UNIVERSITAS INDONESIA

Analisis Penerapan Undang – Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Dalam Tindak Pidana Siber

TESIS

Diajukan sebagai salah satu syarat untuk memperoleh gelar Magister Hukum

Marissa Amalina Shari Harahap
1006789324

FAKULTAS HUKUM
PROGRAM PASCA SARJANA
HUKUM DAN SISTEM PERADILAN PIDANA
JAKARTA
JANUARI 2012

HALAMAN PERNYATAAN ORISINALITAS

Tesis ini adalah hasil karya saya sendiri,
dan semua sumber baik yang dikutip maupun dirujuk
telah saya nyatakan dengan benar.

Nama : Marissa Amalina Shari
HarahapNPM : 1006789324

Tanda Tangan : 

Tanggal : 19 Januari 2012

KATA PENGANTAR

Assalamu`alaikum Warrahmatullahi Wabarakatuh,

Dengan kerendahan hati Penulis memanjatkan puji syukur Alhamdullillah karena atas kehadirat Allah Subhanahu Wa Ta'ala dengan segala karunia, rahmat dan hidayah-Nya yang telah memberikan keridhaan kepada penulis sehingga dapat menyelesaikan Tesis yang berjudul **"Analisis Penerapan Undang – Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Dalam Tindak Pidana Siber".** Dalam rangka memenuhi salah syarat untuk mencapai gelar Magister Hukum pada Fakultas Hukum Universitas Indonesia.

Penulis menyadari bahwa tanpa adanya bantuan, dukungan dan pengarahan dari berbagai pihak selama ini, proses pembelajaran Penulis sampai pada penyusunan tesis ini tidak mungkin akan berjalan baik tanpa bantuan dan bimbingan berbagai pihak.

Maka dalam kesempatan ini penulis mengucapkan rasa terima kasih yang sebesar – besarnya kepada yang terhormat

1. Dr. Hj. Siti Hayati Hoesin, S.H.,M.H selaku Pejabat Dekan, Fakultas Hukum, Universitas Indonesia;
2. Prof. Dr. Rosa Agustina,. S.H.,M.H., selaku Ketua Program Pascasarjana, Fakultas Hukum, Universitas Indonesia;
3. Prof. Mardjono Reksodiputro selaku Ketua Bidang Studi Hukum Pidana , Fakultas Hukum, Universitas Indonesia;
4. Topo Santoso, S.H., M.H., Ph.D., selaku dosen pembimbing yang telah menyediakan waktu, tenaga, dan pemikiran untuk mengarahkan selama penulis dalam penyusunan tesis ini;
5. Bapak dan Ibu Dosen serta Staff Administrasi Program Pascasarjana Fakultas Hukum, Universitas Indonesia.
6. Papie H. Muhammad Zen Bahri Harahap dan Mamie Hj. Darmawati Moelia Siregar yang tiada hentinya memberikan rasa penuh kasih sayang

dalam suka dan suka, memberi doa dan nasehat serta berbagai motivasi kepada penulis;

7. dr. Muhammad Irvanie Rama Harahap dan Muhammad Andiaz Rama Harahap S.E., MBA., kedua kakak penulis telah memberikan dukungan moral dan moril;
8. Para Sahabat yang telah banyak memberikan dukungan apapun penyelesaian tesis ini, you know who you're!;
9. Teman penulis dari semester awal sampai akhir, Kelas Pidana Reguler Angkatan 2010 Program Pascasarjana Fakultas Hukum Universitas Indonesia Anshari Dimyati, Ahmad Ramzy, Auliah Andika, Denny Latumaerissa, Irma Sukardi, Nefa Claudia S, Bagus Satrio, Ria Anggraeni U, Yayad Hidayat, Atika Yuanita P, Eka Nugraha, Andre Paminto.
10. Teman seperjuangan bimbingan penulisan tesis Dilla Romi Aprilia dan Dwi Afrimetty Timora Alhamdullillah perjuangan kita selama ini tidak sia – sia.
11. Teman Penulis dari TK, sampai dengan SMA di Al-Azhar Pusat serta Universitas Trisakti.
12. Teman – teman penulis yang tidak bisa disebutkan satu persatu, terima kasih supportnya.

Penulis mohon maaf apabila ada kesalahan mengenai isi maupun cara penyajian di dalam tesis ini. Akhir kata dengan tesis ini penulis mengharapkan agar tulisan ini bermanfaat bagi pihak lain yang membacanya.

Wassalamualaikum Warahmatullahi Wabarrakatuh.

Jakarta, 13 Januari 2012,

Marissa Amalina Shari Harahap

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Universitas Indonesia, saya yang bertanda tangan di bawah
ini:

Nama	: Marissa Amalina Shari Harahap
NPM	: 1006789324
Program Studi	: Pasca Sarjana
Departemen	: Hukum dan Sistem Peradilan Pidana
Fakultas	: Hukum
Jenis karya	: Tesis

demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Indonesia **Hak Bebas Royalti Noneksklusif (*Non-exclusive Royalty-Free Right*)** atas karya ilmiah saya yang berjudul :

Analisis Penerapan Undang – Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Dalam Tindak Pidana Siber

beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini Universitas Indonesia berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan memublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta
Pada tanggal :
Yang menyatakan

(Marissa Amalina Shari Harahap)

ABSTRAK

Nama : Marissa Amalina Shari Harahap
Program Studi : Hukum dan Sistem Peradilan Pidana

Judul : Analisis Penerapan Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dalam Tindak Pidana Siber

Perkembangan teknologi yang begitu pesat memunculkan berbagai permasalahan di masyarakat. Salah satu akibatnya tersebut adalah terciptanya media baru yang disebut dunia maya. Di dunia maya orang bebas melakukan apapun tanpa diketahui oleh orang lain karena tidak diketahui asal – usul maupun kewarganegaraan asli seseorang. Hal ini dimanfaatkan sebagian orang untuk melakukan tindak kejahatan yang disebut dengan tindak pidana siber. Telah banyak usaha melakukan pengaturan di dunia maya untuk mencegah terjadinya tindak pidana siber baik hukum nasional maupun internasional. Di Indonesia lahirnya Undang – Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Penerapan Undang – Undang No.11 Tahun 2008 ini dinilai masih banyak kelemahan dan kekurangan di dalam mengatur tindak pidana siber serta menimbulkan banyak permasalahan baru.

Kata Kunci :
Hukum Informasi dan Transaksi Elektronik, tindak pidana siber.

ABSTRACT

Name : Marissa Amalina Shari Harahap
Study Program : Law and Criminal Justice System

Title : Analysis of Application of Law No.. 11 Year 2008 on Information and Electronic Transaction in cyber Crime.

Technology development that so advanced of eliciting a variety of the problem in society . one of a consequently is that the creation of new media called the virtual world . In the virtual world a free person do anything without being known by others as of unknown origin the proposal of nor of citizenship a native someone. Some people it is used for committing a crime so called by a criminal offense siber. Has much effort do arrangement online to prevent the occurrence of a criminal offense siber either national or international law. In Indonesia enacted Law No.11 Year 2008 on Information and Electronic Transactions. Application of Act No.11 of 2008 is still considered a lot of weaknesses and shortcomings in regulating cyber crime and raises many new problems in cyber crime.

Keyword:
Information and Electronic Transaction Law, cyber crime.

DAFTAR ISI

HALAMAN JUDUL ..... **i**
HALAMAN PERNYATAAN ORISINALITAS ..... **ii**
HALAMAN PENGESAHAN ..... **iii**
KATA PENGANTAR ..... **iv**
HALAMAN PERSETUJUAN PUBLIKASI KARYA ILMIAH ..... **vi**
ABSTRAKSI ..... **vii**
ABSTRACT ..... **viii**
DAFTAR ISI ..... **ix**
DAFTAR TABEL ..... **xi**

BAB I. PENDAHULUAN **1**
1.1 Latar Belakang 1
1.2 Tinjauan Pustaka 5
1.3 Pernyataan Masalah 6
1.4 Pertanyaan Penelitian 8
1.5 Tujuan Penelitian 8
1.6 Manfaat Penelitian 9
1.7 Metode Penelitian 9
1.8 Kerangka Teori Dan Kerangka Konsep 11
1.8.1 Kerangka Teori 11
1.8.2 Kerangka Konsep.. 16
1.9 Sistematika Penulisan 20

BAB II TINJAUAN PERKEMBANGAN ASPEK – ASPEK YURIDIS MENGENAI INFORMASI DAN TRANSAKSI ELEKTRONIK **22**
2.1 Pengertian Informasi dan Transaksi Elektronik 22
2.2 Penerapan Sesudah Berlakunya Undang – Undang No. 11 Tahun 2008 32

BAB III TINDAK PIDANA SIBER 49
3.1 Jenis – Jenis Tindak Pidana Siber Secara Umum..... 49
3.1.1 Jenis-jenis Tindak pidana siber Secara Umum 49
3.1.2 Kejahatan Menyangkut Identitas..... 53
3.1.3 Kejahatan Terhadap Privavsi 55
3.1.4 Kejahatan Terhadap Sistem Komputer 57
3.1.5 Kejahatan Terhadap Ketertiban Umum 58
3.2 Jenis – Jenis Tindak Pidana Siber di Undang – Undangan 59
3.2.1 United Nations Convention Againt Transnational Organized Crime atau Konvensi Palermo 60
3.2.2 *Convention On Cybercrime*..... 62
3.2.3 International Telecommunications Union (ITU) 69
3.2.4 Peraturan di Indonesia..... 71

BAB IV PENERAPAN UNDANG – UNDANG No.11 Tahun 2008 79
4.1 Kelemahan dari Subtansi Undang- Undang No.11 Tahun 2008..... 81
4.2 Penerapan Undang – Undang No 11 Tahun 2008..... 93
4.2.1 Kasus Pornografi..... 93
4.2.2 Kasus Pencemaran Nama Baik 95

BAB V PENUTUP..... 99
5.1 Kesimpulan 99
5.2 Rekomendasi..... 100

DAFTAR PUSTAKA..... 102

DAFTAR TABEL

Tabel 3.1. Definisi hukum..... 75
Tabel 3.2. Subtantif Hukum..... 76
Tabel 3.3. Prosedur Hukum 77

BAB 1
PENDAHULUAN

1.1 Latar Belakang

Teknologi terus dikembangkan dalam rangka mempermudah manusia melakukan aktifitasnya sehari-hari. Salah satu produk teknologi informasi dan komunikasi kecanggihannya berkembang pesat dan menguasai hampir seluruh aspek kehidupan manusia adalah Internet. Para pelaku bisnis, pejabat, pemerintah dan banyak orang diseluruh dunia menggunakan Internet sebagai bagian dari bisnis nasional dan internasional serta kehidupan pribadi manusia sehari – hari. Eksistensi dari beberapa jenis bisnis justru tidak mungkin berlangsung tanpa adanya Internet.[1]

Teknologi informasi dan komunikasi ini pula telah mengubah perilaku masyarakat dan peradaban manusia secara global.[2] Dengan munculnya Internet, muncul jenis dunia yang baru yang sebelumnya tidak pernah dikenal oleh manusia, yaitu dunia yang disebut "*virtual world*". Munculnya dunia virtual telah mengubah kebiasaan banyak orang terutama dalam kehidupannya terbiasa menggunakan Internet. Mulai dari mengubah cara dan sarana transaksi bisnis atau transaksi perbankan yang dilakukan dengan menggunakan Internet yang berlangsung di dunia virtual disebut dengan transaksi elektronik *(electronic transaction atau e-commerce)*, pendidikan (electronic education), kesehatan (tele-medicine), telekarya, transportasi, industri parawisata, lingkungan, sampai dengan sektor hiburan.

Disamping menciptakan berbagai peluang baru dalam kehidupan masyarakat, Kecanggihan teknologi informasi dan komunikasi tersebut telah memberikan kemudahan kemudahan dalam pekerjaan sehari – hari, Perkembangan teknologi informasi dan komunikasi menyebabkan hubungan dunia menjadi tanpa batas *(borderless)* dan menyebabkan perubahan sosial,

[1] Sutan Remy Syahdeini, *Kejahatan & Tindak Pidana Komputer*, (Jakarta: Pustaka Utama Grafiti, 2009), hlm. 2.

[2] Ahmad M. Ramli, *Cyber Law dan HAKI dalam Sistem Hukum Indonesia*, (Jakarta: Rafika Aditama, 2004), hlm. 1.

ekonomi dan budaya secara signifikan berlangsung yang sangat cepat hal ini ternyata memunculkan kejahatan baru yaitu kejahatan komputer.[3] Di dunia virtual orang melakukan berbagai perbuatan jahat (kejahatan) yang justru tidak dapat dilakukan di dunia nyata. Kejahatan tersebut dilakukan dengan menggunakan komputer sebagai sarana perbuatan.

The *Pew Internet Project* melakukan *online survey* yang diikuti oleh 1.286 ahli. Menurut hasil penelitian tersebut, dalam waktu 10 tahun mendatang Internet akan menjadi demikian pentingnya bagi para pengguna komputer sehingga jaringan Internet akan menjadi sasaran yang sangat mengundang bagi serangan tindak pidana komputer.[4] Jenis tindak pidana komputer ini terbagi dalam dua jenis, yaitu kejahatan dengan motif intelektual. Biasanya jenis yang pertama ini tidak menimbulkan kerugian dan dilakukan untuk kepuasaan pribadi. Jenis kedua adalah kejahatan dengan motif politik, ekonomi atau kriminal yang berpontesi menimbulkan kerugian bahkan perang informasi. Yang termasuk jenis tindak pidana komputer tersebut diantaranya adalah *cybersquatting, identity theft,* kejahatan kartu kredit *(carding), phising, hacking, cyberterrorism, DOS-DDOS attack, online gambling,* penyebaran *malware,* pencurian data dan informasi eletronik, memodifikasi data dan informasi elektronik, pengadaan program komputer secara tidak sah, pornografi anak (*child pornography),* dan *cyberstalking.*[5]

Kejahatan tindak pidana siber[6] masalah yang baru bagi tugas penegak hukum. Konsekuensinya, *electronic information dan electronic transaction* yang memerlukan adanya perlindungan yang kuat terhadap upaya – upaya yang dilakukan oleh pihak – pihak yang tidak bertanggung jawab untuk mengakses informasi yang tersimpan dalam sistem komputer. Kebutuhan perlindungan yang

---

[3] Edmon Makarim, *Kompilasi Hukum Telematika,* Cet. Ke- 1, (Jakarta : Radja Grafindo Persada, 2003), hlm. 385.

[4] Susannah Fox, Janna Quitney Anderson dan Lee Rainie, "The future of Internet", Tersedia di http://www.pewinternetproject.org/pdfs/PIP_Future_of_internet.pdf (9 January 2005).

[5] Sutan Remy Syahdeini, *Op.Cit*., hlm. 8.

[6] Memakai istilah tindak pidana siber karena hal Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik mengatakan demikian.

demikian ini menjadi sangat tinggi apabila menyangkut *electronic information* yang sifatnya sangat rahasia.[7]

Fenomena tindak pidana siber memang harus diwaspadai karena kejahatan ini agak berbeda dengan kejahatan lain pada umumnya. Tindak pidana siber dapat dilakukan tanpa mengenal batas teritorial dan tidak diperlukan interaksi langsung antara pelaku dengan korban kejahatan. Bisa dipastikan dengan sifat global internet, semua negara yang melakukan kegiatan internet hampir pasti akan terkena imbas perkembangan tindak pidana komputer ini.

Sebelum diundangkan Undang - Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Modus kejahatan dalam dunia siber memang agak sulit dimengerti oleh orang – orang yang tidak menguasai pengetahuan teknologi informasi dalam modus operandinya. Sifat ini membuat *cyber crime* berbeda dengan tindak pidana lainnya.[8] Maka apabila di Indonesia ada seseorang yang melakukan perilaku kejahatan di dalam internet sebagai sasaran utama kejahatannya atau menggunakan program internet maka diterapkan Kitab Undang Hukum Pidana sebagai undang – undang pidana umum. Tentu saja hal tersebut dapat dilakukan sepanjang KUHP ditemukan pasal – pasal yang pas dan tepat untuk menjatuhkan pidana.

Demi merespon atas berkembanganya hal tersebut maka Indonesia memasukkan materi tindak pidana siber sebagai salah satu materi delik dalam Rancangan Kitab Undang-Undang Hukum Pidana (R-KUHP) Nasional. Dalam draft R KUHP Nasional 2010 Tindak Pidana terhadap Informatika dan Telematika. Dalam R KUHP Nasional 2010 juga dilakukan redefinisi tentang Barang (Pasal 165)[9], Surat (Pasal 207)[10], Masuk (Pasal 186).[11]

---

[7] *Ibid.*, hlm. 9, mengutip dari Kamlesh K Bajaj & Debjani Nag, *E-Commerce : The Cutting Edge Of Bussiness*, (New Delhi : Tat McGraw-Hill Publishig Limited, 2000), hlm. 427.

[8] Mardjono Reksodiputro, *Kejahatan komputer (Suatu catatan sementara dalam rangka KUHP Nasional yang akan datang) , dalam Kemajuan Pembangunan Ekonomi dan Kejahatan*, (Jakarta: Pusat Pelayanan Keadilan dan Pengabdian Hukum UI, 1997), hlm. 10.

[9] Barang adalah benda berwujud termasuk air dan uang giral dan benda tidak berwujud termasuk aliran listrik , gas , data dan program komputer , jasa termasuk jasa telepon , jasa telekomunikasi atau jasa komputer.

[10] Surat adalah surat yang tertulis diaatas kertas, termasuk juga surat atau data yang tertulis atau tersimpan dalam disket, pita magnetik , atau media penyimpan komputer atau media penyimpan data elektronik lain.

[11] Masuk adalah termasuk mengakses komputer atau masuk kedalam sistem komputer.

Di Indonesia sendiri, ada dua undang – undang yang dapat mengatur tentang informasi dan transaksi elektronik di Indonesia. Yang pertama adalah Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sedangkan yang kedua adalah Undang – Undang No.36 Tahun 1999 tentang Telekomunikasi. Undang – Undang tersebut dikeluarkan karena telah banyak yang bermunculan kejahatan – kejahatan di dunia maya di Indonesia yang sangat merugikan perorangan maupun masyarakat luas. Ada beberapa undang – undang lainnya yang terkait dengan tindak pidana siber seperti Undang – Undang No.8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang, Undang – Undang No.19 Tahun 2002 tentang Hak Cipta yang mengatur perlindungan *software* komputer dan menetapkan sanksi pidana bagi yang melanggarnya.

Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik memilih mengacu model yang bersifat komprehensif artinya materi muatan yang diatur di dalamnya mencakup hal yang luas disesuaikan dengan kebutuhan saat ini. Dalam undang – undang tersebut terdapat beberapa pasal pidana yang merupakan ketentuan pidana khusus disamping berlakunya KUHP sebagai undang – undang tindak pidana umum. Sedangkan Undang – Undang No.36 Tahun 1999 tentang telekomunikasi merupakan pengganti dari undang – undang sebelumnya yaitu Undang – Undang No.3 Tahun 1989 tentang Telekomunikasi. Undang – undang ini dilahirkan sebagai konsekuensi dari adanya perubahan mendasar dalam penyelenggaraan dan cara pandang terhadap telekomunikasi yang memerlukan penataan dan pengaturan kembali penyelenggaraan telekomunikasi nasional.

Undang – Undang No.36 Tahun 1999 tentang Telekomunikasi yang merupakan *lex generalis* dari Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik belum secara spesifik mengatur hal – hal yang berkaitan dengan telekomunikasi dengan Internet. Sama halnya dengan Kitab Undang Hukum Pidana yang sangat terbatas sekali untuk diterapkan terhadap tindak pidana siber.

Sebelumnya masalah tindak pidana siber sudah pernah dibahas oleh Anisah Hikmiyati di dalam tesisnya di tahun 2006 yang berjudul Penentuan *locus*

delictie dalam *Cybercrime* sebagai Usaha Pembaharuan Hukum Pidana Nasional.[12] Penulis membahas masalah mengenai Konvergensi teknologi komputer dengan teknologi informasi dan teknologi komunikasi memunculkan fenomena baru, yaitu internet. *Cybercrime* memanfaatkan jaringan teknologi informasi secara global. Aspek global menimbulkan kondisi seolah – olah dunia tidak ada batasnya (*borderless*). Permasalahan muncul dalam menentukan *locus delictie cyber crime* ini, sehubungan dengan sifat dari internet yang lintas batas. Keadaan ini dapat mengakibatkan pelaku, korban serta tempat dilakukannya tindak pidana (*locus delictie*) terjadi di negara yang berbeda – beda.

Adanya instrumen hukum untuk membrantas *cyber crime* ini dilakukan sebagai salah satu usaha dalam pembaharuan hukum pidana nasional. Ketentuan hukum nasional yang mengatur mengenai tindak pidana siber tetapi pada saat tesis ini dibuat, Undang - Undang No.11 Tahun 2008 belum diundangkan sehingga masih memakai Kitab Undang Hukum Pidana dalam Tesis ini ingin memberikan suatu pemikiran akademis dalam rangka memformulasikan Kitab Undang-Undang Hukum Pidana, demi tercapainya suatu pembaharuan dalam hukum pidana nasional diharapkan hukum dapat mengakomodasi perkembangan teknologi informasi atau setidaknya menjamin adanya kepastian hukum dalam pemanfaatan teknologi informasi, khususnya internet.

Sedangkan Afitrahim M.R dalam tulisan skripsi yang berjudul Yurisdiksi berdasarkan *Convention On Cybercrime*,[13] penulis menjabarkan masalah karena kemajuan teknologi yang sangat pesat, telah banyak pula usaha untuk melakukan pengaturan dalam dunia siber untuk mencegah atau menanggulangi terjadi nya tindak dunia maya baik oleh hukum internasional maupun hukum nasional. Salah satu satunya dengan lahirnya Convention On cybercrime yang dibuat oleh Dewan Eropa.

Aspek yang menjadi perhatian khusus dalam konvensi ini adalah masalah yurisdiksi negara dalam menangani kasus tindak pidana siber karena semua negara tidak senang yurisdiksi negaranya dilampaui oleh negara lain, termasuk

[12] Anisah Hikmiyati, *Penentuan Locus Delictie dalam Cyber Crime Sebagai Usaha Pembaharuan Hukum Pidana Nasional,* (Jakarta;Universitas Indonesia.2006).
[13] Afitrahim, *Yuridiksi Berdasarkan Convention On Cybercrime,* (Depok;Univeritas Indonesia,2009).

Indonesia. Sedangkan untuk pengaturan di negara Indonesia, penulis menggunakan Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Dari uraian tesis Anisah Hikmiyati dan dapat ditarik kesimpulan bahwa tindak pidana siber disaat belum diundangkan Undang - Undang No.11 Tahun 2008 merupakan permasalahan yang serius dalam penyelidikan tindak pidana siber antara lain tanpa ada batas *(borderless)* baik korbannya maupun tersangkannya sehingga perangkat hukum konvesional yang ada di Indonesia belum attau tidak bisa menjangkau secara aktif.

Sedangkan dari skripsi Afitrahim M.R tidak membahas masalah tindak pidana siber dalam Undang – Undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik secara khusus dan mendalam mengenai undang – undang ini.

Dari beberapa uraian di atas, maka penulis dalam tesis ini perlu membahas tentang Penerapan Undang - Undang No.11 Tahun 2008 dalam tindak pidana siber, bagaimana hukum baru ini dalam menanggulangi masalah tindak pidana siber secara rinci dan lebih lanjut. Apakah masih terdapat kekurangan di dalam undang – undang ini, masih ada hambatan serta perlukah undang – undang ini untuk direvisi atau dilakukan perubahan selaku produk hukum yang baru di Indonesia dan belum pernah dilakukannya perubahan dalam Undang - Undang No.11 Tahun 2008, maka penulis menganggap hal ini perlu dikaji lebih lanjut.

1.3 Pernyataan Masalah

Tindak pidana siber ini merupakan kejahatan yang berdimensi baru. Kejahatan ini jenis maupun bentuknya banyak sekali. Dalam Perspektif hukum pidana, kejahatan ini ada yang merupakan kejahatan konvesional tetapi dengan modus baru, pornografi, penipuan, pencemaran nama naik dan sebagainya yang mengunakan media internet sebagai sarana untuk melakukan kejahatan. Disamping itu ada juga kejahatan baru yang tidak dikenal sebelumnya.[14] Dalam sejarah dijumpai munculnya bentuk – bentuk kejahatan baru yang tidak siap

[14] Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cyber Crime)*, (Bandung : Refika Aditama , 2005), hlm. 154.

dihadapi oleh perundang – undangan yang ada. Perkembangan mutakhir adalah maraknya penggunaan komputer dan internet yang memperkenalkan produk baru di dunia perdagangan, juga menyebabkan terjadinya tindak pidana siber (*cyber crime*).[15]

Undang – Undang No. 11 Tahun 2008 dalam era globalisasi informasi telah menempatkan Indonesia sebagai bagian dari masyarakat informasi dunia sehingga mengharuskan dibetuknya pengaturan mengenai pengelolaan Informasi dan Transaksi di tingkat nasional sehingga pembangunan Teknologi Informasi dapat dilakukan secara optimal, merata, dan menyebar keseluruh lapisan masyarakat

Dalam Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dimuat ketentuan – ketentuan mengenai larangan melakukan perbuatan – perbuatan tertentu yang diancam dengan sanksi pidana bagi pelakunya. Tegasnya, Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik menetapkan beberapa perbuatan yang dapat dikriminalisasi sebagai tindak pidana siber dengan sanksi – sanksi nya.

Bab VII dari Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik menentukan perbuatan – perbuatan tertentu yang dilarang untuk dilakukan. Perbuatan – perbuatan tersebut ditentukan di dalam Pasal 27 sampai dengan 37. Sementara itu Bab XI yang terdiri atas Pasal 45 sampai dengan Pasal 52 menentukan kriminalisasi terhadap perbuatan – perbuatan yang dalam Bab VII ditentukan sebagai perbuatan – perbuatan yang dilarang beserta masing – masing sanksi pidananya. Perbuatan – perbuatan yang dilarang dan bersanksi pidana itu merupakan tindak pidana informasi dan transaksi elektronik di Indonesia.[16]

Namun setelah diberlakukan Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik perlu disikapi bahwa tidak mustahil ada tindak pidana siber tertentu yang ternyata belum dinyatakan sebagai tindak pidana karena belum diaturnya di dalam Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.[17] atau dengan kata lain lahirnya

[15] Satjipto Rahardjo, *Penegakan Hukum Progresif* , (Jakarta : Kompas, 2010) , hlm. 23.
[16] Sutan Remy Syahdeini, *Op.Cit*., hlm. 225-226.
[17] *Ibid.*, hlm. 37.

undang undang ini belum semua permasalahan menyangkut tindak pidana siber dapat ditangani. Hal ini disebabkan karena tindak pidana siber masih sulit untuk ditanggulangi bahkan perkembanganya cenderung meningkat terus dan kompleks dengan variasi modus operandinya yang harus segera diantisipasi dan diwaspadai

1.4 Pertanyaan Penelitian

Maka yang menjadi pertanyaan penelitian dalam penulisan penelitian tesis ini adalah :

1. Bagaimana penyelesaian tindak pidana siber di Indonesia menurut Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik?
2. Apakah ketentuan pidana pada Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik merupakan ketentuan yang mampu mengikuti perkembangan tindak pidana siber?
3. Kendala apa sajakah yang dapat dijumpai dalam menegakkan Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dalam pemberantasan tindak pidana siber?

1.5 Tujuan Penelitian

Adapun tujuan dari penelitian tesis dengan judul **"Analisis Penerapan Undang – Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Dalam Tindak Pidana Siber"** ini adalah sebagai berikut:

1. Untuk mengetahui penyelesaian tindak pidana siber di Indonesia menurut Undang – Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
2. Untuk mengetahui dan menganalisis tentang ketentuan pidana pada Undang – Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik merupakan ketentuan yang mampu mengikuti perkembangan tindak pidana siber.
3. Untuk mengetahui kendala apa sajakah yang dapat dijumpai dalam menegakkan Undang – Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dalam pemberantasan tindak pidana siber.

1.6 Manfaat Penelitian

Dalam penulisan penelitian tesis dengan judul **"Analisis Penerapan Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Dalam Tindak Pidana Siber"** ini, setidaknya ada dua manfaat yang kiranya diharapkan akan dapat diperoleh, yaitu sebagai berikut:

Manfaat Teoritis

Dari sisi teoritis, penelitian ini memiliki tujuan untuk memberikan pengertian mengenai apa sesungguhnya yang dimaksud dengan tindak pidana siber, penjabaran bagaimana ketentuan undang – undang yang berlaku di Indonesia, tindak pidana siber apa saja yang diatur diatur di dalam undang – undang yang berlaku dan guna untuk mengetahui kendala apa sajakah yang terjadi dalam penerapan undang – undang tersebut. Dari tujuan – tujuan tersebut, penulisan ini diharapkan dapat membuktikan bahwa tindak pidana siber dapat di atasi atau tidak dengan undang – undang yang sudah berlaku selama ini. Dari sini dapat dilihat perlu atau tidaknya suatu pengembangan atau perubahan undang – undang yang ada sebagai modal penegakan hukum baru yang dapat mengakomodir perkembangan masalah tindak pidana siber yang setiap harinya terus berkembang.

Manfaat Praktis

Dari sisi praktis, penelitian ini diharapkan dapat memberikan masukan dalam hal uji konstituonal undang – undang yang terkait dengan tindak pidana siber yang sudah berlaku di Indonesia dalam rangka pengembangan dan penyempurnaan peraturan peraturan perundang – undangan yang berkaitan dengan teknologi dan transaksi elektronik . Diharapkan akan terwujudnya suatu penerapan undang – undang yang proporsional yang pada akhirnya dapat mengurangi tindak pidana siber yang ada di Indonesia.

1.7 Metode Penelitian

Berdasarkan pertanyaan penelitian yang telah dirumuskan sebelumnya, maka penelitian tesis ini akan menggunakan metode penelitian yang bersifat

yuridis normatif.[18] Dengan pendekatan deskriptif analitis. Teknik pengumpulan data yang digunakan adalah studi kepustakaan. Jenis data yang digunakan untuk menjawab pertanyaan dalam penelitian ini adalah data primer yang terdiri dari :

- KUHP (Kitab Undang – Undang Hukum Pidana) Undang – Undang Nomor 1 Tahun 1960;
- KUHAP (Kitab Undang – Undang Hukum Acara Pidana) Undang – Undang Nomor 8 Tahun 1981;
- Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik;
- Undang – Undang No. 36 Tahun 1999 tentang Telekomunikasi;
- Undang – Undang No. 40 Tahun 1999 tentang Pers;
- Undang – Undang No. 3 Tahun 1997 tentang Pengadilan Anak;
- Undang – Undang No. 19 Tahun 2002 tentang Hak Cipta
- Undang – Undang Nomor 15 Tahun 2003 tentang Penetapan Peraturan Pemerintah Pengganti Undang – Undang Nomor 1 Tahun 2002 tentang Pemberantasan Tindak Pidana Terorisme Menjadi Undang – Undang;
- Undang – Undang No. 14 Tahun 2008 tentang Keterbukaan Informasi Publik;
- Undang – Undang No. 44 Tahun 2008 tentang Pornografi;
- Undang – Undang Nomor 8 Tahun 2010 Tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang;
- Rancangan KUHP (Kitab Undang – Undang Hukum Pidana) Tahun 2010;
- Rancangan KUHAP (Kitab Undang – Undang Hukum Acara Pidana) Tahun 2010;
- The Council of Europe Convention on Cybercrime, Budafest 23.XI.2001;
- International Telcommunication Union

Untuk dapat lebih menyempurnakan jawaban dari pertanyaan penelitian ini, maka penelitian ini juga menggunakan bahan hukum sekunder yang terdiri dari berbagai macam bahan bacaan yang terkait dengan judul penelitian seperti buku-buku mengenai tindak pidana siber, artikel – artikel, jurnal – jurnal, literatur

[18] Soerjono Soekanto dan Sri Mamudji, *Penelitian Hukum Normatif*, (Jakarta : Rajawali Press, 1995), hlm. 33.

lain sebagai pendukung dan peneliti melakukan wawancara dengan kepada pihak yang dianggap kompeten memberikan keterangan mengenai objek yang diteliti, yaitu dengan mewawancarai Ahli Hukum Pidana Pakar Telematika Dr. Edmon Makarim S.Kom, S.H, LL.M.,. Wawancara ini dilakukan untuk mengetahui selama ini tindak pidana siber apa saja yang berkembang di Indonesia, serta jenis perbuatan apa yang tidak dapat dijerat dengan peraturan undang – undang dalam kasus kasus tindak pidana siber yang ada di Indonesia.

Metode pengolahan data yang digunakan adalah pengolahan data secara kualitatif sehingga menghasilkan laporan penelitian dalam bentuk deskriptif analitis.[19]

1.8 Kerangka Teori Dan Kerangka Konsep

1.8.1 Kerangka Teori

Teori adalah serangkaian praposisi atau keterangan yang saling berhubungan dan tersusun dalam sistem deduksi yang mengemukakan penjelasan atas suatu gejala.[20] Manfaat teori hukum dalam penelitian hukum adalah melalui teori hukum, ilmu hukum dapat mencerminkan perkembangan masyarakat. Di sini ilmu hukum tersebut membahas tentang perkembangan hukum yang berkaitan dengan perubahan-perubahan dalam masyarakatnya dan uraian ini barang tentu akan melibatkan pembicaraan mengenai struktur politiknya, pengelompokan sosialnya dan sebagainya.[21] Sementara itu, Peter Mahmud Marzuki berpendapat bahwa untuk menggali makna lebih jauh dari aturan hukum, tidak cukup dilakukan penelitian dalam ruang lingkup dogmatik hukum, melainkan lebih mendalam lagi memasuki teori hukum. Penelitian hukum dalam tataran teori diperlukan bagi mereka yang ingin mengembangkan suatu bidang kajian hukum

[20] Sutan Remy Sjahdeini, *Kebebasan Berkontrak dan Perlindungan Yang Seimbang Bagi Para Pihak Dalam Perjanjian Kredit Bank Di Indonesia,* (Jakarta: Pustaka Utama Grafiti, 2009), hlm. 8.

[21] Disadur dari Satjipto Rahardjo, *Ilmu Hukum,* (Bandung: PT. Citra Aditya Bakti, 1996), hlm. 9.

tertentu.[22] Selain itu menurut Soerjono Soekanto, bagi suatu penelitian, teori memiliki kegunaan sebagai berikut:[23]

1. Teori tersebut berguna untuk lebih mempertajam atau lebih mengkhususkan fakta yang hendak diselidiki atau diuji kebenarannya;
2. Teori sangat berguna di dalam mengembangkan sistem klasifikasi fakta, membina struktur konsep-konsep serta memperkembangkan definisi-definisi;
3. Teori biasanya merupakan suatu ikhtisar daripada hal-hal yang telah diketahui serta diuji kebenarannya yang menyangkut objek yang diteliti;
4. Teori memberikan kemungkinan pada prediksi fakta mendatang, oleh karena telah diketahui sebab-sebab terjadinya fakta tersebut dan mungkin faktor-faktor tersebut akan timbul lagi pada masa-masa mendatang;
5. Teori memberikan petunjuk-petunjuk terhadap kekurangan-kekurangan pada pengetahuan peneliti.

Dalam rangka penelitian tesis ini, arah dari penulisan ini akan dimulai dari pembahasan mengenai *cyber crime* atau tindak pidana siber. Kehidupan masyarakat senantiasa mengalami perubahan. Perubahan – perubahan pada masyarakat dunia dewasa ini, merupakan gejala yang normal, pengaruhnya menjalar dengan cepat ke bagian – bagian lain dari dunia, antara lain berkat adanya teknologi komunikasi modern. Penemuan – penemuan baru di bidang teknologi, terjadinya suatu revolusi, modernisasi pendidikan dan seterusnya terjadi di suatu tempat, dengan cepat dapat diketahui oleh masyarakat lain yang letaknya jauh dari tempat tersebut.[24] Ketika pemanfaatan teknologi informasi semakin banyak dilakukan oleh masyarakat pada berbagai bidang maka terdapat kecenderungan yang mendorong terhadap perubahan sosial yang sangat cepat.[25]

---

[22] Disadur dari Peter Mahmud Marzuki, *Penelitian Hukum*, Cet. Ke-6, (Jakarta: Kencana, 2010), hlm. 72-73.

[23] Soerjono Soekanto, *Pengantar Penelitian Hukum*, Cet. Ke-3, (Jakarta: Penerbit Universitas Indonesia (UI Press), 2006), hlm. 121.

[24] Soerjono Soekanto, *Pokok-Pokok Sosiologi Hukum*, (Jakarta : Rajawali Press, 1998), hlm. 87.

[25] Perubahan sosial adalah segala perubahan pada lembaga kemasyarakatan di dalam suatu masyarakat, yang mempengaruhi sistem sosialnya,termasuk di dalamnya nilai-nilai, sikap-sikap dan pola-pola perilakuan di antara kelompok-kelompok dalam masyarakat. Lihat dalam Soerjono Soekanto, *Pokok-Pokok Sosiologi Hukum*, (Jakarta: PT RajaGrafindo Persada, 2005), hlm. 101.

Kenyataan itu tidak akan menjadi suatu permasalahan yang kompleks apabila perubahan sosial ini mengarah kepada aspek – aspek yang sifatnya positif dan konstruktif tetapi menjadi berbalik kalau perubahan sosial berakses atau berdampak pada perubahan nilai – nilai sosial yang mengabaikan aspek – aspek moral dan norma yang hidup di masyarakat itu sendiri.[26]

Manusia mendapat banyak manfaat dari perkembangan teknologi pada seluruh aspek kehidupannya. Namun disamping manfaat juga terdapat dampak negatif yang perlu diwaspadai, diantaranya adalah perbuatan menyimpang dengan menggunakan tekhnologi tersebut. Dengan demikian tekhnologi yang dihasilkan manusia tidak lepas dari dampak positif dan dampak negatifnya. Sehingga perlu adanya aturan yang mengatur bidang teknologi ini. Perkembangan teknologi yang sangat pesat, menyebabkan hukum selalu tertinggal, terlebih lagi mengenai kejahatan berteknologi tinggi seperti kejahatan internet atau *cyber crime* seolah hukum selalu ketinggalan dari peristiwanya.[27]

Dengan adanya ketertinggalan hukum terhadap suatu peristiwa maka diperlukan peraturan yang dibuat untuk mengatur peristiwa – peristiwa baru tersebut dan penegakan hukumnya akan dipengaruhi oleh beberapa faktor. Menurut Soerjono Soekanto, ada lima unsur yang mempengaruhi penegakan hukum yaitu:[28]

a. Faktor hukumnya sendiri hanya dibatasi oleh undang – undang saja;
b. Faktor penegak hukum, yakni pihak – pihak yang membentuk maupun menerapkan hukumnya.;
c. Faktor sarana atau fasilitas yang mendukung penegakan hukum;
d. Faktor masyarakat yaitu lingkungan dimana hukum tersebut berlaku atau diterapkan;
e. Faktor kebudayaan, yakni hasil karya, cipta dan rasa yang didasarkan pada karsa manusia di dalam pergaulan hidup.

[26] Budi Agus Riswandi, *Hukum Cyberspace*, (Yogyakarta: Gita Negeri, 2006), hlm. 10.
[27] Direktorat Hukum Bank Indonesia dan Fakultas Hukum UGM , "Modus Operandi,Macam dan Jenis Cyber Crimes", (Makalah disampaikan pada *Rekonstruksi Hukum dalam Menanggulangi Kejahatan Dunia Maya di Bidang Perbankan*, Yogyakarta , 27 Oktober 2003), hlm. 55.
[28] Soerjono Soekanto, *Faktor – Faktor yang Mempengaruhi Penegakan Hukum*, Cet. Ke-3, (Jakarta: RajaGrafindo Persada, 1993), hlm. 5.

Dilihat dari permasalahan mengenai Informasi dan Transaksi Elektronik tentang tindak pidana siber maka teori yang dipakai untuk penulisan ini ada beberapa salah satunya teori Pound . Roscoe Pound mengeluarkan sebuah teori tentang keseimbangan kepentingan. Teori Pound tentang *law as a tool of social engineering.*[29] Konteks *social engineering* disini adalah menata kepentingan kepentingan yang ada di masyarakat. Kepentingan –kepentingan itu harus sedemikian rupa sehingga terdapat keadaan yang proporsional. Manfaatnya adalah terbangunya suatu struktur masyrakat sedemikian rupa sehingga secara maksimum mungkin menghindari benturan dan pemborosan.[30] Karena hukum berperan untuk menjamin perubahan – perubahan tersebut terjadi dengan teratur dan tertib.

Pound mengajukan tiga kategori kelompok kepentingan, yaitu kepentingan umum, sosial dan pribadi. Kepentingan – kepentingan yang tergolong kepentingan umum terdiri atas atas dua, yaitu: Kepentingan – kepentingan negara sebagai badan hukum dalam mempertahankan kepribadian dan hakikatnya; dan Kepentingan – kepentingan negara sebagai penjaga kepentingan – kepentingan sosial.[31]

Perkembangan dalam bidang teknologi komputer semakin pesat dengan adanya perkembangan informasi dan tekhnologi komunikasi yang kemudian membawa dampak positif maupun negatif bagi kehidupan manusia, maka negara penting untuk melakukan perubahan – perubahan hukum demi menertibkan penggunaan teknologi maju ini dan mewujudkan keadilan dan kesejahteraan masyarakat. Sehingga perkembangan teknologi membawa kenyamanan dan keamanan terhadap manusia yang membuat dan menggunakannya.

Hukum sebagai *social engineering,* bermakna penggunaan hukum secara sadar untuk mencapai tertib atau keadaan masyarakat sebagaimana dicita – citakan atau untuk melakukan perubahan yang diinginkan. Hukum tidak lagi dilihat dari sekedar sebagai tatanan penjaga *status quo,* tetapi juga dinyakini

---

[29] Roscoe Pound, *Contemporary Jurisdic Theory* , dalam D Llyod (ed), *Introduction to Jurisprudence* , (London, Stences,1965) disadur dari buku karangan Benard L. Tanya, *Teori Hukum Strategi Tertib Mannusia Lintas Ruang dan Generasi*, (Yogyakarta: Genta Publishing , 2010), hlm. 155.

[30] Satjipto Rahardjo, *Ilmu hukum*, (Bandung : Citra Aditya Bakti, 2000), hlm. 155.

[31] Ibid., hlm 155

sebagai sistem pengaturan untuk mencapai tujuan – tujuan tertentu secara terencana.[32]

Hukum pidana adalah hukum yang terikat pada ruang dan waktu, sehingga mengenai kapan dan dimana tindak pidana dilakukan harus jelas diketahui. Penentuan tempat terjadinya tindak pidana menjadi sangat penting, apabila penuntut umum tidak memuat unsur ini dalam dakwaannya mengakibatkan dakwaan tersebut batal demi hukum.[33] Ditengah rangkaian kritik atas realitas krisis otoritas hukum itulah, Nonet – Selznick mengajukan model hukum responsif.[34] Perubahan sosial dan keadilan sosial membutuhkan tatanan hukum yang responsif. Kebutuhan ini, sesungguhnya telah menjadi tema utama dari semua ahli yang sepaham dengan semangat fungsional, pragmatis, dan semangat purposif (berorientasi tujuan), seperti halnya Roscoe Pound, para penganut paham realisme hukum dan kritikus – kritikus kontemporer. Nonet dan Selznick lewat hukum responsif, menempatkan hukum sebagai sarana respons terhadap ketentuan – ketentuan sosial dan anspirasi publik. Sesuai dengan sifatnya yang terbuka, maka tipe hukum ini mengedepankan akomodasi untuk menerima perubahan – perubahan sosial demi mencapai keadilan dan emansipasi publik.[35]

Untuk melihat faktor – faktor yang mempengaruhi penegakan Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dapat memakai teori Lawrence M. Friedman, yaitu bahwa faktor – faktor yang mempengaruhi penegakan hukum meliputi struktur hukum *(legal structure)*, subtansi hukum *(legal subtance)* dan budaya hukum *(legal culture).* Sistem hukum terdiri tiga unsur tersebut dapat dijabarkan sebagai berikut :

a. Struktur, mencangkup instusi – instusi penegakan hukum termasuk penegakan hukumnya ;

---

[32] Satjipto Rahardjo, *Hukum dan Perubahan Sosial* , (Bandung : Alumni , 1983) disandur dari buku Benard L. Tanya, *Op.Cit.*, hlm. 162.

[33] Jan Ramelink, *Hukum Pidana*, (Jakarta: Gramedia Pustaka Utama, 2003), hlm. 195.

[34] Dalam membahas hukum responsif , Nonet dan Selznick memberi perhatian khusus pada variabel – variabel yang berkaitan dengan hukum, yaitu : peranan paksaan dalam hukum, hubungan antara hukum dengan politik , negara , tatanan moral , tempat diskresi, peranan tujuan dalam keputusan – keputusan hukum, partisipasi , legitimasi , dan kondisi – kondisi kepatuhan terhadap hukum. Lihat dalam Phillippe Nonet & Phillip Selznick, *Law and Society in Transition: Toward Tanggapanive Law,* (London : Harper and Row Publisher, 1978), disandur dari buku Benard L. Tanya, *Op.Cit.*, hlm. 205.

[35] *Ibid.*, hlm. 206.

b. Subtansi, mencakup aturan – aturan hukum baik yang tertulis maupun yang tidak tertulis, termasuk putusan pengadilan ;
c. Budaya Hukum, mencakup opini – opini, kebiasaan-kebiasaan, cara berfikir dan cara bertindak, baik dari penegak hukum maupun dari warga masyarakatnya.[36]

Sistem hukum mempunyai struktur, kerangka atau rangkanya, bagian yang tetap bertahan, bagian yang memberi semacam bentuk dan batasan terhadap keseluruhan . Sedangkan maksud dari subtansi adalah aturan, norma, dan pola perilaku nyata manusia yang berada dalam sistem itu. Penekanannya terletak pada hukum yang hidup, bukan hanya pada aturan kitab hukum (law books). Selanjutnya, hal ini membawa kita kepada komponen ketiga yaitu budaya hukum, yaitu sikap manusia terhadap hukum dan sistem hukum; kepercayaan, nilai , pemikiran dan harapannya. Dengan kata lain budaya hukum adalah suasana pikiran sosial dan kekuatan sosial yang menentukan bagaimana hukum digunakan, dihindari atau disalah gunakan. Tanpa budaya hukum sistem hukum itu sendiri tidak akan berdaya.[37]

Internet merupakan media yang bersifat lintas batas wilayah dan negara, sehingga apabila terjadi tindak pidana akan sulit untuk menentukan *locus delictienya*, karena akan bersinggungan dan melibatkan kepentingan negara lain. Hal ini menjadi kendala pula dalam penegakan hukumnya akan tetapi tidak bisa dibiarkan berlarut – larut dan harus segera dicarikan alternatif pemecahannya, salah satunya adalah melakukan revisi terhadap undang – undang yang telah berlaku.

1.8.2 Kerangka Konsep

Perkembangan teknologi khususnya teknologi informasi telah menyebabkan perkembangan yang pesat aktivitas di berbagai sektor kehidupan, khususnya di bidang sosial dan ekonomi. Bahkan hubungan – hubungan di bidang sosial dan ekonomi di masyarakat internasional boleh dikatakan dewasa ini telah

[36] Lawrence M. Friedman, *Hukum Amerika, Sebuah Pengantar, Terjemahan dari Wishnu Basuki*, (Jakarta : Tatanusa, 2001) hal 190.
[37] Ibid., hal 8

memasuki suatu masyarakat yang berorientasi kepada informasi. Hubungan – hubungan *(interaksi)* melalui teknologi informasi tersebut tidak lagi secara fisikal sebagaimana yang terjadi selama ini, namun interaksi tersebut secara *virtual* atau *cyberspace* (dunia maya).[38]

Tindak pidana siber merupakan bentuk kejahatan baru, apabila dibandingkan dengan bentuk – bentuk kejahatan lainnya yang bersifat konvesional *(street crime)* karena tindak pidana siber muncul bersamaan dengan lahirnya revolusi tekhnologi informasi. Tindak pidana dibidang komputer atau dalam bahasa inggris disebut *Cyber Crime* merupakan istilah atau penyebutan kejahatan yang masih tergolong baru sehingga terjemahan dari *cyber crime* itu sendiri beragam. Meskipun belum ada kesamaan mengenai definisi *cyber crime*, namun terdapat pengertian secara universal mengenai tindak pidana di bidang komputer.

Kongres PBB X tentang *Prevention of crime and the treatment of offender* di Vienna , 10 – 17 April 2000 menyebutkan tentang pengertian *cyber crime* yang dibagi dua kategori, yaitu:

"Cyber crime in a narrow sense (computer crime); any illegal behaviour committed by means of electronic operations that targets the security of computer system and the data processed by them; and

Cyber crime in a broader sense (computer related crime); any illegal behavior committed by means of, or in relation to, a computer system network, including such crimes as illegal possession and offering or distributing information by means of a computer of network." [39]

Terjemahan bebas penulis :

Cyber crime dalam pengertian sempit (kejahatan terkait bidang komputer); segala perilaku tidak sah yang dilakukan atas bantuan alat elektronik yang bertujuan mengakses keamanan sistem komputer dan data;

Cyber crime dalam pengertian lebih luas (kejahatan terkait hubungan bidang komputer); segala perilaku tidak sah yang dilakukan atas bantuan, atau dalam hubungan dengan, suatu jaringan sistem komputer, mencakup seperti kejahatan

[38] Mieke Komar Kantaatmadja,et.al, *Cyber Law Suatu Pengantar*, (Bandung;Elips,2001) , hlm 88.
[39] Agus Rahardjo, *Cybercrime, Pemahaman dan Upaya Pencegahan Kejahatan Bertekhnologi*, (Bandung: PT. Citra Aditya Bakti, 2002), hlm. 229.

pemilikan tidak sah dan menawarkan atau membagi – bagikan informasi atas bantuan melalui jaringan komputer.

Black's Law Dictionary mengartikan "*computer crime*" atau "*cyber crime*" adalah: "*crime requiring knowledge of computer technology, such as sabotaging or stealing computer data or using a computer to commit some other crime."* [40]

Terjemahan bebas penulis :
Kejahatan yang membutuhkan pengetahuan tentang teknologi komputer, seperti sabotase atau mencuri data komputer atau menggunakan komputer untuk melakukan beberapa kejahatan lainnya.

Law Dictionary mengartikan *"computer crime"* atau *"cyber crime"* adalah tindak pidana yang termasuk golongan "*cyber law*" yaitu bidang hukum sehubungan dengan komputer dan Internet, termasuk isu mengenai Hak Atas Kekayaan Intelektual (*Intellectual Property Right*), kebebasan mengeluarkan pendapat dan akses bebas mendapatkan informasi. Tindak pidana komputer mengisyaratkan pengetahuan tekhnologi tentang komputer, misalnya sabotase atau pencurian data komputer untuk melakukan kejahatan lainnya.[41]

Cybercrime merupakan salah satu bentuk atau dimensi baru dari kejahatan masa kini yang mendapat perhatian yang luas di dunia internasional. Volodymyr Golubev menyebutnya sebagai *the new form of anti-social behaviour*. Beberapa julukan atau sebutan lainnya untuk kejahatan *cyber crime* ini di dalam berbagai tulisan antara lain sebagai kejahatan dunia maya *(cyber space I virtual space offence)*, dimensi baru dari *high tech crime*, dimensi baru dari *transnasional crime*, dan dimensi baru dari *white collar crime*.[42]

Sedangkan Sutan Remy Syahdeini mendefinisikan tindak pidana di bidang komputer sebagai perilaku jahat yang dilakukan oleh pelakunya dengan menggunakan program komputer sebagai sarana untuk melakukan perbuatan

[40] *Black's Law Dictionary ,* disadur dari Sutan Remy Syahdeini, *Op.Cit*., hlm. 39.
[41] Martin Basiang , *The Contemporary Law Dictionary* , (Indonesia : Red & White Publishing, 2009), hlm. 76.
[42] Barda Nawawi Arief, *Tindak Pidana Mayantara,Perkembangan Cyber Crime di Indonesia*,(Jakarta: Raja Grafindo Persada, 2007) hlm.1

tersebut atau sistem komputer sebagai sasarannya dan belum dikriminalisasi oleh undang – undang pidana sebagai tindak pidana.[43]

Berdasarkan pengertian di atas *computer crime* mencakup perbuatan ilegal terhadap sistem dan data dengan menggunakan sarana elektronik, sedangkan *cyber crime* merupakan kejahatan yang dilakukan dengan media eletronik atau dilakukan sebagian atau sepenuhnya dalam lingkungan elektronik. Dimasa yang akan datang pengertian *cyber crime* dapat saja mengalami perkembangan lain.

Debra L. Shinder membuat kategori *cyber crime* berdasarkan cara kejahatan dilakukan , yaitu:

" Crime commited by violent or potentially violent criminal: Cyberterrorism Assault by threat; Cybertalking; Child Pornography; Non violent crimes; Cybertrespass; Cybertheft; Cyberfraud; Destructive cyber crime ; Other cyber crime , termasuk advertising / soliciting prostitution services over internet, internet gambling, internet drugs sales, cyberlaundering."[44]

Menurut Nitibaskara *cyber crime* mempunyai ciri – ciri khusus sebagai berikut: *Non violence* (tanpa kekerasan); Sedikit melibatkan kontak fisik *(minimize of physical contact);* Menggunakan peralatan *(equipment)* dan teknologi; Memanfaatkan jaringan telematika (telekomunikasi, media dan informatika) global.[45]

Ciri – ciri ini memperlihatkan bahwa tindak pidana di bidang komputer berbeda dengan kejahatan – kejahatan yang ada sebelumnya, mengingat tindak pidana di bidang komputer muncul sebagai dampak dari perkembangan teknologi. Oleh karena itu diperlukan suatu pengaturan yang tegas dan partisipasi aparat penegak hukumnya untuk menimalkan dan mencegah kejahatan ini meluas.

Kitab Undang Hukum Pidana yang sekarang digunakan di Indonesia merupakan warisan jaman kolonial, sehingga terdapat banyak hal yang dirasa kurang memuat identitas nasional serta mencerminkan nilai – nilai budaya masyarakat Indonesia, untuk dilakukan usaha pembaharuan hukum pidana nasional untuk mengikuti perkembangan masyarakat Indonesia. Pembaharuan

---

[43] Sutan Remy Syahdeini, *Op.Cit.*, hlm. 40.

[44] Debra L. Shinder , *Kategori Kejahatan Cybe*r, http://www.yahoo.com . diunduh pada tanggal 10 Oktober 2011

[45] Tubagus Rony Rahman Nitibaskara, *Ketika Kejahatan Berdaulat, Sebuah Pendekatan Kriminologi, Hukum dan Sosiologi*, (Jakarta: Perdaban, 2001), hlm. 45.

hukum ini dilakukan untuk menuju kehidupan yang berkeadilan sesuai dengan nilai – nilai budaya bangsa.

Pembaharuan hukum pidana yang menyeluruh harus meliputi hukum pidana materiil, hukum pelaksana pidana dan hukum pidana formil.[46] ketiganya harus dilakukan pembaharuan secara bersama – sama untuk dapat menjamin tercapainya keadilan dan kepastian hukum.

1.9 Sistematika Penulisan

Sistematika yang akan dipergunakan dalam penulisan ini adalah sebagai berikut :

Bab I **Pendahuluan**

Bab ini menguraikan mengenai latar belakang permasalahan, pernyataan masalah, rumusan permasalahan, tujuan penelitian, manfaat penelitian, metode penelitian, kerangka teori, kerangka konseptual yang digunakan dalam penelitian ini serta sistematika penulisan.

Bab II **Tinjauan Mengenai Perkembangan Aspek – Aspek Mengenai Informasi dan Transaksi Elektronik**

Bab ini memuat tinjauan pustaka yang antara lain membahas tentang berbagai konsepsi dari istilah - istilah yang terkait dengan Informasi dan Teknologi Elektronik. Selain itu juga menguraikan pengaturan tindak pidana siber di Indonesia setelah berlakunya Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Bab III **Tindak Pidana Siber dan Pengaturan**

Bab ini menjelaskan kejahatan atau perbuatan apa saja yang dapat digolongkan sebagai tindak pidana siber yang berkembang secara umum di dalam dunia internasional dan pengaturan dibeberapa konvensi ataupun Undang – Undang serta yang diatur oleh Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

---

[46] Sudarto, *Pembaharuan Hukum Pidana di Indonesia dalam Simposium Pembaharuan Hukum Pidana Nasional*, (Jakarta: Binacipta, 1986), hlm. 26.

Bab IV **Penerapan Undang – Undang No. 11 Tahun 2008**

Bab ini membahas kendala apa saja yang ditemukan di dalam penerapan Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dilihat dari sisi tindak pidana siber. Serta bagaimana penerapan undang – undang ini dalam penyelesaian kasus di Indonesia.

Bab V **Kesimpulan**

Pada bab terakhir memberikan kesimpulan dan saran yang diperoleh dari analisis penguraian pada bab – bab sebelumnya. Kesimpulan ini adalah merupakan jawaban atas pokok permasalah yang ditulis pada awal bab, serta saran yang dibuat penulis mungkin dapat menjadi pembaharuan pengaturan tindak pidana siber sistem hukum positif di Indonesia

BAB II

TINJAUAN PERKEMBANGAN ASPEK – ASPEK YURIDIS MENGENAI INFORMASI DAN TRANSAKSI ELEKTRONIK

2.1 Pengertian Informasi dan Transaksi Elektronik

Sebelum membahas peraturan yang mengatur tentang Informasi dan Transaksi Elektronik sesudah berlakunya Undang - Undang No.11 Tahun 2008, dalam sub bab ini kita harus mengetahui dulu beberapa peristilahan berserta pengertiannya, yang dimuat dalam ketentuan – ketentuan terkait dengan Informasi Transaksi Elektronik yang akan kita bahas untuk menyamakan pandangan dan menghindari timbulnya perbedaan penfsiran mengenai obyek dan pokok masalah dalam penelitian ini.

a. Pengertian Informasi Elektronik dan Dokumen Elektronik

Istilah informasi menurut pengertian kebahasaan adalah penerangan; keterangan; kabar atau pemberitahuan.[47] Pengertian dimaksud sangatlah jarang dipahami pada hari ini. Seringkali dengan mudah informasi dimengerti sebagai isi atau muatan dari dokumen yang sehari – hari dapat ditemui. Informasi yang disampaikan melalui media cetak dan media elektronik adalah salah satu contohnya.

Berdasarkan ketentuan umum dalam Pasal 1 Bab I Undang - Undang No.11 Tahun 2008, pada angka I, yang dimaksud dengan informasi elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *Elektronik Data Interchange* (EDI), surat elektronik (elektronik mail), telegram, teleks, telecopy atau sejenis nya, huruf, tanda, angka, kode akses, simbol, atau perfrasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.[48]

Informasi elektronik merupakan salah satu hal yang diatur secara subtansial dalam Undang - Undang No.11 Tahun 2008 selain transaksi

[47] W.J.S Poerwadarminta, *Kamus Umum Bahasa Indonesia*, (Jakarta; Balai Pustaka, 1999) hlm. 380

[48] Indonesia , *Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik,* UU No. 11 Tahun 2008, LN Tahun 2008.

elektronik. Perkembangan pemanfaatan informasi elektronik dewasa ini, sudah memberikan kenyamanan dan kemanfaatannya. Sebagai contoh, penggunaan email sangat memudahkan setiap orang bisa berkomunikasi melalui pengiriman berita secara cepat, dan dapat melintasi wilayah baik lokal, regional, dan bahkan internasional.

Perbuatan yang dilarang oleh Undang - Undang No.11 Tahun 2008 yang berkaitan dengan informasi elektronik adalah mendistribukan, atau membuat dapat diaksesnya informasi elektronik, yang muatannya berisi melanggar kesusilaan, muatan perjudian, penghinaan atau pencemaran nama baik atau pemerasan dan atau pengancaman. Muatan yang berisi melanggar kesusilaan diantaranya adalah penayangan gambar – gambar porno dalam situs – situs internet maupun telepon seluler. Penayangan gambar porno itu, selain melanggar Undang - Undang No.11 Tahun 2008 juga melanggar Undang – Undang No. 44 Tahun 2008 tentang Pornografi.

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 sistem komputer atau sistem elektronik, termasuk tetapi tidak terbatas pada tulisan, suara gambar, peta, rancangan, foto atau sejenisnya,

b. Pengertian Teknologi Informasi

Dalam Pasal 1 angka 3 Undang - Undang No.11 Tahun 2008, pengertian teknologi informasi adalah suatu teknik untuk mengumpulkan menyiapkan, menyimpan memproses, ,mengumumkan, menganalisis dan atau menyebarkan informasi. Istilah “teknologi informasi” mulai dipergunakan secara luas Tahun 1980-an. Teknologi ini merupakan pengembangan dari teknologi komputer yang dipadukan dengan teknologi telekomunikasi.

Definisi kata “informasi” sendiri secara internasional telah disepakati sebagai “hasil dari pengolahan data” yang secara prinsip memiliki nilai atau *value* yang lebih dibandingkan dengan data mentah. Komputer merupakan bentuk teknologi informasi yang pertama yang dapat melakukan proses

pengolahan data menjadi informasi.[49] Barry B Sookman dalam bukunya yang berjudul *Computer, Internet, and Electronic Commerce Terms: Judicial, Legislave, and Technical Defintions* mengemukakan bahwa defisini informasi memiliki konotasi sangat luas. Perintah atau serangkaian perintah saja telah dapat dimaknai oleh informasi.[50] Dalam kurun waktu yang kurang lebih sama, kemajuan teknologi telekomunikasi terlihat sedemikian pesatnya, sehingga telah mampu membuat dunia menjadi terasa lebih kecil. Dengan demikian komputer merupakan salah satu produk dalam *domain* terknologi informasi disamping *Modem, Router, Cracle, SAP, Pranata Media, Cabling System, VSAT* dan lain sebagainya.[51]

Teknologi informasi disusun oleh tiga komponen utama teknologi.[52] yaitu :

1. Teknologi komputer *(computing)* yang menjadi pendorong utama perkembangan teknologi informasi;
2. Teknologi telekomunikasi yang menjadi inti proses penyebaran informasi secara massal dan mendunia;
3. Muatan komunikasi yang menjadi faktor pendorong utama implementasi teknologi dalam seluruh bidang – bidang kegiatan manusia.

Perkembangan ketiga komponen pembentuk teknologi informasi inipun mulai konvergen mengikuti konsep ilmu informasi yang semakin matang.

c. Pengertian Transaksi Elektronik

Internet telah pula mengubah cara dan sarana transaksi bisnis. Melalui internet transaksi – transaksi bisnis yang selama inui dilakukan di dunia nyata dengan menggunakan kertas dapat dilakukan secara elektronik.

---

[49] Badan Pembinaan Hukum Nasional, *Laporan Tim Forum Dialog Hukum dan Non Hukum Kelompok Kerja Bidang Hukum dan Teknologi,* (Jakarta: Badan Pembinaan Hukum Nasional Kementerian Hukum dan HAM RI,2004) hlm.25

[50] M. Arsyad Sanusi, *Hukum dan Teknologi Informasi*, (Jakarta:Milestone Publisher,2005) hlm.6

[51] Ibid., hlm 26.

[52] Brian K. Williams, Stacey Sawijen and Sarah H. Hurt Chraison in *Using Information Technology, A Practical Introduction to Computer and Communications*, NewYork:Mc-GrawHill, 1989.

Dalam Pasal 1 angka 2 Undang - Undang No.11 Tahun 2008 yang dimaksud dengan transaksi elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer, dan/atau media elektronik lainnya. Transaksi elektronik biasa disebut dengan bahasa inggrisnya *electronic transaction atau e-commerce*.

Perbuatan hukum penyelenggaraan transaksi elektronik dapat dilakukan dalam lingkup publik ataupun privat. Para pihak yang melakukan transaksi elektronis wajib bertikad baik dalam melakukan interaksi dan/atau pertukaran informasi elektronik dan atau dokumen elektronik selama transaksi berlangsung. Penyelenggaraan transaksi elektronis ini diatur dengan peraturan pemerintah.

Transaksi elektronik diatur dalam Pasal 17 Undang - Undang No.11 Tahun 2008 yang berbunyi sebagai berikut :

1. Penyelenggaraan transaksi elektronik dapat dilakukan dalam lingkup publik dan privat.
2. Para pihak yang melakukan transaksi elektronik
3. Ketetntuan lebih lanjut mengenai penyelenggaraan transaksi elektronis sebagaimana dimaksud pada ayat (i) diatur dengan Peraturan Pemerintah.

Dalam penjelasan pasal 17 ayat 1 Undang - Undang No.11 Tahun 2008 dijelaskan bahwa Undang – Undang ini memberikan peluang terhadap pemanfaatan teknologi informasi oleh penyelenggaraan negara, orang, badan usaha, dan atau masyarakat. Pemanfaatan teknologi informasi harus dilakukan secara baik, bijaksana bertanggung jawab, efektif, dan efisien agar dapat diperoleh manfaat yang sebesar – besarnya bagi masyarakat.

Transaksi elektronik yang dituangkan ke dalam kontrak elektronik mengikat para pihak, sebagaimana diatur dalam Pasal 18 ayat (1). Para pihak memiliki kewenangan untuk memilh yang berlaku bagi transaksi elektronik internasional yang dibuatnya (Pasal 18 ayat (2)). Jika para pihak tidak melakukan pilihan hukum dalam traksaksi elektronik internasional hukum yang berlaku disesuaikan pada asas hukum perdata internasional (Pasal 18 ayat (3)). Para pihak memiliki kewenangan untuk menetapkan pengadilan,

arbitrase, atau lembaga penyelesaian sengketa alternatif lainnya, yang bisa berwenang menangani sengketa yang mungkin timbul dari transaksi elektronik internasional yang dilakukannya (Pasal 18 ayat (4)).

Jika para pihak tidak melakukan pilihan hukum sebagaimana yang dimaksud di atas, penetapan kewenangan pengadilan, arbitrase, atau lembaga penyelesaian sengketa alternatif lainnya yang berwenang menangani sengketa yang mungkin timbul dari transaksi tersebut didasarkan pada asas hukum perdata internasional (Pasal 18 ayat (5)). Pilihan hukum yang dimaksud Undang – Undang ini berdasarkan penjelasan Pasal 18 ayat 2 Undang - Undang No.11 Tahun 2008, bahwa pilihan hukum yang dilakukan oleh para pihak dalam kontrak internasional termasuk yang dilakukan secara elektronik dikenal oleh sebutan *choise of law* .

Pasal 19 mengatur mengenai Sistem Elektronik dimana disebutkan dalam pasal ini para pihak yang melakukan Transaksi Elektronik harus menggunakan Sistem Elektronik yang disepakati.

d. Dunia Maya

Istilah *Cyberspace* atau dunia maya pertama kali dipopulerkan oleh William Gibson dalam novel *science fiction* yang berjudul *Neuromancer*[53] sekitar tahun 1980-an, cyberspace didefinisikan sebagai :

" A consensual hallucination experienced daily by billions of legitimate operators, in every nation.... A graphic representation of data abstracted from 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".

Dari definisi di atas dapat dilihat bahwa pada mulanya istilah *cyberspace* tidak ditunjukan untuk menggambarkan interaksi yang terjadi melalui jaringan komputer atau suatu tempat yang tidak terbatas dimana data – data yang diorganisasikan sedemikian rupa ke dalam suatu lintas media.

Sedangkan Ian J.Lloyd mengatakan bahwa *cyberspace* adalah fenomena dunia digital yang telah merasuki segala segi dari kehidupan

[53] Mark D. Rasch, *CriminalLaw and The Internet*, www.cybercrime.net diakses pada tanggal 1 Oktober 2011, Lihat juga di buku *Kompilasi Hukum Telematika* karya Edmon Makarim, hlm 59.

manusia.[54] Dari dua definisi tersebut dapat dipahami bahwa dunia maya merupakan ruang yang tidak dapat terlihat. Ruang ini tercipta ketika terjadi hubungan komunikasi yang dilakukan untuk menyebarkan suatu informasi, dimana jarak secara fisik tidak lagi menjadi halangan.

Dunia maya dan kejahatan dunia maya merupakan dua hal yang tak terpisahkan. Korelasi keduanya apabila dianalogikan seperti hubungan antara bumi dan aktifitas manusia, yaitu hubungan antara mereka media dan aktifitas yang berlangsung di atasnya. Kejahatan dunia maya sebagai suatu aktifitas tidak akan terjadi jika tidak ada medianya, yaitu dunia maya. Namun analogi ini tidak tepat jika kita kaitkan dengan permasalahan batas teritorial dan wilayah, maksudnya jika dunia nyata, kita dengan mudah dapat mengidentifikasikan tempat (lokasi) berlangsungnya suatu aktifitas seseorang. Maka hal yang sama tidak berlaku di dunia maya, karena aktifitas di media tersebut tidak seperti yang terjadi di dunia maya, terlepas dari isu batas wilayah. Permasalahan batas wilayah ini dalam konteks dunia nyata mempunyai arti penting, khususnya dalam hal menentukan hukum mana atau hukum apa yang seharusnya diterapkan dalam suatu peristiwa.[55]

e. Tindak pidana siber (*Cybercrime)*

Tindak pidana siber atau sering disebut dengan *cybercrime* merupakan salah satu bentuk atau dimensi baru dari kejahatan masa kini yang mendapat perhatian yang luas di dunia internasional. Volodymyr Golubev menyebutnya sebagai *the new form of antisocial behaviour.* Beberapa julukan atau sebutan lainnya untuk kejahatan *cyber crime* ini di dalam berbagai tulisan antara lain sebagai kejahatan dunia maya "*cyber space In virtual space offence",*dimensi baru dari *high tech crime*, dimensi baru dari *transnational crime*, dan dimensi baru dari *white collar crime.*[56]

---

[54] Ibid., hlm 13

[55] UNESCO, *The International Demension of Cyberspace Law,* (England: Ashgate Publishing Ltd,2000), hlm128.

[56] Barda Nawawi Arief, Tindak Pidana *Mayantara, Perkembangan Kajian Cyber Crime di Indonesia,* (Jakarta;Raja Grafindo Persada,2007) hlm.1.

Cybercrime disebut juga sebagai kejahatan lahir sebagai dampak negatif dari perkembangan aplikasi internet.[57] Dari pengertian ini bahwa cybercrime mencakup semua jenia kejahatan beserta modus operandinya yang dilakukan sebagai negatif aplikasi internet. Secara umum yang dimaksud kejahatan komputer atau kejahatan didunia syber yaitu upaya memasuki dan atau menggunakan fasilitas komputer atau jaringan komputer tanpa izin dan dengan melawan hukum dengan atau tanpa menyebabkan perubahan dan atau kerusakan pada fasilitas komputer yang dimasuki atau digunakan tersebut. Dengan demikian jelaslah bahwa jika seseorang menggunakan komputer atau bagian dari jaringan komputer tanpa seijin yang berhak, tindakan tersebut sudah tergolong kejahatan komputer.[58]

Perkembangan *cybercrime* yang masih relatif baru mengakibatkan belum adanya definisi yang final terhadap *cybercrime* itu sendiri. Menurut Dokumen Kongres PBB tentang *The Prevention Of Crime and Treatment Of Offlenderes* di Havana, Cuba pada tahun 1999 dan di Wina, Austria Tahun 2000. Menyebutkan ada dua istilah yang dikenal :

a. *Cyber crime in a narrow sense (dalam arti sempit) disebut computer crime; any illegal behaviour directed by means of electronic operation that target the security of computer system and the data processed by them.* Yaitu *Cybercrime* dalam arti sempit adalah setiap tindakan ilegal yang dilakukan menggunakan peralatan elektronik yang ditunjukan pada keamanan sistem komputer dan pemprosesan data yang menggunakan komputer;
b. *Cyber crime in a broader sense* (dalam arti luas) *disebut computer related crime; any illegal behaviour committed by means on relation to, a computer system offering or system or network, including such crime as illegal possession in, offering or distributing information by means of computer system or network.* Yaitu, *Cybercrime* dalam arti luas disebut juga kejahatan yang berhubungan dengan komputer, yaitu setiap perilaku ilegal yang memanfaatkan komputer atau sistem jaringan, termasuk

[57] Ari Juliano Gema, *Cyber Crime : Sebuah Fenomena di Dunia Maya,* www.theceli.com, 2000.
[58] Merry Magdalena dan Maswigrantoro R. Setyadi, *Cyberlaw,Tidak Perlu Takut.* (Yogyakarta:Penerbit Andi,2007) hlm. 37.

kejahatan tertentu dalam menyimpan, menawarkan, atau mendistribusikan informasi secara ilegal menggunakan sistem atau jaringan komputer.[59]

Kepolisisan Republik Indonesia dalam hal ini unit *Cybercrime,* menggunakan parameter berdasarkan dokumen kongres PBB tentang *The Prevention Of Crime and Treatment Of Offlenderes* di Havana, Cuba pada tahun 1999 dan di Wina, Austria Tahun 2000.

Convetion on Cybercrime tidak menganggap terminologi *"cybercrime"* sebagai kata yang urgen untuk didefinisikan. Hanya ada empat kata yang didefinisikan dalam konvensi tersebut, yaitu *"computer system" , "computer data", "service data" dan "traffic data".*[60] Secara umum 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, atau computer crime.*

Menurut Barda Nawawi Arief, pengertian *computer-related crime* sama dengan *cyber crime*. Ronny R. Nitibaskara berpendapat, bahwa kejahatan yang terjadi melalui atau pada jaringan komputer di dalam internet disebut *cybercrime*, kejahatan ini juga dapat disebut kejahatan yang berhubungan dengan komputer (*computer-related crime*), yang mencakup dua hal kategori kejahatan, yaitu kejahatan yang menggunakan komputer sebagai sarana atau alat dan menjadikan komputer sebagai sasaran atau objek kejahatan.[61]

Namun ada pula untuk kejahatan terkait komputer ini dengan istilah kejahatan telematika. Penggunaan istilah Kejahatan Telematika bukan berarti menafikan istilah yang lain namun lebih sebagai pilihan dalam menggambarkan sifat teknologi informatika yang semakin konvergen.[62]

---

[59] Dokumen Kongres PBB tentang *The Prevention Of Crime and Treatment Of Offlenderes* di Havana, Cuba pada tahun 1999

[60] Convention On Cybercrime Article 1.

[61] Widodo, *Sistem Pemidanaan Dalam Cyber Crime, Alternatif Ancaman Pidana Kerja Sosial Dan Pidana Pengawasan Bagi Pelaku Cyber Crime,* (Yogyakarta:Laskbang Mediatama,2009) hlm.23

[62] Ali Wibisono, *Strategi Penanggulangan Kejahatan Telematika,* (Yogyakarta: Atmajaya, 2010) hlm. 1

Menurut Edmon Makarim, dunia siber yang menciptakan fenomena virtual,[63] di dalam kenyataan sering disalah artikan sebagai alam maya, padahal keberadaan dari sistem elektronik itu sendiri adalah konkret karena bentuk komunikasi virtual tersebut sebenarnya dilakukan dengan cara representasi informasi digital (0-1) yang bersifat diskrit.

Istilah kejahatan komputer yang lebih dahulu dikenal memang telah memberikan gambaran mengenai ruang lingkup kejahatan berbasis teknologi informatika. Terlebih lagi hingga kini dalam berbagai sumber istilah kejahatan komputer *(computer crime)* disejajarkan atau diidentikkan dengan istilah siber *(cyber crime)*. Namun demikian, seiring dengan lajunya perkembangan telekomunikasi, media dan informatika, maka istilah komputer nampak hanya merupakan bagian dari keseluruhan teknologi telematika sehingga kurang bisa menggambarkan konvergensinya. Demikian pula dengan istilah "kejahatan internet", kejahatan mayantara atau *cyber crime* yang juga merupakan bagian yang paling konvergen dari telematika. [64]

Dilihat dari asal katanya, *cybercrime* secara harafiah berasal dari kata *cyber* dan *crime*. *Cyber* berasal dari kata *cybernatics* yang di dalam *Encyclopedia of Knowledge*, sebagaimana yang dikutip oleh Edmon Makarim[65] adalah :

"...is a term formely used to describe an interdisciplinary approach to the study of control and communication in animals, humans, machines and organizations. The World."

Berbagai pihak telah mencoba memberikan definisi tentang *cybercrime*, ada yang mendefinisikan *cybercrime* adalah suatu aktivitas yang dilakukan dengan sebuah alat (*PC, laptop, notebook, handphone*) yang terhubung dengan jaringan internet dan aktivitas tersebut melanggar undang – undang.[66] Menurut Goodman & Brenner[67], istilah *cybercrime*, *computer crime* dan

---

63 Makarim.,Op.cit,hlm 3.
64 Ibid.,hlm 2.
65 Makarim.,Op.cit,hlm 6
66 Sutanto, Hermawan Sulistyo, Tjuk Sugiarso,Ed., *Cybercrime: Motif dan Penindakan,Cet 1*,(Jakarta:Pensil-324,2005), hlm.20.
67 Marc D. Goodman dan Susan W.Brenner,*The Emerging Consensus On Criminal Conduct in Cyberspace*,hlm 10 Diakses melalui situs www.lawtechjournal.com/articles/2002/03_020625_goodmanberner.php pada tangga l 5 oktober 2011.

high-tech-crime seringkali digunakan secara bergantian untuk merujuk kepada dua kategori, dimana suatu perbuatan telah dianggap melawan hukum. Dua kategori tersebut adalah pertama, komputer merupakan target bagi perbuatan pelaku. Dalam hal ini pelaku bisa melakukan akses secara ilegal, penyerangan kepada jaringan (pembobolan) dan lain lain yang terkait dengan sistem pengamanan jaringan *(networking)*. Sedangkan kategori yang kedua adalah bahwa perbuatan tersebut mengandung maksud dan tujuan seperti layaknya kejahatan konvesional, misalnya pecurian, pemalsuan dan lain lain.

Goodman dan Brenner melakukan survey mengenai *cybercrime*. Survey ini menunjukan bahwa di negara – negara yang relatif maju teknologi informasinya *cybercrime* dapat dibedakan menjadi delapan kategori, yaitu: akses yang tidak sah, merubah dan memanipulasi data pada komputer secara tidak sah, sabotase terhadap komputer, pemanfaatan sistem informasi secara melawan hukum, penipuan dengan komputer (*computer fraud*, spionase (industrial, keamananan dan lain lain), dan pelanggaran privasi.[68]

Lastwoka dan Hunter mendefinisikan *cybercrime* sama dengan apa yang biasanya disebut sebagai *virtual crime* (kejahatan maya), yaitu suatu kejahatan dilakukan terhadap komputer atau dengan alat bantu komputer.[69] Meskipun gambaran mengenai *cybercrime* cukup beragam, pada dasarnya terdapat karakteristik tertentu yang dapat digunakan untuk mengenali *cybercrime*. Menurut Freddy Harris [70], pada umumnya *cybercrime* memiliki ciri – ciri sebagai berikut: *non-violence* (tanpa kekerasan), sedikit melibatkan kontak fisik (*minimum of physical contact*), menggunakan peralatan dan teknologi, memanfaatkan jaringan telematika global.

Berdasarkan ciri – ciri tersebut, terutama ciri yang terakhir, *cybercrime* dapat terjadi dengan mengaitkan beberapa wilayah hukum atau beberapa negara sekaligus. Hal ini sesuai dengan rekomendasi yang dikeluarkan oleh negara – negara G-8 yang menyatakan bahwa *high-tech* dan *computer-related*

---

68 Godman and Brenner., Op.cit., hlm 79

69 F.Gregory Lastwoka dan Dan Hunter, *Virtual Crime situs* http://papers.ssm.com/sol3/papers.cfm?abstract_id=564801>, pada tanggal 5 oktober 2011.

70 Dikdik M. Arief Mansur dan Elisatris Gultom, *Cyber Law Aspek Hukum Teknologi Informasi, Cet-1*. (Bandung:PT Refika Aditama,2005),hlm.27

crimes termasuk ke dalam *transnational crime*.[71] Masuknya *cybercrime* ke dalam kategori *transnational crime* berarti bahwa tindak pidana siber melibatkan lintas yurisdiksi.

Di Indonesia *cybercrime* dapat diartikan dengan tindak pidana komputer. Definisinya adalah perilaku yang dilakukan oleh pelakunya dengan menggunakan program komputer sebagai sarana untuk menggunakan program komputer sebagai sarana untuk melakukan perbuatan tersebut atau yang dilakukan oleh pelakunya terhadap sistem komputer sebagai sasarannya dan telah dikriminalisasi oleh undang – undang pidana sebagai tindak pidana.[72]

Berdasarkan definisi – definisi di atas, dapatlah dirumuskan bahwa tindak pidana siber itu merupakan segala tindakan yang merugikan orang lain dengan menggunakan komputer sebagai alat untuk melakukan kejahatan serta sistem dan data di dalamnya sebagai target. Atau, *cybercrime* dirumuskan sebagai perbuatan melawan hukum yang dilakukan dengan memakai komputer sebagai sarana/alat atau komputer sebagai objek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain. Secara ringkas tindak pidana siber ini dapat didefinisikan sebagai perbuatan melawan hukum yang dilakukan dengan menggunakan teknologi komputer canggih.

2.2 Penerapan Sesudah Berlakunya Undang – Undang No. 11 Tahun 2008

Di Indonesia, peraturan yang mengatur tentang Informasi dan Transaksi Elektronik baru satu Undang – Undang yang mengatur secara khusus, yaitu Undang - Undang No.11 Tahun 2008 baru di Indonesia. Undang - Undang No.11 Tahun 2008 disahkan dan diundangkan oleh Presiden RI pada tanggal 21 April 2008, bisa dikatakan kita masih sangat tertinggal jauh karena baru satu undang – undang yang mengatur aturan tindak pidana siber. Didalam pasal Undang – Undang No.11 Tahun 2008 diperintahkan untuk membentuk Peraturan Pemerintah yang harus sudah ditetapkan oaling lama dua tahun setelah diundangkannya Undang – Undang No.11 Tahun 2008 tetapi sampai saat ini

[71] G-8 Recommendations on Transnational Crime, akses lewat situs http://www.justice.gc.ca/en/news/g8/doc1.htm#4d, Pada 5 Oktober 2011.

[72] Sutan Remy Syahdeini, *Op.Cit.*, hlm 40

belum ada sebuah Peraturan Pemerintah dibuat agar suatu undang – undang dapat berjalan dengan baik. Pada awalnya hanya ada pengaturan mengenai Telekomunikasi melalui Undang – Undang No. 36 Tahun 1999 tentang Telekomunikasi yang merupakan pengganti Undang-Undang No. 3 Tahun 1989 tentang Telekomunikasi.

Sebelum membahas Undang - Undang No.11 Tahun 2008,maka penulis harus membahas Undang – Undang No. 36 Tahun 1999 karena undang – undang ini merupakan undang – undang pertama mengatur tentang tindak pidana siber.Penyelenggaraan telekomunikasi di Indonesia mengalami perubahan yang sangat signifikan dengan adanya Undang – Undang No. 36 Tahun 1999 tentang Telekomunikasi yang disahkan dan diundangkan pada tanggal 8 September 1999. Undang – undang ini lahir sebagai konsekuensi dari adanya perubahan yang mendasar dalam penyelenggaraan dan cara pandang terhadap telekomunikasi yang memerlukan penataan dan pengaturan kembali penyelenggaraan telekomunikasi nasional.[73] Reformasi di bidang industri telekomunikasi termasuk liberalisasi industri, ketentuan bagi penyelenggaraan baru dan peningkatan struktur kompetitif industri.

Di dalam Undang – Undang No. 36 Tahun 1999 yang pertama kali diatur adalah tentang siapa saja yang berhak menyelenggarakan telekomunikasi sesuai dengan peruntukannya. Pihak – pihak yang melakukan kegiatan telekomunikasi dikenal dengan istilah penyelenggaraan telekomunikasi dapat merupakan perseorangan, korperasi, badan usaha milik daerah, badan usaha swasta, instansi pemerintah dan instansi pertahanan keamanan negara. Pihak – pihak yang berhak menyelenggarakan komunikasi dibahas di bawah ini lebih lanjut :[74]

a. Penyelenggara Jasa Telekomunikasi

   Sebelum membahas para pihak – pihak yang berhak menyelenggarakan telekomunikasi, ada baiknya untuk mengetahui definisi telekomunikasi itu sendiri. Telekomunikasi memiliki pengertian sebagai kegiatan pemancaran, pengiriman dan atau penerimaan dari setiap informasi

[73] Ibid., hlm. 273

[74] Indonesia , *Undang – Undang tentang Telekomunikasi* , UU No.36 Tahun 1999, LN Tahun 1999 No. 154, TLN No.3881. Pasal 1 butir ke – 8.

dalam bentuk, tanda, isyarat, tulisan, gambar, suara dan bunyi melalui sistem kawat , optik, radio atau sistem elektromagnetik lainnya.[75]

Penyelenggara jasa telekomunikasi berfungsi untuk penyelenggaraan telekomunikasi untuk memenuhi kebutuhan masyarakat. Badan penyelenggaraan untuk jasa telekomunikasi dalam negeri (domestik) adalah PT. Telkom dan Badan Penyelenggara untuk jasa telekomunikasi luar negeri (internasional) adalah PT. Indosat. Badan Usaha Milik Negara tersebut diberi wewenang untuk yang menyelenggarakan jasa telekomunikasi, seperti telepon, telex, faksmili, dan sebagainya, maupun jasa telekomunikasi berupa jasa – jasa nilai tambah *(value added service)*. Badan lain di luar badan penyelenggara, baik dalam Bentuk Usaha Milik Swasta (BUMS), Badan Usaha Milik Daerah (BUMD) maupun koperasi juga berhak untuk menyelenggarakan jasa telekomunikasi non dasar. Sedang untuk menyelenggarakan jasa telekomunikasi dasar, badan lain dapat bekerjasama dengan PT. Telkom dan atau PT. Indosat. Bentuk kerjasama antara badan penyelenggara dan badan lain ini telah diatur dalam Peraturan Pemerintah Nomor. 8 Tahun 1993, yaitu apat berbentuk Kerjasama Operasi (KSO), usaha patungan dan kontrak manajemen.

b. Penyelenggaraan Telekomunikasi untuk Keperluan Khusus

Penyelenggaraan telekomunikasi untuk keperluan khusus adalah penyelenggaraan telekomunikasi yang dilakukan oleh instansi pemerinah tertentu, perorangan atau badan hukum untuk keperluan khusus atau keperluan sendiri. Telekomunikasi khusus dapat dilakukan oleh intansi pemerintah tertentu atau badan hukum (perseroan terbatas atau korporasi) yang ditentukan berdasarkan hukum. Telekomunikasi khusus diselenggarakan berdasarkan ijin yang ditetapkan oleh Direktur Jenderal Pos dan Telekomunikasi. Ijin penyelenggaraan telekomunikasi khusus hanya diberikan Badan Hukum apabila wilayah tersebut belum tersedia atau belum terjangkau fasilitas komunikasi yang dapat disediakan oleh badan penyelenggara atau badan lain. Telekomunikasi untuk keperluan khusus hanya dapat diselenggarakan dengan mempertimbangkan kerahasiaan dan

[75] Ibid., Pasal 1 butir ke – 1.

jangkauan atau pengoperasiannya perlu bentuk sendiri. Penyelenggaraan telekomunikasi untuk keperluan khusus adalah : Instansi Pemerintah tertentu untuk pelaksanaan tugas khusus, perseoranganan atau, Badan Hukum.

c. Penyelenggaraan Telekomunikasi untuk Keperluan Pertahanan dan Keamanan

Berdasarkan Peraturan Pemerintah Nomor. 4 Tahun 1992 tentang Penyelenggaraan Telekomunikasi untuk Keperluan Pertahanan dan Keamanan Negara diatur bahwa penyelenggaraan telekomunikasi untuk keperluan pertahanan dan keamanan negara (HANKAMNEG) diselenggarakan oleh DEPHANKAM dan/atau ABRI. Penyelenggaraan diperuntukan bagi pertahanan keamanan negara bukan merupakan penyelenggaraan jasa telekomunikasi.

Undang – undang ini merupakan amandemen dari undang – undang sebelumnya yaitu Undang – Undang No. 3 Tahun 1989 tentang Telekomunikasi dan menjadi undang – undang pertama yang memasukkan *cybercrime* sebagai salah satu pelanggaran di dalam bidang telekomunikasi walaupun undang – undang ini masih tidak tegas menyebutnya. Sehingga sulit diterapkan dan dikenakan terhadap pelakunya. Kebijakan hukum yang terkait dengan masalah pengaturan mengenai cybercrime pada undang – undang ini diatur dalam Pasal 21, Pasal 38 dan Pasal 40 yang berbunyi:[76]

Pasal 21:

“ *Penyelenggaraan telekomunikasi dilarang melakukan kegiatan usaha penyelenggaraan telekomunikasi yang bertentangan dengan kepentingan umum, kesusilaan, keamanan, atau ketertiban umum* “

Pasal 38 :

“ Setiap orang dilarang melakukan perbuatan yang dapat menimbulkan gangguan fisik dan elektromagnetik terhadap penyelenggaraan telekomunikasi.”

[76] Ibid., Pasal 21, Pasal 38 dan Pasal 40.

Pasal 40 :

" *Setiap Orang dilarang melakukan kegiatan penyadapan atas informasi yang disalurkan melalui jaringan telekomunikasi dalam bentuk apapun."*

Di dalam Pasal 21 Undang – Undang Telekomunikasi tersebut tidak mengatur tindak kejahatan dan hal ini tidak diatur pula di dalam ketentuan pidana di dalam Bab VII Ketentuan Pidana Pasal 47 sampai dengan Pasal 57. Ketentuan terhadap Pasal 21 berarti hanya merupakan pelanggaran yang berdasarkan ketentuan Bab VI Pasal 46 sanksinya berupa pencabutan izin. Akibat ringannya sanksi hukum tersebut pornografi dan tindakan pengasutan melalui media telekomunikasi sering terjadi dan dilakukan oleh penyelenggaraan telekomunikasi.

Berdasarkan penjelasan Pasal 38 perbuatan yang dapat digolongkan sebagai perbuatan yang dapat menyebabkan gangguan telekomunikasi adalah:[77]

a. tindakan fisik yang menimbulkan kerusakan suatu jaringan telekomunikasi sehingga jaringan tersebut tidak dapat berfungsi sebagaimana mestinya;
b. tindakan fisik yang mengakibatkan hubungan telekomunikasi tidak berjalan sebagaimana mestinya;
c. penggunaaan alat telekomunikasi yang tidak sesuai dengan persyaratan teknis yang berlaku;
d. penggunaan alat telekomunikasi yang bekerja dengan gelombang radio yang tidak sebagaimana mestinya sehingga menimbulkan gangguan terhadap penyelenggaraan telekomunikasi Iainnya; atau
e. penggunaan alat bukan telekomunikasi yang tidak sebagaimana mestinya sehingga menimbulkan pengaruh teknis yang tidak dikehendaki suatu penyelenggaraan telekomunikasi.

Sedangkan menurut penjelasan Pasal 40 yang dimaksud dengan *Cyberspy* adalah: "kegiatan memasang alat atau perangkat tambahan pada jaringan telekomunikasi untuk tujuan mendapatkan informasi dengan cara tidak sah."

Dari penjelasan pasal 38 dan pasal 40 tersebut dapat kita simpulkan bahwa yang diatur di dalam Undang – Undang ini adalah salah satu perbuatan yang

[77] Ibid., Penjelasan Pasal 38

termasuk dalam kategori tindak pidana siber yaitu *illegal interception.*[78] Disini dapat dilihat Undang – Undang No. 36 Tahun 1999 belum secara khusus mengatur hal – hal yang berkaitan dengan telekomunikasi melalui Internet. Undang – Undang ini juga baru mengatur masalah akses tidak sah melalui sarana telekomunikasi berupa larangan melakukan perbuatan tanpa hak, tidak sah atau memanipulasi akses ke jaringan telekomunikasi dan atau akses ke jasa telekomunikasi khusus, ancaman pidana atas perbuatan ini adalah pidana penjara maksimal 6 tahun dan atau denda maksimal Rp. 200.000.000.- (Dua Ratus Juta Rupiah) [79]

Maka disamping Undang – Undang No. 36 Tahun 1999, Indonesia memerlukan Undang – Undang Internet *(Law of Internet)* atau undang – undang siber *(Cyber Law)*. Undang – Undang Internet sebagai suatu rezim hukum yang baru akan lebih memudahkan untuk dipahami dengan mengetahui ruang lingkup pengaturannya. Undang – Undang Internet merupakan undang –undang khusus mengatur secara eksplisit hal – hal yang menyangkut pengiriman dan penerimaan informasi secara elektronik melalui Internet. Undang – undang tentang Internet tersebut telah lahir yaitu Undang - Undang No.11 Tahun 2008, bila Undang – undang ini dihubungkan dengan Undang – Undang No. 36 Tahun 1999 tentang Telekomunikasi, maka Undang – Undang No. 36 Tahun 1999 tentang Telekomunikasi akan merupakan *lex generalis* sedangkan Undang - Undang No.11 Tahun 2008 merupakan *lex specialis* dari Undang – Undang Telekomunikasi tersebut.

Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik ini dibuat dalam rangka melihat globalisasi informasi telah menempatkan Indonesia sebagai bagian dari masyarakat informasi dunia sehingga mengharuskan dibentuknya pengaturan mengenai pengeolaan Informasi dan Transaksi Elektronik di tingkat nasional sehingga pembangunan Teknologi Informasi dapat dilakukan secara optimal, merata dan menyebar ke seluruh lapisan masyarakat guna mencerdaskan kehidupan bangsa.

Dilihat dari sisi perkembangan dan kemajuan Teknologi Informasi yang demikian pesat telah menyebabkan perubahan kegiatan kehidupan manusia dalam

[78] Cybercrime Convention,Op.Cit., Article 3.
[79] Ibid,.

berbagai bidang yang secara langsung telah mempengaruhi lahirnya bentuk – bentuk perbuatan hukum baru mendukung tekhnologi informasi melalui infrastruktur hukum dan pengaturannya sehingga pemanfaatan teknologi informasi dilakukan secara aman untuk mencegah penyalahgunaannya dengan memperhatikan nilai-nilai agama dan sosial budaya masyarakat Indonesia.[80]

Intinya Fokus utama dari keberadaan Undang - Undang No.11 Tahun 2008 adalah memberikan kepastian hukum terhadap keberadaan suatu data atau informasi yang dihasilkan oleh sistem elektronik berikut akunbilitas sistem elektronik itu sendiri dilengkapi dengan beberapa ketentuan hukum yang mengatur penyelenggaraannya dan akibat pemanfaatannya tersebut baik untuk kepentingan hukum individual, komunal maupun nasional bahkan international.[81]

Secara garis besar materi Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik tersebut dimuat dalam sistematika sebagai berikut:

BAB I : Ketentuan Umum;
BAB II : Asas dan Fungsi;
BAB III : Informasi, Dokumen, dan Tanda Tangan;
BAB IV : Penyelenggara Sertifikasi Elektronik dan Sistem Elektronik;
BAB V : Transaksi Elektronik;
BAB VI : Nama Domain, Hak Kekayaan Intelektual Dan Perlindungan Hak Pribadi;
BAB VII : Perbuatan yang dilarang;
BAB VIII : Penyelesaian Sengketa;
BAB IX : Peran Pemerintah dan Peran Masyarakat;
BAB X : Penyidikan;
BAB XI : Ketentuan Pidana;
BAB XII : Ketentuan Peralihan;

---

[80] Raida L. Tobing, *Jurnal Akhir Penelitian Hukum Tentang Efektifitas Undang – Undang No. 11 tahun 2008 Tentang Informasi dan Transaksi Elektronik,*(Jakarta : Badan Pembinaan Hukum Nasional Kementrian Hukum dan HAM RI,2010) hlm.48 .

[81] Ahmad M, Ramli, *Jurnal Tim Perencanaan Pembangunan Hukum Nasional Bidang Teknologi Informasi dan Komunikasi,* (Jakarta : Badan Pembinaan Hukum Nasional Kementrian Hukum dan HAM RI,2008), hlm.53.

BAB XIII : Ketentuan Penutup;[82]

Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik terdiri dari 13 bab dan 54 pasal yang merupakan rezim hukum baru untuk mengatur *cyberspace* di Indonesia. Pada awalnya pembentukkan undang – undang ini banyak menuai kontroversi karena dianggap akan mematikan kebebasan untuk mengekspresikan diri di *cyberspace*. Beberapa aspek yang penting diatur di dalam Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik adalah sebagai berikut:[83]

a. Aspek yuridis, digunakan pendekatan prinsip perluasan Yurisdiksi (*Extra Territorial Yurisdiction)* dikarenakan transaksi elektronik memiliki karakteristik lintas teritorial dan tidak dapat menggunakan pendekatan hukum konvesional;
b. Aspek pembuktian elektronik (e-evindence), alas bukti elektronik merupakan alat bukti dan memiliki akibat hukum yang sah di muka pengadilan;
c. Aspek informasi dan perlindungan konsumen, pelaku usaha yang menawarkan produk melalui media elektronik wajib menyediakan informasi yang lengkap dan benar, berkaitan dengan syarat – syarat kontrak, produsen dan produk yang ditawarkan;
d. Aspek tanda tangan elektronik, memiliki kekuatan hukum dan akibat hukum yang sah (sejajar dengan tanda tangan manual) selama memenuhi persyaratan sebagaimana ditetapkan di dalam Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik;
e. Aspek pengamanan terhadap tanda tangan elektronik, setiap orang yang terlibat dalam tanda tangan elektronik berkewajiban memberikan pengamanan atas tanda tangan elektronik yang digunakannya;
f. Aspek penyelenggara sertifikasi elektronik, setiap orang berhak menggunakan jasa penyelenggara sertifikasi elektronik untuk tanda tangan elektronik yang dibuat;

[82] Ahmad M, Ramli, *Ibid.*, hlm 48.
[83] Raida L. Tobing, Op.cit., hlm 48

g. Aspek penyelenggaraan sertifikasi elektronik, informasi dan transaksi elektronik diselenggarakan oleh penyelenggara sistem elektronik secara andal, aman, dan beroperasi sebagaimana mestinya serta penyelenggara sistem elektronik bertanggung jawab terhadap penyelengaraan/kemanan sistem elektronik yang diselenggarakannya;

h. Aspek tanda tangan digital *(Digital Signature)*, penggunaan digital signature dapat berubah sesuai dengan isi dokumen dan memiliki sifat seperti tanda tangan konvesional sepanjang dapat dijamin keadalannya secara teknis;

i. Aspek transaksi elektronik, kegiatan transaksi elektronik dapat dilakukan baik dalam lingkup publik maupun privat dan transaksi elektronik yang dituangkan dalam kontrak elektronik mengikat para pihak, serta para pihak memiliki kewenangan untuk memilih hukum yang berlaku bagi transaksi elektronik internasional yang dibuatnya;

j. Aspek nama domain *(domain names)*, yang digunakan sebagai Hak Kekayaan Intelektual (HaKI) oleh seseorang, orang dimaksud berhak memiliki nama domain berdasarkan prinsip *first come first serve* dan informasi elektronik yang disusun menjadi karya intelektual y.n, ada di dalamnya, dilindungi sebagai HaKI berdasarkan perundang – undangan yang berlaku;

k. Aspek perlindungan *privacy*, penggunaan setiap informasi melalui media elektronik yang menyangkut data tentang pribadi seseorang harus dilakukan atas persetujuan bagi orang yang bersangkutan, kecuali ditentukan lain oleh perundang – undangan;

l. Aspek peran Pemerintah dan masyarakat, Pemerintah memfasilitasi pemanfaatan informasi dan transaksi elektronik dengan memperhatikan ketentuan peraturan perundang-undangan yang berlaku;

m. Aspek perlindungan kepentingan umum, Pemerintah berwenang melindungi kepentingan umum dari segala jenis gangguan sebagai akibat penyalahgunaan informasi dan transaksi elektronik yang mengganggu ketertiban umum dan kepentingan nasional serta Pemerintah menetapkan instansi tertentu harus memiliki *back-up e-data* dan data *on-line* ; dan

n. Aspek perbuatan – perbuatan yang dilarang adalah:

(i) Menyebarkan informasi elektronik yang bermuatan pornografi, perjudian, tindak kekerasan, penipuan;

(ii) Menggunakan dan atau mengakses komputer dan atau sistem elektronik dengan cara apapun tanpa hak, dengan maksud untuk memperoleh, mengubah, merusak, atau menghilangkan informasi dalam komputer atau sistem elektronik;

(iii) Menggunakan dan atau mengakses komputer dan atau sistem elektronik dengan cara apapun tanpa hak, dengan maksud untuk memperoleh, mengubah, merusak, atau menghilangkan informasi dalam komputer atau sistem elektronik milik Pemerintah yang karena statusnya harus dirahasiakan atau dilindungi;

(iv) Menggunakan dan atau mengakses komputer dan atau sistem elektronik dengan cara apapun tanpa hak, dengan maksud untuk memperoleh, mengubah, merusak, atau menghilangkan informasi dalam komputer atau sistem elektronik menyangkut pertahanan nasional atau hubungan internasional yang dapat menyebabkan gangguan atau bahaya terhadap Negara dan atau hubungan dengan subjek hukum internasional;

(v) Melakukan tindakan yang secara tanpa hak yang transmisi dari program, informasi, kode atau perintah, komputer dan atau sistem elektronik yang dilindungi Negara menjadi rusak; dan

(vi) Menggunakan dan mengakses komputer dan atau sistem elektronik secara tanpa hak atau melampaui wewenangnya, baik dari dalam maupun luar negeri untuk memperoleh informasi dari komputer dan atau sistem elektronik yang dilindungi oleh Negara.

Prinsip utama dalam Hukum Teknologi Informasi adalah prinsip Yurisdiksi, hal dimaksud dikarenakan tidak serta merta dapat diterapkannya Yurisdiksi Teritorial dalam kegiatan di *cyberspace* yang sering kali terjadi dalam teritorial beberapa negara secara sekaligus. Pendekatan prinsip Yurisdiksi Ekstra-Terorial merupakan upaya untuk dimungkinkannya penerapan Hukum Teknologi Informasi.

Perihal yuridiksi dimuat di dalam Pasal 2 Undang - Undang No.11 Tahun 2008 sebagai berikut:

" Undang – undang ini berlaku untuk setiap Orang yang melakukan perbuatan hukum sebagaimana diatur dalam Undang – undang ini, baik yang berada di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia yang memiliki akibat hukum di wilayah hukum Indonesia dan/atau di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia."

Undang - Undang No.11 Tahun 2008 memiliki jangkauan yurisdiksi tidak semata – mata untuk perbuatan hukum yang berlaku di Indonesia dan/atau dilakukan oleh warga negara Indonesia, tetapi juga berlaku untuk perbuatan hukum yang dilakukan diluar wilayah hukum (yurisdiksi) Indonesia baik oleh warga negara Indonesia maupun warga negara asing atau badan hukum asing yang memiliki akibat hukum di Indonesia, mengingat pemanfaatan Teknologi Informasi untuk Informasi Elektronik dan Transaksi Elektronik dapat bersifat lintas teritorial atau universal.

Pemahaman dari pengertian "merugikan kepentingan Indonesia" adalah meliputi tetapi tidak terbatas pada merugikan kepentingan ekonomi nasional, perlindungan data strategis, harkat martabat bangsa, pertahanan dan keamanan negara, kedaulatan negara, warga negara, serta badan hukum Indonesia.[84]

Sedangkan asas – asas yang berlaku di dalam – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik berdasarkan Pasal 3, maka pemanfaatan Teknologi Informasi dan Transaksi Elektronik dilaksanakan berdasrkan asas kepastian hukum, manfaat, kehati-hatian, itikad baik dan kebebasan memilih teknologi atau netral teknologi.

Kehadiran Undang - Undang No.11 Tahun 2008 akan memberikan manfaat, beberapa diantara nya :

(i) Menjamin kepastian hukum bagi masyarakat yang melakukan transaksi secara elektronik

(ii) Mendorong pertumbuhan ekonomi indonesia

[84] Danrivanto Budhijanto, *Hukum Telekomunikasi, Penyiaran dan Teknologi Informasi:Regulasi dan Konvergensi.*(Bandung; Refika Aditama,2010) hlm. 136.

(iii) Sebagai salah satu upaya untuk mencegah terjadinya kejahatan berbasis teknologi informasi

(iv) Melindungi masyarakat pengguna jasa dengan memanfaatkan teknologi informasi

Dalam Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik ini secara rinci dijelaskan mengenai perbuatan – perbuatan yang dilarang atau segala perbuatan yang digolongkan tindak pidana kejahatan komputer diatur di Bab VII dalam Pasal 27 sampai dengan Pasal 37. Sedangkan di BAB IX yang terdiri atas Pasal 45 sampai dengan Pasal 52 menentukan kriminalisasi tehadap perbuatan - perbuatan yang dilarang atau segala perbuatan yang digolongkan tindak pidana komputer.

Materi muatan dari Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik adalah menyangkut masalah yurisdiksi, perlindungan hak pribadi, asas perdagangan secara *e-commerce*, asas persaingan usaha tidak sehat dan perlindungan konsumen, asas hak atas kekayaan intelektual (HAKI) dan hukum Internasional serta asas *cybercrime*. Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik mengkaji *cyber case* dalam beberapa sudut pandang secara komprehensif dan specifik, fokusya adalah semua kegiatan yang dilakukan dalam dunia maya, kemudian ditentukan pendekatan mana yang paling cocok untuk regulasi Hukum *Cyber* di Indonesia.

Kembali lagi ke fokus utama regulasi dari Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang dititikberatkan kepada memberikan kepastian hukum di kalangan pengguna teknologi dan informasi. Seharusnya Undang – Undang No. 11 Tahun 2008 agar dapat berjalan dengan baik dibuat sejumlah Peraturan Pemerintah yang dapat menjadi pengatur pelaksana yang diamanatkan oleh undang – undang. Paling tidak ada sembilan Peraturan Pemerintah yang seharusnya dibuat untuk dibentuk dalam waktu kurun dua tahun setelah Undang – Undang No. 11 Tahun 2008 disahkan.

Peraturan Pemerintah tersebut adalah :

A. Lembaga Sertifikasi Keandalan (Pasal 10 ayat (2))

B. Tanda Tangan Elektronik (Pasal 11 ayat (2))

C. Penyelenggara Sertifikasi Elektronik (Pasal 13 ayat (6))
D. Penyelenggaraan Sistem Elektronik (Pasal 16 (2))
E. Penyelenggara Agen Elektronik (Pasal 22 ayat (2))
F. Pengelolaan Nama Domain (Pasal 24 ayat (4))
G. Tata Cara Intersepsi (Pasal 31 ayat (4))
H. Peran Pemerintah tentang Pemanfaatan Teknologi Informasi dan Transaksi Elektronik (Pasal 40 (6))[85]

Sejumlah Peraturan Pemerintah tersebut seharusnya ditetapkan paling lambat dua tahun setelah diundangkannya Undang – Undang No.11 Tahun 2008 yaitu pada tanggal 21 April 2008, tetapi sampai saat ini belum ada satupun Peraturan Pemerintah dibuat sebagai mana yang dimaksud. Mengingat teknis prosedur pembuatan Peraturan Pemerintah yang memakan waktu yang tidak sebentar, ditambah urgensi waktu yang semakin pendek maka Kementrian dan Informatika sedang mengupayakan untuk menggabungkan beberapa Peraturan Pemerintah yang diamanatkan tersebut menjadi tiga, yaitu Rancangan Peraturan Pemerintah tentang Penyelenggaraan Informasi Transaksi Elektronik, Rancangan Peraturan Pemerintah Tata Cara Intersepsi *(Lawful Interception)* dan Rancangan Peraturan Pemerintah tentang Perlindungan Data Strategis.

Di tahun yang sama, Tahun 2008 Pemerintah juga mengeluarkan diantaranya dua undang – undang yang masih berhubungan dengan tindak pidana komputer yaitu Undang – Undang No. 14 Tahun 2008 tentang Keterbukaan Informasi Publik dan Undang – Undang No. 44 Tahun 2008 tentang Pornografi.

Undang – Undang No. 14 Tahun 2008 dikeluarkan dan disahkan pada tanggal 30 April 2008. Di dalam Undang – Undang No. 14 Tahun 2008 dibahas pengertian informasi, informasi disini mencakup informasi secara elektronis yang salah media penyebarannya melalui dunia maya. Informasi disini diartikan adalah keterangan, pernyataan, gagasan, dan tanda – tanda yang mengandung nilai, makna, dan pesan, baik data, fakta maupun penjelasannya yang dapat dilihat, didengar, dan dibaca yang disajikan dalam berbagai kemasan dan format sesuai dengan perkembangan teknologi informasi dan komunikasi secara elektronik

[85] Raida L. Tobing, *Op.Cit*., hlm.4.

ataupun non elektronik. Hal ini terdapat dalam Pasal 1 angka 1 Undang – Undang No. 14 Tahun 2008.[86]

Di dalam Undang – Undang No. 14 Tahun 2008 terdapat ketentuan yang dapat dilihat sebagai suatu tindak pidana komputer. Hal ini berlaku apabila sebuah informasi publik disebarkan melalui publik disebarkan melalui dunia maya. Pasal pasal tersebut adalah : [87]

Pasal 54 :

(1) Setiap Orang yang dengan sengaja dan tanpa hak mengakses dan/atau memperoleh dan/atau memberikan informasi yang dikecualikan sebagaimana diatur dalam Pasal 17 huruf a, huruf b, huruf d, huruf f, huruf g, huruf h, huruf i, dan huruf j dipidana dengan pidana penjara paling lama 2 (dua) tahun dan pidana denda paling banyak Rp.10.000.000 (sepuluh juta rupiah).

(2) Setiap Orang yang dengan sengaja dan tanpa hak mengakses dan/atau memperoleh dan/atau memberikan informasi yang dikecualikan sebagaimana diatur dalam Pasal 17 hurufc dan huruf e, dipidana dengan pidana penjara paling lama 3 (tiga) tahun dan pidana denda paling banyak Rp. 20.000.000 (dua puluh juta rupiah).

Pasal 55 :

Setiap Orang yang dengan sengaja membuat Informasi Publik yang tidak benar atau menyesatkan dan mengakibatkan kerugian bagi orang lain dipidana dengan pidana penjara paling lama 1 (satu) tahun dan/atau denda paling banyak Rp.5.000.000 (lima juta rupiah).[88]

Dalam pasal – pasal ini jika jika dikaitkan dengan jenis – jenis tindak pidana siber menurut Undang – Undang No. 11 Tahun 2008 maka terdapat dua perbuatan yaitu, pertama yang terdapat dalam Pasal 54 Undang – Undang No. 14 Tahun 2008 tentang Keterbukaan Informasi Publik yang melarang setiap orang

---

[86] Indonesia , *Undang – Undang No.14 Tahun 2008 tentang Keterbukaan Informasi Publik*, LN Tahun 2008.

[87] Ibid., Pasal 54.

[88] Ibid.,Pasal 55

yang tanpa hak mengakses informasi publik yang tidak aeharusnya dia peroleh juga diatur dalam pasal 32 ayat (2) yang mengatur larangan memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik orang lain yang tidak berhak. Sedangkan perbuatan yang kedua yang termasuk tindak pidana komputer adalah yang diatur dalam Pasal 55 yang melarang setiap orang untuk membuat sebuah informasi publik yang tidak benar dengan cara apapun diatur dalam Pasal 28 ayat (1) Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yaitu larangan melakukan perbuatan menyebarkan berita bohong dan penyesatan dengan menggunakan sistem komputer.

Setelah Undang – Undang No. 14 Tahun 2008, diundangkannya Undang – Undang No. 44 Tahun 2008 tentang Pornografi. Undang – Undang No. 44 Tahun 2008 diundangkan dan disahkan pada tanggal 26 November 2008 terdiri dari VIII Bab dan 45 Pasal. Undang – Undang No. 44 diundangkan karena Pemerintah melihat globalisasi, perkembangan ilmu pengetahuan dan teknologi, khususnya teknologi informasi dan komunikasi telah berkembang secara pesat serta mengambil andil terhadap meningkatnya pembuatan, penyebarluasan, dan penggunaan pornografi yang memberikan pengaruh buruk terhadap moral dan kepribadian luhur bangsa Indonesia. [89]

Oleh karena hal tersebut, Undang – Undang No. 44 Tahun 2008 tentang Pornografi mengakomodir keterlibatan Informasi dan Transaksi Elektronik terkait dengan pembuatan, penyebarluasan, dan penggunaan pornografi. Pasal – pasal tersebut adalah:

Pasal 1:

(3) *Segala jenis layanan pornografi yang disediakan oleh orang perseorangan atau korporasi melalui pertunjukan langsung, televisi kabel, televisi teresterial,radio, telepon, internet dan komunikasi elektronik lainnya serta surat kabar, majalah, dan barang cetak lainnya.* Secara gak langsung Pasal ini menjelaskan tentang Jasa Pornografi.

[89] Indonesia , *Penjelasan Undang – Undang tentang Pornografi* , UU No. 44 Tahun 2008, LN Tahun 2008.

Pasal 18 :

(a) Melakukan pemutusan jaringan pembuatan dan penyebarluasan produk pornografi atau jasa pornografi, termasuk pemblokiran pornografi melalui internet;

Pasal 19 :

(a) Melakukan pemutusan jaringan pembuatan dan penyebarluasan produk pornografi atau jasa pornografi, termasuk pemblokiran pornografi melalui internet di wilayahnya;

Pasal 24 :

Di samping alat bukti sebagaimana diatur dalam Undang-Undang tentang Hukum Acara Pidana, termasuk juga alat bukti dalam perkara tindak pidana meliputi tetapi tidak terbatas pada:

(a). barang yang memuat tulisan atau gambar dalam bentuk cetakan atau bukan cetakan, baik elektronik, optik, maupun bentuk penyimpanan data lainnya; dan

(b). data yang tersimpan dalam jaringan internet dan saluran komunikasi lainnya.[90]

Pasal 25 :

(1) Untuk kepentingan penyidikan, penyidik berwenang membuka akses, memeriksa, dan membuat salinan data elektronik yang tersimpan dalam fail komputer, jaringan internet, media optik, serta bentuk penyimpanan data elektronik lainnya.

(2) Untuk kepentingan penyidikan, pemilik data, penyimpan data, atau penyedia jasa layanan elektronik berkewajiban menyerahkan dan/atau membuka data elektronik yang diminta penyidik.

(3) Pemilik data, penyimpan data, atau penyedia jasa layanan elektronik setelah menyerahkan dan/atau membuka data elektronik sebagaimana

[90] Ibid., Pasal 1, Pasal 18, Pasal 19, Pasal 24.

dimaksud pada ayat (2) berhak menerima tanda terima penyerahan atau berita acara pembukaan data elektronik dari penyidik.

Pasal 26 :

Penyidik membuat berita acara tentang tindakan sebagaimana dimaksud dalam Pasal 25 dan mengirim turunan berita acara tersebut kepada pemilik data, penyimpan data, atau penyedia jasa layanan komunikasi di tempat data tersebut didapatkan.[91]

Pasal 27 :

(1) Data elektronik yang ada hubungannya dengan perkara yang sedang diperiksa dilampirkan dalam berkas perkara.

(2) Data elektronik yang ada hubungannya dengan perkara yang sedang diperiksa dapat dimusnahkan atau dihapus.

(3) Penyidik, penuntut umum, dan para pejabat pada semua tingkat pemeriksaan dalam proses peradilan wajib merahasiakan dengan sungguh-sungguh atas kekuatan sumpah jabatan, baik isi maupun informasi data elektronik yang dimusnahkan atau dihapus.

Pasal 28 :

(1) Pemusnahan dilakukan terhadap produk pornografi hasil perampasan.

(2) Pemusnahan produk pornografi sebagaimana dimaksud pada ayat (1) dilakukan oleh penuntut umum dengan membuat berita acara yang sekurang-kurangnya memuat:

(3) nama media cetak dan/atau media elektronik yang menyebarluaskan pornografi;

a. b. nama, jenis, dan jumlah barang yang dimusnahkan;

b. hari, tanggal, bulan, dan tahun pemusnahan; dan

c. keterangan mengenai pemilik atau yang menguasai barang yang dimusnahkan.[92]

---

[91] Ibid., Pasal 25, Pasal 26 dan Pasal 27.

[92] Ibid., Pasal 28.

Dalam pasal – pasal di atas jika dikaitkan dengan jenis – jenis tindak pidana siber menurut Undang – Undang No.11 Tahun 2008 terdapat di dalam Pasal 27 ayat (1) yang mengatur ponografi pada umumnya yaitu larangan melakukan pebuatan yang bermuatan melanggar kesusilaan. Di dalam Penjelasan Pasal 27 ayat (1) Undang – Undang No.11 Tahun 2008 sama sekali tidak ada penjelasan mengenai apa yang dimaksudkan dengan " kesusilaan". Dengan tidak adanya pengertian yang jelas apakah pengertian "kesusilaan" dimaksudkan sama dengan pengertian pornografi oleh pembuat undang – undang.[93]

Selain dua perundang – undangan diatas, pada tahun 2010 diundangkanya Undang – Undang No.8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang. Di didalam undang – undang ini juga mengatur alat bukti yang sah dalam kasus tindak pidana pencucian uang yang diatur didalam pasal 73 yang berbunyi :

Alat bukti yang sah dalam pembuktian tindak pidana Pencucian Uang ialah :

a.alat bukti sebagaimana dimaksud dalam Hukum Acara Pidana; dan/atau
b.alat bukti lain berupa informasi yang diucapkan,dikirimkan,diterima,atau dsimpan secara elektronik dengan alat optik atau alat yang serupa optik dan Dokumen.

Bab ini telah memberikan gambaran kepada kita tentang Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan beberapa Undang – Undang yang diundangkan setelah Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang berkaitan dengan tindak pidana siber.

Dari penulisan di atas dapat disimpulkan bahwa Indonesia telah memiliki kebijakan yang berhubungan dengan hukum Teknologi Informasi setelah diundangkannya Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik pada tanggal 21 April 2008. Produk hukum yang baru ini dibuat sedemikian rupa berkaitan dengan hal cyberspace atau dunia maya ini dianggap sangat penting oleh pemerintah untuk memberikan

[93] Sutan Remy Syahdeini, *Op.Cit*., hlm 227.

keamanan dan kepastian hukum dalam lingkup pemanfaatan teknologi informasi, media, dan komunikasi agar dapat berkembang secara optimal.

BAB III
TINDAK PIDANA SIBER

3.1 Jenis – Jenis Tindak pidana siber Secara Umum

Seperti pengertiannya, jenis – jenis tindak pidana siber secara umum banyak sekali dan berbeda – beda karena pandangan setiap ahli hukum memiliki pandangan masing – masing selain itu juga belum ada kesepakatan yang seragam mengenai pengertian tindak pidana siber itu sendiri sehingga membuat terjadinya perbedaan. Banyak jenis kejahatan komputer yang telah berkembang secara pesat sejak diperkenalkannya Internet berkaitan dengan pengembangan dan perkembangan teknologi informasi. Perkembangan dari waktu ke waktu jenis – jenis tindak pidana siber bermunculan dengan upaya pembentukan undang – undang untuk mengkriminalisasi kejahatan – kejahatan baru tersebut menjadi tindak pidana. Disetiap negara berbeda- beda dalam mengatur tindak pidana siber. Berikut ini jenis – jenis tindak pidana siber secara umum adalah :

3.1.1 Kejahatan Terhadap Harta Kekayaan

Banyak jenis kejahatan komputer yang telah muncul sejak diperkenalkannya Internet berkaitan dengan pengembangan dan perkembangan teknologi informasi. Dari waktu ke waktu jenis – jenis kejahatan komputer bermunculan dan berpacu dengan upaya pembentuk undang – undang untuk menkriminalisasi kejahatan – kejahatan baru tersebut menjadi tindak pidana.

(1) Cybersquatting

Domain name[94] adalah aset yang sangat berharga karena dapat diperjual-belikan, disewa, dapat menjadi situs pemasangan iklan sehingga menjadi sumber keuangan, bahkan dapat dijaminkan, maka para penjahat melihat peluang untuk menjadikan *domain name* sebagai objek perdagangan, yaitu dengan melakukan *cybersquatting. Cybersquatting* adalah perbuatan yang dilakukan oleh seorang spekulator untuk mendaftarkan suatu *domain*

[94] *Domain name* adalah nama dari suatu website di dalam jaringan Internet. *Domain name* merupakan kombinasi dari huruf – huruf dan angka – angka yang mengidentifikasi *website* tertentu pada Internet.

name mendahului pihak lain, yaitu pihak yang sesungguhnya akan menggunakan *domain name* tersebut.[95]

Tujuan pelaku mendahului mendaftarkan *domain name* tersebut adalah untuk ditawarkan kepada pihak yang sesungguhnya akan menggunakan *domain name* tersebut adalah untuk ditawarkan kepada pihak yang sesungguhnya akan menggunakan *domain name* tersebut dengan memperoleh keuntungan besar. Pelaku *cybersquatting* disebut *cybersquatter.* Pada kejahatan *cybersquatting,* pendaftaran *domain name* dilakukan dengan menggunakan nama orang apabila korbannya adalah seorang tokoh ternama yang di era Internet ini tentunya perlu memiliki website pribadi. Tokoh – tokoh terkenal itu misalnya tokoh politik dan para selebritis seperti bintang film, apabila korbanya adalah perusahaan, yang digunakan adalah nama perusahaan atau *trademark* atau *service merk* perusahaan tersebut.[96]

Sejak internet menjadi sumber marketing yang sangat penting dipertengahan Tahun 1990-an, muncul berbagai sengketa mengenai pendaftaran – pendaftaran *domain name*.[97] Sengketa tersebut dapat terjadi antar perusahaan yang terkait dengan nama yang sama atau serupa dengan *domain name* tersebut di berbagai sektor industri atau antar negara. Sengketa tersebut banyak terjadi antara para pemilik asli dari nama – nama terkenal atau merek – merek dagang yang telah terlebih dahulu didaftarkan oleh para spekulator. Tujuan dari para spekulator adalah untuk menjual *domain name* tersebut kepada para pemilik asli nama – nama yang telah dipakai dalam *domain name* tersebut.[98]

Oleh karena perusahaan pendaftar penerima permohonan pendaftaran nama tersebut berdasarkan asas "siapa duluan dia yang akan dilayani terlebih dahulu" (*on first come, first served basis*), maka dimungkinkan bagi pendaftar untuk mencuri start terlebih dahulu mendaftarkan nama perusahaan-perusahaan maupun tokoh-tokoh tersebut. Inilah awal mula terjadinya tindak pidana komputer menyangkut perihal *domain name* yang disebut dengan

[95] Ibid.,hlm 49.
[96] Ibid.,hlm 50.
[97] IP/IT-Update. *Domain Names,* http://www.ipit-update.com/dns.htm.
[98] Sutan Remy Syahdeini, *Op.Cit.*, hlm 52.

cybersquatting. Hal yang paling penting dengan pendaftaran *domain name* adalah kecepatan. Artinya secepatnya mendaftarkan *domain name* yang memuat nama ada *trademark* atau *service mark* perusahaannya sebelum orang lain melakukannya.[99]

Salah satu contoh kasus yang terkenal ada kasus Microsoft Corporation. *Domain name* www.microsoft.org telah didaftarkan oleh Amit Mehtora jauh sebelum Microsoft Corporation bermaksud untuk mendaftarkan *domain name*-nya. Keterlambatan Microsoft Corporation bermaksud untuk mendaftarkan domain name yang mengandung namanya sendiri atau trademark-nya sebelum orang lain mendaftarkan nama tersebut mengakibatkan munculnya masalah hukum bagi Microsoft Coorporation. Sekalipun Microsoft Coorporation tidak dapat memakai www.microsoft.org sebagai *domain name*-nya berlakunya asas "*on first come, first served basis*" dalam pendaftaran domain name.[100]

(2) Pembajakan HAKI

Internet telah menimbulkan masalah baru dibidang Hak Atas Kekayaan Intelektual (HAKI). *Copyright, trademark, patent, trade secret,* dan *moral right* sangat terpengaruh oleh Internet. Internet memiliki beberapa karakteristik teknis yang membuat masalah – masalah HAKI tumbuh dengan subur.[101] Salah satu masalah yang timbul adalah berkaitan dengan pembajakan hak cipta.[102]

3.1.2 Kejahatan Menyangkut Identitas

Kejahatan – kejahatan komputer yang menyangkut identitas berupa pencurian identitas orang lain yang tersimpan secara *computerized*, yang apabila diketahui oleh orang lain maka dapat merugikan korban secara materil maupun immateri. Salah satu bentuk kejahatan tersebut adalah menggunakan identitas

[99] Ibid.,hlm 52.
[100] Ibid.,hlm 53
[101] George B. Delta & Jeffrey H. Matsuura, *Law Of The internet*. (Aspen Law & Business,2000). Page. 5
[102] Sutan Remy Syahdeini, *Op.Cit*., hlm 62

orang lain guna memalsukan kartu kredit dalam kejahatan yang disebut dengan *carding.*

(1) Phising atau Identity Theft

Phising merupakan salah satu bentuk dari kejahatan Internet yang disebut identity theft. *Phishing* adalah pengiriman e-mail palsu atau *spoofed e-mail* kepada seseorang atau suatu perusahaan atau suatu organisasi dengan menyatakan bahwa pengirim adalah suatu entitas bisnis yang sah. Pengiriman *e-mail* tersebut menampilkan e-mail itu dalam bentuk dan dengan isi seperti suatu *e-mail* yang bukan *e-mail* palsu. Penerima yang mengira bahwa *e-mail* yang diterimanya itu adalah *e-mail* yang bukan *e-mail* palsu akan menanggapi *e-mail* tersebut dengan mengunjungi *website* pengirim *e-mail* dan kemudian terpancing untuk mengungkapkan informasi mengenai diri dari penerima *e-mail* palsu tersebut, antara lain mengungkapkan password, nomor *credit card*, nomor *social security* dan nomor rekening bank sebagaimana yang diminta oleh pengirim *e-mail* dalam *e-mail* nya itu. *Website* tersebut sengaja dibuat untuk mencuri informasi pribadi korbannya.[103]

Pada umumnya *phising* memang dilakukan melalui email, tetapi ada pula yang dilakukan melalui sms pada *handphone*. Sekalipun banyak *e-mail* palsu tersebut tampil menyakinkan seperti yang asli, yaitu lengkap dengan logo perusahaan dan menampilkan *links* kepada *website* yang asli, tetapi banyak yang tampil sangat menggelikan karena dilakukan oleh seseorang yang bukan profesional. Hal itu tampak dari formatnya yang cenderung seperti asal – asalan, terjadinya kesalahan – kesalahan *grammar* dalam kalimat – kalimat yang ditulis, dan terjadinya kekeliruan *spelling* dari kata – kata yang digunakan.[104]

(2) Carding

Carding atau *credit card fraud* adalah suatu kejahatan kartu kredit, merupakan salah satu bentuk dari pencurian *(theft)* dan kecurangan *(fraud)* di dunia internet yang dilakukan oleh pelakunya dengan menggunakan kartu kredit *(credit card)* curian atau kartu kredit palsu yang dibuatnya sendiri.

---

[103] University of Bristol, *Phising,* http://www.bristol.ac.uk/is/computing/advice/security/protectyou/idtheft/phish.html,

[104] Ibid.,

Tujuannya tentu saja adalah untuk membeli barang secara tidak sah atas beban rekening dari pemilik kartu kredit yang sebenarnya atau untuk menarik dana secara tidak sah dari suatu rekening bank milik orang lain.[105]

Modus operasi dari *Carding* ini adalah :

a. Dengan mencuri kartu kredit atau *credit card;*
b. Dengan menanamkan *spyware parasites;*
c. *Spyware parasites* ini dapat melakukan pencurisn identitas (identity theft) dan dapat menelusuri nomor-nomor kartu kredit ketika seorang pemegang kartu kredit menggunakan kartu kreditnya untuk berbelanja secara *online;*
d. Seorang petugas toko *(merchant)* menyalin tanda tangan terima penjualan *(sale receipt)* dari barang yang dibeli oleh pelanggan dengan tujuan untuk dapat digunakan melakukan kejahatan dikemudian hari;
e. Dengan melakukan *skimming.*

Skimming merupakan suatu *hi-tech method*, yaitu si pelaku memperoleh informasi mengenai izin pribadi korban atau mengenai rekening korban dari kartu kredit, surat izin mengemudi (SIM), kartu tanda penduduk (KTP), atau paspor anda. Pelaku menggunakan suatu alat elektronik *(electronic device)* untuk informasi tersebut.[106]

3.1.3 Kejahatan Terhadap Privasi

Kejahatan terhadap privasi adalah kejahatan komputer terhadap privasi pihak lain. Korban yang dapat menjadi sasaran kejahatan ini dapat berupa seseorang, organisasi bukan badan hukum, badan hukum swasta antara lain yayasan, koperasi, perusahaan, partai politik yang berbadan hukum dan milik negara yang antara lain BUMN, bank sentral, lembaga – lembaga negara , pemerintah, lembaga swadaya masyarakat, komunitas masyarakat dan lain sebagainya.

(1) *Cyberstalking*

Seperti halnya dengan kejahatan – kejahatan komputer pada umunya, demikian juga definisi dari *cyberstalking* belum ada yang sudah diterima

[105] Sutan Remy Syahdeini, *Op.Cit.*, hlm 82.
[106] http://idtheft.about.com/od/methodsofthef1/p/Skimming.htm?p-1

secara universal. *Cyberstalking* berasal dari dua kata, yaitu "*cyber"* dan *"stalking"*. Arti *cyber* telah kita diketahui bersama sebelumnya. Arti yuridis dari *"stalking"* adalah:[107]

"*harass somebody persistently: to harass somebody criminally by persistent, inappropriate, and unwanted attention, e.g. by constantly following, telephoning, e-mailing, or writting to him or her."*

Gangguan baru dapat dikatakan *stalking* hanya apabila gangguan tersebut dilakukan terus- menerus atau tidak henti – hentinya dengan melakukan perbuatan – perbuatan yang tidak diinginkan oleh pihak pengganggu. Misalnya mengikuti, menelepon, mengirim *e-mail*, mengirim surat kepada seseorang terus-menerus tanpa henti dalam waktu berhari – hari lamanya. Sudah tentu isi dari telepon, isi *e-mail*, isi surat dari penganggu tersebut sangat tidak disukai oleh orang yang diganggu sehingga sangat menjengkelkan.[108]

Apabila *stalking* itu dilakukan dengan menggunakan Internet maka perbuatan *stalking* itu disebut *cybertalking*. *Cyberstalking* adakalanya disebut *cyberharassment,*kebanyakan orang menyebut dua kata itu dalam tindak pidana ini. Sedangkan pelaku kejahatanya disebut *cyberstalker*[109].

(2) *Cyberterrorism*

Dengan perkembangan teknologi informasi yang sangat pesat, terutama perkembangan Internet, telah muncul bentuk terorisme baru yang disebut dengan cyberterrorism. Dari istilah ini saja secara mudah dapat diduga bahwa terorisme tersebut pasti dilakukan dengan menggunakan program komputer sebagai sarananya.

Untuk melakukan *cyberterrorism*, pelaku *cyberterrorism* yang disebut *cyberterrorist*, harus terlebih dahulu mampu membobol sistem komputer pihak yang akan diteror. Dengan demikian, sebelum melakukan teror pelaku harus berhasil melakukan hacking terhadap sistem komputer pihak yang akan diteror. Dengan kata lain seorang *cyberterrorist* adalah *hacker* atau *cracker* yang dalam melakukan *hacking* bertujuan untuk melakukan teror.

---

[107] Sutan Remy Syahdeini, *Op.Cit*., hlm 93.
[108] Ibid.,hlm 94
[109] Wired Safety, *Cyberstalking and Harassment FAQ*, http://www.wiredsafety.org/cyberstalking_harassment/csh0.html.

Dengan munculnya terorisme melalui jaringan komputer atau menggunakan program komputer, maka terorisme dapat terjadi baik didunia nyata atau didunia virtual. *Cyberterrorism* adalah terorisme dengan menggunakan komputer atau melalui dunia virtual. Ternyata belum ada definisi mengenai terorisme itu sendiri yang disepakati secara global. Oleh karena itu belum pula terdapat kesepakatan mengenai apa yang disebut dengan *cyberterrorism*.[110]

3.1.4 Kejahatan Terhadap Sistem Komputer

Kejahatan yang dilakukan dengan memasuki ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. Biasanya pelaku kejahatan *(hacker)* melakukan dengan maksud sabotase ataupun pencurian informasi penting dan rahasia. Namun begitu, ada juga yang melakukannya hanya karena merasa tertantang untuk mencoba keahliannya menembus suatu sistem yang memiliki tingkat proteksi tinggi.

(1) Hacking and Cracking

Dalam dunia komputer, terdapat dua istilah yang semula berbeda artinya tetapi dalam perkembangannya menjadi dua istilah yang memiliki arti yang sama. Kedua istilah itu adalah *hacking* dan *cracking*. Hacking adalah perbuatan membobol sistem komputer. Tindak pidana didunia maya ini adalah melakukan perbuatan memasuki sistem komputer orang lain tanpa izin atau otoritasi dari pemiliknya. Pelaku *hacking* adalah *hacker.*[111]

Menurut Susan W. Brenner: [112] *"Hacking is gaining unauthorised access to a computer system and, as such is conceptually analogous to real-world tresspassing"*. Sementara itu yang dimaksudkan dengan cracking menurut Brenner adalah:[113] "*Gaining unathorised accsess to a computer system for the purpose of committing a crime "inside" the system, is conceptually analogues to burglary ".*

---

110 Gabriel Weimann, Cyberterrorism; How Real Is the Threat?. http://www.usip.org/pubs/specialreports/sr119.pdf.

111 Sutan Remy Syahdeini, *Op.Cit*., hlm.118

112 Susan W. Brenner. *" Cybercrime ; re-thingking crime control* strategies", sebagaimana dimua dalam Crime Online,Edited by Yvonne Jewkes, Milan Publishing,2007 page 13-14

113 Ibid., page 13-14

Apabila hal itu terjadi di dunia nyata, *cracking* sama dengan *burglary* atau pencurian. Menurut para *hacker*, tujuan *cracker* adalah membobol *secure system* dari komputer, sedangkan tujuan para *hacker* hanyalah untuk memperoleh pengetahuan tentang sistem – sistem komputer. Media massa telah menggunakan istilah *hacker* bagi orang – orang yang mengakses sistem – sistem komputer tanpa memperoleh otorisasi dengan tujuan untuk mencuri dan menyalahgunakan data yang tersimpan dalam sistem – sistem komputer tersebut, yaitu istilah *hacker* seharusnya disebut *cracker*, bukan *hacker*.[114]

3.1.5 Kejahatan Terhadap Ketertiban Umum

Merupakan kejahatan dengan memasukan data atau informasi ke Internet tentang sesuatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum. Sebagai contohnya, pemuatan suatu berita bohong atau fitnah yang akan menghancurkan martabat atau harga diri pihak lain, hal – hal yang berhubungan dengan pornografi atau pemuatan suatu informasi yang merupakan rahasia negara, agitasi dan propaganda untuk melawan pemerintahan yang sah dan sebagainya.

(1) Perjudian di Internet

Perjudian Internet *(Internet gambling, online gambling,* atau *cyberspace gambling)* ternyata merupakan merupakan industri yang berkembang sangat pesat kelahirannya. Perjudian Internet telah memusingkan perusahaan – perusahaan penerbit kartu kredit berkenaan dengan penggunaan kartu kredit oleh para penjudian.

Para penegak hukum mengemukakan bahwa perjudian di Internet dapat digunakan untuk melakukan pencucian uang. Para penegak hukum mengemukakan bahwa masalah – masalah anonimitas *(anonymity)* dan yurisdiksional *(jurisdictional)* yang merupakan ciri dari perjudian Internet merupakan sarana yang sangat menguntungkan bagi para pencuci uang.[115]

(2) Pornografi Anak di Internet

---

114 Webopedia, Hacker, http://www.webopedia.com/TERM/h/hacker.html.

115 U.S Government Accountability Office, *internet Gambling, An Overview of the Issues*, Dec 2002, http://www.gao.gov/new.items/d0389.pdf.

Pornografi anak atau *child pornography* atau *child porn* adalah bahan – bahan porno yang menampilkan anak – anak. Kebanyakan negara menyebutkan hal ini dengan sebagai bentuk dari *child sexual abuse* dan merupakan hal yang melanggar hukum. Dimana child pornography berupa foto- foto yang menampilkan anak – anak yang terlibat dalam perilaku seksual dan memproduksi bahan – bahan tersebut dengan sendirinya dilarang hukum sebagai child sexual abuse di kebanyakan negara.

Perkembangan dan meningkatnya akses kepada Internet, serta penggunaan teknologi *home – computer* telah mengubah besar – besaran cara distribusi gambar – gambar porno ini karena mudahnya melakukan akses kepada Internet dan makin murahnya biaya produksi dan distribusi gambar – gambar tersebut terutama secara lintas batas negara. Teknologi komputer telah mentransformasikan produksi dari gambar – gambar ini ke dalam suatu industri global yang canggih.[116]

3.2 Jenis – Jenis Pengaturan Tindak pidana siber di dalam perundang - undangan.

Instrumen – Instrumen hukum Internasional dibidang tindak pidana siber ini merupakan sebuah fenomena baru dalam tatanan hukum internasional modern. Sebelumnya, masalah tindak pidana siber mendapatkan perhatian yang memadai dari negara – negara sebagai subjek hukum internasional. Munculnya kejahatan baru yang tidak hanya bersifat lintas batas negara (*bordeless*, transnasional) tetapi juga terwujud dalam tindakan – tindakan virtual ini telah menyadarkan masyarakat internasional bahwa memang diperlukan perangkat hukum internasional yang baru yang dapat digunakan sebagai kaidah hukum internasional untuk mengatasi kasus – kasus tindak pidana siber.[117]

Di dalam perkembangan di antar negara tindak pidana siber mengakibatkan setiap negara memiliki kebijakan kriminalisasi yang berbeda – beda. Sifat tindak pidana siber yang berkarakter lintas negara telah menjadikan tindak pidana siber tidak saja merupakan persoalan nasional namun sudah menjadi

[116] National Centre For Missing & Exploited Children, *What Is Child Pornography?*, http://www.missingkids.com/missingkids/servlet/PageServlet?PageId=1504.
[117] Arsyad Sanusi, *Cybercrime*, (Jakarta: Milestone Publisher, 2011), hlm 267

persoalan international. Hal ini terlihat dari rekomendasi yang dikeluarkan oleh PBB melalui kongresnya atau juga *Council Of Europe*.[118]

Penanggulangan tindak pidana siber dengan demikian juga menjadi persoalan negara – negara di dunia. Pengaturannya juga berbeda – beda di setiap negara.

3.2.1 *United Nations Convention Againt Transnational Organized Crime* atau Konvensi Palermo

United Nations Convention Againt Transnasional Organized Crime atau Konvensi Palermo diselenggarakan pada tahun 2000. Dalam Konvensi Palermo ini ditetapkan beberapa jenis kejahatan yang termasuk dalam kejahatan transnasional, yaitu : Kejahatan Narkotika, Kejahatan Genosida, Kejahatan Uang Palsu,Kejahatan di luas bebas, dan *Cybercrime*.

Ini berarti bahwa tindak pidana siber dalam *United Nations Convention Againt Transnasional Organized Crime* atau Konvensi Palermo ini dipandang sebagai bagian dari bentuk kejahatan transnasional. Sehingga bangsa – bangsa atau negara – negara di dunia harus mematuhi konvensi ini guna menjamin hubungan yang lebih baik dengan bangsa – bangsa di dunia. Tujuan dari Konvensi Palermo dirumuskan dalam Pasal 1 Konvensi, sebagai berikut: "Tujuan dari konvensi palermo adalah untuk meningkatkan kerjasama dengan semua negara di dunia guna memerangi kejahatan transnasional yang terorganisir".[119]

Konvensi ini diselenggarakan di tengah – tengah situasi semakin merebaknya kejahatan transnasional, antara lain tindak pidana siber yang sudah merambah ke semua dunia dan bersifat meresahkan. Pasal 2 Huruf (c) Konvensi Palermo mengisyaratkan bahwa *cybercrime* merupakan kejahatan yang serius sehingga ancaman hukuman minimalnya adalah 4 tahun penjara atau lebih. Hal ini berarti bahwa pelaku kejahatan transnasional yang terkait dengan *cybercrime* akan mendapat ancaman hukuman minimal 4 tahun penjara.[120]

Disamping menegaskan ancaman hukuman pidana bagi pelaku *cybercrime*, Konvensi Palermo juga mengajak dunia internasional untuk bersama

[118] Ibid.,hlm 267
[119] Ibid.,hlm 268
[120] Ibid.,hlm 268

– sama memerangi *cybercrime* dengan menghimbau negara – negara di dunia untuk membuat perangkat hukum yang mengatur tentang masalah *cybercrime* serta mengadopsi prinsip – prinsip hukum Konvensi Palermo yang disesuaikan dengan prinsip – prinsip hukum domestik masing – masing negara. Artinya, setiap negara diminta untuk membuat hukum yang mengatur tentang penegakan *cybercrime* sebagai bukti keseriusan untuk melaksanakan kaidah – kaidah Konvensi Palermo.

Konvensi ini dimaksudkan untuk semakin terjaminnya keamanan internasional dalam mengahdapi kejahatan transnasional melalui upaya kerjasama internasional. Sebagaimana ditegaskan dalam Pasal 27 ayat 1, sebagai berikut ini :

"Negara – negara akan bekerjasama erat satu sama lain sesuai dengan prinsip – prinsip hukum dan administrasi masing – masing negara guna meningkatkan efektivitas penegakan hukum dalam memerangi tindak pelanggaran sebagaimana tercakup dalam Konvensi dan tiap – tiap negara wajib nengadopsi langkah – langkah efektif tersebut "

Bentuk kerjasama internasional yang dimaksud oleh Konvensi Palermo ini dapat berupa pembentukan suatu organisasi atau secara bersama – sama merespon setiap informasi mengenai tindak kejahatan *cybercrime*. Secara lebih terperinci, bentuk – bentuk implementasi dari Konvensi Palermo dituangkan dalam Pasal 34 yaitu :

a. Setiap negara harus mengambil langkah – langkah yang di perlukan termasuk upaya – upaya legislasi dan tindakan – tindakan administratif sesuai dengan prinsip – prinsip dan hukum domestik untuk menjamin terlaksananya kewajiban – kewajiban sebagaimana dimaksud dalam Konvensi ini;
b. Terhadap pelanggaran – pelanggaran sebagaimana dimaksud dalam Pasal 5,6,8 dan 23 Konvensi ini, baik yang dilakukan oleh pribadi – pribadi maupun kelompok harus dilakukan upaya – upaya transnasional;
c. Setiap negara harus mengadopsi Konvensi ini.

Ketentuan Pasal 34 Konvensi Palermo inilah yang menjadi dasar dibentuknya aturan – aturan hukum yang mengaturnya upaya menanggulangi kejahatan transnasional, dalam hal ini *cybercrime*.[121]

3.2.2 Convention On Cybercrime.

Pada tanggal 23 November 2001 *EU Convetion on Cybercrime* di Budapest, adalah konvensi sebagai sumber hukum *cybercrime* international. Sekitar 30 negara sepakat untuk menandatangani *Convention on Cybercrime*. Konvensi ini merupakan kerjasama multilateral yang diadakan guna menanggulangi penyebaran aktivitas kriminal melalui internet dan jaringan komputer lainnya. Melalui kerjasama ini diharapkan dapat menggugah masyarakat internasional untuk ikut berpartisipasi dalam penanggulangan kejahatan berteknologi tinggi.[122]

Konvensi Budapest tentang *cybercrime* ini juga merupakan perjanjian internasional pertama yang berupaya mencari penyelesaian masalah kejahatan komputer dan kejahatan internet melalui upaya harmonisasi hukum nasional, peningkatan tehnik – tehnik investigasi serta peningkatan kerjasama antar bangsa. Konvensi ini dipelopori dan dirancang oleh Dewan Eropa di Strasburg dengan melibatkan partisipasi aktif dari negara – negara pengama seperti Kanada, Jepang dan Cina.[123]

Pada tanggal 1 Maret 2006, Protokol Tambahan Konvensi *Cybercrime* mulai berlaku. Negara – Negara yang telah meratifikasi protokol tambahan ini didorong tambahan ini didorong untuk mengkriminalisasi penyebarluasan materi – materi yang bersifat rasis dan yang dapat menyebarkan *xenophobia* melalui sistem komputer, atau ancaman dan penghinaan yang dimotivasi oleh rasisme dan *xenophobia*.[124]

Konvensi Budapest ini juga merupakan perjanjian internasional pertama mengenai kejahatan yang dilakukan melalui internet dan jaringan komputer lainnya, terutama yang berhubungan dengan pelanggaran hak cipta, penipuan

[121] Ibid., hlm 270.
[122] Ibid., hlm 270.
[123] Ibid., hlm 270.
[124] Ibid., hlm 271.

yang berhubungan dengan komputer, pornografi anak dan pelanggaran keamanan jaringan.[125]

Subtansi Konvensi *Budafest* ini mencakup area yang cukup luas bahkan mencakup pula kebijakan pemidanaan (*criminalization policy*) yang bertujuan melindungi masyarakat dari bahaya *cybercrime* baik melalui undang – undang maupun kerjasama internasional.

Tujuan utama konvensi ini, sebagaimana ditetapkan dalam bagian pembukaan, adalah untuk mengupayakan terwujudnya kebijakan pidana bersama yang bertujuan untuk melindungi masyarakat dari ancaman *cybercrime*, khususnya melalui pengadopsian peraturan perundangan – undangan yang sesuai dan memajukan kerjasama internasional. Tujuan utama Konvensi ini adalah untuk:

a. Mengharmonisasikan materi – materi hukum domestik mengenai pelanggaran – pelanggaran yang terkait dengan cybercrime dan mengharmonisasikan ketentuan – ketentuan hukum dalam bidang cybercrime
b. Memberikan kekuatan yang dibutuhkan oleh hukum acara pidana nasional negara – negara bagi terlaksanannya penyelidikan dan penuturan terhadap pelanggaran – pelanggaran cybercrime maupun pelanggaran – pelanggaran lainnya yang dilakukan dengan menggunakan saran sistem komputer atau yang terkait dengan bukti bukti elektronik;
c. Membentuk rezim kerjasama internasional yang cepat dan efektif[126]

Menurut *Convention on Cybercrime* tindak pidana siber diatur di dalam *Chapter II,* Konvensi ini terbagi dalam dua kategori dasar yaitu *cybercrime* dalam arti sempit dan *cybercrime* dalam arti luas. Adapun tindak pidana dalam arti sempit tersebut adalah:

a. Akses Ilegal

Dalam Bahasa Indonesia disebut dengan Akses Ilegal melingkupi pelanggaran dasar dari ancaman – ancaman yang berbahaya dari serangan

[125] Ibid., hlm 271.
[126] Ibid., hlm 271

terhadap keamanan data dan sistem komputer.[127] Perlindungan terhadap pelanggaran ini merupakan gambaran dari kepentingan organisasi atau kelompok dan orang – orang yang ingin mengatur, menjalankan dan mengendalikan sistem mereka berjalan tanpa adanya gangguan dan hambatan. *Illegal Access* diatur dalam Pasal 2 Konvensi ini yang berbunyi:

> *"Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system."*[128]

Pasal ini merupakan ketentuan pertama yang mengatur mengenai masalah cybercrime. Sebagai contoh dari kejahatan ini adalah *hacking, cracking atau computer trespassing.* Gangguan jenis ini memberikan akses kepada pelaku terhadap data-data penting (termasuk password atau informasi sistem) dan rahasia-rahasia, yang mungkin digunakan untuk membeli barang dengan menggunakan informasi kartu kredit milik orang lain atau mendorong pelaku untuk melakukan bentuk pelanggaran berkenaan dengan komputer yang lebih berbahaya, seperti pemalsuan atau penipuan dengan komputer.[129]

Pasal ini juga menyatakan bahwa masing- masing pihak harus memberlakukan perundang – undangan tersebut dan langkah – langkah lain yang mungkin diperlukan untuk menetapkan sebagai pelanggaran kriminal berdasarkan undang – undang domestiknya, apabila dilakukan secara sengaja, akses ke seluruh atau sebagian sistem komputer tanpa hak. Suatu pihak dapat mensyaratkan bahwa suatu pelanggaran dilakukan dengan melanggar langkah – langkah pengamanan, dengan tujuan untuk mendapatkan data komputer atau maksud tidak jujur lainnya, atau terkait dengan sistem komputer yang tersambung ke sistem komputer lainnya.

---

[127] Council of Europe, Explanatory Report To The Convention On Cybercrime (ETS No 185), poin ke 44.
[128] Convention On Cybercrime Pasal 2
[129] Mike Keyser, "*The Council of Europe Convention On Cybercrime"*, (Journal of Transnational Law and Policy, volume12, 2003) Page.300

Pemahaman mengenai access sebagaimana disebut dalam ketentuan pasal ini, terdiri dari memasuki seluruh atau sebagian dari suatu sistem komputer (hardware, bagian-bagian, data yang tersimpan pada sistem yang terpasang, direktori-direktori, lalu-lintas data-data dan data yang berkenaan dengan isi). Namun demikian akses yang dilakukan ini tidak termasuk di dalamnya dengan kegiatan mengirimkan email atau file ke sistem tersebut. Access yang dimaksud meliputi kegiatan memasuki sistem komputer lainnya baik yang terkoneksi melalui jaringan komunikasi umum, tatu terhadap suatu sistem komputer pada jaringan yang sama seperti pada suatu Local Area Network (LAN) atau intranet dalam suatu organisasi. Cara komunikasi yang dilakukan baik dari satu lokasi tertentu dengan cara remote maupun dengan penghubung wireless pada jarak yang dekat tidak masalah.[130]

Ketentuan pasal ini juga menerangkan mengenai pentingnya permasalahan tanpa hak yang harus ada pada suatu pelanggaran yang dilakukan . Bukanlah suatu pelanggaran pidana terhadap akses yang disetujui oleh pemilik atau pemegang hak dari suatu sistem atau bagian dari pemilik atau pemegang hak tersebut.[131] Kondisi ini dapat terjadi apabila dibutuhkan pengujian terhadap keamanan suatu sistem.

b. Penyadapan Ilegal

Penyadapan ilegal atau dalam bahasa inggrisnya Illegal interception diatur di dalam Pasal 3 *Convention on Cybercrime* yang berisi:

> "*Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system,including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system."*[132]

Berdasarkan pasal ini, masing – masing pihak harus memberlakukan perundang – undangan tersebut dan langkah lain yang mungkin diperlukan

[130] Council of Europe, .op cit., poin ke 46
[131] Council of Europe,.op cit., poin ke 47
[132] Convention On Cybercrime Op.Cit., Pasal 3

untuk menetapkan sebagai pelanggaran kriminal berdasarkan undang – undang domestiknya, apabila dilakukan secara sengaja, penyadapan tanpa hak, yang dilakukan secara teknis, atas tramisi – tramisi data komputer non-publik ke, dari atau, dalam suatu sistem komputer, termasuk sistem elektromagnetik dari sistem komputer yang membawa data komputer tersebut. Suatu pihak dapat mensyaratkan bahwa suatu pelanggaran dilakukan dengan maksud yang tidak jujur, atau terkait dengan sistem komputer yang tersambung ke sistem komputer lainnya.

Menyatakan tidak sah tindakan pencegatan atau menahan tanpa hak bentuk pemindahan data komputer yang dilakukan secara pribadi yang dilakukan melalui faximile, email, atau pemindahan file. Tujuan dari pasal ini adalah perlindungan atas hak atas kebebasan dalam komunikasi data. Pelanggaran ini hanya ditujukan terhadap pemindahan pribadi dari data komputer.

Pengertian *interception* secara teknis dijelaskan dala*m Explanatory Report To The Convention on Cybercrime* yaitu *;*

> *"Interception by techincal means relates to listening to, monitoring or surveillance of the content of communications, to the procuring of the content of data either directly, through access and use of the computer system, or undirectly through the use of electronic eavesdropping or taping devices.Interception may also involving recording."*[133]

Salah satu bagian dari pelanggaran yang dimaksud dari ketentuan pasal ini adalah melakukan penahanan komunikasi atau menghambat proses komunikasi dengan menggunakan perangkat elektronik untuk mendengarkan pembicaraan orang lain atau menggunakan peralatan untuk menyadap komunikasi. Klasifikasi ini hanya berlaku pada komunikasi data komputer yang dilakukan secara pribadi, klasifikasi ketentuan ini mengacu pada sifat pemindahan dan sifat dari data yang dipindahkan.

c. Gangguan Data

Konvensi mengatur mengenai *data interference* [134] yang berbunyi bahwa :

[133] Council of Europe,.op cit., poin ke 53
[134] Convention On Cybercrime Op.Cit. Art 4.

1. *Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.*
2. *A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.*

Ketentuan perusakan data menjadi tindak pidana bertujuan untuk memberikan perlindungan yang sama terhadap data komputer dan program komputer sebagaimana dengan benda-benda berwujud. Sebagai contoh adalah memasukan kode-kode jahat (malicous codes), Viruses, dan Trojan Horse ke suatu sistem komputer merupakan pelangagaran menurut ketentuan pasal ini.

Berdasarkan Pasal 4 ayat (1) *Convention on Cybercrime* merupakan tindak pidana apabila dilakukan dengan terencana tindakan merusak, menghapus, memperburuk, mengubah atau mengembangkan, suatu data komputer tanpa hak.[135] Ketentuan yang diatur dalam pasal ini berusaha untuk memberi jaminan bahwa data yang dikirimkan melaui jaringan internet atau pemindahan data yang dilakukan melaui suatu jaringan adalah sama dengan data yang dikirimkan oleh si pengirim. Kepentingan perlindungan hukum dalam pasal ini adalah keutuhan dan berfungsi sebagaimana mestinya penggunaan data komputer yang tersimpan atau program-program komputer.[136]

Kesimpulan dari pasal ini adalah masing – masing pihak harus memberlakukan perundang – undangan tersebut dan langkah langkah lain yang mungkin diperlukan untuk menetapkan sebagai pelanggaran kriminal berdasarkan undang – undang domestiknya, apabila dilakukan secara sengaja, penghancuran, penghapusan, perusakan, perubahan, *atau* penyembunyian data komputer tanpa hak. Suatu pihak menahan haknya mensyaratkan bahwa tindakan yang dijelaskan dalam ayat 1 berakibat kerugian serius.

d. Gangguan terhadap Sistem

System interfence[137] diatur dalam Pasal 5 Konvensi yang menyatakan bahwa :

[135] The Convention On Cybercrime
[136] Council of Europe,.op cit.Poin ke 60.
[137] The Convention On Cybercrime

"Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data."

Dalam Pasal 5 konvensi ini disebutkan bahwa *system interference* ditetapkan sebagai pelanggaran pidana apabila *"...when committed intentionally, the serious hindering without right of the functioning of a computer system..."*, harus dilakukan dengan memasukan, menyebarkan, merusak, menghapus atau menyembunyikan data komputer.[138] Pengganggguan terhadap sistem dijadikan sebagai tindak pidana bertujuan untuk mencegah "*...the serious hindering without right of the functioning of a computer system...."* . Sebagai contoh adalah serangan *denial-of-service* yang dilakukan dengan tehnik *hacking*, pembuatan kode jahat seperti virus. Contoh tersebut dapat memperlambat penggunaan sistem komputer yang mengakibatkan pengguna tidak dapat mengakses suatu *website.*

Jadi, menurut pasal ini, masing – masing pihak harus memperlakukan perundang – undangan tersebut dan langkah – langkah lain yang mungkin diperlukan untuk menetapkan sebagai pelanggaran kriminal berdasarkan undang – undang domestiknya, apabila dilakukan secara sengaja, penghalangan serius tanpa hak terhadap fungsi dari suatu sistem komputer dengan melakukan, input, transmisi, penghancuran, penghapusan, atau penyembunyian data komputer.[139]

Sedangkan *cybercrime* dalam arti luas, perbuatan yang terkait dengan komputer karena dilakukan dengan komputer, serta kejahatan yang terkait dengan pornografi anak, dan pelanggaran hak atas kekayaan intelektual.

Efektifitas dan efisiensi pelaksanaan Konvensi *Budafest* ini masih perlu dicari format yang tepat karena, lazimnya suatu konvensi internasional terbentur dalam pelaksanaannya. Salah satu unsur yang menjadi tantangan

[138] Council of Europe,.op cit.Poin 66

[139] Suharyo, S.H.,M.H, *Jurnal Tim Penelitian Hukum Tentang Penerapan Bantuan Timbal Balik Dalam Masalah Pidana Terhadap Kasus – Kasus Cybercrime*, (Jakarta : Badan Pembinaan Hukum Nasional Kementrian Hukum dan HAM RI,2010), hlm.38.

dalam penerapan Konvensi *Budafest* ini adalah perbedaan persepsi terhadap masalah yang bermuara dari perbedaan kepentingan pribadi dan pengalaman. Terlebih lagi, dalan konteks cybercrime ketiadaan batas dalam menanggulanginnya merupakan hal baru dslam sejarah penegakan hukum. Dengan kata lain, masalah kejahatan di dunia maya tetap akan menyita waktu banyak pihak untuk mendapatkan penyelelsaian yang tepat dikarenakan dampak burukknya telah menyebar secara luas ke berbagai lapisan negara dan masyarakat.[140]

Walaupun belum ada bentuk kerjasama internasional yang benar – benar efektif menghilangkan perilaku kejahatan di dunia maya, namun Konvensi Budafest ini merupakan satu landasan penting bagi adanya kerjasama – kerjasama lanjutan berkaitan dengan isu yang sama. Setidaknya, merebaknya fenomena *cybercrime* telah menyadarkan berkaitan dengan penguasaan teknologi komputer agar pandangan bahwa pelaku kejahatan *cyber* selalu selangkah lebih maju dapat ditumbangkan.[141]

Konvensi *Budafest* ini telah disepakati oleh Uni Eropa sebagai Konvensi yang terbuka untuk diakses oleh negara manapun di dunia. Hal ini berarti bahwa konvensi ini terbuka untuk dijadikan norma dan instrumen hukum internasional dalam mengatasi *cybercrime*, tanpa mengurangi kesempatan setiap individu anggota masyarakat untuk tetap mengembangkan kreatifitasnya dalam pengembangan teknologi informasi.[142]

3.2.3 Peraturan International Telecommunications Union (ITU)

International Telecommunications Union pada awalnya bernama International Telegraph Union yang didirikan di Paris pada tanggal 17 Mei 1865 yang pada saat itu bertujuan meningkatkan keselarasan dalam jaringan telegraf nasional dari masing – masing negara dan meliputi standardisasi pengalokasian spektrum radio dan mengorganisasikan perjanjian rangkaian interkoneksi antara negara – negara berbeda untuk memungkinkan panggilan telepon internasional.

[140] Arsyad Sanusi, *Cybercrime.,* op.cit.,hlm 272
[141] Ibid.,hlm.272
[142] Ibid.,hlm.272

Pada tahun 1947, International Telecommunication Union (ITU) kemudian menjadi organ khusus dari Perikatan Bangsa Bangsa, yang bermarkas di Jenewa, Switzeland, disamping gedung utama kampus PBB. Negara Republik Indonesia menjadi anggota ITU tidak lama setelah itu,yaitu semenjak pengakuan kedaulatan Indonesia tepatnya pada tanggal 1 Januari 1949 . Tujuan utama ITU adalah untuk meningkatkan hubungan kerjasama diantara negara – negara anggotanya dan untuk membantu perkembangan segala bentuk telekomunikasi dunia.

Sampai pada tahun 1980-an , sebagian besar anggota ITU adalah perwakilan atau administrasi dari pemerintah yang bertanggung jawab untuk pengoperasian telekomunikasi dan sekaligus regulator dalam bidang telekomunikasi di negara masing – masing. Mendasarkan adanya pemilahan fungsi operasional dan regulator dalam bidang telekomunikasi di negara masing – masing. Mendasarkan adanya pemilahan fungsi opeasional dan regulator serta liberalisasi yang berangsur – angsur di bidang telekomunikasi yang dilakukan oleh sejumlah besar negara – negara anggota ITU, menjadikan perubahan paradigma di dalam ITU. Sehingga situasi saat ini adalah sangat berbeda dari keadaan dimana ITU pada saat pertama kali didirikan. Mandat yang diberikan kepada ITU dalam rangka melaksanakan fungsinya sebagai berikut :

> "*While fully recognizing the sovereign right of each country to regulate its telecommunication and having regard to the growing importance of telecommunication for the preservation of peace and the social and economic development of all countries, the plenipotentiaries of the contracting governments, which the object of facilitating peaceful relations, international coorperation and economic and social develpoment among peoples by means of efficient telecommunication services, have agreed to establish this Convention which is the basic instrument of International Telecommunication Union."*[143]

Terjemahan bebas penulis :

"Sementara sepenuhnya mengakui hak kedaulatan setiap negara untuk mengatur telekomunikasi dan dengan memperhatikan semakin pentingnya telekomunikasi untuk pelestarian perdamaian dan pembangunan sosial dan ekonomi dari seluruh negara, plenipotentiaries dari pemerintah kontrak, dimana tujuan memfasilitasi hubungan damai, kerjasama internasional dan develpoment ekonomi dan sosial di antara masyarakat dengan cara yang efisien layanan telekomunikasi, telah sepakat

[143] Pembukaan International Telecommunication Convention, Nairobi 1982, yang berlaku semenjak tanggal 1 Januari 1984 (Pasal 52 International Telecommunication Convention ITU, Nairobi 1982)

untuk membentuk Konvensi ini yang merupakan instrumen dasar dari International Telecommunication Union. "

International Telecommunications Union terbagi tiga hal yaitu :

a. Radiocommunication Sector Bureu (ITU-R);

   Hal – hal yang berkaitan dengan radio maka tugas ini didelegasikan kepada *Radiocommunication Sector*/ITU-R yang dahulu dikenal dengan CCIR. ITU-R akan mendapatkan dari *World Radiocommunication Conference* (WCR) yang bersidang setiap dua tahun sekali untuk revisi – revisi atas ketentuan di dalam *Radio Regulation* ITU.

b. Telecommunication Standardization Bureu (ITU-T);

   Hal – hal yang berkaitan dengan standarisasi telekomunikasi, termasuk pula di dalamnya hal tentang interkoneksi dari sistem radio yang dipergunakan untuk telekomunikasi, didelegasikan kepada Telecommunications Standardidazation Sector/ITU-T yang dahulunya dikenal dengan CCITTA mendapatlan arahan World Telecomunications Standarization Conference yang bersidang setiap empat tahun sekali.

c. Telecommunication Development Bureu (ITU-D)

   ITU memberikan mandatnya kepada Telecomunication Development Sector/ ITU-D untuk membantu perkembangan telekomunikasi internasional. ITU-D mendapatkan pengarahan dari World Development Conference yang bersidang 4 tahun sekali.[144]

3.2.4 Peraturan di Indonesia

Pemanfaatan Informasi dan Teknologi Elektronik saat ini merupakan bagian sangat penting dari aktifitas masyarakat dan pemerintah. Ini terbukti makin meluasnya penggunaan Teknologi Informasi di berbagai sektor kehidupan seperti sektor perekonomian serta transaksi – transaksi lainnya, disamping untuk kepentingan untuk kepentingan riset ilmu pengetahuan dan pengembangan teknologi.

Beberapa terobosan penting yang dimiliki Undang - Undang No.11 Tahun 2008 antara lain : tanda tangan elektronik diakui memiliki kekuatan hukum sama

[144] Danrivanto.,Op.Cit,hlm.10

dengan tanda tangan konvesional (tinta basah dan materai) dan diakui bukti elektronik diakui seperti alat bukti lainnya yang diatur dalam KUHAP. Undang - Undang No.11 Tahun 2008 berlaku untuk tiap orang yang melakukan perbuatan hukum, baik berada di wilayah Indonesia maupun di luar Indonesia, yang memiliki akibat hukum di Indonesia, penyelesaian sengketa juga dapat diselesaikan dengan metode penyelesaian sengketa alternatif atau arbitrase.[145]

Dalam Undang - Undang No.11 Tahun 2008 dimuat ketentuan – ketentuan mengenai larangan melakukan perbuatan – perbuatan tertentu yang diancam dengan sanksi pidana bagi pelakunya. Tegasnya Undang - Undang No.11 Tahun 2008 menetapkan beberapa perbuatan yang dikriminalisasi sebagai tindak pidana di dalam dunia maya dengan sanksi – sanksi nya. Tindak pidana tersebut adalah ;

i. *Indecent Materials/Ilegal Content* (Konten Ilegal)

Setiap orang dengan sengaja dan tanpa hak mendistribusikan, mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan, perjudian, pencemaran nama baik serta pemerasan, pengancaman, serta menimbulkan rasa kebencian berdasarkan atas SARA serta yang berisi ancaman kekerasan. Hal ini terdapat di dalam Pasal 27,28 dan 29 Undang - Undang No.11 Tahun 2008.[146]

Tindak pidana di dalam dunia maya yang dimaksud Pasal di atas adalah pornografi, pornografi anak, penghinaan dan atau pencemaran nama baik, pemerasan dan atau pengancaman, penyebaran berita bohong dan penyesatan, penyebaran informasi yang bermuatan SARA, pengiriman informasi bermuatan ancaman kekerasan atau menakut – nakuti.

ii. *Illegal Access* (Akses Ilegal)

Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik orang lain dengan cara apapun untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik

[145] Buku Panduan Untuk Memahami UU No.11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik,Seputar UU. No 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE), www.depkominfo.go.id.
[146] Ibid.,hlm 8

serta melanggar,menerobos,melampaui atau menjebol sistem pengamanan. Hal ini terdapat dalam Pasal 30 Undang - Undang No.11 Tahun 2008.[147] Tindak pidana di dalam dunia maya yang dimaksud Pasal di atas adalah Pembobolan Komputer dan/atau Sistem Elektronik.

iii. *Illegal Interception* (Penyadapan Ilegal)

Setiap orang dengan sengaja dan tanpa hak melakukan intersepsi atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu 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. Hal ini terdapat dalam Pasal 31 Undang - Undang No.11 Tahun 2008.[148] Tindak pidana di dalam dunia maya yang dimaksud Pasal di atas adalah Intersepsi atau Penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik yang disimpan dalam Komputer dan/atau Sistem Elektronik.

iv. *Data Interference* (Gangguan Data)

Setiap orang dengan sengaja dan tanpa hak mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan, memindahkan atau mentransfer suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik kepada Sistem Elektronik Orang lain yang tidak berhak, sehingga mengakibatkan terbukanya suatu Informasi Elektronik dan/atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya. Hal ini terdapat dalam Pasal 32 Undang - Undang No.11 Tahun 2008.[149] Tindak pidana di dalam dunia maya yang dimaksud Pasal di atas adalah Mengusik Informasi/Dokumen Elektronik, Memindahkan atau Mentransfer Informasi/Dokumen Elektronik.

v. *System Interference* (Gangguan Sistem)

[147] Ibid.,hlm 8
[148] Ibid.,hlm 8
[149] Ibid.,hlm 8

Setiap orang dengan sengaja dan tanpa hak melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya. Hal ini terdapat dalam Pasal 33 Undang - Undang No.11 Tahun 2008.[150] Tindak pidana di dalam dunia maya yang dimaksud Pasal di atas adalah Tindak Pidana Komputer terhadap Sistem Elektronik. Sasaran dari tindak pidana ini adalah terganggunya "Sistem Elektronik".

vi. *Misuse of devices* (Penyalahgunaan Perangkat)

Setiap orang dengan sengaja dan tanpa hak memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki perangkat keras atau perangkat lunak komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan yang dilarang dan sandi lewat Komputer, Kode Akses, atau hal yang sejenis dengan itu, yang ditujukan agar Sistem Elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan yang dilarang. Hal ini terdapat dalam Pasal 34 Undang - Undang No.11 Tahun 2008.[151] Tindak pidana di dalam dunia maya yang dimaksud Pasal di atas adalah memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan atau memiliki fasilitas untuk perbuatan yang dilarang sebagaimana yang diatur dari Pasal 27 ke 31 Undang - Undang No.11 Tahun 2008.

vii. *Computer related fraud & forgery* (Penipuan dan pemalsuan yang berkaitan dengan komputer)

Setiap orang dengan sengaja dan tanpa hak 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. Hal ini terdapat dalam Pasal 35 Undang - Undang No.11 Tahun 2008.[152]

[150] Ibid.,hlm 9
[151] Ibid.,hlm 9
[152] Ibid.,hlm 9

Dari ketiga Peraturan Perundang – undangan di atas maka penulis ingin memberikan gambaran perbandingan ketiga peraturan perundang – undangan tersebut. Dari segi definisi, subtantif hukum dan prosedur hukum yang ada.

Tabel 3.1. Definisi hukum [153]

Convetion On Cybercrime	ITU	Indonesia
a. computer system; b. computer data; c. service provider; dtraffic data.	(a) Access (b) Computer (c) Computer Data (d) Computer Program (e) Computer System (f) Content Data (g) Critical Infrastructure (h) Cyberspace (i) Damage (j) Disruption (k) Interception (l) Interference (m) Loss (n) Malware (o) Network (p) Service Provider (q) Subscriber Information (r) Traffic Data	• teknologi informasi • komputer – hardware – software • jaringan komputer • informasi elektronik – konten • dokumen elektronik – subscriber information – traffic data – computer data • Akses • Intersepsi • Kerusakan • Kerugian • Sistem Elektronik – semua perangkat & prosedur terkait • Penyelenggara Sistem Elektronik

[153] Edmon Makarim, *Slide Cybersecurity and Cybercrime : UU ITE dan RUU TIPITI* , hlm.9

Tabel 3.2. Subtantif Hukum

Convention On Cybercirme	ITU	Indonesia
Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems. illegal access, illegal interception, data interference, system interference, misuse of devices, Title 2 – Computer-related offences computer-related forgery, computer-related fraud Title 3 – Content-related offences offences related to child pornography and offences related to copyright and neighbouring rights. Title 4 – Offences related to infringements of copyright and related rights Title 5 – Ancillary liability and sanctions Attempting and aiding or abetting Corporate liability Sanctions & Measures	*Title 2. Substantive Provisions; Acts Against Computers, Computer Systems, Networks, Computer Data, Content Data, and Traffic Data* sect. 2. Unauthorized Access to Computers, Computer Systems, and Networks sect. 3. Unauthorized Access to or Acquisition of Computer Data, Content Data, Traffic Data sect. 4. Interference and Disruption sect. 5. Interception sect. 6. Misuse and Malware sect. 7. Digital Forgery sect. 8. Digital Fraud, Procure Economic Benefit sect. 9. Extortion sect. 10. Aiding, Abetting, and Attempting sect. 11. Corporate Liability	• Penyalahgunaan Komptr/ Kompt sbg sarana: – Penyebaran Informasi ilegal (Illegal materials) – Pelanggaran Hak Cipta (offences related to copyright) – Pemalsuan atau Penipuan (*computer related fraud & forgery*) • Komputer sebagai sasaran – Akses tanpa hak dan/atau melawan hukum (Illegal Access) – Intersepsi Melawan Hukum (Illegal Interception) – Gangguan/Pengrusakan Data (Data Interference) – Gangguan/Pengrusakan Sistem (System Interference) – Penyalahgunaan Perangkat (Misuse of Device)

Tabel di atas merupakan perbandingan subtantif hukum [154] dan satu lagi adalah perbandingan mengenai prosedur hukum.[155]

Tabel 3.3. Prosedur Hukum

Convention Of Cybercrime	ITU	Indonesia
• Title 1-common provisions a. scope of procedural provisions b. Conditions & safeguards => • Title 2 - expedited preservation of stored computer data a. expedited preservation of stored computer data b. expedited • title 3 - production order • title 4 - search & seizure of stored computer Data • title 5 - real time collection of computer data a. real time collection of traffic data b. interception of content data • Sect. 3. Jurisdiction	*Title 3: Procedural Provisions for Criminal Investigations and Proceedings for Offenses Within this Law* sect. 12. Scope of Procedural Provisions sect. 13. Conditions and Safeguards sect. 15. Expedited Preservation and Partial Disclosure of Traffic Data sect. 17. Production Order sect. 18. Search and Seizure of Stored Data sect. 19. Interception (RealTime Colection) of Traffic Data sect. 20. Interception (RealTime Collection) of Content Data *Title 4: Jurisdictional Provisions* sect. 21. Jurisdiction	• KUHAP – penggeladahan rumah & badan – penyitaan • benda terkait tindak pidana – Pemeriksaan surat • UU ITE – Penyidikan: penggeledahan dan penyitaan memerlukan izin pengadilan – Condition & safeguards: • Privasi • Pelayanan Publik • Kerahasiaa • Keutuhan/Integritas Data • UU Telekomunikasi – kerahasiaan berita – larangan penyadapan secara langsung, hrs lewat operator

[154] Ibid.,hlm 10
[155] Ibid.,hlm 11

Jika melihat uraian dalam bab ini, tindak pidana siber hanya dipahami sebagai sesuatu hal yang baru akan selesai jika ada perumusan hukum positif *"Lex Specialist"* yang sejelas – jelasnya dalam suatu perumusan delik formil yang detail sehingga setiap ada suatu penamaan tindak pidana baru seperti *Identity Theft, Spamming, Phissing,*dan lain lain maka seakan harus dirumuskan lagi suatu rumusan yang baru.

BAB IV
PEMBAHASAN

Pembahasan Teknologi Informasi, media, dan komunikasi telah mengubah baik perilaku masyarakat maupun peradaban manusia global. Perkembangan teknologi informasi dan komunikasi telah pula menyebabkan hubungan dunia menjadi tanpa batas *(bordeless)* dan menyebabkan perubahan sosial, ekonomi, dan budaya secara signifikan berlangsung demikian cepat. Teknologi informasi saat ini menjadi pedang bermata dua karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan dan peradaban manusia sekaligus menjadi sarana efektif perbuatan melawan hukum.

Berkaitan dengan hal tersebut, perlu diperhatikan sisi keamanan dan kepastian hukum dalam pemanfaatan teknologi informasi, media dan komunikasi agar dapat berkembang secara optimal. Untuk mengatasi gangguan keamanan dalam penyelenggaraan sistem elektronik, pendekatan hukum bersifat mutlak karena tanpa kepastian hukum, persoalan pemanfaatan teknologi informasi yang kurang optimal. Untuk itulah, pemerintah mengundangkan Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik pada tanggal 21 April 2008.

Peraturan perundang – undangan yang mengatur aktifitas – aktifitas pemanfaatan teknologi informasi di Indonesia, di dalam – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik memiliki keunikan tersendiri, karena undang – undang ini berlaku untuk setiap orang yang melakukan perbuatan hukum sebagaimana diatur di dalam undang – undang ini,baik yang berada di luar hukum Indonesia, yang memiliki akibat hukum di wilayah hukum Indonesia dan/atau diluar wilayah hukum Indonesia dan merugikan kepentingan Indonesia. Sehingga dapat dimaknai bahwa undang – undang ini memiliki ruang lingkup yang berbeda dan lebih luas dari peraturan perundang – perundangan yang telah ada sebelumnya dalam menangani masalah tindak pidana siber.

Asas dan tujuan undang – undang ini adalah pemanfaatan Teknologi Informasi dan Transaksi Elektronik dilaksanakan berdasarkan asas kepastian hukum, manfaat, kehati – hatian, itikad baik dan kebebasan memilih teknologi

dan netral teknologi. jadi dapat diartikan bahwa penggunaan teknologi informasi dan transaksi elektronik diharapkan dijamin dengan kepastian hukum, memiliki manfaat, penuh kehati-hatian, beritikad baik, dan adanya kebebasan memilih teknologi dan netral.

Namun disahkannya sebuah Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik bukan berarti undang – undang ini telah menjadi sebuah hukum yang mutlak dan tidak bisa lagi dirubah atau diganti. Sebaliknya justru harus adanya perbaikan dan perubahan dilakukan terhadap Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan Peraturan Pemerintah sebagai pelengkap karena setelah diterapkan diketahui mempunyai kelemahan, terutama kelemahan tersebut fatal sifatnya.

Dalam pelaksanaannya,Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik banyak menuai pro dan kontra. Bahkan kehadiran Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dituding tidak dapat menurunkan tingkat kejahatan siber secara signifikan, sehingga memunculkan pertanyaan keefektifan Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik itu sendiri terutama dari aspek pidananya.

Berdasarkan hasil penelitian, aspek pidana yang terkandung dalam Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik menimbulkan banyak permasalahan. Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sendiri sebenarnya telah dirancang sedemikian rupa oleh pemerintah Indonesia agar dapat secara optimal menjerat tindak pidana siber dengan modus operandinya. Namun dalam realitanya, tetap saja terdapat faktor – faktor tertentu yang menjadi hambatan bagi penegakan hukum secara umum.

Faktor – faktor penghambat yang dimaksud saling berkaitan erat satu sama lainnya, dan merupakan esensi serta tolak ukur dari efektifitas penerapan penegakan hukum. Faktor – faktor tersebut adalah :

a. Subtansi Hukum : peraturan perundang – undangan ;
b. Penegakan Hukum yakni pihak yang membentuk maupun menerapkan hukum.

Ada beberapa hal yang penting yang perlu menjadi sorotan dalam Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik terkait dengan kepentingan penegakan hukum terhadap tindak pidana siber diantara nya adalah masalah asas teritorial dan klasifikasi alat bukti yang sah. Kedua hal tersebut dianggap penting karena terkait dengan pembuktian dalam tindak pidana siber. Tapi tidak menutup kemungkinan masih ada masalah lain yang juga sama pentingnya untuk menjadi sorotan dalam Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Dalam hal pembuktian terhadap tindak pidana, Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik telah memberikan terobosan baru dengan adanya pengakuan terhadap *digital evidence* sebagai alat bukti yang sah dengan beberapa persyaratan tertentu, sebagaimana diatur dalam Bab III Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Hal ini sangat penting dalam penanganan kasus tindak pidana siber mengingat kejahatan tersebut dilakukan dengan menggunakan teknologi terutama internet. Sehingga keberadaan bukti – bukti sebagaimana dalam kejahatan konvesional seperti surat – surat atau dokumen – dokumen tertulis lainnya akan sangat sulit didapat *(paperless)*.

4.1. Kelemahan dari Subtansi Hukum Undang – Undang No. 11 Tahun 2008

Dilihat dari subtansi hukumnya, Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik memiliki beberapa kelemahan dalam pasal – pasal yang menyangkut tindak pidana siber. Pasal yang menjadi sorotan sebagai berikut ini :

a. Adanya pengelompokan perbuatan yang dilarang yang berbeda – beda di dalam satu pasal. Padahal, di dalam KUHP perbuatan yang dilarang itu diatur sendiri – sendiri. Hal ini salah satunya bisa terlihat di dalam Pasal 27 Undang – Undang No. 11 Tahun 2008 tentang 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.

Di dalam Pasal 27 pada ayat (1) ditemukan kelemahan lainnya yaitu sama sekali tidak ada penjelasan mengenai apa yang dimaksud dengan "kesusilaan" kesusilaan dalam standar pandangan yang bagaimana dapat diartikan dengan kesusilaan. Setiap orang pasti ada perbedaan dalam mendefiniskan arti kata kesusilaan tersebut. Dengan tidak adanya penjelasan kesusilaan tersebut, tidak jelas apakah pengertian kesusilaan dimaksud sama dengan pengertian pornografi yang dimaksud di dalam Undang – Undang No. 11 Tahun 2008.

Istilah "kesusilaan" dalam Pasal 27 ayat (1) itu tidak dapat begitu saja dianggap merupakan padanan kata pornografi yang merupakan terjemahan dari kata *Pornography* dalam bahasa inggris. Hal ini sangat dibedakan dengan pengertian kesusilaan dan pornografi di dalam Kamus Besar Bahasa Indonesia yang dibuat oleh Pusat Bahasa Departemen Pendidikan Nasional. [156]

[156] Pusat Bahasa, Departemen Pendidikan Nasional. *Kamus Besar Bahasa Indonesia.*Edisi ke-3 Tahun 2008.

Menurut KBBI, kesusilaan berasal dari kata susila yang berarti baik budi bahasanya; beradab; sopan selain itu juga dapat diartikan sebagai adat istiadat yang baik; sopan santun; kesopanan; keadaban; kesusilaan. Juga diartikan sebagai pengertian tentang adab. Sementara itu kesusilaan menurut KBBI bermakna perihal susila yang berkaitan dengan adab dan sopan santun. Selain itu diartikan pula norma yang baik;kelakuan yang baik; tata krama yang luhur.

Sementara itu, pornografi menurut KBBI adalah penggambaran tingkah laku secara erotis dengan lukisan atau tulisan untuk membangkitkan nafsu birahi. Arti yang lain adalah bahan bacaan yang dengan sengaja dan semata – mata dirancang untuk membangkitkan nafsu birahi dalam seks. Dengan kata lain pornografi adalah kata lain dari cabul atau pencabulan.

Dari penjelasan tersebut di atas jelaslah bahwa arti kesusilaan tersebut jelas bahwa arti kesusilaan sangat jauh berbeda dari arti pornografi. Kesusilaan berkaitan dengan adab atau sopan santun sedangkan pornografi berkaitan dengan pencabulan atau berkaitan dengan perbuatan cabul. Ternyata di dalam Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik telah menyamaratakan antara kata kesusilaan dengan pornografi. Dengan demikian Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik melakukan kesalahan yang sangat mendasar.

Undang – Undang No. 11 Tahun 2008 bermaksud memberi sanksi terhadap perbuatan – perbuatan yang melanggar kesusilaan atau melanggar kesopanan yang awalnya hanya diberikan sanksi sosial atau moral setelah berlakunya undang – undang ini maka hal tersebut dikenai sanksi pidana maka bisa dikatakan Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik telah melakukan kriminalisasi yang berlebihan atau disebut *over criminalization*.

Dapat dipastikan bahwa sasaran sesungguhnya dari Undang – Undang No. 11 Tahun 2008 dalam Pasal 27 ayat (1) bukanlah melakukan perbuatan melanggar kesusilaan tapi melainkan perbuatan memiliki muatan pornografi dengan kata lain, yang dilarang adalah perbuatan yang dapat membangkitkan nafsu birahi seks. Karena hal tersebut ayat ini mutlak harus dilakukannya perubahan tidak menyamakan arti kesusilaan dengan pornografi.

Pada pasal 54 ayat (1) mengancam sanksi pidana yang lebih berat apabila tindak pidana yang dimaksud di dalam Pasal 27 ayat (1) menyangkut kesusilaan atau eksploitasi seksual terhadap anak. Isi dari pasal 52 ayat (1) sebagai berikut : " Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 ayat (1) menyangkut kesusilaan atau eksploitasi seksual terhadap anak dikenakan pemberatan sepertiga pidana pokok".

Di sini Undang – Undang No. 11 Tahun 2008 tidak memberikan batasan umur bagi mereka yang masih tergolong anak. Di beberapa negara di dalam peraturan undang – undangnya memberikan batasan umur bagi mereka yang masih tergolong anak yaitu di bawah umur 18 tahun atau sampai dengan 18 tahun. Maka apakah yang menjadi acuan batasan umur di dalam Undang – Undang No. 11 Tahun 2008. Sebagian besar undang – undang tindak pidana siber justru memfokuskan diri bukan pada tindak pidana siber di pornografi pada umumnya tetapi kepada pornografi anak.

Hal ini tertera dalam *Convention of Cybercrime*, dan batasan umur pada konvensi ini untuk dikategorikan anak adalah setiap orang yang berumur di bawah 18 tahun. Mengenai batas yang ditentukan oleh konvensi ini untuk dikategorikan sebagai anak adalah setiap orang yang berumur dibawah 18 tahun. Namun demikian, apabila suatu negara telah ikut menandatangani konvensi ini bermaksud memberikan batas yang lebih rendah daripada 18 tahun hendaknya tidak kurang dari 16 tahun. Jika mengacu pada KUHP yang menjadi *lex generalis* Undang – Undang No. 11 Tahun 2008 maka sesuai dengan Pasal 45 yaitu sebelum umur 16 tahun. Sedangkan menurut Undang – Undang No.3 Tahun 1997 tentang Pengadilan Anak batas umur anak antara 8 tahun tetapi belum mencapai umur 18 tahun dan belum pernah menikah.

Di dalam Pasal 27 ayat (2) tidak terdapat penjelasan terhadap definisi tentang perjudian. Apabila definisi dari perjudian adalah suatu kegiatan yang melibatkan uang dan/atau barang berharga lainnya, dimana terjadi perpindahan kepemilikan uang dan/atau barang berharga tersebut atas dasar pertaruhan yang dimenangkan secara untung – untungan, maka perdagangan saham jelas – jelas masuk dalam kategori perjudian, bahkan perebutan kekuasaan dikancah dunia politikpun dapat bisa masuk dalam kategori ini. Selain itu kelemahan dari pasal

ini hanya penyelenggara pengelola perjudian yang kena tindak pidana sedangkan pelaku perjudian tidak di tindak pidana berdasarkan Pasal 27 *jo* Pasal 45 Undang – Undang No. 11 Tahun 2008 artinya seseorang hanya dapat dipidana berdasarkan ketentuan pasal ini apabila Informasi dan/atau Dokumen Elektronik tersebut memiliki muatan perjudian.

Di dalam Pasal 27 ayat (3), di dalam dunia maya atau internet tindak pidana siber yang diatur dalam pasal ini disebut dengan *cyberstalking* tetapi dalam ayat pada pasal ini memiliki muatan penghinaan dan/atau pencemaran nama baik. Tetapi tidak adanya penjelasan maksud penghinaan dan/atau pencemaran nama baik menurut siapa dan apa batasan dari penghinaan dan/atau pencemaran nama baik tersebut serta batasan tentang unsur – unsur penghinaan dan pencemaran nama baik tidak terlalu jelas sehingga menimbulkan ambiguitas sehingga interpretasinya akan sangat tergantung pada subjektifitas dari pelapor/korban, penegak hukum sendiri dan ahli bahasa. Oleh karena itu materi dalam pasal tersebut banyak mendapatkan pro – kontra dari masyarakat terutama dikaitkan dengan isu kebebasan pers yang terancam dengan pasal tersebut sebagaimana dinyatakan dalam Pasal 1 ayat (11) Undang – Undang No. 40 Tahun 1999 tentang pers yang berbunyi : " Hak Jawab adalah seseorang atau sekelompok orang untuk memberikan tanggapan atau sanggahan terhadap pemberitaan berupa fakta yang merugikan nama baiknya." Kebebasan pers kebebasan yang bertanggung jawab dan kebebasan pers yang dilandasi oleh penghormatan terhadap Hak Asasi Publik, Seharusnya Pasal 27 ayat (3) ini dapat direvisi menjadi memiliki muatan tuduhan yang tidak dapat dibuktikan kebenarannya.

Begitu juga di dalam Pasal 27 ayat (4), memiliki muatan pemerasan dan/atau pengancaman. Tidak ada satu otoritas pun yang berwenang menurut undang – undang untuk memberikan hak kepada siapapun untuk melakukan pemerasan atau pengancaman. Di dalam undang – undang ini tidak dijelaskan apa yang dimaksudkan dengan pemerasan dan pengancaman. Pasal ini bisa dapat berfungsi sebagai "pasal karet" yang tidak bisa memberikan kepastian hukum. Pengancaman yang diatur dalam pasal ini adalah janji pengancam yang terkandung dalam ancamannya buka berupa "akan melakukan kekerasan" terhadap pihak yang diancam.

Ditemukan juga bahwa dalam satu pasal, antara ayat yang satu dengan yang lainnya terlihat berdiri sendiri (parsial) dan seperti tidak ada keterkaitannya sama skali hal ini ada di dalam Pasal 30 Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik 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 apa pun 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 apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

Di dalam ketentuan Pasal 30 ayat (1) seseorang hanya dapat dipidana apabila yang diakses oleh pelaku adalah komputer dan/atau Sistem Elektronik. Yang menjadi korban tindak pidana tersebut adalah pemilik komputer dan/atau Sistem Elektronik tersebut. Pasal tersebut menegaskan bahwa cara apapun yang ditempuh oleh pelaku dalam mengakses Komputer dan atau Sistem Komputer tersebut bukanlah merupakan faktor penentu bagi dapat atau tidak dapatnya pelaku dipertanggung jawabkan secara pidana.

Perlu dicermati bahwa Pasal 30 ayat (1) terdapat bukan saja unsur tanpa hak seperti dalam pasal – pasal sebelumnya tetapi juga unsur melawan hukum. Namun , kata yang digunakan adalah tanpa hak atau melawan hukum bukan tanpa hak dan melawan hukum.

Undang – Undang No. 11 Tahun 2008 menggunakan istilah sistem elektronik, sedangkan *Convention of Cybercrime* mengunakan istilah *computer system*. Menurut Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, sistem elektronik yaitu sebagaimana didefinisikan dalam Pasal 1 angka 5 adalah:

> "Serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan,

menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik.“

Sementara menurut *Convention of Cybercrime*, yang dimaksud dengan computer system adalah :

“ *any device or a group of interconnected or related devices, one more of which, pursuant to a program, performs automatic processing of data*. “

Membandingkan keduannya, dapat disimpulkan bahwa kedua istilah tersebut berbeda. Oleh karena itu di pasal ini menggunakan kalimat mengakses komputer dan/atau sistem elektronik, maka berarti pada pasal ini mengatur bukan saja perbuatan yang dilarang mengakses sistem elektronik tetapi juga bila mengakses sistem komputer.

Tegasnya Undang – Undang No. 11 Tahun 2008 telah mengkriminalisasikan perbuatan yang ditunjukan baik kepada sistem komputer yang berupa peralatan maupun yang ditunjukkan kepada sistem elektronik yang berwujud perangkat dan prosedur elektronik.

Namun dalam praktiknya untuk dapat melakukan perbuatan yang dilarang oleh Pasal 30 ayat (1) tersebut yaitu untuk dapat mengakses komputer dan atau sistem elektronik yang antara lain berisi data elektronik dan informasi elektronik, tidak mungkin dilakukan apabila tidak menggunakan komputer atau melalui sistem komputer.

Sama hal nya dengan Pasal 30 ayat (1) , Pasal 30 ayat (2) tidak menentukan bahwa pelaku hanya dapat dibebani pertanggungjawaban pidana apabila dalam mengakses Komputer dan/atau Sistem Elektronik tersebut harus dilakukan dengan cara tertentu. Pasal ini mengabaikan kepedulian terhadap cara apapun yang dilakukan pelaku dalam mengakses komputer dan/atau Sistem Komputer tetap dapat dituntut berdasarkan Pasal 30 ayat (2).

Seseorang hanya dapat dituntut dalam pasal ini apabila bertujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik. Kalau tujuannya hanya mengintip isi Informasi Elektronik dan/atau Dokumen Elektronik dari komputer dan/atau Sistem Komputer yang berhasil dibobolnya. Namun apakah

mungkin seorang pelaku akan tidak melihat atau membaca apa isi komputer dan/atau sistem komputer yang berhasil dibobolnya? Karena pelaku membaca isi Komputer dan/atau Sistem Komputer itu, maka pembobol pasti akan memperoleh Informasi Elektronik dan/atau Dokumen Elektronik yang terdapat dalam komputer tersebut.

Dapat disimpulkan bahwa pasal ini mengatur larangan setiap orang untuk tidak melakukan *illegal accsess* dengan cara apapun contohnya *hacking, cracking* maupun *cyber trespassing.*

b. Permasalahan selanjutnya adalah adanya ketidakkonsistenan dalam penulisan pada Pasal 31 Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik 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 apa pun 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.

Meskipun tidak memberikan pengaruh besar terhadap penerapan Undang – Undang No. 11 Tahun 2008, namun tentu saja memberikan pandangan buruk dalam penulisan suatu peraturan Perundang – undangan. Pasal 31 menyimpulkan bahwa melarang setiap orang untuk melakukan penyusupan ke Sistem Elektronik milik orang lain, kecuali atas dasar permintaan institusi para penegak hukum. Ini artinya semua orang yang melakukan tindakan melawan hukum menggunakan Sistem Elektronik dapat dengan aman menyimpan semua informasi yang dimilikinya selama tidak diketahui oleh penegak hukum, yang mana ini mudah dilakukan karena orang lain tidak diperbolehkan mengakses Sistem Elektronik miliknya dan dengan demikian tidak dapat memperoleh bukti bukti awal yang dibutuhkan untuk melakukan pengaduan.

c. Pada Pasal 32 dan 34 Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang berbunyi :

   Pasal 32 :

   (1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah,mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik.

   (2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun 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.

Dan Pasal 34 :

(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 33

(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.

Hal ini dapat menimbulkan kesulitan dalam hal pembuktian. Hal ini dikarenakan ketidakjelasan unsur – unsur yang dibuktikan pada kedua pasal tersebut. Pada Pasal 32, apakah pembuktiannya harus semua unsur cara atau cukup salah satunya saja. Padahal kalau salah satu unsur saja tidak terbukti, maka tersangka harus dibebaskan dari segala tuntutan hukum. Sedangkan pada Pasal 34, pengecualian Pasal 34 ayat (1) apakah hanya berlaku terhadap kegiatan penelitian atau pengujian sistem elektronik ataukah kegiatan penelitian dan pengujian sistem elektronik untuk perlindungan sistem elektronik itu sendiri

d. Adanya pasal khusus yang mengatur tentang "mengakibatkan kerugian bagi orang lain. Pada 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 "

Lalu bagaimana dengan Pasal 35, apakah tidak termasuk dalam Pasal 36 ini, Apakah Pasal 35 tertutup kemungkinan mengakibatkan kerugian bagi orang lain?

e. Adanya pasal yang mengabaikan yurisdiksi hukum.

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 berads di wilayah yurisdiksi Indonesia."

Pasal 37 ini dibuat agar dalam kondisi dimana seseorang yang berada di Indonesia atau warga negara Indonesia melakukan penipuan terhadap warga negara lain dengan menggunakan server yang ada di negara lain, orang tersebut dapat dijerat dengan Undang – Undang No. 11 Tahun 2008. Akan tetapi karena Pasal 27 mengatur tindakan – tindakan yang tidak memiliki standar yang sama di negara lain ditambah dengan Pasal 34 yang mengatur penjualan perangkat keras dan lunak, artinya aturan yang termuat pada Pasal 27 dan Pasal 34 belum tentu mempunyai standar yang sama dengan negara lain. Pasal 37 otomatis mengalami konflik yurisdiksi.

Kita berikan saja contoh bila seorang Warga Negara Indonesia, memproduksi perangkat lunak komputer khusus untuk perjudian selama berada di Kota X, Negara Y, dan perangkat lunak tersebut dikirim ke Indonesia untuk diinstal di komputer yang berada di Indonesia, untuk diekspor ke Negara Y, lalu orang tersebut kembali ke Indonesia, maka berdasarkan Pasal 37, Pasal 34 dan Pasal 27 seseorang tersebut ini dapat dikenakan sanksi karena ia melakukannya buka untuk tujuan penelitian atau pengujian, karena didaerah yurisdiksi hukum dimana tindakan itu dilakukan, sama sekali tidak terjadi pelanggaran hukum. Pasal 37 ini telah mengabaikan yurisdiksi hukum.

f. Kandungan penjelasan pasal tidak sinkron dengan pasal yang dijelaskan.

Penjelasan Pasal 30 ayat (2) Undang – Undang No.11 Tahun 2008:

"Secara teknis perbuatan yang dilarang sebagaimana dimaksud pada ayat ini dapat dilakukan, antara lain dengan:

a. melakukan komunikasi, mengirimkan, memancarkan atau sengaja berusaha mewujudkan hal – hal tersebut kepada siapa pun yang tidak berhak untuk menerimanya; atau
b. sengaja mengahalangi agar informasi dimaksud tidak dapat atau gagal diterima oleh yang berwenang menerimanya di lingkungan pemerintah dan/atau pemerintah daerah.

Ternyata kandungan penjelasan Pasal 30 ayat (2) tidak sesuai untuk menjelaskan Pasal 30 ayat (2), Penjelasan Pasal ini lebih sesuai untuk menjelaskan Pasal 32 ayat (2) yang berbunyi :

"Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik orang lain tidak berhak."

Mungkin masih ada kelemahan lain mengenai pasal – pasal tindak pidana siber, kelemahan – kelemahan ini bisa ada karena tidak melibatkan masyarakat pengguna teknologi informasi secara meluas dalam penyusunan Undang – Undang No.11 Tahun 2008.

Menurut Edmon Makarim[157] Undang – Undang No. 11 Tahun 2008 telah cukup memadai mengatur aspek hukum pemanfaatan teknologi informasi. Pendapat ini juga didasari atas asumsi bahwa jika semua pemangku kepentingan berjalan dengan baik untuk *"integrated criminal justice system"*. Ironi melihat pihak – pihak di dalam negeri cenderung kurang mengapresiasikan Undang – Undang No. 11 Tahun 2008 sedangkan akademisi luar negeri justru sangat menghargai bahwa Undang – Undang No. 11 Tahun 2008 cukup baik. Dalam wawancara ini juga dapat diketahui bila terjadi benturan atau beberapa kasus itu terjadi karena kesalahpahaman dan aneka benturan kepentingan di dalamnya.

Selanjutnya, Undang – Undang No. 11 Tahun 2008 tidak hanya mengatur tentang tindak pidana siber dalam perspektif penyalahgunaan yang terjadi karena

[157] Wawancara dengan narasumber pada tanggal 16 Desember 2011 di Fakultas Hukum Universitas Indonesia,Depok.

niatan jahat si pelaku, melainkan juga memberikan kewajiban bagi penyelenggara untuk melakukan tata kelola Teknologi Informasi Komunikasi yang baik.

Namun diakui, Undang – Undang No. 11 Tahun 2008 juga membutuhkan sedikit perubahan atau penambahan untuk kesempurnaanya khususnya tentang *Procedural Law* selebihnya tidak ada karena Undang – Undang No. 11 Tahun 2008 dibuat sedemikian rupa antara perpaduan dari *Convention of Cybercrime dan International Telecommunication Union* maka dari itu Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dianggap suatu produk hukum yang lengkap untuk mengatasi tindak pidana siber di Indonesia. Jika tindak pidana siber hanya dipahami sebagai suatu hal yang baru akan selesai jika ada perumusan hukum positif *"Lex Specialist"* yang jelas – jelasnya dalam suatu perumusan delik formil yang detail, sehingga setiap ada suatu penamaan tindak pidana baru maka seakan harus dirumuskan lagi suatu rumusan baru lalu dimana penerapan *progressive justice* itu sendiri bila hal ini dipermasalahkan terus menerus. Demikian kesimpulan wawancara masalah Undang – Undang No. 11 Tahun 2008.

4.2 Penerapan Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

4.2.1 Kasus Pornografi

Kasus pornografi yang sangat menghebohkan tahun 2010 yaitu kasus video porno yang melibatkan Nazriel Ilham,vokalis salah satu band ternama di Indonesia, dengan lawan main Luna Maya dan Cut Tari.

Dalam kasus ini terdakwa Nazriel Ilham yang biasa disebut dengan Ariel didakwa dengan Pasal 29 Undang – Undang No. 44 Tahun 2008 tentang Pornografi yang berbunyi :

> "Setiap orang yang memproduksi, membuat, memperbanyak, menggandakan, menyebarluaskan, menyiarkan, mengimpor, mengekspor, menawarkan, memperjualbelikan, menyewakan, atau menyediakan pornografi sebagaimana dimaksud dalam Pasal 4 ayat (1) dipidana dengan pidana penjara paling singkat 6 (enam) bulan dan paling lama 12 (dua belas) tahun dan/atau pidana denda paling sedikit Rp. 250.000.000,00.- (dua ratus lima puluh juta rupiah)

dan paling banyak Rp. 6.000.000.000,00.- (enam miliar rupiah) jo Pasal 56 KUHP. Dalam dakwaan jaksa sebelumnya Ariel juga didakwa dengan dua pasal lainya, yaitu Pasal 282 Ayat (1) KUHP dan Pasal 27 Ayat (1) Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Pasal 27 Ayat (1) Undang – Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik jo Pasal 45 ayat (1) Undang – Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik mengatur tentang perbuatan mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya informasi elektronik dan/atau pencemaran nama baik. Sedangkan Pasal 282 Ayat (1) KUHP mengatur tentang perbuatan menyiarkan, mempertontonkan atau menempel tulisan/gambar yang dikenalnya melanggar kesopanan, dengan ancaman pidana selama – lamanya 1 tahun 4 bulan.

Dalam Pertimbangan Hukumnya, Majelis Hakim menyatakan Ariel terbukti membuat, memberikan kesempatan dan menyediakan materi lalu menyebarluaskan materi pornografi pada terdakwa lain Reza Rizaldy yang merupakan musik editor studio yang dimiliki oleh produsen band Peterpan yang dimana Ariel menjadi salah satu personil di dalamnya, menemukan keberadaan video porno itu di hard disk milik Ariel. Menurut Majelis Hakim ini merupakan kesalahan fatal bagi Ariel dan Majelis Hakim tidak sependapat dengan pembelaan pengacara Ariel yang mangatakan bahwa apa yang dilakukan Ariel adalah privasi, persoalan pribadi yang dilindungi oleh hukum dan dari sisi pelaku juga tidak ada upaya maksimal untuk menghapus video tersebut.

Ariel menyangkal bahwa dirinya yang ada di dalam video tersebut. Hal ini sangat bertentangan dengan apa yang dikatakan oleh salah satu yang termasuk di dalam video tersebut yaitu Cut Tary yang menyatakan bahwa benar dirinya yang ada di dalam video tersebut. Sikap Ariel yang menyangkal dan tidak menyesali perbuatannyabagi majelis hakim itu suatu keheranan. Selain itu, penyebaran video porno yang dilakukan Ariel menurut hakim menjadi catatan buruk diranah pornografi di Indonesia. Sebagai publik figur harusnya dapat memahami jika video ini dampaknya luar biasa. Atas berbagai pertimbangan itu, menurut hakim kasus ini sudah memenuhi unsur – unsur Pasal 29 No.44 Tahun 2008 Undang –

Undang tentang Pornografi yang dituntutkan kepada Ariel. Sedangkan hal yang meringankan kepada terdakwa adalah masih muda dan belum pernah berurusan dengan hukum Pada akhirnya, majelis hakim memutuskan untuk menjatuhkan hukuman penjara pada terdakwa Ariel selama 3 tahun 6 bulan dan denda sebesar Rp. 250.000.000,00.-

Sedangkan terdakwa yang menyebarkan video hingga menjadi skandal besar, Reza Rizaldy dijatuhi hukuman lebih ringan dari Ariel divonis 2 tahun penjara dikurangi masa tahanan dan denda Rp. 250.000.000,00.- subsidier tiga bulan kurungan. Hakim, menilai Reza Rizaldy telah meresahkan masyarakat karena telah menyebarkan video asusila di dunia maya.

Selain kasus pornografi yang terjadi di Indonesia, jenis tindak pidana siber *Illegal content* merupakan tindak pidana siber yang sering terjadi di Indonesia. Illegal content ini adalah tindakan memasukkan data dan atau informasi ke dalam internet yang dianggap tidak benar, tidak etis dan melanggar hukum atau mengganggu ketertiban umum. Salah satu contoh *illegal content* yang sering ditemui adalah dalam bidang pornografi *(cyberporn)*. *Cyberporn* atau situs pornografi itu sendiri merupakan kegiatan yang dilakukan dengan membuat, memasang, mendistribusikan dan menyebarkan material yang berbau pornografi, cabul dan mengekspos hal – hal yang tidak pantas.

Situs pornografi telah menjadi salah satu dalang rusaknya mentalitas generasi muda bangsa. Pemerintah telah mengeluarkan Undang – Undang No.11 Tahun 2008 dan Undang – Undang No.44 Tahun 2008 guna mengatasi laju situs pornografi di Indonesia beberapa selain dari Pasal 281-283 Kitab Undang – Undang Hukum Pidana melarang pornografi dalam bentuk apapun dan Undang – Undang Nomor 2009 pada Pasal 5 Ayat (1) dan Pasal 13 Ayat (1) Huruf (a).

4.2.2 Kasus Pencemaran Nama Baik

Kompas.com pada tanggal 3 Juni 2009 mengusung *headline "*Undang – Undang Informasi dan Transaksi Elektronik Bukan Alat Membungkam." Undang – Undang No.11 Tahun 2008 digunakan untuk membawa Prita Mulyasari terkena kasus masalah Informasi dan Transaksi Elektronik.

Prita Mulyasari didakwa melakukan pencemaran nama baik Rumah Sakit Omni Internasional, Prita dijerat Pasal 27 ayat (3) Undang – Undang No.11 Tahun 2008 dengan sanksi pidana penjara maksimum 6 tahun dan/atau denda maksimal 1 milyar rupiah. Tragisnya, terhadap Prita diberlakukan penahanan oleh pihak kejaksaan. Pihak kejaksaan mendasarkan penahanan Prita pada dakwaan tersier dalam Pasal 27 ayat (3) tersebut dan subsidier Pasal 311 KUHP. Sesungguhnya tidak akan ada menyeret Prita untuk merasakan kurungan.

Prita pun dilepaskan karena penahananya yang didasarkan pada Undang – Undang No.11 Tahun 2008 dianggap berlebihan. Paling tidak ada dua alasan untuk menjelaskannya. Pertama kata "tanpa hak" dimaknai sangatlah sempit. Padahal, seorang Prita sebagai salah satu konsumen rumah sakit, dia memiliki hak untuk menyampaikan apa yang dikeluhkannya melalui email yang dibuatnya hak sebagai konsumen. Itu pun dijamin di dalam Undang – Undang No.8 Tahun 1999 tentang Perlindungan Konsumen. Kedua, dalam Undang – Undang No.11 Tahun 2008 pada Pasal 43 ayat 6 dijelaskan secara nyata dalam hal melakukan penangkapan dan penahanan, penyidik melalui penuntut umum wajib meminta penetapan ketua pengadilan negeri setempat dalam waktu satu kali dua puluh empat jam. Sedangkan dalam kasus Prita tidak ditempuh cara- cara yang sudah ditetapkan dalam Undang – Undang No.11 Tahun 2008.

Menurut Ronny, M.Kom, Keterangan Ahli Judicial Review di Mahkamah Kontitusi Undang – Undang No.11 Tahun 2008 di Mahkamah Konstitusi, dalam kaca mata hukum, penafsiran dan pemberlakuan Undang – Undang No.11 Tahun 2008 mutlak berpegangan pada putusan Mahkamah Konstitusi R.I Nomor 50/PUU-VI/2008 tentang judicial review Undang – Undang No.11 Tahun 2008 terhadap Undang – Undang Dasar 1945, salah satu pertimbangan Mahkamah berbunyi "keberlakuan dan tafsir atas Pasal 27 ayat (3) Undang – Undang No.11 Tahun 2008 tidak dapat dipisahkan dari norma hukum pokok dalam Pasal 310 dan Pasal 311 KUHP".

Pertimbangan Mahkamah tersebut dapat diartikan penafsiran Pasal 27 ayat (3) Undang – Undang No.11 Tahun 2008 merujuk pada pasal – pasal penghinan dalam KUHP khususnya Pasal 310 yang berbunyi :

(1) Barang siapa sengaja menyerang kehormatan atau nama baik seseorang dengan menuduhkan suatu hal, yang maksudnya terang supaya hal itu diketahui umum diancam karena pencemaran dengan pidana penjara paling lama sembilan bulan atau pidana denda paling banyak empat ribu lima ratus rupiah.

(2) Jika hal itu dilakukan dengan tulisan atau gambaran yang disiarkan, dipertunjukkan atau ditempelkan di muka umum, maka diancam karena pencemaran tertulis dengan pidana penjara paling lama satu tahun empat bulan atau pidana denda paling banyak empat ribu lima ratus rupiah.

(3) Tidak merupakan pencemaran atau pencemaran tertulis, jika perbuatan jelas dilakukan demi kepentingan umum atau karena terpaksa untuk membela diri

Dan Pasal 311 yang berbunyi :

(1) Jika yang melakukan kejahatan pencemaran atau pencemaran tertulis diperbolehkan untuk membuktikan apa yang dituduhkan itu benar, tidak membuktikannya dan tuduhan dilakukan bertentangan dengan apa yang diketahui, maka dia diancam melakukan fitnah dengan pidana penjara paling lama empat tahun.

(2) Pencabutan hak – hak berdasarkan Pasal 35 No 1 sampai dengan 3 dapat dijatuhkan.

Prita menyampaikan pesan kepada teman – temannya agar berhati – hati atas pelayanan rumah sakit dan jangan terpancing dengan kemewahan rumah sakit. Prita sengaja menulis pesan tersebut dengan maksud memberi pelajaran penting kepada khalayak umum agar lebih berhati – hati terhadap pelayanan rumah sakit. Peringatan tersebut ia tekankan supaya kasus yang menimpanya tidak dialami orang lain. Dengan fakta tersebut, sebetulnya tidak dapat dikatakan melakukan penghinaan dan/atau pencemaran nama baik, karena pesan yang disampaikan untuk kepentingan umum. Hal ini telah ditegaskan dalam Pasal 310 ayat (3) KUHP.

Selain Prita beberapa orang lainnya juga pernah mendapat ancaman dengan menggunakan Pasal 27 (3) Undang – Undang No.11 Tahun 2008, atau

disebut pasal karet ini. Bambang Kisminarso misalnya, polisi sempat menahannya berserta anaknya M.Naziri atas tuduhan telah menghina anak presiden dalam pelanggaran ketentuan pencemaran nama baik melalui Undang – Undang No.11 Tahun 2008 dikarenakan Bambang Kisminarso mengajukan pengaduan kepada Komisi Pengawasan Pemilu Daerah bahwa para pendukung putra presiden Indonesia Susilo Bambang Yudhoyono , Edhi Baskoro telah membagi – bagikan uang kepada calon pemilih atau *money politic*.

Pasal 27 ayat (3) Undang – Undang No.11 Tahun 2008 mempunyai syarat pembuktian yang cukup sulit. Seseorang yang melanggar harus dibuktikan memiliki motif sengaja mencemarkan nama baik. Oleh karenanya penyidik jangan gegabah menggunakan pasal tersebut jika belum mempunyai alat bukti yang cukup karena dunia maya sangat berbeda dengan dunia nyata.

BAB V
PENUTUP

5.1. Kesimpulan

Teknologi informasi telah mengubah perilaku dan pola hidup secara global. Perkembangan teknologi informasi telah pula menyebabkan dunia menjadi tanpa batas (borderless) dan menyebabkan perubahan sosial, budaya, ekonomi dan pola penegakan hukum yang secara signifikan berlangsung demikian cepat. Namun demikian teknologi informasi dan komunikasi juga menimbulkan permasalahan penerapannya. Beberapa potensi kerugian yang dapat disebabkan oleh pemanfaatan teknologi informasi dan dan komunikasi secara kurang tepat di antaranya masalah tindak pidana siber. Kondisi tersebut yang menyebabkan setiap gelombang perkembangan teknologi selalu diikuti dengan instrumen hukum yang mendukung. Dengan kata lain, bahwa hukum yang berkembang mengikuti perkembangan teknologi informasi dan komunikasi dewasa ini merupakan cerminan dari dinamika dari peradaban masyarakat itu sendiri

Diundangkan Undang – Undang No. 11 Tahun 2008 sesungguhnya merupakan salah satu bagian terpenting dari hukum siber yang sangat ditunggu keberadaannya di Indonesia karena sebenarnya telah dirancang secara optimal agar dapat menjerat pelaku tindak pidana siber. Namun dalam realitanya beberapa masalah yang memerlukan perhatian lebih lanjut antara lain pembahasan tentang telekomunikasi global, sistem pengamanan komunikasi elektronik, perbandingan Undang –Undang tentang Informasi dan Elektronik. Sedangkan faktor – faktor penghambat juga merupakan masalah karena keterkaitan antara satu dan lainnya, faktor penghambat itu antara lain masalah peraturan perundang – undangan, penegak hukum, dan masyarakatnya itu sendiri sebagai sasaran penerapan dan penegakan hukum.

Masih banyaknya kelemahan atau kekurangan pada Undang – Undang No.11 Tahun 2008 yang perlu ditinjau kembali terhadap pasal – pasal yang diundangkan untuk dilengkapi atau disesuaikan ataupun diubah dengan aturan hukum di bidang Informasi dan Transaksi Elektronik agar tidak menimbulkan berbagai celah hukum di dalamnya.

Terkaitan dengan semakin canggihnya modus kejahatan tindak pidana siber yang semakin berkembang pesat, para pembuat undang – undang dan penegak hukum belum melakukan perubahan sama sekali kualitas dan kuantitas undang – undang ini malah cenderung undang – undang ini menuai banyak pro dan kontra dianggap tidak dapat menurunkan tingkat kejahatan tindak pidana siber secara signifikan sehingga memunculkan tudingan bahwa undang – undang ini tidak berjalan secara efektif terutama dari aspek pidananya.

Undang – Undang No.11 Tahun 2008 masih membutuhkan penambahan kesempurnaan khususnya tentang *Procedural Law* dan hal yang masih menjadi persoalan dan perlu dicarikan solusinya adalah mengenai sifat khusus dari bidang teknologi informasi, yang penanganannya harus dilakukan oleh orang yang memahami teknologi informasi dan komunikasi serta perlunya pembaharuan Undang – Undang atau menerbitkan Peraturan Pemerintah yang mengakomodir sifat kekhususan dari bidang teknologi informasi dan komunikasi.

5.2 Rekomendasi

Masih banyaknya kelemahan terhadap pasal – pasal mempunyai kesalahan yang dapat digolongkan fatal di Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dimana harus segera untuk dilakukannya perubahan, pencabutan atau penambahan tafsir terhadap pasal – pasal yang berkaitan dengan tindak pidana siber antara lain yaitu :

a. Pasal – pasal 27 dimana keempat ayat yang terdapat dalam pasal tersebut memiliki kekurangan masing – masing diantaranya unsur unsur pidana yang jelas baik di pasal maupun di penjelasan pasal terutama Pasal 27 ayat (3) dimana pasal ini disebut dengan pasal karet. Kondisi ini tentu harus segera diakhiri, pasal pencemaran nama baik di Undang – Undang No.11 Tahun 2008 haru segera di cabut. Pemerintah harus segera mengagendakan untuk mengajukan Rancangan Undang – Undang Revisi Undang – Undang No, 11 Tahun 2008 yang isi agendanya pencabutan atau perubahan Pasal 27 ayat (3) jika tidak akan menimbulkan banyak korban dimasa akan datang.
b. Adanya pengelompokan perbuatan yang dilarang berbeda – beda ke dalam satu buah pasal tetapi ayat yang berbeda.

c. Adanya pengelompokan ketentuan pidana dalam satu buah pasal tertentu untuk sejumlah jenis perbuatan tindak pidana yang dilarang yang berbeda – beda.
d. Bertitik tolak dari Undang – Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik perlu segera diterbitkan sembilan Peraturan Pemerintah yang seharusnya dibentuk dalam kurun waktu dua tahun setelah Undang – Undang No.11 Tahun 2008 disahkan karena hal ini terdapat dalam Pasal 54 ayat (2), Depkominfo yang sedang mengupayakan untuk menggabungkan beberapa Peraturan Pemerintah yang diamanatkan tersebut menjadi tiga saja yaitu Rancangan Peraturan Pemerintah tentang Penyelenggaraan Informasi dan Transaksi Elektronik, Rancangan Peraturan Pemerintah tentang Tata Cara Intersepsi *(Lawful interception)* dan Rancangan Peraturan Pemerintah tentang Perlindungan Data Strategis. Mengenai pembentukan Peraturan Pemerintah tentang Tata Cara Intersepsi, idelanya ditindaklanjuti dengan pembentukan Peraturan Pemerintah yang lebih menitikberatkan pada pengaturan mengenai tata cara/prosedur/mekanisme saja.

Undang – Undang ini perlu ditinjau kembali agar dilengkapi atau disesuaikan ataupun diubah karena sudah banyak menimbulkan berbagai penafsiran dan beberapa celah hukum didalamnya. Terkait dengan semakin canggihnya modus tindak pidana siber Informasi dan Transaksi Elektronik yang berkembang dengan pesat, para penegak hukum harus terus mengupdate kualitas dan kuantitas kemampuannya dibidang Informasi dan Transaksi Elektronik agar kemampuan penegak hukum tidak tertinggal jauh dibelakang.

DAFTAR PUSTAKA

A. Buku

Arief, Barda Nawawi., Tindak Pidana *Mayantara, Perkembangan Kajian Cyber Crime di Indonesia,* (Jakarta;Raja Grafindo Persada,2007

Bajaj K , Kamlesh & Debjani Nag.*E-Commerce: The Cutting Edge Of Bussiness*.New Delhi: Tat McGraw-Hill Publishig Limited, 2000.

BBasiang , Martin *The Contemporary Law Dictionary* , Indonesia : Red & White Publishing, 2009.

Brenner, Susan W. *" Cybercrime ; re-thingking crime control* strategies",Edited by Yvonne Jewkes, Milan Publishing,2007.

Budhijanto, Danrivanto., *Hukum Telekomunikasi, Penyiaran dan Teknologi Informasi:Regulasi dan Konvergensi*.Bandung; Refika Aditama,2010

Delta, George B.& Jeffrey H. Matsuura, *Law Of The internet*. Aspen Law & Business,2000.

Friedman, Lawrence M.,*Hukum Amerika, Sebuah Pengantar, Terjemahan dari Wishnu Basuki,* Jakarta : Tatanusa, 2001

Liyod, D.Ed.*Introduction to Jurisprudence*. London: Stences, 1965.

Kamus Besar Bahasa Indonesia Pusat Bahasa, Departemen Pendidikan Nasional.Edisi ke-3 Tahun 2008.

Kantaatmadja, Mieke Komar.Et.al. *Cyber Law Suatu Pengantar*.Bandung: Elips, 2001.

M., Dikdik Arief Mansur dan Elisatris Gultom, *Cyber Law Aspek Hukum Teknologi Informasi, Cet-1*. Bandung:PT Refika Aditama,2005

Magdalena, Merry dan Maswigrantoro R. Setyadi, *Cyberlaw,Tidak Perlu Takut.*Yogyakarta:Penerbit Andi,2007

Makarim, Edmon. *Kompilasi Hukum Telematika*.Cet.Ke- 1. Jakarta: Radja Grafindo Persada, 2003.

Marzuki, Peter Mahmud.*Penelitian Hukum*. Cet. Ke-6. Jakarta: Kencana, 2010.

Nazir, M.*Metode Penelitian*.Jakarta: Ghalia Indah, 1999.

Nitibaskara, Tubagus Rony Rahman. *Ketika Kejahatan Berdaulat , Sebuah Pendekatan Kriminologi, Hukum dan Sosiologi*.Jakarta: Perdaban, 2001.

Nonet, Phillippe& Phillip Selznick. *Law and Society in Transition: Toward Tanggapanive Law*.London: Harper and Row Publisher, 1978.

Poerwadarminta, W.J.S *Kamus Umum Bahasa Indonesia*, Jakarta; Balai Pustaka, 1999

Rahardjo, Agus. *Cybercrime, Pemahaman dan Upaya Pencegahan Kejahatan Bertekhnologi*.Bandung: PT. Citra Aditya Bakti, 2002.

Rahardjo, Satjipto. *Penegakan Hukum Progresif*, Jakarta: Kompas, 2010.

_____.*Ilmu Hukum*. Bandung: PT. Citra Aditya Bakti, 1996.

_____.*Hukum dan Perubahan Sosial*.Bandung: Alumni, 1983.

Ramli, Ahmad M.*Cyber Law dan HAKI dalam Sistem Hukum Indonesia*. Jakarta: Rafika Aditama, 2004.

Ramelink, Jan. *Hukum Pidana*. Jakarta: Gramedia Pustaka Utama, 2003.

Reksodiputro, Mardjono.*Kejahatan komputer (Suatu catatan sementara dalam rangka KUHP Nasional yang akan datang), dalam Kemajuan Pembangunan Ekonomi dan Kejahatan* .Jakarta : Pusat Pelayanan Keadilan dan Pengabdian Hukum UI, 1997.

Riswandi, Budi Agus.*Hukum Cyberspace*. Yogyakarta: Gita Negeri, 2006.

Sanusi, Arsyad., *Cybercrime*, Jakarta: Milestone Publisher, 2011.

_____.*Hukum dan Teknologi Informasi*, Jakarta:Milestone Publisher,2005

Soekanto, Soerjono.*Pengantar Penelitian Hukum*. Cet. Ke-3. Jakarta: Penerbit Universitas Indonesia (UI Press), 2006.

_____. *Pokok- Pokok Sosiologi Hukum*.Jakarta: Rajawali Press, 1998.

_____.*Faktor – Faktor yang Mempengaruhi Penegakan Hukum.* Cet ke-3. Jakarta: RajaGrafindo Persada, 1993.

_____. dan Sri Mamudji.*Penelitian Hukum Normatif*.Jakarta: Rajawali Press , 1995.

Sudarto.*Pembaharuan Hukum Pidana di Indonesia dalam Simposium Pembaharuan Hukum Pidana Nasional*.Jakarta : Binacipta , 1986.

Sutanto, Hermawan Sulistyo, Tjuk Sugiarso,Ed., *Cybercrime: Motif dan Penindakan,Cet 1*,(Jakarta:Pensil-324,2005.

Syahdeini, Sultan Remy.*Kejahatan & Tindak Pidana Komputer*.Jakarta: Pustaka Utama Grafiti , 2009.

_____.*Kebebasan Berkontrak dan Perlindungan Yang Seimbang Bagi Para Pihak Dalam Perjanjian Kredit Bank Di Indonesia*.Jakarta: Pustaka Utama Grafiti, 2009.

Tanya, Benard L. *Teori Hukum Strategi Tertib Manusia Lintas Ruang dan Generasi*.Yogyakarta: Genta Publishing, 2010.

UNESCO, *The International Demension of Cyberspace Law*,England: Ashgate Publishing Ltd,2000

Wahid , Abdul dan Mohammad Labib.*Kejahatan Mayantara (Cyber Crime).* Bandung: Refika Aditama, 2005.

Wibisono, Ali., *Strategi Penanggulangan Kejahatan Telematika*, Yogyakarta: Atmajaya, 2010.

Widodo, *Sistem Pemidanaan Dalam Cyber Crime, Alternatif Ancaman Pidana Kerja Sosial Dan Pidana Pengawasan Bagi Pelaku Cyber Crime*, Yogyakarta Laskbang Mediatama,2009

Williams,Brian K., Stacey Sawijen and Sarah H. Hurt Chraison in *Using Information Technology, A Practical Introduction to Computer and Communications*, NewYork:Mc-GrawHill, 1989

B. Peraturan Perundang-Undangan.

Indonesia. *Undang-Undang Hukum Pidana Indonesia*.

_____. *Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana Indonesia, Lembaran Negara 1981/76, Tambahan Lembaran Negara Nomor 3209;*

_____. *Undang-Undang tentang Informasi dan Transaksi Elektronik*. UU No. 11 Tahun 2008.

_____.*Undang-Undang tentang Telekomunikasi*. UU No. No. 36 Tahun 1999.

_____. *Undang-Undang tentang Keterbukaan Informasi Publik.* UU No. 14 Tahun 2008.

_____. *Undang-Undang tentang Pornografi*. UU No.44 Tahun 2008.

_____. *Undang-Undang tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang*. UU No. 8 Tahun 2010.

_____. *Rancangan Kitab Undang-Undang Hukum Pidana Indonesia*. 2010.

_____. *Rancangan Undang-Undang Hukum Acara Pidana Indonesia*.2010.

Convention on Cybercrime. Budafest 23.XI.2001.

C. Internet

Shinder, Debra L. "Kategori Kejahatan Cyber".Tersedia di http://www.yahoo.com.

Fox, Susannah, Janna Quitney Anderson dan Lee Rainie."The future of Internet". Tersedia di http://www.pewinternetproject.org/pdfs/PIP_Future_of_internet.pdf (9 Januari 2005).

G-8 Recommendations on Transnational Crime, http://www.justice.gc.ca/en/news/g8/doc1.htm#4d,.

Gema, Ari Juliano.,*Cyber Crime : Sebuah Fenomena di Dunia Maya*,www.theceli.com, 2000.

Goodman,. Marc D dan Susan W.Brenner,*The Emerging Consensus On Criminal Conduct in*

Cyberspace,www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.php

IP/IT-Update. *Domain Names,* http://www.ipit-update.com/dns.htm.

Kementerian Komunikasi dan Informatika Republik Indonesia, Buku Panduan Untuk Memahami UU No.11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik,Seputar UU. No 11 Tahun

2008 Tentang Informasi dan Transaksi Elektronik (UU ITE), www.depkominfo.go.id.

Lastwoka., F.Gregory dan Dan Hunter, *Virtual Crime situs http://papers.ssm.com/sol3/papers.cfm?abstract_id=564801*

National Centre For Missing & Exploited Children, *What Is Child Pornography?*, http://www.missingkids.com/missingkids/servlet/PageServlet?PageId=1504.

Rasch, Mark D. *CriminalLaw and The Internet*, www.cybercrime.net.

Safety, Wired.,*Cyberstalking and Harassment FAQ*, http://www.wiredsafety.org/cyberstalking_harassment/csh0.html.

Shinder , Debra L.,*Kategori Kejahatan Cyber*, http://www.yahoo.com .

http://idtheft.about.com/od/methodsofthef1/p/Skimming.htm?p-1

University of Bristol, *Phising*, http://www.bristol.ac.uk/is/computing/advice/security/protectyou/idtheft/phish.html

U.S Government Accountability Office, *internet Gambling,An Overview of the Issues*, Dec 2002, http://www.gao.gov/new.items/d0389.pdf.

Webopedia, Hacker, http://www.webopedia.com/TERM/h/hacker.html.

Weimann, Gabriel., Cyberterrorism; How Real Is the Threat?. http://www.usip.org/pubs/specialreports/sr119.pdf.

D. Makalah

Badan Pembinaan Hukum Nasional, *Laporan Tim Forum Dialog Hukum dan Non Hukum Kelompok Kerja Bidang Hukum dan Teknologi*, Jakarta: Badan Pembinaan Hukum Nasional Kementerian Hukum dan HAM RI,2004

Direktorat Hukum Bank Indonesia dan Fakultas Hukum UGM."Modus Operandi,Macam dan Jenis Cyber Crimes". Makalah disampaikan pada *Rekonstruksi Hukum dalam Menanggulangi Kejahatan Dunia Maya di Bidang Perbankan*. Yogyakarta , 27 Oktober 2003.

Keyser, Mike "*The Council of Europe Convention On Cybercrime"*, Journal of Transnational Law and Policy, volume12, 2003.

Ramli, Ahmad M.,*Jurnal Tim Perencanaan Pembangunan Hukum Nasional Bidang Teknologi Informasi dan Komunikasi*, (Jakarta : Badan

Pembinaan Hukum Nasional Kementrian Hukum dan HAM RI,2008.

Reksodiputro, Mardjono."Hukum dalam Abad Perkembangan Tekhnologi Informasi".Depok: 1 April 1998.

Suharyo, S.H.,M.H, *Jurnal Tim Penelitian Hukum Tentang Penerapan Bantuan Timbal Balik Dalam Masalah Pidana Terhadap Kasus – Kasus Cybercrime,* (Jakarta : Badan Pembinaan Hukum Nasional Kementrian Hukum dan HAM RI,2010),

Tobing, Raida L., *Jurnal Akhir Penelitian Hukum Tentang Efektifitas Undang – Undang No. 11 tahun 2008 Tentang Informasi dan Transaksi Elektronik,*(Jakarta : Badan Pembinaan Hukum Nasional Kementrian Hukum dan HAM RI,2010)

E. Skripsi dan Tesis

Afitrahim, *Yuridiksi Berdasarkan Convention On Cybercrime*, (Depok: Univeritas Indonesia,2009).

Hikmiyati, Anisah. "Tesis Penentuan Locus Delictie Dalam Cyber Crime Sebagai Usaha Pembaharuan Hukum Pidana Nasional".Jakarta: Universitas Indonesia, 2006.