UPAYA KRIMINALISASI DALAM HAL PENANGGULANGAN KEJAHATAN CYBER CRIME[1]

Oleh : Verrel Senza Nathaniel Rasso[2]
Roy Ronny Lembong [3]
Ollij Aneke Kereh[4]

ABSTRAK

Tujuan dilakukannya apenelitian ini yaitu untuk mengetahui bagaimana upaya kriminalisasi terhadap kejahatan dibidang teknologi Informasi di dunia maya (*Cyber Crime)* dan bagaimana penanggulangan kejahatan dibidang teknologi Informasi dunia maya *(Cyber Crime)* melalui hukum pidana yang dengana metode penelitian hukumnormatif disimpulkan: 1. Persoalan mengenai kebijakan kriminalisasi, yang selama ini sudah dilakukan tidak secara tegas menentukan dimasa mendatang mana yang sebaiknya digunakan untuk mengatur *cyber crime,* apakah Undang-Undang ITE (Informasi dan Transaksi Elektronik) atau RUU KUHP. Persoalannya adalah apabila kedua RUU itu disetujui dan diundangkan bukankan aturan mengenai *cyber crime* akan berlebihan bahkan apabila kedua ketentuan ini akan mengaturnya maka akan menimbulkan perbedaan dalam penerapannya dari kedua aturan yang ada. Sehingga perlu adanya ketegasan dalam aturan yang ada terkait dengan menggunakan teknologi informasi melalui peraturan perundang-undangan tersendiri. 2. Munculnya kejahatan baru *(cyber crime)* merupakan suatu fenomena yang memerlukan penanggulangan secara cepat dan akurat. Perubahan terhadap beberapa ketentuan yang terdapat dalam Kitab Undang-undang Hukum Pidana merupakan salah satu cara yang dapat dipergunakan untuk mengatasi jenis kejahatan baru tersebut. Mengingat dalam KUHP pengaturannya masih bersifat umum namun beberapa ketentuan yang ada dapat diterapkan mengingat kondisi hukum dan peraturan yang belum juga diundangkan mengatur di bidang *Cyber crime.*

Kata kunci: kriminalisasi; cyber crime;

PENDAHULUAN

A. Latar Belakang Penulisan

Cyberspace berbicara tentang dunia elektronik, ruang virtual dimana orang dapat hadir tanpa harus ada/perlu eksistensi secara fisik, yang mana keberadaan dan aktivitas manusia tersebut dapat diwujudkan melalui bahasa 0 dan 1. Pikiran, niat, dan emosi seseorang dapat diwujudkan melalui bits. Akan tetapi, sama seperti dunia realita, dalam cyberspace juga banyak terjadi kejahatan-kejahatan, yang lebih sering disebut sebagai cyber crime. Kejahatan dalam ruang virtual ini dapat berupa kejahatan konvensional maupun tindakan-tindakan orang yang kemudian di kriminalisasi sebagai bentuk kejahatan baru yang hanya mungkin terjadi dalam ruang virtual.

B. Perumsan Masalah

1. Bagaimana upaya kriminalisasi terhadap kejahatan dibidang teknologi Informasi di dunia maya (*Cyber Crime)*?
2. Bagaimana penanggulangan kejahatan dibidang teknologi Informasi dunia maya *(Cyber Crime)* melalui hukum pidana?

C. Metode Penelitian

Skripsi ini merupakan karya tulis yang dapat diklasifikasikan sebagai bagian dari penelitian Yuridis Normatif.

HASIL PEMBAHASAN

A. Upaya Kriminalisasi *Cyber Crime*

Kebijakan kriminalisasi merupakan suatu kebijakan dalam menetapkan suatu perbuatan yang semula bukan tindak pidana (tidak dipidana) menjadi suatu tindak pidana (perbuatan yang dapat dipidana). Jadi pada hakikatnya, kebijakan kriminalisasi merupakan bagian dari kebijakan kriminal (*criminal policy*) dengan menggunakan sarana hukum pidana (*penal*) sehingga itu termasuk bagian dari kebijakan hukum pidana (*penal policy*), khususnya kebijakan formulasi. Pertanyaan tentang kriminalisasi muncul ketika kita dihadapkan pada suatu perbuatan yang merugikan orang lain atau masyarakat yang hukumnya belum ada atau belum ditemukan. Berkaitan dengan kebijakan kriminalisasi terhadap perbuatan yang masuk dalam kategori *cyber crime* sebagai tindak

[1] Artikel Skripsi
[2] Mahasiswa pada Fakultas Hukum Unsrat, NIM. 17071101385
[3] Fakultas Hukum Unsrat, Magister Ilmu Hukum
[4] Fakultas Hukum Unsrat, Magister Ilmu Hukum

pidana perlu dikemukakan beberapa persoalan penting, yaitu:

1. Persoalan kriminalisasi timbul karena dihadapan kita terdapat perbuatan yang berdimensi baru, sehingga muncul pertanyaan adakah hukumnya untuk perbuatan tersebut. Kesan yang muncul kemudian adalah terjadinya kekosongan hukum yang akhirnya mendorong kriminalisasi terhadap perbuatan tersebut. Sebenarnya dalam persoalan *cyber crime*, tidak ada kekosongan hukum, ini terjadi jika digunakan metode penafsiran yang dikenal dalam ilmu hukum dan ini yang mestinya dipegang oleh aparat penegak hukum dalam menghadapi perbuatan-perbuatan yang berdimensi baru yang secara khusus belum diatur dalam undang-undang. Persoalan menjadi lain jika ada keputusan politik untuk menetapkan *cyber crime* dalam perundang-undangan tersendiri di luar KUHP atau undang-undang khusus lainnya. Sayangnya dalam persoalan mengenai penafsiran ini, para hakim belum sepakat mengenai teori beberapa perbuatan. Misalnya *carding,* ada hakim yang menafsirkan masuk dalam kateori penipuan, ada pula yang memasukkan dalam kategori pencurian. Untuk itu sebetulnya perlu dikembangkan pemahaman kepada para hakim mengenai teknologi informasi agar penafsiran mengenai suatu bentuk *cyber crime* ke dalam pasal-pasal dalam KUHP atau undang-undang lain tidak membingungkan.
2. Dilihat dari pengertian kriminalisasi, sesungguhnya kriminalisasi tidak harus berupa membuat undang-undang khusus diluar KUHP, dapat pula dilakukan tetap dalam koridor KUHP melalui amandemen. Akan tetapi proses antara membuat amandemen KUHP dengan membuat undang-undang khusus hampir sama, baik dari segi waktu maupun biaya, ditambah dengan ketidaktegasan sistem hukum kita yang tidak menganut sistem kodifikasi secara mutlak, menyebabkan munculnya bermacam-macam undang-undang khusus. Kriminalisasi juga terkait dengan persoalan harmonisasi, yaitu harmonisasi materi/substansi dan harmonisasi eksternal (internasional/global). Mengenai harmonisasi substansi, bukan hanya KUHP yang akan terkena dampak dari dibuatnya undang-undang tentang *cyber crime*. Kementerian Komunikasi dan Informasi RI mencatat ada 21 undang-undang dan 25 RUU yang akan terkena dampak dari undang-undang yang mengatur *cyber crime*.[5] Ini merupakan pekerjaan besar di tengah kondisi bangsa yang belum stabil secara politik maupun ekonomi. Harmonisasi eksternal berupa penyesuaian perumusan pasal-pasal *cyber crime* dengan ketentuan serupa dari negara lain, terutama dengan *Draft Convention on Cyber Crime* dan pengaturan *cyber crime* dari negara lain. Harmonisasi ini telah dilaksanakan baik dalam RUU ITE maupun dalam RUU KUHP. Judge Stenin Schjolberg dan Amanda M. Hubbard mengemukakan dalam persoalan *cyber crime* ini diperlukan standarisasi dan harmonisasi dalam tiga area, yaitu *legislation, criminal enforcement* dan *judicial* review.[6] Ini menunjukkan bahwa persoalan harmonisasi merupakan persoalan yang tidak berhenti dengan diundangkannya undang-undang yang mengatur *cyber crime*, lebih dari itu adalah kerjasama dan harmonisasi dalam penegakan hukum dan peradilannya.
3. Berkaitan dengan harmonisasi substansi, ada bagian yang tak disinggung dalam buku tersebut, terutama mengenai jenis pidana. Mengingat *cyber crime* merupakan kejahatan yang menggunakan atau bersaranakan teknologi komputer, maka diperlukan

[5] Kementerian Komunikasi dan Informasi RI, *RUU Informasi dan Transaksi Elektronik Sebagai Infrastruktur Fundamental Pengembangan Sisfonas,* Jakarta, 28 Juni 2005.

[6] Judge Stein Schjölberg dan Amanda M. Hubbard, *Harmonizing National Legal Approaches on Cybercrime,* WSIS Thematic Meeting on Cybersecurity, ITU, Geneva, 2005, Hal. 143.

modifikasi jenis sanksi pidana bagi pelakunya. Jenis sanksi pidana tersebut adalah tidak diperbolehkannya/dilarang si pelaku untuk menggunakan komputer dalam jangka waktu tertentu. Bagi pengguna komputer yang sampai pada tingkat ketergantungan, sanksi atau larangan untuk tidak menggunakan komputer merupakan derita yang berat. Jangan sampai terulang kembali kasus Imam Samudera – terpidana kasus terorisme Bom Bali I – yang dengan leluasa menggunakan *laptop* di dalam selnya.

4. Setelah harmonisasi dilakukan, maka langkah yang selanjutnya adalah melakukan perjanjian ekstradisi dengan berbagai negara. *Cyber crime* dapat dilakukan lintas negara sehingga perjanjian ekstradisi dan kerjasama dengan negara lain perlu dilakukan terutama untuk menentukan yurisdiksi kriminal mana yang hendak dipakai. Pengalaman menunjukkan karena ketiadaan perjanjian ekstradisi, kepolisian tidak dapat membawa pelaku kejahatan kembali ke tanah air untuk diadili.

   Hal lain yang luput dari perhatian adalah pertanggungjawaban *Internet Service Provider* (ISP) sebagai penyedia layanan internet dan Warung Internet (Warnet) yang menyediakan akses internet. Posisi keduanya dalam *cyber crime* cukup penting sebagai penyedia dan jembatan menuju jaringan informasi global, apalagi Warnet telah ditetapkan sebagai ujung tombak untuk mengurangi kesenjangan digital di Indonesia.

Tindak Pidana Cyber crime dalam UU ITE diatur dalam 9 Pasal, dari Pasal 27 sampai dengan Pasal 35. Dalam 9 pasal tersebut dirumuskan 20 bentuk atau jenis tindak pidana ITE. Pasal 36 tidak merumuskan bentuk tindak pidana ITE tertentu, melainkan merumuskan tentang dasar pemberatan pidana yang diletakkan pada akibat merugikan orang lain pada tindak pidana yang diatur dalam Pasal 27 sampai dengan Pasal 34. Sementara ancaman pidananya ditentukan dalam Pasal 45 sampai Pasal 52. Adapun rumusan pasal-pasal tersebut adalah sebagai berikut:“Pasal 27 yang berbunyi :1)Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan. 2)Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian. 3)Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik.4)Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman.“Pasal 28 yang berbunyi:1)Setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik.2)Setiap Orang dengan sengaja dan tanpa hak menyebarkan yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antar golongan (SARA).”“Pasal 29 yang berbunyi: “Setiap Orang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi.”“Pasal 30 yang berbunyi:1)Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun.2)Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apapun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.3)Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.”“Pasal 31 yang berbunyi:1)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.2)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 apapun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan.3)Kecuali intersepsi sebagaimana dimaksud pada ayat (1) dan ayat(2), intersepsi yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi penegak hukum lainnya yang ditetapkan berdasarkan undang-undang.4)Ketentuan lebih lanjut mengenai tata cara intersepsi sebagaimana dimaksud pada ayat (3) diatur dengan Peraturan Pemerintah.”“Pasal 32 yang berbunyi: 1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apapun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik public; 2)Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apapun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak; 3)Terhadap perbuatan sebagaimana dimaksud pada ayat (1) yang mengakibatkan terbukanya suatu Informasi Elektronik dan/atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya.”“Pasal 33 yang berbunyi: “Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apapun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya.”“Pasal 34 yang berbunyi:1)Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki: a) perangkat keras atau perangkat lunak Komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33; b) sandi lewat Komputer, Kode Akses, atau hal yang sejenis dengan itu yang ditujukan agar Sistem Elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 2)Tindakan sebagaimana dimaksud pada ayat (1) bukan tindak pidana jika ditujukan untuk melakukan kegiatan penelitian, pengujian Sistem Elektronik, untuk perlindungan Sistem Elektronik itu sendiri secara sah dan tidak melawan hukum.”“Pasal 35 yang berbunyi: “Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik.”“Pasal 36 yang berbunyi: “ Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 34 yang mengakibatkan kerugian bagi Orang lain.”“Pasal 37 yang berbunyi: “Setiap Orang dengan sengaja melakukan perbuatan yang dilarang sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 36 di luar wilayah Indonesia terhadap Sistem Elektronik yang berada di wilayah yurisdiksi Indonesia.”Dari uraian rumusan pasal-pasal bentuk-bentuk tindak pidana Cyber crime menurut Undang-undang Nomor 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik dapat diklasifikasikan menjadi 2 bentuk yakni:

1) Cyber crime yang menggunakan komputer sebagai alat kejahatan, yakni Pornografi Online (Cyber-Porno), Perjudian Online, Pencemaran nama baik melalui media sosial, penipuan melalui komputer, pemalsuan melalui komputer, pemerasan dan pengancaman melalui komputer, penyebaran berita bohong

melalui komputer, pelanggaran terhadap hak cipta, cyber terrorism

2) Cyber crime yang berkaitan dengan komputer, jaringan sebagai sasaran untuk melakukan kejahatan, yakni akses tidak sah (illegal acces), mengganggu sistem komputer dan data komputer, penyadapan atau intersepsi tidak sah, pencurian data, dan menyalahgunakan peralatan komputer.

Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.Perbuatan yang dilarang dalam Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik sama dengan perbuatan yang dilarang dengan Perubahan Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik tidak ada penambahan maupun pengurangan tindak pidana tersebut yang diancam pemidanaannya, sehingga bentuk-bentuk cyber crime masih sama dengan undang-undang sebelumnya.

B. Penanggulangan *Cyber crime* Melalui Sarana Penal

Kebijakan penanggulangan *cyber crime* dengan hukum pidana termasuk bidang *penal policy* yang merupakan bagian dari *criminal policy* (kebijakan penanggulangan kejahatan). Dilihat dari sudut *criminal policy*, upaya penanggulangan kejahatan (termasuk penanggulangan *cyber crime*) tidak dapat dilakukan semata-mata secara parsial dengan hukum pidana (sarana penal), tetapi harus pula ditempuh dengan pendekatan integral/sistemik. Sebagai salah satu bentuk *high tech crime* yang dapat melampaui batas-batas negara (bersifat *transnasional/transborder*), merupakan hal yang wajar jika upaya penanggulangan *cyber crime* juga harus ditempuh dengan pendekatan teknologi (*techno prevention*). Di samping itu, diperlukan pula pendekatan budaya/kultural, pendekatan moral/edukatif, dan bahkan pendekatan global melalui kerjasama internasional. Dalam pencegahan dan penanggulangan *cyber crime* dengan menggunakan sarana penal, merupakan salah satu upaya yang strategis sehingga pembahasan dari aspek ini perlu dilakukan. *Cyber crime* merupakan kejahatan yang dilakukan dengan dan memanfaatkan teknologi, sehingga pencegahan dan penanggulangan dengan sarana penal tidaklah cukup. Untuk itu diperlukan sarana lain berupa teknologi itu sendiri sebagai sarana non penal. Teknologi itu sendiri pun sebetulnya belum cukup jika tidak ada kerjasama dengan individu maupun institusi yang mendukungnya. Pengalaman negara-negara lain membuktikan bahwa kerjasama yang baik antara pemerintah, aparat penegak hukum, individu maupun institusi dapat menekan terjadinya *cyber crime*.

Tidak ada jaminan keamanan di *cyberspace,* dan tidak ada sistem keamanan komputer yang mampu secara terus menerus melindungi data yang ada di dalamnya. Para *hacker* akan terus mencoba untuk menaklukkan sistem keamanan yang paling canggih, dan merupakan kepuasan tersendiri bagi *hacker* jika dapat membobol sistem keamanan komputer orang lain. Langkah yang baik adalah dengan selalu memutakhirkan sistem keamanan komputer dan melindungi data yang dikirim dengan teknologi yang mutakhir pula.

Pada persoalan *cyberporn* atau *cyber sex*, persoalan pencegahan dan penanggulangannya tidaklah cukup hanya dengan melakukan kriminalisasi yang terumus dalam bunyi pasal. Diperlukan upaya lain agar pencegahannya dapat dilakukan secara efektif. Pengalaman beberapa Negara menunjukkan bahwa kerjasama antara pemerintah, aparat penegak hukum, dan masyarakat dapat mengurangi angka kriminalitas. Berikut pengalaman beberapa Negara itu.

1. Di Swedia, perusahaan keamanan internet, NetClean Technology bekerjasama dengan Swedish National Criminal Police Department dan NGO ECPAT, mengembangkan program *software* untuk memudahkan pelaporan tentang pornografi anak. Setiap orang dapat *mendownload* dan *menginstalnya* ke komputer. Ketika seseorang meragukan apakah material yang ada di internet itu legal atau tidak, orang tersebut dapat menggunakan *software*

itu dan secara langsung akan segera mendapat jawaban dari ECPAT Swedia.

2. Di Inggris, British Telecom mengembangkan program yang dinamakan Clean Feed untuk memblok situs pornografi anak sejak Juni 2004. Untuk memblok situs, *British Telecom* menggunakan daftar hitam dari *Internet Watch Foundation* (IWF). Saat ini British Telecom memblokir kira-kira 35.000 akses ilegal ke situs tersebut. Dalam memutuskan apakah suatu situs hendak diblok atau tidak, IWF bekerjasama dengan Kepolisian Inggris. Daftar situs itu disebarluaskan kepada setiap ISP, penyedia layanan isi internet, perusahaan filter/*software* dan operator *mobile phone*.
3. Norwegia mengikuti langkah Inggris dengan bekerja sama antara Telenor dan Kepolisian Nasional Norwegia, Kripos. Kripos menyediakan daftar situs *child pornography* dan Telenor memblok setiap orang yang mengakses situs itu. Telenor setiap hari memblok sekitar 10.000 sampai 12.000 orang yang mencoba mengunjungi situs itu.
4. Kepolisian Nasional Swedia dan Norwegia bekerjasama dalam memutakhirkan daftar situs *child pornography* dengan bantuan ISP di Swedia. Situs-situs tersebut dapat diakses jika mendapat persetujuan dari polisi.
5. Mengikuti langkah Norwegia dan Swedia, ISP di Denmark mulai memblokir situs *child pornography* sejak Oktober 2005. ISP di sana bekerjasama dengan Departemen Kepolisian Nasional yang menyediakan daftar situs untuk diblokir. ISP itu juga bekerjasama dengan NGO Save the Children Denmark. Selama bulan pertama, ISP itu telah memblokir 1.200 pengakses setiap hari. [7]

Sebenarnya Internet Service Provider (ISP) di Indonesia juga telah melakukan hal serupa, akan tetapi jumlah situs yang diblokir belum banyak sehingga para pengakses masih leluasa untuk masuk ke dalam situs tersebut, terutama situs yang berasal dari luar negeri. Untuk itu ISP perlu bekerjasama dengan instansi terkait untuk memutakhirkan daftar situs *child pornography* yang perlu diblok.

Faktor penentu lain dalam pencegahan dan penanggulangan *cyber crime* dengan sarana non penal adalah persoalan tentang etika. Dalam berinteraksi dengan orang lain menggunakan internet, diliputi oleh suatu aturan tertentu yang dinamakan *Netiquette* atau etika di internet. [8] Meskipun belum ada ketetapan yang baku mengenai bagaimana etika berinteraksi di internet, etika dalam berinteraksi di dunia nyata *(real life*) dapat dipakai sebagai acuan.

Meski Indonesia menduduki peringkat pertama dalam *cyber crime* pada tahun 2004, akan tetapi jumlah kasus yang diputus oleh pengadilan tidaklah banyak. Dalam hal ini angka *dark number* cukup besar dan data yang dihimpun oleh Polri juga bukan data yang berasal dari investigasi Polri, sebagian besar data tersebut berupa laporan dari para korban. Ada beberapa sebab mengapa penanganan kasus *cyber crime* di Indonesia tidak memuaskan:

1. *Cyber crime* merupakan kejahatan dengan dimensi *high-tech*, dan aparat penegak hukum belum sepenuhnya memahami apa itu *cyber crime.* Dengan kata lain kondisi sumber daya manusia khususnya aparat penegak hukum masih lemah.
2. Ketersediaan dana atau anggaran untuk pelatihan SDM sangat minim sehingga institusi penegak hukum kesulitan untuk mengirimkan mereka mengikuti pelatihan baik di dalam maupun luar negeri.
3. Ketiadaan Laboratorium Forensik Komputer di Indonesia menyebabkan waktu dan biaya besar. Pada kasus Dani Firmansyah yang mengakses situs KPU, Polri harus membawa harddisk ke Australia untuk meneliti jenis kerusakan

[7] Nitibaskara, Tb. Ronny R., *Problem Yuridis Cybercrime,* Makalah pada Seminar tentang Cyber Law, diselenggarakan oleh Yayasan Cipta Bangsa, Bandung, 2000, hal. 23.

[8]. *Ibid*

yang ditimbulkan oleh perbuatan tersebut.

4. Citra lembaga peradilan yang belum membaik, meski berbagai upaya telah dilakukan. Buruknya citra ini menyebabkan orang atau korban enggan untuk melaporkan kasusnya ke kepolisian.
5. Kesadaran hukum untuk melaporkan kasus ke kepolisian rendah. Hal ini dipicu oleh citra lembaga peradilan itu sendiri yang kurang baik, faktor lain adalah korban tidak ingin kelemahan dalam sistem komputernya diketahui oleh umum, yang berarti akan mempengaruhi kinerja perusahaan dan *web masternya*.

Upaya penanganan *cyber crime* membutuhkan keseriusan semua pihak mengingat teknologi informasi khususnya internet telah dijadikan sebagai sarana untuk membangun masyarakat yang berbudaya informasi. Keberadaan undang-undang yang mengatur *cyber crime* memang diperlukan, akan tetapi apalah arti undang-undang jika pelaksana dari undang-undang tidak memiliki kemampuan atau keahlian dalam bidang itu dan masyarakat yang menjadi sasaran dari undang-undang tersebut tidak mendukung tercapainya tujuan pembentukan hukum tersebut.

Kitab Undang-undang Hukum Pidana (KUHP) telah mengatur hubungan-hubungan hukum tentang kejahatan yang berkaitan dengan komputer yang kemudian berkembang menjadi *cyber crime*. Setidaknya ada dua pendapat yang berkembang sejalan dalam menangani kasus kejahatan yang berhubungan dengan komputer yang secara tidak langsung juga berkaitan dengan masalah *cyber crime* yakni;

1. KUHP mampu untuk menangani kejahatan di bidang komputer Mardjono Reksodiputro, pakar kriminolog dari Universitas Indonesia yang menyatakan bahwa kejahatan komputer sebenarnya bukanlah kejahatan baru dan masih terjangkau oleh KUHP untuk menanganinya. Pengaturan untuk menangani kejahatan komputer sebaiknya diintegrasikan ke dalam KUHP dan bukan ke dalam undang-undang tersendiri.
2. Kejahatan yang berhubungan dengan komputer memerlukan ketentuan khusus dalam KUHP atau undang-undang tersendiri yang mengatur tindak pidana dibidang komputer.

Bahwa hukum pidana yang ada tidak siap menghadapi kejahatan komputer, karena tidak segampang itu menganggap kejahatan komputer berupa pencurian data sebagai suatu pencurian. Kalau dikatakan pencurian harus ada barang yang hilang. Sulitnya pembuktian dan kerugian besar yang mungkin terjadi melatarbelakangi pendapatnya yang mengatakan perlunya produk hukum baru untuk menangani kejahatan komputer agar dakwaan terhadap pelaku kejahatan tidak meleset. Adanya ketentuan baru yang mengatur permasalahan tindak pidana komputer. Tindak pidana yang menyangkut komputer haruslah ditangani secara khusus, karena cara-caranya, lingkungan, waktu dan letak dalam melakukan kejahatan komputer adalah berbeda dengan tindak pidana lain.

Ketentuan-ketentuan yang terdapat dalam KUHP tentang *cyber cri*me masih bersifat global. Namun berdasarkan tingkat kemungkinan terjadinya kasus dalam dunia maya *(cyber)* dan kategorisasi kejahatan *cyber* menurut *draft convention on cyber crime* maupun pendapat para ahli.[9] Mengkategorikan beberapa hal yang secara khusus diatur dalam KUHP dan disusun berdasarkan tingkat intensitas terjadinya kasus tersebut yaitu;

a. Ketentuan yang berkaitan dengan delik pencurian;
b. Ketentuan yang berkaitan dengan perusakan/penghancuran barang;
c. Delik tentang pornografi;
d. Delik tentang penipuan;
e. Ketentuan yang berkaitan dengan perbuatan memasuki atau melintasi wilayah Orang;
f. Delik tentang penggelapan;
g. Kejahatan terhadap ketertiban umum;
h. Delik tentang penghinaan;
i. Delik tentang pemalsuan surat;

[9] Data diambilkan dari The Cybercrime Convention Committee (T-CY), *Strengthening Co-Operation Between Law Enforcement and the Private Sector, Examples of How the Private Sector has Blocked Child Pornographic Sites,* Strasbourg, 20 February 2006.

j. Ketentuan tentang pembocoran rahasia dan;
k. Delik tentang perjudian.

a.d. a. Ketentuan yang berkaitan dengan delik pencurian

Delik tentang pencurian dalam dunia maya termasuk salah satu delik yang paling populer diberitakan media massa. Pencurian disini tidak diartikan secara konvensional yakni tentang perbuatan mengambil barang secara nyata. Dalam kasus pencurian di Internet, barang yang dicuri yakni berupa data *digital* baik yang berisikan data transaksi keuangan milik orang lain maupun data yang menyangkut *software* (program) ataupun data yang menyangkut hal-hal yang bersifat rahasia.

Delik pencurian diatur dalam Pasal 362 KUHP dan variasinya diatur dalam Pasal 363 KUHP, yakni tentang pencurian dengan pemberatan; Pasal 364 KUHP tentang pencurian ringan, Pasal 365 tentang pencurian yang disertai dengan kekerasan; Pasal 367 KUHP tentang pencurian di lingkungan keluarga

Pasal 362 KUHP berbunyi :

> "Barangsiapa mengambil barang sesuatu, yang seluruhnya atau sebagian kepunyaan orang lain, dengan maksud untuk dimiliki secara melawan hukum, diancam karena pencurian, dengan pidana penjara paling lama lima tahun atau pidana denda paling banyak sembilan ratus rupiah."

Menurut hukum pidana, pengertian benda diambil dari penjelasan Pasal 362 KUHP yaitu segala sesuatu yang berwujud atau tidak berwujud, (misalnya listrik) dan mempunyai nilai di dalam kehidupan ekonomi dari seseorang. Data atau program yang tersimpan di dalam media penyimpanan disket atau sejenisnya yang tidak dapat diketahui wujudnya dapat berwujud dengan cara menampilkan pada layar penampil komputer *(screen)* atau dengan cara mencetak pada alat pencetak *(printer)*. Dengan demikian data atau program komputer yang tersimpan dapat dikategorikan sebagai benda seperti pada penjelasan Pasal 362 KUHP.

Namun dalam sistem pembuktian kita terutama yang menyangkut elemen penting dari alat bukti (Pasal 184 KUHAP ayat (1) huruf c) masih belum mengakui data komputer sebagai bagiannya karena sifatnya yang *digital*. Padahal dalam kasus *cyber crime* data elektronik sering kali menjadi barang bukti yang ada. Karenanya sangat realistis jika data elektronik dijadikan sebagai bagian dari alat bukti yang sah.

Pengertian "mengambil" pada *computer related crime* ialah mengambil dalam arti "mengkopi", yaitu mengambil sesuai dengan aslinya atau merekam data atau program yang tersimpan di dalam suatu disket dan sejenisnya ke disket lain dengan cara memberikan instruksi-instruksi tertentu pada komputer sehingga data atau program yang asli masih utuh dan tidak berubah dalam posisi semula .

Menurut penjelasan Pasal 362 KUHP, barang yang sudah diambil dari kekuasaan pemiliknya itu, juga harus berpindah dari tempat asalnya; padahal dengan mengkopi, data asli masih tetap ada pada media penyimpan semula. Namun untuk kejahatan komputer (termasuk didalamnya *cyber crime*) di sini, pengertian mengambil adalah melepaskan kekuasaan atas benda itu dari pemiliknya untuk kemudian dikuasai dan perbuatan itu dilakukan dengan sengaja dengan maksud untuk dimiliki sendiri: sehingga perbuatan mengopi yang dilakukan dengan sengaja tanpa ijin dari pemiliknya dapat dikategorikan sebagai perbuatan "mengambil" sebagaimana yang dimaksud dengan penjelasan Pasal 362 KUHP.

Dalam sistem jaringan (*network*), pengkopian data dapat dilakukan secara mudah tanpa harus melalui izin dari pemilik data. Hanya sebagian kecil saja dari informasi dan data di internet yang tidak bisa “diambil” oleh para pengguna internet. Pencurian bukan lagi hanya berupa pengambilan barang/material berwujud saja, tetapi juga termasuk pengambilan data secara tidak sah.

Penggunaan fasilitas *Internet Service Provider* (ISP) untuk melakukan kegiatan *hacking* dan *carding* erat kaitannya dengan delik pencurian yang diatur dalam Pasal 362 KUHP. Pencuri biasanya lebih mengutamakan memasuki sistem jaringan perusahaan finansial seperti penyimpanan data kartu kredit, komputer-komputer di bank atau situs-situs belanja on-line yang ditawarkan di media internet dan data yang didapatkan secara melawan hukum itu diharapkan memberi keuntungan bagi si pelaku. Keuntungan ini

dapat berupa keuntungan langsung (uang tunai) ataupun keuntungan yang didapat dari menjual data ke pihak ketiga (menjual data ke perusahaan pesaing).

a.d. b. Ketentuan yang berkaitan dengan perusakan, penghancuran barang

Ketentuan tersebut sangat berkaitan erat dengan kejahatan yang *hacking* dan *cracking* . Dalam kejahatan komputer (*computer crime*), perbuatan perusakan, penghancuran barang mempunyai pengertian suatu perbuatan yang dilakukan dengan suatu kesengajaan untuk merusak/menghancurkan media disket atau media penyimpan sejenis lainnya yang berisikan data atau program komputer sehingga akibat perbuatan tersebut data atau program yang dimaksud menjadi tidak berfungsi lagi dan pekerjaan-pekerjaan yang melalui proses komputer tidak dapat dilaksanakan. Sedangkan pada kejahatan mayantara *(cyber crime)* perbuatan perusakan dan penghancuran barang ini tidak saja ditujukan untuk merusak/menghancurkan media disket atau media penyimpan sejenis lainnya melainkan dapat juga perbuatan merusak dan menghancurkan tersebut ditujukan terhadap suatu data, *web site* ataupun *home page*. Delik ini juga termasuk didalamnya perbuatan merusak barang-barang milik publik *(Crime Against Public Property).*

Ketentuan mengenai perbuatan perusakan, penghancuran barang diatur dalam Pasal 406-412 KUHP. Apabila kejahatan tersebut ditujukan pada sarana dan prasarana penerbangan diatur dalam Pasal 479a-479h, 479m, dan 479p KUHP.

Pasal 406 KUHP berbunyi :

(1) Barangsiapa dengan sengaja melawan hukum menghancurkan, merusakkan, membikin tidak dapat dipakai lagi atau menghilangkan barang sesuatu yang seluruhnya atau sebagian adalah kepunyaan orang lain, diancam dengan pidana dipenjara paling lama dua tahun delapan bulan atau denda paling banyak empat ribu lima ratus rupiah

(2) Dijatuhkan pidana yang sama terhadap orang, yang dengan sengaja dan melawan hukum membunuh, merusakan, membikin tidak dapat digunakan atau menghilangkan hewan yang seluruhnya atau sebagian adalah kepunyaan orang lain

Pengertian-pengertian dalam Pasal 406 KUHP dapat dijelaskan sebagai berikut :

a. Pengertian "menghancurkan" *(vermaelen)*
   Menghancurkan atau membinasakan dimaksudkan sebagai merusak sama sekali sehingga suatu barang tidak dapat berfungsi sebagaimana mestinya.
b. Pengertian "merusakkan"
   Merusakkan dimaksudkan sebagai memperlakukan suatu barang sedemikian rupa namun kurang dan membinasakan *(beschadigen)*. Contoh perbuatan merusak data atau program komputer yang terdapat di internet dengan cara menghapus data atau program, membuat cacat data atau program, menambahkan data baru ke dalam suatu situs *(web)* atau sejenisnya secara acak. Dengan kata lain, perbuatan tersebut mengacaukan isi media penyimpanannya.
c. Pengertian "membikin / membuat tidak dapat dipakai lagi"
   Tindakan itu harus sedemikian rupa, sehingga barang itu tidak dapat diperbaiki lagi. Kaitannya dengan kejahatan maya *(cyber crime)* adalah perbuatan yang dilakukan tersebut menyebabkan data atau program yang tersimpan dalam media penyimpan *(data base*) atau sejenisnya menjadi tidak dapat dimanfaatkan (tidak berguna lagi). Hal ini disebabkan oleh data atau program telah dirubah sebagian atau seluruhnya, atau dirusak pada suatu bagian atau seluruhnya, atau dihapus pada sebagian atau pada keseluruhannya.
d. Pengertian menghilangkan
   Pengertian menghilangkan adalah membuat sehingga barang itu tidak ada lagi. Kaitannya dengan *cyber crime* ialah perbuatan menghilangkan atau menghapus data yang tersimpan pada *data base* (bisa juga tersimpan dalam suatu *web*) atau sejenisnya sehingga mengakibatkan semua atau sebagian dari data atau program menjadi hapus sama sekali.

Berdasarkan pengertian-pengertian mengenai perbuatan "menghancurkan", merusak, "membuat tidak dapat dipakai lagi" dan "menghilangkan" dapatlah disimpulkan bahwa makna dan perbuatan-perbuatan tersebut terdapat kesesuaian yang pada intinya perbuatan tersebut menyebabkan fungsi dari data atau program dalam suatu jaringan menjadi berubah/berkurang.

Perbuatan penghancuran atau perusakan barang yang dilakukan dengan kemampuan *hacking*-nya bukanlah perbuatan yang bisa dilakukan oleh semua orang awam. Kemampuan tersebut dimiliki secara khusus oleh orang yang mempunyai keahlian dan kreatifitas dalam memanfaatkan sistem, program, maupun jaringan. Motif untuk kejahatan ini sangat beragam yakni misalnya motif ekonomi, politik, pribadi atau motif kesenangan semata.

a.d. c. Ketentuan yang berkaitan dengan pornografi

Hadirnya media internet secara global menyebabkan siapa saja dapat untuk mengakses situs-situs yang tersedia secara mudah. Ketentuan tentang pornografi dalam dunia maya tidak saja hanya berupa tindak pidana penyebaran gambar-gambar yang dianggap tabu/porno untuk dipertontonkan kepada publik, melainkan juga dimanfaatkan sebagai media transaksi prostitusi secara *online*. Situs-situs porno tersebut juga menjual/menawarkan gambar-gambar bahkan cerita-cerita porno kepada setiap orang yang mengunjungi situs tersebut dengan pembayaran melalui transfer *online*. Kehadiran situs-situs porno jelas tidak sesuai dengan budaya Indonesia.

Delik yang berkaitan dengan pornografi diatur dalam Pasal 282 KUHP, yang bunyinya sebagai berikut

(1) Barangsiapa menyiarkan, mempertunjukkan atau menempelkan, gambaran atau benda, yang diketahui isinya dan melanggar kesusilaan, atau barangsiapa dengan maksud untuk disiarkan, dipertunjukkan atau ditempelkan di muka umum, membikin tulisan, gambaran atau benda tersebut, memasukkan ke dalam negeri, meneruskannya, mengeluarkannya dari negeri, atau mempunyai dalam persediaan, ataupun barangsiapa secara terang-terangan atau dengan mengedarkan surat tanpa diminta, menawarkannya atau menunjukkannya sebagai bisa di dapat. Diancam dengan pidana penjara paling lama satu tahun enam bulan atau denda paling tinggi tiga ribu rupiah.

(2) Barangsiapa menyiarkan, mempertunjukkan atau menempelkan di muka umum tulisan, gambaran atau benda yang melanggar kesusilaan atau barangsiapa dengan maksud untuk disiarkan, dipertunjukkan atau ditempelkan di muka umum, membuatnya, memasukkannya ke dalam negeri, meneruskan, mengeluarkannya dari negeri atau mempunyai dalam persediaan, atau barangsiapa secara terang-terangan atau dengan mengedarkan surat tanpa diminta, menawarkan atau menunjukkan sebagai bisa di dapat, diancam jika ada alasan kuat baginya untuk menduga bahwa tulisan, gambaran atau benda itu melanggar kesusilaan dengan pidana penjara paling lama sembilan bulan atau denda paling banyak tiga ratus rupiah.

(3) Kalau yang bersalah, melakukan kejahatan tersebut dalam ayat pertama, sebagai pencaharian atau kebiasaan, dapat dijatuhi pidana penjara paling lama dua tahun delapan bulan atau denda paling banyak lima ribu rupiah.

Perbuatan-perbuatan yang diancam hukuman, baik dalam ayat (1) maupun ayat (2) dari pasal tersebut ada tiga macam, yakni :

a. menyiarkan, mempertunjukkan atau menempelkan dengan terang-terangan tulisan dan sebagainya;
b. membuat, memasukkan ke dalam negeri, mengirim langsung ke dalam negeri, mengirim langsung ke luar negeri, membawa ke luar atau menyediakan tulisan dan sebagainya untuk disiarkan, dipertunjukkan atau ditempelkan dengan terang-terangan;

c. dengan terang-terangan atau dengan sengaja menyiarkan suatu tulisan menawarkan dengan tidak diminta atau menunjukkan, bahwa tulisan dan sebagainya itu boleh didapat.

Arti "menyiarkan, mempertunjukkan atau menempelkan dengan terang-terangan" yakni;

i. Yang dapat disiarkan adalah misalnya; surat kabar, majalah, buku, surat selebaran atau lainnya, yang dibuat dalam jumlah banyak.
ii. "Mempertunjukkan" berarti memperlihatkan kepada orang banyak.
iii. "Menempelkan" berarti melekatkan disuatu tempat yang mudah diketahui oleh orang banyak. [10]

Internet sendiri menurut hemat penulis termasuk klasifikasi tempat yang mudah diketahui oleh orang banyak dan termasuk sarana/tempat "penyiaran".

a.d. d. Ketentuan yang berkaitan dengan penipuan

Perbuatan memanipulasi keterangan untuk mencari keuntungan melalui media internet dapat "ditafsirkan" sebagai perbuatan menyesatkan yang ada dalam delik penipuan seperti yang tertuang dalam Pasal 378 KUHP dan Pasal 379a KUHP apabila hal tersebut berkaitan dengan pembelian barang.

PENUTUP

A. Kesimpulan

1. Persoalan mengenai kebijakan kriminalisasi, yang selama ini sudah dilakukan tidak secara tegas menentukan dimasa mendatang mana yang sebaiknya digunakan untuk mengatur *cyber crime,* apakah Undang-Undang ITE (Informasi dan Transaksi Elektronik) atau RUU KUHP. Persoalannya adalah apabila kedua RUU itu disetujui dan diundangkan bukankan aturan mengenai *cyber crime* akan berlebihan bahkan apabila kedua ketentuan ini akan mengaturnya maka akan menimbulkan perbedaan dalam penerapannya dari kedua aturan yang ada. Sehingga perlu adanya ketegasan dalam aturan yang ada terkait dengan menggunakan teknologi informasi melalui peraturan perundang-undangan tersendiri.
2. Munculnya kejahatan baru *(cyber crime)* merupakan suatu fenomena yang memerlukan penanggulangan secara cepat dan akurat. Perubahan terhadap beberapa ketentuan yang terdapat dalam Kitab Undang-undang Hukum Pidana merupakan salah satu cara yang dapat dipergunakan untuk mengatasi jenis kejahatan baru tersebut. Mengingat dalam KUHP pengaturannya masih bersifat umum namun beberapa ketentuan yang ada dapat diterapkan mengingat kondisi hukum dan peraturan yang belum juga diundangkan mengatur di bidang *Cyber crime.*

B. Saran

Munculnya kejahatan dengan mempergunakan internet sebagai alat bantunya *(cyber crime)* lebih disebabkan oleh faktor keamanan si pelaku dalam melakukan kejahatan. Masih kurangnya aparat penegak hukum yang memiliki kemampuan dalam hal cyber crime dan belum adanya peraturan perundang-undangan yang mengatur kejahatan ini mengakibatkan adanya kesulitan bagi penegak hukum dalam menangani tindak pidana *cyber crime* yang terjadi di Indonesia sekarang ini.

Oleh karena itu, sudah waktunya pemerintah melakukan berbagai upaya guna mencegah semakin meningkatnya kejahatan *siber (cyber crime)* ini, diantaranya melalui peningkatan kualitas dan kuantitas aparat penegak hukum yang menguasai teknologi informasi termasuk internet, meningkatkan sarana dan prasarana pendukung bagi penyelidikan dan penyidikan kejahatan *siber*. Serta segera menyusun undang-undang yang mengatur kejahatan *siber*.

DAFTAR PUSTAKA

Agus Raharjo., *Cyber crime*, Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi.
Citra.Aditya.Bakti,Bandung.,2002.

Budi Suhariyanto,. *Tindak Pidana Teknologi Informasi (Cybercrime) : Urgensi*

[10] Nazura Abdul Manap., Cyber-crimes: Problem and Solutions Under Malaysian Law., makalah pada Seminar Nasional Money Laundering dan Cyber Crime dalam Perspektif Penegakan Hukum di Indonesia., Laboratorium Hukum Pidana FH Universitas Surabaya, 24 Februari 2001.

Pengaturan dan Celah Hukumnya,. PT Raja Grafindo Persada, Jakarta, 2013.

Eddy Djunaedi Karnasudirdja,.*Yurisprudensi Kejahatan Komputer*,. CV Tanjung Agung, Jakarta, 1993.

Edmon Makarim, *Pelanggaran HKI di Bidang Telematika*, Makalah pada Workshop Penegakan Hukum di Bidang TIK yang diselenggarakan oleh Depkominfo dan BPHN,Jakarta,2007.

Data diambilkan dari The Cyber crime Convention Committee (T-CY), *Strengthening Co-Operation Between Law Enforcement and the Private Sector, Examples of How the Private Sector has Blocked Child Pornographic Sites,* Strasbourg, 20 February 2006.

Golose, Petrus Reinhard,. *Penegakan Hukum Cyber Crime dalam Sistem Hukum Indonesia dalam Seminar Pembuktian dan Penanganan Cyber Crime di Indonesia*, FHUI, Jakarta, 2007

Jeane Neltje Saly, *Cyber Law Dalam Perspektif Hukum Nasional*, makalah dalam Workshop Penegakan Hukum di Bidang TIK yang diselenggarakan oleh Depkominfo dan BPHN di Hotel Accacia Jakarta 31 Oktober 2007.

John Naisbitt, Nana Naisbitt dan Douglas Philips, *High Tech, High Touch, Pencarian Makna di Tengah Perkembangan Pesat Teknologi,* Mizan, Bandung, 2001.

Kementerian Komunikasi dan Informasi RI, *RUU Informasi dan Transaksi Elektronik Sebagai Infrastruktur Fundamental Pengembangan Sisfonas,* Jakarta, 28 Juni 2005.

Nazura Abdul Manap*., Cyber-crimes: Problem and Solutions Under Malaysian Law*., makalah pada Seminar Nasional *Money Laundering dan Cyber Crime* dalam Perspektif Penegakan Hukum di Indonesia., Laboratorium Hukum Pidana FH Universitas Surabaya, 24 Februari 2001

Nitibaskara, Tb. Ronny R., Problem Yuridis *Cybercrime,* Makalah pada Seminar tentang Cyber Law, diselenggarakan oleh Yayasan Cipta Bangsa, Bandung, 29 Juli 2000

Satjipto Rahardjo, **,** *Ilmu Hukum*, Citra Aditya Bakti, Bandung, 1996.

Sitompul, Josua,. *Cyberspace, cybercrimes, cyberlaw: Tinjauan Aspek Hukum Pidana*, PT. Tatanusa, Jakarta, 2012

Tien S. Saefullah, *Yurisdiksi Sebagai Upaya Penegakan Hukum Dalam Kegiatan Cyberspace*, Pusat Studi Cyber Law FH UNPAD, Bandung, 2002.

---------,. *Aspek Hukum Kejahatan Mayantara*, Aswindo, Yogyakarta, 2011

Widodo, *Hukum Pidana di Bidang Teknologi Informasi, Cybercrime Law: Telaah Teoritik dan Bedah Kasus*, Aswaja Pressindo, Yogyakarta, 2013