RT, RW akhirnya diberikanlah E-KTP hal yang sama juga terjadi dengan tanda pengenal lain seperti, SIM, kartu BPJS dan sebagainya. Kesemua kartu identitas ini memiliki sumber bukti yang jelas sehingga dapat diterima di depan pengadilan. Sehingga manakala Hakim bertanya tentang jati diri dari seorang terdakwa, sering penuntut akan mengajukan bukti tersebut hal ini

sudah umum adanya. Sedangkan ketika pelanggar tindak pidana dunia maya melakukan apa yang disebut dengan carding, hacking, cracking, tidak ada pembuktiannya. Ketika Hakim dipertunjukkan protokol internet maka harus ada keterangan para ahli dan juga bukti-bukti lain. Keterangan ahli telematika seperti Roy Suryo hanyalah sebagai pendukung dan bukan sebagai pembukti yang dapat memastikan kalau orang tersebut adalah orang yang sama ketika suatu perbuatan pelanggaran hukum terjadi.

Bahkan dalam Undang-Undang tentang Informasi dan Teknologi Elektronik protokol internet tidak diatur, sehingga manakala seseorang diajukan maka pembuktian orang tersebut adalah sangat lemah bahkan bisa dikatakan sumir karena tidak diketahui secara jelas, apakah orang tersebut yang telah memindahkan data atau informasi elektronik sehingga terjadi suatu peristiwa hukum sulit dibuktikan kebenarannya dan hal ini dapat dibuktikan jika protokol internetnya diketahui sementara hal ini belum diatur dalam perundang-undangan manapun. Seperti kita dapat melihat dalam

kasus Prita Mulyasari, sebenarnya jika melihat kasus pemindahan informasi elektronik berupa e-mai; sehingga akhirnya terkirim kerumah sakit tersebut, maka sebenarnya pengakuan saudari Pritalah yang menyebabkan seorang hakim berkesimpulan Prita yang membuka kasus tersebut, sebaliknya Prita sendiri tidak dapat dibuktikan bahwa Dia yang telah mengirimkan data atau informasi elektronik tersebut.

Pemberantasan Tindak Pidana Siber **Teori Penanggulangan Kejahatan**

Dalam usaha untuk menanggulangi kejahatan mempunyai dua cara yaitu preventif (mencegah sebelum terjadinya kejahatan) dan tindakan represif (usaha sesudah terjadinya kejahatan). Berikut ini diuraikan pula masing-masing usaha tersebut :

1. Tindakan Preventif

Tindakan preventif adalah tindakan yang dilakukan untuk mencegah atau menjaga kemungkinan akan terjadinya kejahatan. Menurut A. Qirom Samsudin M, dalam kaitannya untuk melakukan tindakan preventif adalah mencegah kejahatan lebih baik daripada

mendidik penjahat menjadi baik kembali, sebab bukan saja diperhitungkan segi biaya, tapi usaha ini lebih mudah dan akan mendapat hasil yang memuaskan atau mencapai tujuan.

Selanjutnya Bonger berpendapat cara menanggulangi kejahatan yang terpenting adalah :

- 1) Preventif kejahatan dalam arti luas, meliputi reformasi dan prevensi dalam arti sempit;
- 2) Prevensi kejahatan dalam arti sempit meliputi :
 - a. Moralistik yaitu menyebarluaskan sarana-sarana yang dapat memperteguh moral seseorang agar dapat terhindar dari nafsu berbuat jahat.
 - b. Abalionistik yaitu berusaha mencegah tumbuhnya keinginan

kejahatan meniadakan faktor-faktor yang terkenal sebagai penyebab timbulnya kejahatan, Misalnya memperbaiki ekonomi (pengangguran, kelaparan, mempertinggi peradaban, dan lain-lain);

- 3) Berusaha melakukan pengawasan dan pengontrolan terhadap kejahatan dengan berusaha menciptakan:
 - a. Sistem organisasi
 - b. Sistem peradilan yang objektif
 - c. Hukum (perundang-undangan) yang baik.
- 4) Mencegah kejahatan dengan pengawasan dan patrol yang teratur;
- 5) Prevensi kenakalan anak-anak sebagai sarana

pokok dalam usaha
prevensi kejahatan pada
umumnya.

2. Tindakan Represif

Tindakan Represif adalah segala tindakan yang dilakukan oleh aparat penegak hukum sesudah terjadinya tindakan pidana.

Tindakan Represif terlebih menitikberatkan terhadap orang yang melakukan tindak pidana, yaitu antara lain dengan memberikan hukum (pidana) yang setimpal atas perbuatannya. Tindakan ini sebenarnya dapat juga dipandang sebagai pencegahan untuk masa yang akan datang. Tindakan ini meliputi cara aparat penegak hukum dalam melakukan penyidikan, penyidikan lanjutan, penuntutan pidana, pemeriksaan dipengadilan, eksekusi dan seterusnya sampai pembinaan narapidana.

Penanggulangan kejahatan secara represif ini dilakukan juga dengan tehnik rehabilitas, menurut Cressy terdapat dua

konsepsi mengenai cara atau tehnik rehabilitasi, yaitu :

1. Menciptakan sistem program yang bertujuan untuk menghukum penjahat, sistem ini memperbsiki antara lain hukuman bersyarat dan hukuman kurungan.
2. Lebih ditekankan pada usaha agar penjahat dapat berubah menjadi orang biasa, selama menjalankan hukuman dicarikan pekerjaan bagi terhukum dan konsultasi psikologis, diberikan kursus keterampilan agar kelak menyesuaikan diri dengan masyarakat.

Tindakan represif juga disebutkan sebagai pencegahan khusus, yaitu suatu usaha untuk menekankan jumlah kejahatan dengan memberikan hukuman (pidana) terhadap pelaku kejahatan dan berusaha pula melakukan perbuatan dengan jalan memperbaiki si pelaku yang berbuat kejahatan. Jadi lembaga permasyarakatan bukan hanya tempat untuk mendidik narapidana untuk tidak

lagi menjadi jahat atau melakukan kejahatan yang pernah dilakukan.

Kemudian upaya penanggulangan kejahatan yang sebaik-baiknya harus memenuhi persyaratan sebagai berikut:

- 1) Sistem dan perasi kepolisian yang baik.
- 2) Peradilan yang efektif.
- 3) Hukum dan perundang-undangan yang berwibawa.
- 4) Koordinasi antar penegak hukum dan aparat pemerintah yang serasi.
- 5) Partisipasi masyarakat dalam penanggulangan kejahatan.
- 6) Pegawai dan kesiagaan terhadap kemungkinan timbulnya kejahatan.
- 7) Pembinaan organisasi kemasyarakatan.⁵

Penggunaan ProtokolInternet dalam Pemberantasan Kasus Kriminal Kejahatan Siber.

Ada beberapa contoh kasus yang dapat disebutkan terkait dengan kejahatan siber dan pemberantasan kejahatan siber.

1) Kasus Presiden JW vs MAA.

MAA adalah seorang lulusan SMP dan bekerja sebagai

tukang tusuk sate diwarung sate Margani, depan PI. Yang ditahan Bareskrim Polri atas tuduhan pornografi dan penghinaan dengan melanggar pasal 310 dan 311 KUHP, pasal 156 dan 157 KUHP, pasal 27, 45, 32, 35, 36, 51 UU ITE atas tindakannya mengunggah gambar hasil rekayasa yang menunjukkan Presiden JW beradegan seksual dengan mantan presiden MW di media sosial. Sebetulnya aparat dapat membuktikan bahwa dia adalah seorang yang telah melakukan penistaan dengan jalan media internet melalui protokol internet dan sebenarnya bukti dari kepolisian adalah lemah karena protokol internet ini belum diakui keberadaannya menurut sistim hukum di indonesia. Dan ketika akhirnya Presiden JW mencabut proses hukum yang terjadi maka tidaklah terjadi suatu proses hukum dan ataupun pembuktian yang harus dilakukan sehingga kembali tindak pidana semacam ini belum mendapat pengakuan

⁵Soejono D, *Pnanggulangan kejahatan (Crime Prevention)*, Alumni,Bandung, 1976, hal.32

bahwa tindak pidana semacam ini dapat dibuktikan secara terang jelas. Kasus ini berakhir dengan dicabutnya gugatan presiden JW kepada MAA.

2) Kasus RSP vs MS

Kasus ini menimpa mantan Direktur Utama perusahaan penerbangan di Indonesia, RSP yang didakwa melakukan pencemaran nama baik diakibatkan oleh email yang dikirimnya ke Dewan Komisaris perusahaan penerbangan di Indonesia tersebut. Kasus bermula saat RSP menjabat komisaris Utama dengan tugas melakukan fungsi kontrol dan pengawasan terhadap jalannya perusahaan. RSP menerima pesan email dengan seseorang tentang adanya penyimpangan di perusahaannya yang dilakukan bawahannya. Email itu lalu diteruskannya kepada jajaran direksi untuk dilakukan verifikasi dan audit.

Ternyata belakang RSP dilaporkan ke Polda Metro Jaya pada Mei 2012 karena dinilai

telah melakukan pencemaran nama baik. RSP dikenakan pasal 45 ayat 1 UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Kasus ini berakhir dengan dijatuhkannya hukuman percobaan kepada RSP.

3. Kasus MR vs Kr

Kasus ini bermula ketika MR menjalin hubungan asmara dengan K sehingga Kr meminta foto bugil dari Kr dan dipenuhi, dikarenakan kemudian Kr menolak meneruskan hubungan dengan MR kemudian MR akhirnya karena dendam menyebarkan foto tersebut dengan nuansa kebencian dan permusuhan serta mengikutsertakan unsur agama, yang bertujuan agar Kr dan suaminya berpisah. Penyebaran foto tersebut dilakukan melalui sosial media dengan akun facebook. Kasus ini berakhir dengan dijatuhkannya putusan pidana penjara 4 tahun dan 6 bulan serta denda Rp.10.000.000,00 (sepuluh juta rupiah)

Banyak kasus lain yang berkaitan dengan dunia maya ini berhenti ditengah jalan baik karena pembuktian akan hal ini adalah sangat tidak jelas dan hanya berdasarkan keterangan ahli. Hal ini di perparah dengan minimnya aparat penegak hukum akan apa yang dimaksud protokol internet. Secara umum kesulitan para penyidik untuk menjadikan protokol internet dan juga hal ini sekaligus menambah permasalahan dalam tindak pidana siber yang sejak awal kemunculannya sudah sangat sulit untuk dilakukan penindakan. Beberapa alasan yang menjadikan tindak pidana siber sulit untuk dilakukan penindakan adalah :

1. Kecapatan operasional dan kapasitas penyimpanan perangkat keras komputer membuat tindak pidana sangat sulit di deteksi (the operational speeds and storage capacity of computer hardware makes criminal activity very difficult to detect)

2. Aparat penegak hukum seringkali tidak memiliki keahlian teknis yang diperlukan untuk menangani tindak pidana yang terjadi dalam lingkungan pengolahan data (law enforcement officials often lack the necessary technical expertise to deal with criminal activity in the data proessing environment)
3. Banyak korban kejahatan komputer telah gagal untuk membuat rencana yang memungkinkan untuk menangani kejahatan komputer (many victims of computer crime have failed to create contingency plans to deal with computer crime)
4. Sekali tindak pidana telah terdeteksi, banyak perusahaan enggan untuk melaporkan tindak pidana tersebut karena takut terjadinya publisitas yang

merugikan, kehilangan goodwill, malu, hilangnya kepercayaan public kehilangan investor, atau dampak ekonomi (once criminal activity has been detected, many businesses have been reluctant to report criminal activity because of fear of adverse publicity, loss of public confidence, investor loss, loss of goodwill, embarrassment, loss of confidence investor loss, or economic repercussions).⁶

Secara umum tindak pidana siber masih sangat sulit untuk dilakukan pemberantasan karena hal tersebut dan secara khusus Undang-Undang ITE masih sangat memerlukan perubahan perbaikan, karena masih banyak

cakupan internet yang belum terjangkau, penerapan pasal yang terkadang tidak dapat dan alat bukti yang masih minim menjadikan seringkali pengajuan seseorang menjadi tersangka dalam tindak pidana siber dan kemudian ditingkatkan menjadi terdakwa, sangat sumir dan kurang dapat dibenarkan,. Kasus yang menimpa mantan Direktur Utama Merpati Rudy Setyopurnomo yang didakwa melakukan pencemaran nama baik diakibatkan oleh email yang dikirimkannya ke Dewan Komisaris Merpati, membuktikan bahwa aparat penegak hukum masih belum dapat mengklasifikasikan tindak pidana siber yang patut untuk dilakukan penyidikan dan tidak patut. Dan akhirnya sampai putusan kasasi,

⁶Grbiole Zeviar-Geese, The Sate of The Law on Cyberjurisdiction and cybercrime on the Internet, <http://www.gonzagajil.org/pdf/volume1/zeviar-Geese/Zeviar-Geese.pdf>,retrieve.

tidak ada satupun pasal dikenakan untuk mantan Dirut Merpati, karena tindakan tersebut bukan pencemaran nama baik, karena pelaporan yang merupakan fungsi dari direktur sebagai organ perseroan Direksi yang berkewajiban untuk melaporkan setiap ada tindakan yang tidak sepatutnya dilakukan oleh bawahannya. Bahwa kemudian si pelapor merasa ada indikasi pencemaran nama baik, tentunya dapat diberikan kesempatan pada pemeriksaan internal perusahaan dan tidak memenuhi klasifikasi pencemaran nama baik.

D. Penutup

1. Kesimpulan

- a. Masih banyak pelanggaran pidana dalam hak atas kekayaan intelektual dalam dunia maya yang tidak terjamin oleh Negara.
- b. Pengguna dunia maya masih terlindungi di Indonesia dengan

minimnya ketentuan yang mengatur hal ini dan peraturan yang masih melindungi hal yang berada di permukaan dan belum menyentuh hal yang berada pada paparan isi.

- c. Masih diperlukan upaya yang lebih mendalam untuk melakukan kajian akan hal ini dalam melakukan pemberantasan kejahatan siber.
- d. Kejahatan siber semakin merajarela dengan upaya yang sia-sia dari aparat khususnya mengenai penerbitan segala bentuk peraturan yang sama sekali tidak menyentuh tindak pidana itu sendiri. Contohnya : pembentukan peraturan tentang hate speech, bagaimana mungkin hate speech ini diatur dalam peraturan sendiri yang seharusnya dimasukkan dalam rancangan ketentuan pidana yang menyeluruh atas tindak pidana dunia maya.
- e. Masih terpecah-pecahnya ketentuan yang mengatur kejahatan siber menyebabkan pemerintah semakin sulit untuk mengadakan pengaturan dan penindakan. Diharuskan adanya

kodefikasi akan hal ini selama ini hanya berdasarkan yurisprudensi yang masih sangat sedikit.

2. Saran-saran

1. Pemerintah masih perlu untuk menyelesaikan perubahan Undang-Undang Telekomunikasi bersama dengan DPR secara lebih cepat tetapi lebih mampu menyelesaikan hal ini dengan penuh pendalaman akan esensi dari protokol internet ini.
2. Para aparat penegak hukum diharapkan untuk lebih mampu menelaah pengertian protokol internet dan istilah lain dalam dunia maya secara lebih tepat sehingga mereka dapat mengambilnya sebagai alat bukti dan bilamana perlu mengkorelasikan dengan undang-undang lain yang memungkinkan mereka untuk melakukan penindakan sehingga dapat ditindak lanjuti oleh aparat kejaksaan.
3. Upaya penindakan yang sering diklasifikasikan sebagai upaya pengelakan terhadap tindakan

tindakan pidana seseorang, harus disikapi secara lebih mendalam. Sering seseorang yang sebenarnya telah melakukan tindak pidana dan di bully di sosial media kemudian melakukan counter dengan Undang-Undang ITE. Sehingga hal ini menjadi alat untuk menutupi tindak kejahatan itu sendiri.

DAFTAR PUSTAKA

Buku

- Abdul Wahid dan Muhammad Habib. 2005. *Kejahatan Mayantara (Cyber Crime)*. Refika Aditama, Bandung
- D. Soedjono, 1976, *Penanggulangan Kejahatan (Crime Prevention)*, Alumni, Bandung.
- Emma Nurita, Cyber Notary, *Pemahaman Awal Dalam konsep pemikian*, Refika, Bandung.
- Grbiole Zeviar-Geese, *The State of The Law on Cyberjurisdiction and Cybercrime on the Internet*
- M. Yahya Harahap, 2004, *Hukum Acara Perdata tentang Gugatan*,

*Persidangan, Penyitaan, Pembuktian,
dan Putusan Pengadilan*, Sinar Grafika,
Jakarta,.

R. Setiawan, 1992, *Aneka Masalah
Hukum dan Hukum Acara Perdata*, Cet
I, Alumni, Bandung.

R. Subekti. 1995, *Hukum Pembuktian*,
Pradnya Paramita, Jakarta.

Sigid Suseno, 2012, *Yuridiksi
Tindak/Pidana Siber*, Refika Aditama,
Bandung

Widodo, 2009, *Sistem Pidanaaan
dalam Cyber Crime*, CV. Aswaja
Pressindo, Yogyakarta.

Peraturan Perundangan

Kitab Undang-Undang Hukum Pidana

Kitab Undang-Undang Hukum Acara
Pidana

Kitab Undang-Undang Hukum Acara
Perdata

Undang-Undang Noor 11 Tahun 2008
tentang Informasi dan Transaksi
Elektronik