TINJAUAN YURIDIS PEMBUKTIAN CYBER CRIME DALAM PERSPEKTIF HUKUM POSITIF INDONESIA

SKRIPSI

Untuk Memenuhi Sebagian Syarat-Syarat
Untuk Memperoleh Gelar Kesarjanaan
Dalam Ilmu Hukum

Oleh :

Dwi Rendra Wiratama

0310103048

DEPARTEMEN PENDIDIKAN NASIONAL

FAKULTAS HUKUM

UNIVERSITAS BRAWIJAYA

MALANG

2009

LEMBAR PERSETUJUAN

TINJAUAN YURIDIS PEMBUKTIAN CYBER CRIME
DALAM PERSPEKTIF HUKUM POSITIF INDONESIA

Oleh :
DWI RENDRA WIRATAMA
NIM. 0310103048

Pembimbing Utama,	Pembimbing Pendamping,
Drs. Adami Chazawi, SH., MH	**Bambang Sugiri, SH., MH**
NIP. 130518932	NIP. 131415736

Mengetahui,
Ketua Bagian Hukum Pidana

Setiawan Nurdayasakti, SH., MH
NIP. 131839360

LEMBAR PENGESAHAN

TINJAUAN YURIDIS PEMBUKTIAN CYBER CRIME
DALAM PERSPEKTIF HUKUM POSITIF INDONESIA

Oleh :

DWI RENDRA WIRATAMA

NIM. 0310103048

Skripsi ini disahkan oleh Dosen Pembimbing pada tanggal : .....

Pembimbing Utama,	Pembimbing Pendamping,
Drs. Adami Chazawi, SH., MH	**Bambang Sugiri, SH., MH**
NIP. 130518932	NIP. 131415736
Ketua Majelis Penguji	Ketua Bagian Hukum Pidana
Abdul Madjid,S.H.,M.Hum	**Setiawan Nurdayasakti, SH., MH**
NIP. 131652669	NIP. 131839360

Mengetahui,
Dekan Fakultas Hukum
Universitas Brawijaya

Herman Suryokumoro, S.H, M.S.
NIP : 131472741

KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Tuhan Yang Maha Esa yang telah melimpahkan rahmat dan hidayah-Nya sehingga penulis dapat menyelesaikan skripsi ini. Penulisan skripsi ini diajukan sebagai salah satu syarat untuk menyelesaikan pendidikan program sarjana strata satu pada Jurusan Ilmu Hukum Fakultas Hukum Universitas Brawijaya Malang.

Dalam menyelesaikan skripsi ini, penulis telah banyak mendapat bantuan, arahan dan bimbingan dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis mengucapkan terima kasih yang sebesar-besarnya kepada :

1. Kedua orang tua yang telah mengantarkan saya menggapai cita-cita sampai detik ini dan seterusnya.
2. Bapak Herman Suryokumoro, S.H., M.S. selaku Dekan Fakultas Hukum Universitas Brawijaya.
3. Bapak Setiawan Nurdayasakti, S.H., M.H. selaku Ketua Bagian Hukum Pidana.
4. Bapak Drs. Adami Chazawi, SH., MH. selaku Dosen Pembimbing I, atas bimbingan dan sarannya.
5. Bapak Bambang Sugiri, SH., MH. selaku Dosen Pembimbing II, atas bimbingan dan sarannya.
6. Pihak-pihak lain yang turut membantu selesainya skripsi ini, yang tidak dapat disebutkan satu-persatu.

Akhir kata, penulis mohon maaf yang sebesar-besarnya jika dalam proses pembuatan skripsi ini terdapat kesalahan baik yang disengaja maupun yang tidak disengaja.

Semoga skripsi ini bermanfaat bagi yang memerlukannya.

Malang, 25 Desember 2008

Penulis

DAFTAR ISI

Lembar Persetujuan i

Lembar Pengesahan ii

Kata Pengantar iii

Daftar Isi iv

Abstraksi vi

Bab I PENDAHULUAN

A. Latar Belakang Masalah 1

B. Rumusan Masalah 6

C. Tujuan Penelitian 7

D. Manfaat Penelitian 7

E. Sistematika Penulisan 9

Bab II KAJIAN PUSTAKA

A. Tindak Pidana 11

B. Pengamanan Telekomunikasi Menurut Undang-Undang Nomor 36 Tahun 1999 Tentang Telekomunikasi 13

C. Komputer 14

D. Internet 14

E. Pengertian Informasi, Transaksi Elektronik Dan Dokumen Elektronik Menurut Undang-Undang No. 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik 15

F. Pengertian Pembuktian Dan Hukum Pembuktian 16

G. Pengertian Alat Bukti Menurut Undang-Undang No. 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik 19

H. Kejahatan Dunia Maya 20

I. Bentuk-Bentuk Cyber Crime 22

Bab III METODE PENELITIAN

A. Jenis Penelitian 40
B. Fokus Masalah 40
C. Bahan-Bahan Hukum 41
D. Teknik Pengumpulan Data 42
E. Teknik Analisa 42

Bab IV PEMBAHASAN

A. Gambaran Umum Tentang Cyber Crime 43
B. Kendala-Kendala Yuridis Yang Dihadapi Oleh Perangkat Hukum Di Indonesia Dalam Menangani Para Pelaku Kejahatan Dunia Maya Terkait Dengan Masalah Pembuktian 51
C. Upaya-Upaya Yuridis Yang Dapat Dilakukan Terkait Dengan Masalah Pembuktian Oleh Perangkat Hukum Di Indonesia 52

Bab V PENUTUP

A. Kesimpulan 63
B. Saran 64

DAFTAR PUSTAKA 66

ABSTRAKSI

Dwi Rendra Wiratama, Hukum Pidana, Fakultas Hukum Universitas Brawijaya, Februari 2007, **TINJAUAN YURIDIS PEMBUKTIAN CYBER CRIME DALAM PRESPEKTIF HUKUM POSITIF INDONESIA,** Drs. Adami Chazawi, SH.,MH., Bambang Sugiri, SH.,MH.

Penulisan skripsi ini dilatar belakangi oleh sulitnya lembaga hukum seperti pengadilan dan kepolisian dalam melaksanakan proses penyidikan, ksususnya dalam hal pembuktian cyber crime. Mengingat sarana dan prasarana yang dimiliki oleh lembaga hukum kita kurang memenuhi standart kelayakan dalam kasus cyber crime. Selain itu, kurangnya tenaga ahli yang bekerja dalam lembaga-lembaga hukum di Indonesia juga merupakan kesulitan dalam mencegah, maupun mengatasi permasalahan yang berkaitan dengan cyber crime.

Berdasarkan hal-hal tersebut, maka dirumuskan permasalahan mengenai kendala-kendala yang dihadapi oleh pengadilan untuk menangani para pelaku Kejahatan dunia Maya terkait dengan masalah pembuktian *Cyber Crime* tersebut, dan upaya-upaya apa saja yang dapat dilakukan untuk mengatasi masalah-masalah yang terkait dengan proses pembuktian dalam tindak pidana *Cyber Crime* yang dapat dilakukan oleh pengadilan sesuai dengan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

Dalam penulisan skripsi, penulis menggunakan metode penelitian dengan pendekatan normatif, tinjauan yuridis normatif, yaitu dengan melakukan identifikasi terhadap isu-isu hukum yang bekembang dalam masyarakat, mengkaji penerapan-penerapan hukum dalam masyarakat, mengkaji pendapat para ahli-ahli hukum terkait dan analisa kasus dalam dokumen-dokumen untuk memperjelas hasil penelitian, kemudian ditinjau aspek praktis dan aspek akademis keilmuan hukumnya dalam penelitian hukum.

BAB I

PENDAHULUAN

A. LATAR BELAKANG MASALAH

Keunggulan komputer berupa kecepatan dan ketelitiannya dalam menyelesaikan pekerjaan sehingga dapat menekan jumlah tenaga kerja, biaya serta memperkecil kemungkinan melakukan kesalahan, mengakibatkan masyarakat semakin mengalami ketergantungan kepada komputer. Dampak negatif dapat timbul apabila terjadi kesalahan yang ditimbulkan oleh peralatan komputer yang akan mengakibatkan kerugian besar bagi pemakai (*user*) atau pihak-pihak yang berkepentingan. Kesalahan yang disengaja mengarah kepada penyalahgunaan komputer.[1]

Usaha mewujudkan cita-cita hukum (*rechtside*) untuk mensejahterakan masyarakat melalui kebijakan hukum pidana tidak merupakan satu-satunya cara yang memiliki peran paling strategis. Dikatakan demikian karena hukum pidana hanya sebagai salah satu dari sarana kontrol masyarakat (sosial).

Teknologi informasi dan komunikasi telah mengubah perilaku mayarakat dan peradaban manusia secara global. Di samping itu, perkembangan teknologi informasi telah menyebabkan dunia menjadi tanpa batas *(borderless)* dan menyebabkan perubahan sosial yang 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 arena efektif perbuatan melawan hukum.

---

[1] **Andi Hamzah**, 1990, *Aspek-aspek Pidana di Bidang Komputer*, Sinar Grafika, Jakarta, hal. 23-24.

Saat ini telah lahir suatu rezim hukum baru yang dikenal dengan Hukum Siber, yang diambil dari kata *Cyber Law* adalah istilah hukum yang terkait dengan pemanfaatan teknologi informasi.[2] Istilah lain yang digunakan adalah Hukum Teknologi Informasi *(Law Of Information Technology)*, Hukum Dunia Maya *(Virtual World Law)* dan hukum Mayantara. Itilah-itilah tersebut lahir mengingat kegiatan internet dan pemanfaatan teknologi informasi berbaris *virtual*. Istilah hukum siber digunakan dalam tulisan ini dilandasi pemikiran bahwa *cyber* jika diidentikan dengan *"Dunia Maya"* akan cukup menghadapi persoalan jika harus membuktikan suatu persoalan yang diasumsikan sebagai "maya", sesuatu yang tidak terlihat dan semu.

[3]Terdapat tiga pendekatan untuk mempertahankan keamanan di *cyberspace*, *pertama* adalah pendekatan teknologi, *kedua* pendekatan sosial budaya-etika, dan *ketiga* pendekatan hukum. Untuk mengatasi keamanan gangguan pendekatan teknologi sifatnya mutlak dilakukan, sebab tanpa suatu pengamanan jaringan akan sangat mudah disusupi, diintersepsi, atau diakses secara ilegal dan tanpa hak.

Melihat fakta hukum sebagaimana yang ada pada saat ini, dampak perkembangan ilmu pengetahuan dan teknologi yang telah disalah gunakan sebagai sarana kejahatan ini menjadi teramat penting untuk diantisipasi bagaimana kebijakan hukumnya, sehingga *Cyber Crime* yang terjadi dapat dilakukan upaya penanggulangannya dengan hukum pidana, termasuk dalam hal ini adalah mengenai sistem pembuktiannya. Dikatakan teramat penting

---

[2] Akta Komunikasi dan Multimedia 1998, Akta Tanda Tangan Digital 1997, (Akta 562), Akta Jenayah Komputer 1997 (563), dan Akta Teleperubahan 1997 (564), Mohd. Safar Hasim, mengenali Undang-undang Media Dan Siber, Utusan Publications& Distributors SdnBhd,2002, hlm. 118-dst.

[3] **Prof. Dr. Ahmad M Ramli, SH.MH,** *Prinsip-prisnsip Cyber Law Dan kendala Hukum Positif Dalam Menanggulangi Cyber Crime*, Fakultas Hukum Universitas Padjajaran,2004, hlm. 2.

karena dalam penegakan hukum pidana dasar pembenaran seseorang dapat dikatakan bersalah atau tidak melakukan tindak pidana, di samping perbuatannya dapat dipersalahkan atas kekuatan Undang-undang yang telah ada sebelumnya (asas legalitas), juga perbuatan mana didukung oleh kekuatan bukti yang sah dan kepadanya dapat dipertanggungjawabkan (unsur kesalahan). Pemikiran demikian telah sesuai dengan penerapan asas legalitas dalam hukum pidana (KUHP) kita, yakni sebagaimana dirumuskan secara tegas dalam Pasal 1 ayat (1) KUHP " Nullum delictum nulla poena sine praevia lege poenali" atau dalam istilah lain dapat dikenal, " tiada pidana tanpa kesalahan".

Bertolak dari dasar pembenaran sebagaimana diuraikan di atas, bila dikaitkan dengan *Cyber Crime*, maka unsur membuktikan dengan kekuatan alat bukti yang sah dalam hukum acara pidana merupakan masalah yang tidak kalah pentingnya untuk diantisipasi di samping unsur kesalahan dan adanya perbuatan pidana. Akhirnya dengan melihat pentingnya persoalan pembuktikan dalam *Cyber Crime*, makalah ini hendak mendeskripsikan pembahasan dalam fokus masalah Hukum Pembuktian terhadap *Cyber Crime* dalam Hukum Pidana Indonesia.

Oleh karena alasan-alasan tersebut di atas, bagaimana pembuktian-pembuktian dalam *Cyber Crime* cukup sulit dilakukan mengingat, bahwa hukum di Indonesia yang mengatur masalah ini masih banyak cacat hukum yang dapat dimanfaatkan oleh para pelaku *Cyber Crime* untuk lepas dari proses pemidaan.

[4]Bentuk-bentuk Cyber Crime pada umumnya yang dikenal dalam masyaakat dibedakan menjadi 3 (tiga) kualifikasi umum, yaitu :

a. Kejahatan Dunia Maya yang berkaitan dengan kerahasiaan, integritas dan keberadaan data dan sistem komputer

- *Illegal access* (akses secara tidak sah terhadap sistem komputer)
- *Data interference* (mengganggu data komputer)
- *System interference* (mengganggu sistem komputer)
- *Illegal interception in the computers, systems and computer networks operation* (intersepsi secara tidak sah terhadap komputer, sistem, dan jaringan operasional komputer)
- *Data Theft* (mencuri data)
- *Data leakage and espionage* (membocorkan data dan memata-matai)
- *Misuse of devices* (menyalahgunakan peralatan komputer)

b. Kejahatan Dunia Maya yang menggunakan komputer sebagai alat kejahatan

- *Credit card fraud* (penipuan kartu kredit)
- *Bank fraud* (penipuan terhadap bank)
- *Service Offered fraud* (penipuan melalui penawaran suatu jasa)
- *Identity Theft and fraud* (pencurian identitas dan penipuan)
- *Computer-related fraud* (penipuan melalui komputer)
- *Computer-related forgery* (pemalsuan melalui komputer)
- *Computer-related betting* (perjudian melalui komputer)

---

[4] **Natalie D Voss**, Copyright © 1994-99 Jones International and Jones Digital Century, "*Crime on The Internet*", Jones Telecommunications & Multimedia Encyclopedia. http://www.digitalcentury.com/encyclo/*update/articles.html*

- *Computer-related Extortion and Threats* (pemerasan dan pengancaman melalui komputer)

c. Kejahatan Dunia Maya yang berkaitan dengan isi atau muatan data atau sistem komputer

- *Child pornography* (pornografi anak)
- *Infringements Of Copyright and Related Rights* (pelanggaran terhadap hak cipta dan hak-hak terkait)
- *Drug Traffickers* (peredaran narkoba), dan lain-lain.

Kegiatan siber meskipun bersifat virtual dapat dikategorikan sebagai tindakan dan perbuatan hukum yang nyata. Secara yuridis dalam hal ruang siber sudah tidak pada tempatnya lagi untuk kategorikan sesuatu dengan ukuran dalam kualifikasi hukum konvensional untuk dijadikan obyek dan perbuatan, sebab jika cara ini yang ditempuh akan terlalu banyak kesulitan dan hal-hal yang lolos dari jerat hukum. Kegiatan siber adalah kegiatan virtual yang berdampak sangat nyata, meskipun alat buktinya bersifat elektronik. Dengan demikian, subyek pelakunya harus dikualifikasikan pula sebagai orang yang telah melakukan perbuatan hukum secara nyata.[5]

Penggunaan hukum pidana dalam mengatur masyarakat (lewat peraturan perundang-undangan pidana) pada hakekatnya merupakan bagian dari suatu langkah kebijakan (*policy*). Selanjutnya untuk menentukan bagaimana suatu langkah (usaha) yang rasional dalam melakukan kebijakan tidak dapat pula dipisahkan dari tujuan kebijakan pembangunan itu sendiri secara integral. Dengan demikian dalam usaha untuk menentukan suatu kebijakan apapun (termasuk kebijakan hukum pidana) selalu terkait dan tidak

[5] Pasal 5 Undang-undang Nomor 11 Tahun 2008 tentang informasi dan transaksi elektronik (UU ITE), Kementrian komunikasi dan informasi RI.

terlepaskan dari tujuan pembangunan nasional itu sendiri; yakni bagaimana mewujudkan kesejahteraan bagi masyarakat.

Selain itu, perkembangan hukum di Indonesia terkesan lambat, karena hukum hanya akan berkembang setelah ada bentuk kejahatan baru. Jadi hukum di Indonesia tidak ada kecenderungan yang mengarah pada usaha preventif atau pencegahan, melainkan usaha penyelesaiannya setelah terjadi suatu akibat hukum. Walaupun begitu, proses perkembangan hukum tersebut masih harus mengikuti proses yang sangat panjang, dan dapat dikatakan, setelah negara menderita kerugian yang cukup besar, hukum tersebut baru disahkan.

Kebijakan hukum nasional kita yang kurang bisa mengikuti perkembangan kemajuan teknologi tersebut, justru akan mendorong timbulnya kejahatan-kejahatan baru dalam masyarakat yang belum dapat dijerat dengan menggunakan hukum yang lama. Padahal negara sudah terancam dengan kerugian yang sangat besar, namun tidak ada tindakan yang cukup cepat dari para pembuat hukum di Indonesia untuk mengatasi masalah tersebut.

B. RUMUSAN MASALAH

1. Apakah kendala-kendala yuridis apa saja yang dihadapi oleh Perangkat hukum di Indonesia untuk menangani para pelaku Kejahatan dunia Maya terkait dengan masalah pembuktian *Cyber Crime* tersebut?
2. Upaya-upaya apa saja yang dapat dilakukan untuk mengatasi masalah-masalah yang terkait dengan proses pembuktian dalam tindak pidana *Cyber Crime* yang dapat dilakukan oleh Perangkat Hukum Di Indonesia?

C. TUJUAN PENELITIAN

1. Untuk Mengetahui, apakah hukum positif Indonesia sudah mampu untuk menjerat para pelaku Kejahatan Dunia Maya (*Cyber Crime*), karena sebenarnya Kejahatan Dunia Maya telah memenuhi unsur-unsur obyektif dan subyektif dalam Hukum Positif Indonesia.
2. Untuk mengetahui kendala yuridis apa saja yang dihadapi oleh pengadilan dalam menanggulangi *Cyber Crime*, serta kendala-kendala pengadilan dalam melakukan proses penyidikan terkait dengan pengumpulan alat-alat bukti Kejahatan Dunia Maya (*Cyber Crime*).
3. Untuk mengetahui upaya-upaya yang dapat dilakukan oleh pengadilan dalam melakukan proses pembuktian pada para pelaku tindak pidana *Cyber Crime*, mengingat sulitnya proses pemidaan terkait dengan sedikitnya alat bukti dalam tindak pidana tersebut.

D. MANFAAT PENELITIAN

Manfaat dari penelitian ini adalah :

1. Manfaat Teoritis :

   Secara teori dapat menambah ilmu pengetahuan mengenai *Cyber Crime* yang dapat melampaui belahan dunia manapun dan siapapun, karena para pelaku kejahatan ini bersifat internasional. Selain itu dapat memasu perkembangan ilmu hukum dalam menciptakan hukum, khususnya bidang hukum pidana, dengan pengaplikasian yang mudah dijangkau bagi semua kalangan.

2. Manfaat Praktis :

   a. Bagi Pemerintah (kepolisian, dinas sosial, dan Kejaksaan Negeri) :

      - Perlu adanya suatu bentuk sosialisasi hukum dan pelaksanaannya secara menyeluruh dan merata, khususnya pada kalangan muda yang bergelut di bidang yang memiliki tingkat intensitas tinggi dengan hal-hal yang mendekati perbuatan melawan hukum.
      - Pemberian struktur keamanan lebih pada segala mediasi yang mendukung terjadinya tindak pidana *Cyber Crime*, agar dapat mengurangi jumlah angka tindak pidana ini.

   b. Bagi para pelaku tindak pidana *Cyber Crime* :

      - Bagi pelaku kejahatan komputer, bahwa kejahatan yang mereka lakukan dapat dijerat dengan pidana yang cukup berat, karena pihak yang dirugikan cukup banyak, termasuk negara-negara di dunia. Oleh karena itu dibutuhkan banyak pengetahuan bagi mereka tentang hukum positif Indonesia.

   c. Bagi kalangan masyarakat umum :

      - Untuk memberi pengetahuan lebih tentang hukum positif Indonesia, karena selama ini masyarakat cenderung tidak peduli selama dirinya tidak dirugikan. Sebenarnya, secara tidak langsung masyarakat awam juga ikut dirugikan, dengan adanya kerugian yang dialami oleh negara, baik secara materiil, maupun moril.

E. SISTEMATIKA PENULISAN

Dalam sub bab ini diberikan gambaran yang jelas dan terarah mengenai penyusunan laporan skripsi. Berikut dikemukakan sistematika dan alur pembahasan yang terbagi dalam :

BAB I : PENDAHULUAN

Berisi tentang latar belakang dari permasalahan-permasalahan yang ditimbulkan dari Kejahatan Dunia Maya (*Cyber Crime*), khususnya dalam proses pembuktiannya. Selain itujuga berisi perumusan masalah, tujuan dan kegunaan serta metode analisis data yang dilakukan dalam penulisan skripsi.

BAB II : KAJIAN PUSTAKA

Dalam Bab ini diuraikan tentang pengertian dari pembuktian secara umum dan khusus, Kejahatan Dunia Maya (*Cyber Crime*), dan hukum-hukumnya, serta bentuk-bentuk dari Kejahatan Dunia Maya berikut dengan pengertiannya.

BAB III : METODE PENELITIAN

Dalam bab ini akan dijelaskan mengenai jenis metode pendekatan yang digunakan oleh peneliti dalam melakukan penelitian, penelitian ini dilakukan dengan menggunakan pendekatan normatif, tinjauan yuridis normatif, yaitu dengan mengkaji literatur-literatur yang berkaitan, pendapat para ahli-ahli hukum terkait dan analisa kasus dalam dokumen-dokumen untuk memperjelas hasil penelitian.

BAB IV : PEMBAHASAN

Dalam bab ini akan dibahas mengenai kedudukan Kejahatan Dunia Maya dalam Hukum Positif di Indonesia. Selain itu juga akan dibahas tentang permasalahan-permasalahan yang ditimbulkan oleh Kejahatan Dunia Maya (*Cyber Crime*) terkait dengan proses pemidaan, apakah dapat dijerat dengan menggunakan hukum yang berlaku saat ini.

BAB V : PENUTUP

Dalam bab ini akan berisi kesimpulan dari hasil pembahasan bab-bab sebelumnya dan berisi saran-saran yang diharapkan dapat menjadi masukan yang berguna dan bermanfaat bagi instansi yang terkait.

DAFTAR PUSTAKA

BAB II

KAJIAN PUSTAKA

A. TINDAK PIDANA

Tindak pidana berasal dari suatu istilah dalam hukum belanda yaitu *strafboarfeit*. Ada pula yang mengistilahkan menjadi *delict* yang berasal dari bahasa latin *delictum*. Hukum pidana negara *anglo saxon* memakai istilah *offense atau criminal act.*

Oleh karena itu KUHP Indonesia bersumber pada Wetbook van strafrecht Belanda, maka memakai istilah aslinya pun sama yaitu *Strafboarfeit.*[6]

Strafboarfeit telah diterjemahkan dalam bahasa indonesia sebagai:

i. Perbuatan yang dapat atau oleh dihukum.
ii. Peristiwa pidana.
iii. Perbuatan pidana.
iv. Tindak pidana dan
v. Delik.[7]

Kemudian pemakaian istilah tindak pidana dan kejahatan seringkali mengalami kerancuan dan tumpang tindih dalam pemakaian istilah ini. Seperti yang telah dijelaskan di atas bahwa istilah yang dipakai dalam rumusan pasal pasal yang ada dalam rumusan KUHP adalah istilah tindak pidana, walaupun buku II bertitel kejahatan. Dalam hukum pidana sendiri istilah tindak pidana dikenal dengan strafbarfeit dan memiliki penjelasan yang berbeda beda akan tetapi intinya sama yaitu peristiwa pidana atau sebagai tindak pidana. Menurut Van Hamel,

---

6 **Andi hamzah,** 1994, *Asas-Asas Hukum Pidana*, Rineka Cipta, Jakarta, hal 84

7 **S.R Sianturi,** *Asas Hukum Pidana Di Indonesia dan Penerapannya*, Alumni Ahaem Pelete

strafbarfeit adalah kelakuan orang yang dirumuskan dalam *wet* atau undang-undang yang bersifat melawan hukum yang patut dipidana (*strafwaardig*) dan dilakukan dengan kesalahan[8].

Menurut P. Simons yang menggunakan istilah peristiwa pidana adalah perbuatan atau tindakan yang diancam dengan pidana oleh Undang-undang, bertentangan dengan hukum dan dilakukan oleh orang yang mampu bertanggung jawab. Simon memandang semua syarat untuk menjatuhkan pidana sebagai unsur tindak pidana dan tidak memisahkan unsur yang melekat pada perbuatannya *(crime act)* tindak pidana dengan unsur yang melekat pada aliran tindak pidana *(criminal responsibility* atau *criminal liability* atau pertanggung jawaban pidana). Kemudian dia menyebut unsur unsur tindak pidana, yaitu perbuatan manusia, diancam dengan pidana, melawan hukum, dilakukan dengan kesalahan, oleh orang yang mampu bertanggung jawab

Unsur-unsur tersebut oleh simon dibedakan antara unsur obyektif dan unsur subyektif. Yang termasuk unsur obyektif adalah : Perbuatan orang, akibat yang kelihatan dari perbuatan itu, dan kemungkinan adanya keadaan tertentu yang menyertainya. Unsur subyektif adalah orang yang mampu bertanggung jawab dan adanya kesalahan[9].

Moeljatno memberikan pengertian tentang perbuatan pidana adalah perbuatan yang dilarang oleh suatu aturan hukum larangan mana disertai ancaman (sanksi) yang berupa pidana tertentu, barang siapa melanggar larangan tersebut. Larangan tersebut ditujukan kepada perbuatan, sedangkan ancaman pidananya

---

8 **Moeljatno,** 1987, *Asas-Asas Hukum Pidana*, Bina Aksara, Jakarta, hal 56

9 **Masruchin Ruba'i - Made S. Astuti Djajuli,** 1989, *Hukum pidana I*, Malang, hal 35

ditujukan pada orang yang menimbulkan kejadian itu[10]. Moeljatno memisahkan antara *criminal act* dan *criminal responsibility* yang menjadi unsur tindak pidana.

Menurut Moeljatno hanyalah unsur-unsur yang melekat pada *criminal act* (perbuatan yang dapat dipidana). Sedangkan yang termasuk unsur-unsur tindak pidana adalah perbuatan (manusia), memenuhi rumusan Undang-undang, bersifat melawan hukum

B. PENGAMANAN TELEKOMUNIKASI MENURUT UNDANG-UNDANG NOMOR 36 TAHUN 1999 TENTANG TELEKOMUNIKASI

Pasal 40 Undang-undang No. 3 Tahun 1999 Tentang Telekomunikasi:

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

Ketentuan Pidana Pasal 40 tersebut, selanjutnya diatur dalam Pasal 56 Undang-undang No. 36 tahun 1999 Tentang Telekomunikasi :

> *"Barang siapa melanggar ketentuan sebagaimana dimaksud dalam pasal 40, dipidana dengan pidana penjara paling lama 15 (lima belas) tahun."*

Unsur Obyektifnya adalah :

- Mengambil data atau informasi
- Menggunakan data atau informasi
- Seluruhnya atau sebagian kepunyaan orang lain

Unsur Subyektif adalah :

- Secara melawan hukum

[10] **Moeljatno,** *Op Cit*, Hal 59

C. KOMPUTER

Institut Komputer Indonesia mendefinisikan komputer sebagai berikut: "Suatu rangkaian peralatan-peralatan dan fasilitas yang bekerja secara elektronis, bekerja dibawah kontrol suatu *operating system*, melaksanakan pekerjaan berdasarkan rangkaian instruksi-instruksi yang disebut program serta mempunyai internal storage yang digunakan untuk menyimpan *operating system*, program dan data yang diolah."[11]

Operating system berfungsi untuk mengatur dan mengkontrol sumber daya yang ada, baik dari hardware berupa komputer, *Central Processing Unit* (CPU) dan *memory/storage* serta *software* komputer yang berupa program-program komputer yang dibuat oleh *programmer*. Jenis-jenis *Operating System* antara lain PC-DOS (Personal Computer Disk Operating System), MS-DOS (Microsoft Disk Operating System), Unix, Microsoft Windows, dan lain-lain.

D. INTERNET

Internet adalah Sistem informasi global yang menghubungan berbagai jaringan komputer secara bersama-sama dalam suatu ruang global berbasis Internet Protocol.

Internet merupakan jaringan luas dari komputer yang lazim disebut dengan *Worldwide network*. Internet merupakan jaringan komputer yang terhubung satu sama lain melalui media komunikasi, seperti kabel telepon, serat optik, satelit ataupun gelombang frekuensi. Jaringan komputer ini dapat berukuran kecil seperti *Lokal Area Network* (LAN) yang biasa dipakai secara intern di kantor-kantor,

---

[11] **Institut Komputer Indonesia (IKI), 1981**, *Pengenalan Komputer (Introduction to Computer)*, hal. 1, dikutip dari Andi Hamzah, Loc. cit..

bank atau perusahaan atau biasa disebut dengan intranet, dapat juga berukuran superbesar seperti internet.[12]

The Federal Networking Council (FNC) memberikan definisi mengenai internet dalam resolusinya tanggal 24 Oktober 1995 sebagai berikut:

"Internet refers to the global information system that –

i. is logically linked together by a globally unique address space based in theInternet Protocol (IP) or its subsequent extensions/follow-ons;

ii. is able to support communications using the Transmission ControlProtocol/Internet Protocol (TCP/IP) suite or its subsequent extension/followons,and/or other Internet Protocol)IP)-compatible protocols; and

iii. Providers, uses or makes accessible, either publicly or privately, high levelservices layered on the communications and related infrastructure described herein."[13]

E. PENGERTIAN INFORMASI, TRANSAKSI ELEKTRONIK DAN DOKUMEN ELEKRONIK MENURUT UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK (UU ITE)

Dalam ketentuan umum Pasal 1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik disebutkan, bahwa Informasi elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, electronic data

---

12 **Agus Raharjo**, 2002, *Cybercrime*, PT Citra Aditya Bakti, Bandung, hal. 59.

13 ***Ibid.,*** hal. 60

interchange (EDI), surat elektronik (electronic mail), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol, atau perforasi yang telah dioleh yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.

Sedangkan Transaksi Elektronik adalah perbuatan hukum yang dilakukan menggunakan Komputer, jaringan Komputer, dan/atau media elektronik lainnya. Dokumen Elektronik adalah setiap informasi elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui komputer atau sistem elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, kode akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.

F. PENGERTIAN PEMBUKTIAN DAN HUKUM PEMBUKTIAN

Menurut R. Subekti, membuktikan ialah meyakinkan hakim tentang kebenaran dalil atau dalil-dalil yang dikemukakan dalam suatu persengketaan. Lebih lanjut dikatakan bahwa pembuktian itu hanyalah diperlukan dalam persengketaan atau perkara dimuka Hakim atau Pengadilan. Kemudian menurut Sudikno Mertokusumo menerangkan bahwa pembuktian mengandung beberapa pengertian, yaitu arti logis, konvensional dan yuridis.

Membuktikan dalam arti logis adalah memberikan kepastian dalam arti mutlak, karena berlaku bagi setiap orang dan tidak memungkinkan adanya bukti lawan. Untuk membuktikan dalam arti konvensional, disinipun membuktikan

berarti juga memberikan kepastian, hanya saja bukan kepastian mutlak, melainkan kepastian nisbi atau relatif sifatnya. Dan membuktikan dalam arti yuridis berarti memberi dasar yang cukup kepada hakim yang memeriksa perkara yang bersangkutan guna memberi kepastian tentang kebenaran peristiwa yang diajukan. Dengan demikian membuktian adalah suatu cara yang diajukan oleh pihak yang berperkara dimuka persidangan atau pengadilan untuk memberikan dasar keyakinan bagi hakim tentang kepastian kebenaran suatu peristiwa yang terjadi.

[14]Hukum Pembuktian adalah merupakan sebagian dari hukum acara pidana yang mengatur macam-macam alat bukti yang sah menurut hukum, sistem yang dianut dalam pembuktian, syarat-syarat dan tata cara mengajukan bukti tersebut serta kewenangan hakim untuk memerima, menolak dan menilai suatu pembuktian.

Sumber hukum pembuktian adalah undang-undang, doktrin atau ajaran, dan jurisprudensi. Karena hukum pembuktian bagian dari hukum acara pidana, maka sumber hukum yang pertama adalah Undang-undang nomor 8 Tahun 1981, Tentang Hukum Acara Pidana atau KUHAP. Lembaran Negara Republik Indonesia Tahun 1981 Nomor 76 dan penjelasannya yang dimuat dalam Tambahan Lembaran Negara Republik Indonesia Nomor 3209.

Apabila di dalam praktik menemui kesulitan dalam penerapannya atau menjumpai kekurangan atau untuk memenuhi kebutuhan maka dipergunakan doktrin atau yurisprudensi.

Alat bukti adalah segala seuatu yang ada hubungannya dengan suatu perbuatan, dimana dengan alat-alat bukti tersebut, dapat dipergunakan sebagai

[14] **Drs. Sasangka, SH., MH. dan Lily Rosita, SH., MH,** 2003, Hukum Pembuktian Dalam Perkara Pidana, Bandung. Hal 10.

bahan pembuktian guna menbimbulkan keyakinan hakim atas kebenaran adanya suatu tindak pidana yang telah dilakukan oleh terdakwa.

Sistem pembuktian adalah pengaturan tentang macam-macam alat bukti yang boleh dipergunakan, penguraian alat bukti dan dengan cara-cara bagaimana alat bukti tersebut dipergunakan dan dengan cara bagaimana hakim harus membentuk keyakinannya.

Tujuan dan guna pembuktian bagi para pihak yang terlibat dalam proses pemeriksaan persidangan adalah :

a. Bagi penuntut umum, pembuktian adalah merupakanusaha untuk meyakinkan hakim yakni berdasarkan alat bukti yang ada, agar menyatakan seorang terdakwa bersalah sesuai dengan surat atau catatan dakwaan.

b. Bagi terdakwa atau penasehat hukum, pembuktian merupakan usaha sebaliknya, untuk meyakinkan hakim, yakni berdasarkan alat bukti yang ada, agar menyatakan terdakwa dibebaskan atau dilepaskan dari tuntutan hukum atau meringankan pidananya. Untuk itu terdakwa atau penasehat hukum jika mungkin harus mengajukan alat-alat bukti yang menguntungkan atau meringankan pihaknya. Biasanya bukti tersebut di sebut bukti kebalikan.

c. Bagi hakim atas dasar pembuktian tersebut yakni dengan adanya alat-alat bukti yang ada dalam persidangan baik yang berasal dari penuntut umum atau penasehat hukum/terdakwa dibuat dasar untuk membuat keputusan.

[15]Bahwa pada dasarnya seluruh kegiatan dalam proses hukum penyelesaian perkara pidana, sejak penyidikan sampai putusan akhir diucapkan di muka persidangan oleh majelis hakim adalah berupa kegiatan yang berhubungan dengan pembuktian atau kegiatan untuk membuktikan. Walaupun hukum pembuktian perkara pidana terfokus pada proses kegiatan pembuktian di sidang pengadilan, tetapi sesungguhnya proses membuktikan sudah ada dan dimulai pada saat penyidikan. Bahkan, pada saat penyelidikan, suatu pekerjaan awal dalam menjalankan proses perkara pidana oleh negara.

Menurut Drs. Adami Chazawi, SH.,MH., yang dimaksud dengan mencari bukti sesungguhnya adalah mencari alat bukti, karena bukti tersebut hanya terdapat atau dapat diperoleh dari alat bukti dan termasuk barang bukti. Bukti yang terdapat pada alat bukti itu kemudian dinilai oleh pejabat penyelidik untuk menarik kesimpulan, apakah bukti yang ada itu menggambarkan suatu peristiwa yang diduga tindak pidana ataukan tidak. Bagi penyidik, bukti yang terdapat dari alat bukti itu dinilai untuk menarik kesimpulan, apakakah dari bukti yang ada itu sudah cukup untuk membuat terang tindak pidana yang terjadi dan sudah cukup dapat digunakan untuk menemukan tersangkanya.

G. PENGERTIAN ALAT BUKTI MENURUT UNDANG - UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK

Dalam Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik pasal 5 ayat 1 dan 2 mendeskripsikan bahwa Dokumen

[15] **Adami Chazawi**, 2006, Hukum Pembuktian Tindak Pidana Korupsi, hal 13.

elektronik dan Informasi Elektronik adalah merupakan alat bukti yang sah. Selain dalam pasal 44 Undang-undang yang sama mengatakan :

"Alat bukti penyidikan, penuntutan dan pemeriksaan di sidang pengadilan menurut ketentuan Undang-Undang ini adalah sebagai berikut :

a. alat bukti sebagaimana dimaksud dalam ketentuan Perundang-undangan; dan

b. alat bukti lain berupa Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud dalam Pasal 1 angka 1 dan angka 4 serta Pasal 5 ayat (1), ayat (2), dan ayat (3)."

H. KEJAHATAN DUNIA MAYA (*CYBER CRIME*)

Kejahatan adalah perbuatan merugikan orang lain dan/atau sekelompok orang dan/atau instasi yang dilakukan dengan bertujuan untuk menguntungkan diri sendiri, baik secara materi maupun kejiwaannya. Kejahatan dapat dilakukan dengan menggunakan fasilitas apapun sebagai alat untuk nelakukan perbuatannya, termasuk di dalamnya adalah perangkat Informasi dan Transaksi Elektronik, contohnya seperti komputer, *credit card*, televisi, dan lain sebagainya.

Istilah *cyberspace* muncul pertama kali dari novel William Gibson berjudul Neuromancer pada tahun 1984[16]. Istilah *cyberspace* pertama kali digunakan untuk menjelaskan dunia yang terhubung langsung *(online)* ke internet oleh Jhon Perry Barlow pada tahun 1990.

Secara etimologis, *istilah cyberspace* sebagai suatu kata merupakan suatu istilah baru yang hanya dapat ditemukan di dalam kamus mutakhir. Cambridge

[16] **William Gibson**, 1984, *Neuromancer*, New York:Ace, hal. 51, dikutip dari Agus Raharjo, op.cit., hal. 92-93.

Advanced Learner's Dictionary memberikan definisi *cyberspace* sebagai *"the Internet considered as an imaginary area without limits where you can meet people and discover information about any subject"*[17]. *The American Heritage Dictionary of English Language Fourth Edition* mendefinisikan cyberspace sebagai "*the electronic medium of computer networks, in which online communication takes place*"[18]. Pengertian *cyberspace* tidak terbatas pada dunia yang tercipta ketika terjadi hubungan melalui internet. Bruce Sterling mendefinisikan *cyberspace* sebagai *the 'place' where a telephone conversation appears to occur*[19].

Kejahatan Dunia Maya (*Cyber Crime*) merupakan suatu tindak kejahatan atau perbuatan melawan hukum yang dilakukan dengan menggunakan mediasi dunia maya atau *Virtual World*, salah satunya adalah melalui internet. Perbuatan melawan hukum dalam dunia maya sangat tidak mudah untuk diatasi dengan mengandalkan hukum positif konvensional. Indonesia saat ini sudah merefleksikan diri dengan negara-negara lain seperti Malaysia, Singapura, India, atau negara-negara maju seperti Amerika Serikat, dan negara-negara Uni Eropa yang secara serius mengintegrasikan regulasi Hukum Siber ke dalam instrumen hukum positif nasionalnya.[20]

Cyber Law atau disebut juga Hukum Siber adalah hukum yang mengatur tentang kejahatan dunia maya, yang secara internasional digunakan untuk istilah hukum yang terkait dengan pemanfaatan teknologi informasi yang tidak bertanggung jawab. Sebutan Hukum Siber di beberapa negara lain adalah *Law Of*

---

17 **http://dictionary.cambridge.org**

18 **http://www.bartleby.com**

19 **Bruce Sterling, 1990**, *The Hacker Crackdown, Law and Disorder on the electronic Frontier*, Massmarket Paperback, electronic version available at http://www.lysator.liu.se/etexts/hacker

20 **Leonard, Eamon, Ahmad M. Ramli, Kimberley, Paul, *et.al.*,** *Government Of Indonesia Information Infrastructure Development Project (IIDP), op.cit.*, hlm. 170 dst.

Information Technology, Virtual World Law dan *Hukum Mayantara.* Istilah-istilah tersebut lahir mengingat kegiatan internet dan pemanfaatan teknologi informasi yang tidak bertanggung jawab yang berbasis virtual atau maya.

Istilah Hukum Siber digunakan dalam tulisan ini dilandasi pemikiran, bahwa *cyber* jika diidentikan dengan dunia maya akan cukup menghadapi persoalan ketika terkait dengan pembuktian dan penegakan hukumnya. Mengingat para penegak hukum akan menghadapi kesulitan jika harus membuktikan suatu persoalan yang diasumsikan sebagai "maya", sesuatu yang tidak terlihat atau semu.

I. BENTUK-BENTUK CYBER CRIME

[21]*Cyber Crime* yang berkaitan dengan kerahasiaan, integritas dan keberadaan data dan sistem komputer:

a. Illegal Access (akses secara tidak sah terhadap sistem komputer)

Yaitu dengan sengaja dan tanpa hak melakukan akses secara tidak sah terhadap seluruh atau sebagian sistem komputer, dengan maksud untuk mendapatkan data komputer atau maksud-maksud tidak baik lainnya, atau berkaitan dengan sistem komputer yang dihubungkan dengan sistem komputer lain. *Hacking* merupakan salah satu dari jenis kejahatan ini yang sangat sering terjadi.

Perbuatan melakukan akses secara tidak sah terhadap sistem komputer belum ada diatur secara jelas di dalam sistem perundang-undangan di Indonesia. Untuk sementara waktu, Pasal

[21] **Natalie D Voss**, Copyright © 1994-99 Jones International and Jones Digital Century, "*Crime on The Internet*", Jones Telecommunications & Multimedia Encyclopedia, hal. 5-7, http://www.digitalcentury.com/encyclo/*update/articles.html*

22 Undang-Undang Republik Indonesia Nomor 36 Tahun 1999 tentang Telekomunikasi dapat diterapkan. Pasal 22 Undang-Undang Nomor 36 Tahun 1999 Tentang Telekomunikasi menyatakan: “setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah, atau memanipulasi :

- Akses ke jaringan telekomunikasi; dan/atau
- Akses ke jasa telekomunikasi; dan/atau
- Akses ke jaringan telekomunikasi khusus.”

Pasal 50 Undang-Undang Nomor 36 Tahun 1999 Tentang Telekomunikasi memberikan ancaman pidana terhadap barang siapa yang melanggar ketentuan Pasal 22 Undang-Undang Nomor 36 Tahun 1999 Tentang Telekomunikasi dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp. 600.000.000,00 (enam ratus juta rupiah). Namun setelah Undang-undang Informasi dan Transaksi Elektronik diundangkan, pasal 22 Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi sudah tidak perlu digunakan lagi. Karena pasal 30 Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik sudah mampu menjerat pelaku.

Dalam pasal 30 Undang-undang Nomor 11 tahun 2008 Tentang Informasi dan Transaksi elektronik disebutkan, bahwa “setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau sistem Elektronik Milik orang lain (ayat 1) dengan cara apa pun, (ayat 2) dengan cara apa pun dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen

elektronik, (ayat 3) dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan."

Ketentuan pidana pasal 30 Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik diatur dalam pasal 46 Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. untuk ayat 1, ketentuan pidananya yaitu pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp. 600.000.000,00 (enam ratus juta rupiah). Sedangkan ayat 2 pasal 46 memberikan ketentuan pidana penjara paling lama 7 (tujuh) tahun dan/atau pidana denda paling banyak Rp. 700.000.000,00 (tujuh ratus juta rupiah).

Untuk ayat 3, ketentuan pidanannya adalah pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp. 800.000.000,00 (delapan ratus juta rupiah).

b. Data Interference (mengganggu data komputer)

Yaitu dengan sengaja melakukan perbuatan merusak, menghapus, memerosotkan (*deterioration*), mengubah atau menyembunyikan (*suppression*) data komputer tanpa hak. Perbuatan menyebarkan virus komputer merupakan salah satu dari jenis kejahatan ini yang sering terjadi.

Pasal 38 Undang-Undang Telekomunikasi belum dapat menjangkau perbuatan *data interference* maupun *system interference* yang dikenal di dalam c*yber crime*. Jika perbuatan *data interference* dan *system interference* tersebut mengakibatkan

kerusakan pada komputer, maka Pasal 406 ayat 1 KUHP dapat diterapkan terhadap perbuatan tersebut.

Pasal 32 ayat 1 Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik berbunyi :

"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 elektronikmilik orang lain atau milik publik."

Isi dari pasal tersebut di atas dapat digunakan untuk menjerat pelaku kejahatan tersebut, karena unsur-unsur pidananya telah terpenuhi.

Ketentuan Pidananya diatur dalam pasal 28 ayat 1 Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, yaitu pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp. 2.000.000.000,00 (dua miliar rupiah).

c. **System Interference** (mengganggu sistem komputer)

Yaitu dengan sengaja dan tanpa hak melakukan gangguan terhadap fungsi sistem komputer dengan cara memasukkan, memancarkan, merusak, menghapus, memerosotkan, mengubah, atau menyembunyikan data komputer. Perbuatan menyebarkan program virus komputer dan *E-mail bombings* (surat elektronik

berantai) merupakan bagian dari jenis kejahatan ini yang sangat sering terjadi.

Pasal 38 Undang-Undang Telekomunikasi belum dapat menjangkau perbuatan *data interference* maupun *system interference* yang dikenal di dalam c*yber crime*. Jika perbuatan *data interference* dan *system interference* tersebut mengakibatkan kerusakan pada komputer, maka Pasal 406 ayat (1) KUHP dapat diterapkan terhadap perbuatan tersebut.

Namun tidak demikian apabila yang rusak hanya sistem atau data dari komputer tersebut. Untuk kerusakan pada sistem, dasar hukumnya diatur dalam pasal 33 Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, *"Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apapun yang mengakibatkan sistem elektronik menjadi tidak bekerja sebagaimana mestinya."*

Kemudian untuk ketentuan pidananya diatur dalam pasal 49 Undang-undang Nomor 11 tahun 2008 Tentang Informasi Dan Transaksi elektronik, yaitu pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak 10.000.000,000,00 (sepuluh miliar rupiah).

d. Illegal Interception In The Computers, Systems And Computer Networks Operation (intersepsi secara tidak sah terhadap komputer, sistem, dan jaringan operasional komputer)

Yaitu dengan sengaja melakukan intersepsi tanpa hak, dengan menggunakan peralatan teknik, terhadap data komputer, sistem komputer, dan atau jaringan operasional komputer yang bukan diperuntukkan bagi kalangan umum, dari atau melalui sistem komputer, termasuk didalamnya gelombang elektromagnetik yang dipancarkan dari suatu sistem komputer yang membawa sejumlah data. Perbuatan dilakukan dengan maksud tidak baik, atau berkaitan dengan suatu sistem komputer yang dihubungkan dengan sistem komputer lainnya.

Pasal 31 ayat 1 Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik telah mengatur permasalahan sebagai berikut :

"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."

Sedangkan untuk ketentuak pidananya ada pada pasal 47 Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, sebagai berikut :

"Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam pasal 31 ayat (1) dan ayat (2) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp. 800.000.000,00 (delapan ratus juta rupiah)."

e. Data Theft (mencuri data)

Yaitu kegiatan memperoleh data komputer secara tidak sah, baik untuk digunakan sendiri ataupun untuk diberikan kepada orang lain. *Identity theft* merupakan salah satu dari jenis kejahatan ini yang sering diikuti dengan kejahatan penipuan *(fraud).* Kejahatan ini juga sering diikuti dengan kejahatan *data leakage*.

Perbuatan melakukan pencurian data sampai saat ini tidak ada diatur secara khusus, bahkan di Amerika Serikat sekalipun. Pada kenyataannya, perbuatan *Illegal access* yang mendahului perbuatan *data theft* yang dilarang, atau jika *data theftss* diikuti dengan kejahatan lainnya, barulah ia menjadi suatu kejahatan bentuk lainnya, misalnya *data leakage and espionage* dan *identity theft and fraud.*

Pencurian data merupakan suatu perbuatan yang telah mengganggu hak pribadi seseorang, terutama jika si pemiik data tidak menghendaki ada orang lain yang mengambil atau bahkan sekedar membaca datanya tersebut. Pasal 32 ayat 2 Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik dapat digunakan untuk menjerat pelaku. *"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"*, dapat dipidana dengan ketentuan pidana sebagaimana diatur dalam pasal 48 ayat 2, yaitu pidana penjara

paling lama 9 (sembilan) tahun dan/atau denda paling banyak Rp. 3.000.000.000,00 (tiga miliar rupiah).

f. Data Leakage And Espionage (membocorkan data dan memata-matai)

Yaitu kegiatan memata-matai dan atau membocorkan data rahasia baik berupa rahasia negara, rahasia perusahaan, atau data lainnya yang tidak diperuntukkan bagi umum, kepada orang lain, suatu badan atau perusahaan lain, atau negara asing."

Karena Undang-undang Informasi Dan Transaksi elektronik belum mencakup perbuatan tersebut, maka sementara perbuatan membocorkan dan memata-matai data atau informasi yang berisi tentang rahasia negara diatur di dalam Pasal 112, 113, 114, 115 dan 116 KUHP. Pasal 323 KUHP mengatur tentang pembukaan rahasia perusahaan yang dilakukan oleh orang dalam (*insider*).

Sedangkan perbuatan membocorkan data rahasia perusahaan dan memata-matai yang dilakukan oleh orang luar perusahaan dapat dikenakan Pasal 50 jo. Pasal 22, Pasal 51 jo. Pasal 29 ayat (1), dan Pasal 57 jo. Pasal 42 ayat (1) Undang-Undang Nomor 36 tahun 1999 Tentang Telekomunikasi.

g. Misuse Of Devices (menyalahgunakan peralatan komputer)

Yaitu dengan sengaja dan tanpa hak, memproduksi, menjual, berusaha memperoleh untuk digunakan, diimpor, diedarkan atau cara lain untuk kepentingan itu, peralatan, termasuk

program komputer, password komputer, kode akses, atau data semacam itu, sehingga seluruh atau sebagian sistem komputer dapat diakses dengan tujuan digunakan untuk melakukan akses tidak sah, intersepsi tidak sah, mengganggu data atau sistem komputer, atau melakukan perbuatan-perbuatan melawan hukum lain.

Perbuatan Misuse of devices pada dasarnya bukanlah merupakan suatu perbuatan yang berdiri sendiri, sebab biasanya perbuatan ini akan diikuti dengan perbuatan melawan hukum lainnya.

Kejahatan tersebut diatur dalam pasal 34 ayat 1a dan 1b Undang-undang Informasi Dan Transaksi Elektronik. Sedangkan ketentuan pidanannya ada dalam pasal 50 Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, yaitu pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp. 10.000.000.000,00 (sepuluh miliar rupiah).

[22]Selain itu ada juga kualifikasi Kejahatan Dunia Maya yang menggunakan komputer sebagai alat kejahatan, yaitu :

a. Credit Card Fraud (penipuan kartu kredit)

Penipuan kartu kredit merupakan perbuatan penipuan biasa yang menggunakan komputer dan kartu kredit yang tidak sah sebagai alat dalam melakukan kejahatannya. Perbuatan tersebut dapat diancam dengan Pasal 378 KUHP, yaitu *"Barang siapa*

[22] ***Ibid,*** hal. 7-8

dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat, ataupun rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi hutang rnaupun menghapuskan piutang diancam karena penipuan dengan pidana penjara paling lama empat tahun."

b. Bank Fraud (penipuan terhadap bank)

Bank Fraud merupakan penipuan terhadap bank, yang dilakukan dengan menggunakan komputer sebagai alat untuk melakukan transaksi-transaksi dengan modus operansi yang berbeda-beda, sehingga perbuatan tersebut dapat diancam dengan Pasal 378 KUHP karena belum ada Undang-undang yang secara khusus mengatur perbuatan tersebut.

c. Service Offered Fraud (penipuan melalui penawaran suatu jasa)

Penipuan melalui penawaran jasa yang ada dalam internet dapat berupa *e-mail, Community Service,* dan lain-lain. Biasanya, bentuk jasa yang diberikan tidak sesuai dengan yang ditawarkan.

Penipuan melalui penawaran jasa merupakan perbuatan penipuan biasa yang menggunakan komputer sebagai salah satu alat dalam melakukan kejahatannya sehingga dapat diancam dengan Pasal 378 KUHP.

Selain itu, juga dapat digunakan pasal 28 ayat 1 Undang-undang Informasi Dan Transaksi Elektronik. Dan untuk ketentuan pidananya diatur dalam pasal 45 ayat 2 Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, yaitu pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp. 1.000.000.000,00 (satu miliar rupiah), tergantung dari modus operandinya.

d. Identity Theft And Fraud (pencurian identitas dan penipuan)

Pencurian identitas dan penipuan identitas sering kita temui pada kalangan masyarakat awam, seperti contohnya, ketika melakukan pendaftaran e-mail dengan menggunakan identitas palsu atau menggunakan identitas orang lain.

Pencurian identitas yang diikuti dengan melakukan kejahatan penipuan dapat diancam dengan Pasal 362 KUHP, Pasal 378 KUHP, dan pasal 28 ayat 1 Undang-undang Informasi Dan Transaksi Elektronik, tergantung dari modus operandi perbuatan yang dilakukannya, karena Belum ada Undang-undang yang secara khusus mengatur hal tersebut.

e. Computer-Related Fraud (penipuan melalui komputer)

Penipuan melalui komputer adalah penipuan yang sangat sering kita jumpai, dengan berbagai modus operandi, yang salah satunya dengan memberikan penawaran akan melipatgandakan uang, atau berupa investasi saham yang sebenarnya tidak ada dapat

diancam dengan pasal 378 KUHP, oleh karena itu pasal 28 ayat 1 Undang-undang Informasi Dan Transaksi Elektronik dapat kita gunakan untuk menjerat pelaku dengan modus operandi tersebut.

f. Computer-Related Forgery (pemalsuan melalui komputer)

Pemalsuan yang dapat dilakukan menggunakan komputer terdapat bermacam-macam modus operandinya. Contohnya seperti pemalsuan sertifikat, surat-surat berharga, dokumen dan data elektronik dengan menggunakan fasilitas multimedia.

Pemalsuan data elektronik (informasi elektronik, dan/atau dokumen elektronik) melalui komputer dapat dikenakan Pasal 35 Undang-undang Informasi Dan Transaksi Elektronik, *"Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan informasi elektronik dan/atau dokumen elektronik dengan tujuan agar informasi elektronik tyerebut dianggap seolah-olah data yang otentik"*, yang ketentuan pidananya diatur dalam pasal 51 ayat 1 Undang-undang Informasi Dan Transaksi Elektronik.

Sedangkan apabila data tersebut berbentuk fisik, maka akan di jerat dengan pasal 253 – 262 KUHP, yaitu pemalsuan materai dan merek, pasal 263 – 276 KUHP, yaitu tentang pemalsuan surat, dan pasal 378 KUHP, tergantung dari modus operandi pelakunya.

g. Computer-Related Betting (perjudian melalui komputer)

Perjudian memalui komputer, belakangan ini sangat marak. Biasanya kita akan diminta untuk membuka rekening on-line, dimana, saldo kita adalah merupakan uang yang akan kita gunakan untuk bermain bermacam-macam judi. Dan saldo tersebut dapat kita cairkan kembali bila kita mau, tapi tentu saja sudah dipotong bunga oleh perusahaan jasa yang kita gunakan.

Perjudian melalui komputer merupakan perbuatan melakukan perjudian biasa yang menggunakan komputer sebagai alat dalam mendukung tindakannya, sehingga perbuatan tersebut sementara dapat diancam dengan Pasal 303 KUHP.

Namun setelah Undang-undang Informasi Dan Transaksi Elektronik disahkan, untuk bandar digunakan undang tersendiri, yaitu Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik pasal 27 ayat 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"*. Dan ketentuan pidananya diatur dalam pasal 45 ayat 1 Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, yaitu pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp. 1.000.000.000,00 (satu miliar rupiah).

h. Computer-Related Extortion And Threats (pemerasan dan pengancaman melalui komputer)

Pemerasan dan pengancaman yang menggunakan komputer, biasanya dilakukan dengan menggunakan e-mail sebagai alatl. Seperti halnya surat kaleng, pengirim biasanya akan sulit dilacak, apalagi jika *e-mail account* yang digunakan untuk melakukan kejahatan ini berisi identitas palsu.

Pemerasan dan pengancaman melalui komputer merupakan perbuatan pemerasan biasa yang menggunakan komputer sebagai alat dalam operasionalisasi-nya sehingga perbuatan tersebut dapat diancam dengan Pasal 27 ayat 4 Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, yaitu :

> *"Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau menstransmisikan dan/atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan pemerasan dan/atau pengancaman."*

dengan ketentuan pidana dalam pasal 45 ayat 1, yaitu pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp. 1.000.000.000,00 (satuy miliar rupiah).

Selain itu, juga pasal 29 Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik juga mengatur permasalahan yang sama, namun tindakan tersebut dilakukan dengan tujuan pribadi. Ketentuan pidananya diatur dalam pasal 45 ayat 3 Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, yaitu pidana penjara paling lama 12 (dua

belas) tahun dan/atau denda paling banyak Rp. 2.000.000.000,00 (dua miliar rupiah).

[23]Kejahatan Dunia Maya yang berkaitan dengan isi atau muatan data atau sistem komputer, antara lain :

a. Child Pornography (pornografi anak)

Pornografi dalam dunia maya dapat dengan mudah kita akses, dan tentu saja oleh anak-anak juga bukan hal yang sulit. Karena pada saat ini, anak-anak dapat mengakses komputer dengan mudah, baik dalam lembaga pendidikan tempat dia belajar, maupun dalam lingkungan keseharian mereka.

Ditambah lagi apalagi fasilitas *Browsing* yang kita miliki tidak dilengkapi dengan *Pop-up Blocker*, akan sangat mudah bagi situs-situs ilegal menyusup masuk, dan tiba-tiba akan muncul begitu saja dilayar komputer kita.

Perbuatan memproduksi, menawarkan, dan menyebarkan pornografi anak melalui sistem komputer dapat diancam dengan Pasal 282 KUHP. Perbuatan akses pornografi untuk anak belum ada diatur di dalam undang-undang dan perlu segera diatur mengingat semakin banyaknya peminat pornografi anak akan memacu semakin meningkatnya pula produksi, penawaran, dan peredaran pornografi anak.

Namun Undang-undang Informasi Dan Transaksi Elektronik lebih mengatur secara khusus permasalahan ini dalam

---

[23] ***Ibid,*** hal. 9

pasal 27 ayat 1, *"Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau menstransmisikan dan/atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan melanggar kesusilaan."* Dengan ketentuan pidana yang berbeda pulayang diatur dalam pasal 45 ayat 1 Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, yaitu pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp. 1.000.000.000,00 (satuy miliar rupiah).

b. Infringements Of Copyright And Related Rights (pelanggaran terhadap hak cipta dan hak-hak terkait)

Infringements Of Copyright and Related Rights adalah merupakan pelanggaran hak cipta melalui fasilitas internet. Belakangan ini yang sering kita jumpai adalah fasilitas *download* yang disediakan oleh beberapa website. Contohnya adalah lagu. tanpa kita harus mengeluarkan biaya untuk membeli kaset original, kita akan dapat mendapatkan lagu-lagu yang kita kehendaki.

Dalam hal ini, tentu saja pencipta lagu, peyanyinya dan perusahaan rekaman akan sangat dirugikan. Karena selain hak-haknya dilanggar, mereka juga dirugikan secara materi.

Pelanggaran hak cipta dan hak-hak terkait dapat diancam dengan ketentuan pidana yang terdapat di dalam Undang-Undang Hak Cipta dan hak-hak terkait,misalnya Undang-undang 31 Tahun 2000 Tentang Desain Industri, Undang-undang No.19 Tahun 2002

Tentang Hak Cipta, Undang-undang Nomor 14 Tahun 2001 Tentang PATEN, dan lain sebagainya. Kejahatan ini bisa tergolong menjadi *cyber crime* disebabkan perbuatan yang secara insidental melibatkan penggunaan komputer dalam pelaksanaannya.

Selain itu pasal 30 ayat 2 Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik juga mengatur permasalahan ini :

> *"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."*

Ketentuan pidananya diatur dalam pasal 46 ayat 2 Undang-undang Informasi Dan Transaksi Elektronik, yaitu pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp. 700.000.000,00 (tujuh ratus juta rupiah).

c. Drug Traffickers (peredaran narkoba), dan lain-lain.

Peredaran norkoba dengan menggunakan internet biasanya akan menggunakan fasilitas *e-mail* dan *chatting/messenger* yang *account*-nya dapat kita peroleh dengan mudah, baik secara gratis, maupun dengan biaya yang tidak terlalu mahal. Karena privacy dalam fasilitas-fasilitas tersebut sangat dijaga oleh perusahaan-perusahaan penyedia jasa tersebut.

Peredaran narkotika dan obat-obatan terlarang juga merupakan suatu perbuatan biasa yang disebabkan secara

insidental melibatkan penggunaan komputer dalam pelaksanaannya sehingga digolongkan pula sebagai *cyber crime*. Oleh karena itu, perbuatan *drug traffickers* dapat diancam pidana sesuai dengan ketentuan yang diatur dalam Undang-Undang No. 5 Tahun 1997 tentang Psikotropika dan Undang-Undang Nomor 22 Tahun 1997 tentang Narkotika.

BAB III

METODOLOGI PENELITIAN

A. Jenis Penelitian

Menggunakan pendekatan normatif, tinjauan yuridis normatif, yaitu dengan melakukan identifikasi terhadap isu-isu hukum yang bekembang dalam masyarakat, mengkaji penerapan-penerapan hukum dalam masyarakat, mengkaji pendapat para ahli-ahli hukum terkait dan analisa kasus dalam dokumen-dokumen untuk memperjelas hasil penelitian, kemudian ditinjau aspek praktis dan aspek akademis keilmuan hukumnya dalam penelitian hukum.

B. Fokus Masalah

Fokus permasalahan dalam penelitian ini adalah terletak pada sulitnya penerapan hukum pada *Cyber Crime*, dikarenakan sulitnya melakukan pembuktian-pembuktian terhadap Tindak kejahatan tersebut. Kesulitan dalam pembuktian kasus terebut juga diikuti lemahnya hukum yang mengatur permasalahan mengenai kejahatan dunia maya ini.

Selain itu, para pengelola *cyberspace* kurang memberikan pengamanan yang lebih terhadap *cyberspace* yang dikelolanya, padahal para pengelola *cyberspace* juga tidak ingin dirugikan oleh keberadaan para hacker yang memanfaatkan lemahnya *security system* dalam *cyberpace* terebut. Hal ini justru akan memudahkan para pelaku kejahatan Cyber Crime untuk melakukan aksinya.

C. Bahan-bahan Hukum

Bahan-bahan Hukum adalah merupakan bahan-bahan yang diperoleh berdasarkan dari bahan bahan hukum primer, sekunder dan tersier

- ***Bahan Primer*** : Konsep-konsep hukum yang berkaitan dengan *cyber crime*, dan *cyber law* yang mengatur tentang tindak pidana virtual yang tercantum di dalam :
  - Undang-undang Nomor 31 Tahun 2000 Tentang Desain Industri.
  - Undang-undang Nomor 19 Tahun 2002 Tentang Hak Cipta.
  - Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (ITE).
  - *Uniform Domain Name Dispute Resolution Policy* (UDRP)
  - *European Threaty Series* Nomor 185, "*Convention On Cyber Crime 2000"*

- ***Bahan Sekunder :*** Merupakan bahan-bahan hukum yang diambil dari pendapat atau tulisan para ahli dalam bidang cyber untuk digunakan dalam membuat konsep-konsep hukum yang berkaitan dengan penelitian ini dan dianggap sangat penting.

- ***Bahan Tersier :*** Merupakan bahan-bahan yang digunakan sebagai rujukan untuk mengetahui konsep hukum yang ada, yaitu melalui :
  - Kamus Hukum
  - Kamus Bahasa Indonesia
  - Kamus Bahasa Inggris

D. Teknik Pengumpulan Data

Dilakukan dengan melakukan penelusuran bahan hukum melalui alat bantu catatan untuk dapat digunakan sebagai landasan teoritis berupa pendapat atau tulisan para ahli sehingga dapat diperoleh informasi dalam bentuk ketentuan formal dan resmi oleh pihak yang berkompeten dalam bidang ini.

E. Teknik Analisa

Menggunakan teknik *content analysis*, yaitu pengumpulan bahan bahan hukum dan diinterpretasi, dan untuk ketentuan hukum dipakai interpretasi teleologis yaitu berdasar pada tujuan norma. Selain itu juga digunakan pendekatan Undang-undang baru terkait dengan *cyber crime*, yaitu Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (UU ITE).

BAB IV

PEMBAHASAN

A. GAMBARAN UMUM TENTANG CYBER CRIME

- **Kejahatan Dan Kemajuan Dunia Teknologi**

Keunggulan komputer berupa kecepatan dan ketelitiannya dalam menyelesaikan pekerjaan sehingga dapat menekan jumlah tenaga kerja, biaya serta memperkecil kemungkinan melakukan kesalahan, mengakibatkan masyarakat semakin mengalami ketergantungan kepada komputer. Dampak negatif dapat timbul apabila terjadi kesalahan yang ditimbulkan oleh peralatan komputer yang akan mengakibatkan kerugian besar bagi pemakai (*user*) atau pihak-pihak yang berkepentingan. Kesalahan yang disengaja mengarah kepada penyalahgunaan komputer.[24]

Pada tahun 1982 telah terjadi penggelapan uang di bank melalui komputer sebagaimana dapat dilihat dalam Putusan Mahkamah Agung Nomor 363 K/Pid/1984 tanggal 25 Juni 1984 mengenai. “Suara Pembaharuan” edisi 10 Januari 1991 memberitakan tentang dua orang mahasiswa yang membobol uang dari sebuah bank swasta di Jakarta sebanyak Rp. 372.100.000,00 dengan menggunakan sarana komputer.

Perkembangan lebih lanjut dari teknologi komputer adalah berupa *computer network* yang kemudian melahirkan suatu ruang komunikasi dan informasi global yang dikenal dengan internet.

---

[24] **Andi Hamzah**, 1990, *Aspek-aspek Pidana di Bidang Komputer*, Sinar Grafika, Jakarta, hal. 23-24.

Penggunaan teknologi komputer, telekomunikasi, dan informasi tersebut mendorong berkembangnya transaksi melalui internet di dunia. Perusahaan-perusahaan berskala dunia semakin banyak memanfaatkan fasilitas internet. Sementara itu tumbuh transaksi-transaksi melalui elektronik atau on-line dari berbagai sektor, yang kemudian memunculkan istilah *e-banking, e-commerce, e-trade,e-business, e-retailing*.

Perkembangan yang pesat dalam pemanfaatan jasa internet juga mengundang terjadinya kejahatan. c*yber crime* merupakan perkembangan dari *computer crime*. Rene L. Pattiradjawane menyebutkan bahwa konsep hukum *cyberspace*, *cyberlaw* dan *cyberline* yang dapat menciptakan komunitas pengguna jaringan internet yang luas (60 juta), yang melibatkan 160 negara telah menimbulkan kegusaran para praktisi hukum untuk menciptakan pengamanan melalui regulasi, khususnya perlindungan terhadap milik pribadi.[25] John Spiropoulos mengungkapkan bahwa *cyber crime* memiliki sifat efisien dan cepat serta sangat menyulitkan bagi pihak penyidik dalam melakukan penangkapan terhadap pelakunya.[26]

Pada dasarnya setiap kegiatan atau aktifitas manusia dapat diatur oleh hukum. Hukum disini direduksi pengertiannya menjadi peraturan perundang-undangan yang dibuat oleh negara, begitu pula aktifitas kejahatan mayantara yang menjadikan internet sebagai sarana utamanya ini. Dalam kaitan dengan teknologi informasi khususnya dunia maya, peran hukum adalah melindungi pihak-pihak yang lemah terhadap eksploitasi dari pihak yang kuat atau berniat

---

25 **Rene L. Pattiradjawane**, "*Media Konverjensi dan Tantangan Masa Depan*", Kompas, 21 Juli 2000.

26 **Jhon Sipropoulus**, 1999, "*Cyber Crime Fighting*, The Law Enforcement Officer's Guide to Online Crime", The Natinal Cybercrime Training Partnership, Introduction.

jahat, disamping itu hukum dapat pula mencegah dampak negatif dari ditemukannya suatu teknologi baru.

Akan tetapi pada kenyataannya hukum sendiri belum dapat mengatasi secara riil terhadap permasalahan-permasalahan yang ditimbulkan oleh teknologi khususnya teknolgi nformasi. Salah satu bukti kongkretnya adalah timbulnya berbagai kejahatan di dunia *cyber* yang ternyata belum bisa diatasi sepenuhnya oleh hukum.[27]

Saat ini berbagai upaya telah dipersiapkan untuk memerangi *cyber crime*. *The Organization for Economic Co-operation and Development (OECD)* telah membuat guidelines bagi para pembuat kebijakan yang berhubungan dengan computer related crime , dimana pada tahun 1986 OECD telah mempublikasikan laporannya yang berjudul *"computer related crime: analysis of legal policy"*. Laporan ini berisi hasil survei terhadap peraturan perundang-undangan negara-negara anggota beserta rekomendasi perubahannya dalam menanggulangi computer related crime tersebut, yang mana diakui bahwa sistem telekomunikasi juga memiliki peran penting didalam kejahatan tersebut.

Melengkapi laporan OECD, *The Council of Europe* (CE) berinisiatif melakukan studi mengenai kejahatan tersebut. Studi ini memeberikan guidelines lanjutan bagi para pengambil kebijakan untuk menentukan tindakan-tindakan apa yang seharusnya dilarang berdasakan hukum pidana negara-negara anggota dengan tetap mempehatikan keseimbangan antara hak-

---

[27] **ITAC,** "III Common View Paper On Cyber Crime:, IIC 2000 Millenium Congress, September 19th, 2000.

hak sipil warga negara dan kebutuhan untuk melakukan proteksi terhadap *computer related crime* tersebut.

Pada perkembangannya, CE membentuk Committee of Experts on Crime ini Cyber space of The Committee on Crime problem, yang pada tanggal 25 April 2000 telah mempublikasikan D*raft Convension on Cyber Crime* sebagai hasil kerjanya, yang menurut Prof. Susan Brenner dari *University of Daytona School of Law*, merupakan perjanjian internsional pertama yang mengatur hukum pidana dan aspek proseduralnya untuk berbagai tipe tindak pidana yang berkaitan erat dengan penggunaan komputer, jaringan atau data, serta berbagai penyalahgunaan sejenis.

- **Hubungan Antara Kejahatan, Cyber Crime Dan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik**

Cyber crime merupakan suatu perbuatan merugikan orang lain atau instansi yang berkaitan dan/atau pengguna fasilitas dengan sistem Informasi dan Transaksi Elektronik yang bertujuan untuk menguntungkan diri sendiri maupun orang lain secara materi, maupun hanya untuk sekedar memuaskan jiwa pelaku atau orang lain tersebut. Oleh karena itu, maka tindakan atau perbuatan tersebut merupakan suatu kejahatan dan merupakan perbuatan melanggar hukum, karena adanya unsur-unsur dimana ada pihak-pihak lain yang merasa dirugikan oleh perbuatan tersebut.

Cyber Crime adalah merupakan suatu perbuatan melanggar hukum yang secara khusus di diatur dalam Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. Karena KUHP tidak cukup kuat untuk menjerat pelaku *cyber crime*, mengingat masalah pengaturan alat bukti

yang tercantum dalam KUHP dan KUHAP belum memasukan alat bukti digital yang merupakan alat bukti dalam cyber crime di dalamnya.

Dalam pasal 27 – 37 Undang-undang ITE adalah merupakan perbuatan yang berkaitan dengan Informasi Dan Transaksi Elektronik yang dilarang oleh undang-undang tersebut. Berkaitan dengan hal tersebut pembuktiannya diatur dalam Bab X tentang Penyidikan, khususnya pasal 43 ayat 5e :

> *"melakukan pemeriksaan terhadap alat dan/atau sarana yang berkaitan dengan kegiatan Teknologi Informasi yang diduga digunakan untuk melakukan tindak pidana berdasarkan Undang-uindang ini"*

dan dalam pasal yang sama ayat 5h tentang saksi ahli :

> *"meminta bantuan ahli yang diperlukan dalam penyidikan terhadap tindak pidana berdasarkan undang-undang ini"*

Serta dalam pasal 44 UU ITE :

> *"Alat bukti penyidikan, penuntutan dan memerikasaanh di sidang pengadilan menurut ketentuan undang-undang ini adalah sebagai berikut :*
>
> a. *alat bukti sebagaimana dimaksud dalam ketemtuan Perundang-undangan; dan*
> b. *alat bukti lain berupa Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud dalam pasal 1 angka 1 dan angka 4 serta pasal 5 ayat (1), ayat (2), dan ayat (3)."*

- **Dunia Sebelum Berlakunya Hukum Kejahatan *Cyber Crime***

[28]Jauh sebelum adanya komputer dan kejahatan komputer, ada banyak bentuk pelanggaran dan kejahatan. Teknologi komputer dapat digunakan sebagai fasilitas para pelaku kejahatan komputer seperti pencurian dan penggelapan. Kejahatan komputer saat ini dicirikan dengan manipulasi otorisasi user program komputer, sebagai contoh, mencuri uang dari bank dan dari para pengusaha lainnya. Kejahatan komputer fase awal diantaranya adalah penyerangan sistem telephone dan network atau pentransferan uang menggunakan perangkat elektronik. Karena komputer pada awalnya terpusat dan tidak interkoneksi, peluang terjadinya kejahatan komputer lebih terbatas berupa penyalahgunaan sistem otorisasi user.

Sebelum adanya hukum kejahatan komputer, para pelaku dan hakim apabila berurusan dengan kejahatan komputer akan menggunakan konsep hukum criminal tindakan pencurian, perusakan properti, penyalahgunaan dan kejahatan kriminal. Pada waktu itu, komputer masih berukuran besar, *stand-alone* mesin, dan akses ke computer tersebut secara umum terbatas oleh terminal fisik yang berhubungan dengan computer *mainframe*. Kebanyakan kejahatan komputer dilakukan oleh orang dalam atau dekat dengan orang dalam. Pengguna komputer yang memiliki legitimasi dengan hak akses ke komputer tersebut, seperti pengembang perangkat lunak, vendor dan pengguna lainnya yang memiliki otorisasi adalah para pelaku utama kejahatan-kejahatan komputer ini, yang meliputi kejahatan pencurian data oleh karyawan, informasi dan “properti” lainnya yang ada di komputer. Bentuk penyalahgunaan komputer lainnya meliputi perusakan perangkat lunak,

---

28 **Muhammad Bagir,** Tugas Proteksi Dan Pengamanan Sistem Informasi / Teknologi Informasi Hal 3 - 5

perangkat keras atau data dalam komputer tersebut, umumnya kejahatan komputer juga terjadi karena adanya balas dendam terhadap pemecatan karyawan atau akibat dari perselisihan terhadap persetujuan lisensi perangkat lunak.

Penyalahgunaan komputer pada awalnya masih kecil, kejadian atau peristiwa yang terpencil. Tipe kejahatan yang melibatkan karyawan seperti cyberspace. Ketika seorang karyawan melihat file atau informasi rahasia lainnya, atau mencuri barang dari seorang karyawan, aktivitas-aktivitas demikian juga berlaku dalam *cyberspace*.

Berkaitan dengan pengertiannya, prinsip klaim hak juga menginformasikan penentuan kebiasaan berbuat kriminal. Sebagai contoh, seorang karyawan yang telah menerima sebuah pasword dari karyawan lainnya, yang memberikan petunjuk bahwa database tertentu boleh diakses padahal tidak dinyatakan bersalah karena berbuat kriminalitas jika dia mengakses database tersebut. Bagaimanapun, prinsip klaim hak tidak sama dengan karyawan yang mencuri password dari koleganya untuk mengakses database yang sama, karena aksesnya tidak terotorisasi; karyawan ini telah melakukan tindakan kriminal.

Harus ada pembedaan mengenai apa yang dimaksud tidak etis dan apa yang dimaksud ilegal; respon hukum terhadap suatu masalah harus proporsional terhadap aktivitas yang dilakukan. Hanya jika kebiasaan tersebut diputuskan benar-benar merupakan kriminalitas dan perbuatan kriminal yang dilarang serta penuntutan yang harus dilakukan. Hukum kriminal, oleh karenanya, harus dilakukan dan diimplementasikan dengan pengendalian.

Sejarah telah menunjukkan bahwa kejahatan komputer dilakukan oleh masyarakat luas seperti: para Siswa, amatiran, teroris dan anggota kelompok kejahatan yang terorganisir. Yang membedakannya adalah kejahatan yang dilakukannya. Individu yang melakukan akses sistem komputer tanpa maksud berbuat kejahatan lebih jauh harus dibedakan dari karyawan lembaga keuangan yang mengambil atau mentransfer uang dari akun pelanggan.

Level keahlian tertentu untuk kejahatan komputer merupakan sebuah topik yang kontroversial. Beberapa mengklaim bahwa level keahlian bukan sebuah indikator kejahatan komputer, sedangkan yang lain mengklaim bahwa kejahatan komputer yang jelas potensial, merupakan subjek yang sangat termotivasi untuk menerima tantangan perubahan teknologi, karakteristik yang juga diinginkan seorang karyawan dalam wilayah pemrosesan data.

Banyak survey pemerintah dan sektor swasta menunjukkan bahwa kejahatan komputer cenderung bertambah. Sulit untuk menghitung dampak ekonomis kejahatan ini, bagaimanapun, karena banyak yang tidak pernah dideteksi atau dilaporkan. Kejahatan komputer dapat dibagi menjadi dua kategori, yakni kejahatan terhadap komputer dan kejahatan menggunakan komputer.

Semua tingkatan operasi komputer rentan terhadap aktivitas kejahatan, apakah sebagai target kejahatan atau instrument kejahatan atau keduanya. Input operasi, pemrosesan data, output operasi dan komunikasi semuanya telah menggunakan tujuan gelap.

B. KENDALA-KENDALA YURIDIS YANG DIHADAPI OLEH PERANGKAT HUKUM DI INDONESIA DALAM MENANGANI PARA PELAKU CYBER CRIME TERKAIT DENGAN MASALAH PEMBUKTIAN

Walaupun Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik telah disahkan oleh pemerintah, namun belum cukup mencakup semua aspek dari kejahatan dunia maya.

Drug Trafficker, transaksi Narkoba melalui jaringan internet masih diatur dengan menggunakan Undang-Undang No. 5 Tahun 1997 tentang Psikotropika dan Undang-Undang Nomor 22 Tahun 1997 tentang Narkotika, sedangkan dalam undang-undang tersebut tidak diatur mengenai transaksi obat-obatan terlarang tersebut jika dilakukan menggunakan jaringan internet.

Selain itu, *Credit Card Fraud (Carding)* dan *Bank Fraud*, juga masih menggunakan peraturan hukum yang konvensional mengenai penipuan, yaitu Pasal 378 KUHP. Dalam Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Transaksi Elektronik belum diatur tentang masalah penipuan ini, mengingat sebenarnya kejahatan ini merupakan kejahatan yang dilakukan dengan menggunakan Media Informasi dan fasilitas Transaksi Elektronik yang disediakan pada jaringan internet.

Selain itu, kita tidak bisa terus mengacu pada Undang-Undang Informasi Dan Transaksi Elektronik saja, mealainkan kita harus menyusun konsep Kitab Undang-undang Hukum Pidana yang baru. Karena KUHP lama sudah tidak dapat lagi menjangkau tindak-tindak pidana baru yang tercipta oleh perkembangan jaman, untuk itu dibutuhkan konsep-konsep baru tentang KUHP kita.

Selain itu, menurut Madjono Reksodiputro, pakar kriminolog dari Universitas Indonesia yang menyatakan bahwa kejahatan komputer sebenarnya bukanlah kejahatan baru dan masih terjangkau oleh KUHP untuk menanganinya. Pengaturan untuk menangani kejahatan komputer sebaiknya diintegrasikan ke dalam KUHP dan bukan ke dalam undang-undang tersendiri.

C. UPAYA-UPAYA YURIDIS YANG DAPAT DILAKUKAN TERKAIT DENGAN MASALAH PEMBUKTIAN OLEH PERANGKAT HUKUM DI INDONESIA

Dalam upaya-upaya yang dapat dilakukan terkait dengan masalah pembuktian oleh pengadilan dan penyidikan oleh POLRI dalam *cyber crime* dapat digunakan berbagai macam cara, antara lain dengan mengoptimalkan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, mengembangkan pengetahuan dan kemampuan penyidik dalam Dunia Cyber, menambahkan dan meningkatkan fasilitas komputer forensik dalam POLRI.

Kejahatan internet atau yang lebih populer dengan istilah *cyber crime* ini dapat dilakukan tanpa mengenal batas teritorial dan tidak diperlukan interaksi langsung antara pelaku dan korban kejahatan. Dengan sifat seperti itu, semua negara termasuk Indonesia yang melakukan aktivitas internet akan terkena imbas dari perkembangan kejahatan dunia maya.

Para *hacker* selalu mencari celah untuk menggunakan keahliannya melakukan kejahatan. Memudarnya batas-batas geografi dalam abad 21 yang dikenal sebagai abad informasi ini telah mengubah cara pandang terhadap penyelesaian dan praktik kejahatan dari model lama (konvensional) ke model baru (elektronik). Kekuatan jaringan dan komputer pribadi berbasis pentium

menjadikan setiap komputer sebagai alat yang potensial bagi para pelaku kejahatan.

Globalisasi aktivitas kriminal yang memungkinkan para penjahat melintas batas elektronik merupakan masalah nyata dengan potensi memengaruhi negara, hukum, dan warga negaranya. Fakta ini tak bisa dimungkiri karena internet dapat dijadikan sarana yang efektif untuk mencapai tujuan-tujuan negatif yang diinginkan tanpa batasan geografis dan teritorial.

a. Optimalisasi Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

Sebenarnya upaya untuk mengatasi kejahatan internet ini sudah disepakati di Hongaria pada 23 November 2001. Saat itu ada lebih kurang 30 negara menandatangani *Convention On Cyber Crime* sebagai wujud kerja sama multilateral untuk menanggulangi aktivitas kriminal melalui internet dan jaringan komputer lainnya. Namun, upaya penanggulangan kejahatan internet ini menemukan masalah dalam hal yurisdiksi. Pengertian yurisdiksi sendiri adalah kekuasaan atau kemampuan hukum negara terhadap orang, benda, atau peristiwa (hukum). Yurisdiksi ini merupakan refleksi dari prinsip dasar kedaulatan negara, kesamaan derajat negara, dan prinsip tidak campur tangan.

Dalam konteks ini Indonesia bisa memainkan perannya bersama-sama dengan negara-negara lain di dunia untuk mengatasi masalah kejahatan internet. Dalam lingkup nasional, kejahatan internet pada saatnya akan menjadi bentuk kejahatan serius yang dapat membahayakan keamanan individu, masyarakat, bangsa, dan negara Indonesia.

Apabila Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik dilihat dalam perspektif penanggulangan penyalahgunaan internet di atas, maka semestinya tak perlu ada pro dan kontra. Ini karena pada dasarnya kehadiran UU itu untuk melindungi masyarakat dari kerugian dan kehancuran akhlak yang akan berimplikasi pada kelangsungan hidup berbangsa dan bernegara. Walaupun demikian, kehadiran perangkat hukum itu pun tidak secara otomatis dapat menghentikan langkah para *hacker*. Bahkan, boleh jadi perangkat hukum ini akan memancing keberanian mereka untuk mencari titik-titik lemahnya sehingga mereka bisa terus melancarkan aksinya.

Selain itu, kita tidak dapat selalu mengacu pada Undang-undang Informasi Transaksi elektronik dan Kitab Undang-undang Hukum Pidana lama saja, melainkan mengikuti perkembangan jaman kita membutuhkan KUHP baru.

Dalam pasal 5 ayat 1 dan 2 Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik mendeskripsikan bahwa Dokumen elektronik dan Informasi Elektronik adalah merupakan alat bukti yang sah. Selain dalam pasal 44 Undang-undang yang sama mengatakan :

"Alat bukti penyidikan, penuntutan dan pemeriksaan di sidang pengadilan menurut ketentuan Undang-Undang ini adalah sebagai berikut:

a. alat bukti sebagaimana dimaksud dalam ketentuan Perundang-undangan; dan

b. alat bukti lain berupa Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud dalam Pasal 1 angka 1 dan angka 4 serta Pasal 5 ayat (1), ayat (2), dan ayat (3).”

[29]Selain deskripsi undang-undang ITE tersebut, dikenal pula alat bukti digital. Tindakan kejahatan tradisional umumnya meninggalkan bukti kejahatan berupa bukti-bukti fisikal, karena proses dan hasil kejahatan ini biasanya juga berhubungan dengan benda berwujud nyata. Dalam dunia komputer dan internet, tindakan kejahatan juga akan melalui proses yang sama. Proses kejahatan yang dilakukan tersangka terhadap korbannya juga akan mengandalkan bantuan aspek pendukung dan juga akan saling melakukan pertukaran atribut.

Namun dalam kasus ini aspek pendukung, media, dan atribut khas para pelakunya adalah semua yang berhubungan dengan sistem komputerisasi dan komunikasi digital. Atribut-atribut khas serta identitas dalam sebuah proses kejahatan dalam dunia komputer dan internet inilah yang disebut dengan bukti-bukti digital.

[30]Perangkat yang menggunakan format data digital untuk menyimpan informasi memang sangat banyak. Meskipun dalam artikel ini cakupannya hanya seputar perangkat komputer dan jaringan saja, namun perangkat-perangkat lain juga memiliki potensi untuk menyimpan buktibukti digital. Seperti misalnya perangkat ponsel, smart card, bahkan microwave juga bisa berperan sebagai sumber buktibukti digital. Berdasarkan pertimbangan inilah maka dibuat tiga kategori besar untuk sumber bukti digital, yaitu:

---

29 ***Pembuktian Tindak Pidana Cyber Crime,*** Yuyun Yulianah, SH, MH. Halaman 7

30 ***Ibid,*** Halaman 8 - 11

- ***Open Computer Systems***

  Perangkat-perangkat yang masuk dalam kategori jenis ini adalah apa yang kebanyakan orang pikir sebagai perangkat komputer. Sistem yang memiliki media penyimpanan, keyboard, monitor, dan pernak-pernik yang biasanya ada di dalam komputer masuk dalam kategori ini. Seperti misalnya laptop, desktop, server, dan perangkat-perangkat sejenis lain. Perangkat yang memiliki sistem media penyimpanan yang kian membesar dari waktu ke waktu ini merupakan sumber yang kaya akan bukti-bukti digital. Sebuah file yang sederhana saja pada sistem ini dapat mengandung informasi yang cukup banyak dan berguna bagi proses investigasi. Contohnya detail seperti kapan file tersebut dibuat, siapa pembuatnya, seberapa sering file tersebut di akses, dan informasi lainnya semua merupakan informasi penting.

- ***Communication Systems***

  Sistem telepon tradisional, komunikasi wireless, Internet, jaringan komunikasi data, merupakan salah satu sumber bukti digital yang masuk dalam kategori ini. Sebagai contoh, jaringan Internet membawa pesan-pesan dari seluruh dunia melalui e-mail. Kapan waktu pengiriman e-mail ini, siapa yang mengirimnya, melalui mana si pengirim mengirim, apa isi dari e-mail tersebut merupakan bukti digital yang amat sangat penting dalam investigasi.

- ***Embedded Computer Systems***

  Perangkat telepon bergerak (ponsel), personal digital assistant (PDA), smart card, dan perangkat-perangkat lain yang tidak dapat disebut komputer tapi memiliki sistem komputer dalam bekerjanya dapat digolongkan dalam kategori ini. Hal ini dikarenakan bukti-bukti digital juga dapat tersimpan di sini.

  Sebagai contoh, sistem navigasi mobil dapat merekam ke mana saja mobil tersebut berjalan. Sensor dan modul-modul diagnosa yang dipasang dapatmenyimpan informasi yang dapat digunakan untuk menyelidiki terjadinya kecelakaan, termasuk informasi kecepatan, jauhnya perjalanan, status rem, posisi persneling yang terjadi dalam lima menit terakhir. Semuanya merupakan sumber-sumber bukti digital yang amat berguna.

b. Penegakan Hukum Cyber Crime Dengan Menggunakan Sarana Non-Penal

Meskipun hukum pidana digunakan sebagai ultimum remidium atau alat terakhir apabila bidang hukum yang lain tidak dapat mengatasinya, tetapi harus disadari bahwa hukum pidana memiliki keterbatasan kemampuan dalam menanggulangi kejahatan. Keterbatasan-keterbatasan tersebut dikemukakan oleh Barda nawawi Arief sebagai berikut :[31]

a. Sebab-sebab kejahatan yang demikian kompleks berada di luar jangkauan hukum pidana;

---

31 ***Barda Nawawi Arief,*** Beberapa Aspek Kebijakan Penegakan dan Pengembangan Hukum Pidana, (Bandung: PT Citra Aditya Bakti, 1998), halaman. 46-47

b. Hukum pidana hanya merupakan bagian kecil (subsistem) dari sarana control social yang tidak mungkin mengatasi masalah kejahatan sebagai masalah kemanusiaan dan kemayarakatan yang sangat kompleks (sebagai masalah sosio-psikologis, sosio-politik, sosio-ekonomi, sosio-kultural dan sebagainya);
c. Penggunaan hukum pidana dalam menanggulangi kejahatan hanya merupakan "kurieren am symptom", oleh karena itu hukum pidana hanya merupakan "pengobatan simptomatik" dan bukan "pengobatan kausatif";
d. Sanksi hukum pidana merupakan "remedium" yang mengandung sifat kontradiktif/paradoksal dan mengandung unsur-unsur serta efek sampingan yang negatif;
e. Sistem pemidanaan bersifat fragmentair dan individual/personal, tidak bersifat struktural/fungsional;
f. Keterbatasan jenis sanksi pidana dan sistem perumusan sanksi pidana yang bersifat kaku dan imperatif;
g. Bekerjanya/berfungsingnya hukum pidana memerlukan sarana pendukung yang lebih bervariasi dan memerlukan "biaya tinggi".

Keterbatasan-keterbatasan hukum pidana inilah yang tampaknya dialami oleh Polri yang menggunakan hukum pidana sebagai landasan kerjanya. Sebab kejahatan yang kompleks ini terlambat diantisipasi oleh Polri sehingga ketika terjadi kasus yang berdimensi baru mereka tidak secara tanggap menanganinya. Untuk itu, pencegahan kejahatan tidak selalu harus menggunakan hukum pidana. Agar penegakan hukum cyber crime ini dapat dilakukan secara menyeluruh maka tidak hanya pendekatan

yuridis atau penal yang dilakukan, tetapi dapat juga dilakukan dengan pendekatan non-penal.

Dalam konteks cyber crime ini erat hubungannya dengan teknologi, khususnya teknologi computer dan telekomunikasi sehingga pencegahan cyber crime dapat digunakan melalui saluran teknologi atau disebut juga techno-prevention. Langkah ini sesuai dengan apa yang telah diungkapkan oleh International Information Industri Congress (IIIC) sebagai berikut :[32]

> *The IIIC recognizes that government action and international treaties to harmonize laws and coordinate legal procedures are keying the fight cyber crime, but warns that these should not be relied upon as the only instrument. Cyber crime is enabled by technology and requires as healthy reliance on technology for its solution.*

Pendekatan teknologi ini merupakan subsistem dalam sebuah sistem yang lebih besar, yaitu pendekatan budaya, karena teknologi merupakan hasil dari kebudayaan atau merupakan kebudayaan itu sendiri. Pendekatan budaya atau cultural ini perlu dilakukan untuk membangun atau membangkitkan kepekaan warga masyarakat dan aparat penegak hukum terhadap masalah *cyber crime* dan menyebarluaskan atau mengajarkan etika penggunaan computer melalui media pendidikan. Pentingnya pendekatan budaya ini, khususnya upaya mengembangkan

---

[32] ***Ibid,*** Halaman 5

kode etik dan perilaku (code of behavior and ethics) terungkap juga dalam pernyataan IIIC sebagai berikut :[33]

IIIC members are also committed to participate in the development of code behaviour and ethics around computer and Internet use, and in campaigns for the need for ethical and responsible online behaviour. Given the international reach of Internet crime, computer and Internet users around the world must be made aware of the need for high standards of conduct in cyber space.

Ketidaksiapan hukum dan polri dalam penegakan hukum *cyber crime* ini menyebabkan pencegahan dengan menggunakan teknologi dan budaya menjadi alat yang ampuh. Hal ini terungkap dari korban hacking yang merasa nyaman dengan pendekatan teknologi untuk menanggulangi *cyber crime.* Ketika situs mereka dirusak, mereka menggunakan teknologi dalam memperbaikinya dan mengantisipasinya dengan menggunakan sistem pengamanan yang ketat.

Dalam Resolusi Kongres PBB VIII/1990 mengenai *Computer-related crimes* sebagaimana dikutip oleh Barda Nawawi Arief, bahwa menghimbau Negara-negara anggota untuk mengintensifkan upaya-upaya penanggulangan penyalahgunaan komputer yang lebih efektif dengan mempertimbangkan langkah-langkah sebagai berikut :[34]

1. Melakukan Modernisasi hukum pidana material dan hukum acara pidana

---

33 ***Ibid***

34 ***Barda Nawawi Arief***, Masalah, hlm. 238-239

2. Mengembangkan tindakan-tindakan pencegahan dan pengamanan komputer
3. Melakukan langkah-langkah untuk membuat peka warga warga masyarakat, aparat pengadilan dan penegak hukum, terhadap pentingnya pencegahan kejahatan yang berhubungan dengan computer
4. Melakukan upaya-upaya pelatihan bagi para hakim, pejabat dan aparat penegak hokum mengenai kejahatan ekonomi dan *cyber crime*
5. Memperluas *rule of ethics* dalam penggunaan computer dan mengajarkannya melalui kurikulum informatika
6. Mengadopsi kebijakan perlindungan korban *cyber crime* sesuai dengan deklarasi PBB mengenai korban dan mengambil langkah-langkah untuk mendorong korban melaporkan adanya *cyber crime*.

Tidak hanya pendekatan penal dan non-penal yang diperlukan dalam penanggulangan *cyber crime* ini, mengingat *cyber crime* yang dapat dilakukan oleh orang dengan melalui batas Negara, maka perlu dilakukan kerja sama dengan Negara lain. Bentuk kerja sama ini dapat berupa kerjasama ekstradisi maupun harmonisasi hukum pidana subtantif sebagaimana terungkap dari hasil Kongres Perserikatan Bangsa-Bangsa (PBB) X/2000 : *"The harmonization of substantive criminal law with regard to cyber crimes is essential if international cooperation is to be achieved between law enforcement and the judicial authorities of different States"*.

Menurut Agus Raharjo bahwa salah satu langkah lagi agar penanggulangan *cyber crime* ini dapat dilakukan dengan baik,

maka perlu dilakukan kerja sama dengan *Internet Service Provider (ISP)* atau penyedia jasa internet. Meskipun *Internet Service Provider (ISP)* hanya berkaitan dengan layanan sambungan atau akses Internet, tetapi *Internet Service Provider (ISP)* memiliki catatan mengenai ke luar atau masuknya seorang pengakses, sehingga ia sebenarnya dapat mengidentifikasikan siapa yang melakukan kejahatan dengan melihat *log file* yang ada.[35]

Dari paparan penegakan hukum dengan sarana non-penal ini, maka menurut penulis cara non- penal inilah yang lebih diutamakan dari pada sarana penal dengan konsekuensi segera menyiapkan penegak hukum yang menguasai teknologi informasi. Atau lebih jelasnya kita sangat membutuhkan Polisi *Cyber*, Jaksa *Cyber,* Hakim *Cyber* dalam rangka penegakan hukum *Cyber Crime* di Indonesia tanpa adanya penegak hukum yang mempuni di bidang teknologi informasi, maka akan sulit menjerat penjahat-penjahat cyber oleh karena kejahatan *cyber* ini *locos delicti*-nya bisa lintas negara.

35 ***Agus Raharjo***, Cyber, halaman. 248

BAB V

PENUTUP

A. KESIMPULAN

Berdasarkan uraian pembahasan tersebut di atas, dapat ditarik kesimpulan sebagai berikut :

1. Asas legalitas dalam hukum pidana Indonesia memberikan garis kebijakan agar mewujudkan perlindungan hukum terhadap tindakan sewenang-wenang penguasa/penyelenggara negara terhadap kepentingan hukum bagi masyarakyat dan hak asasi manusia. Maka sistem pembuktian berdasarkan KUHAP secara formil tidak lagi dapat menjangkau dan sebagai landasan hukum pembuktian terhadap perkara *Cyber Crimes*, sebab modus operandi kejahatan dibidang *Cyber Crime* tidak saja dilakukan dengan alat canggih tetapi kejahatan ini benar-benar sulit menentukan secara cepat dan sederhana siapa sebagai pelaku tindak pidananya. Oleh karena itu dibutuhkan optimalisasi Undang-undang Nomor 11 tahun 2008 Tentang Informasi Dan Transaksi Elektronik.
2. Kelemahan perangkat hukum dalam penegakan hukum pidana khususnya perkara *Cyber Crimes* banyak memiliki keterbatasan. Hal demikian dapat dirasakan seperti apabila kejahatan yang terjadi aparat penegak hukumnya belum siap bahkan tidak mampu (gagap teknologi) untuk mengusut pelakunya dan alat-alat bukti yang dipergunakan dalam hubungannya dengan bentuk kejahatan ini sulit terdeksi.

3. Kelemahan lain ada pada perangkat komputer forensik yang belum dimiliki oleh POLRI, mengingat penting keberadaannya dalam mencegah, maupun menangani kasus-kasus yang berkaitan dengan *Cyber Crime.*

B. SARAN

Berdasarkan temuan yang ada selama penelitian maka disarankan kepada para pengguna internet agar mematuhi norma – norma serta harus beretika baik ketika sedang menjelajahi dunia maya. Selain itu saran juga ditujukan kepada pihak yang berwenang dalam hal ini pemerintah Indonesia melalui Departemen Informasi dan Teknologi agar memenuhi kedua prasyarat dan meningkatkan kinerja dibawah ini yakni :

1. Pembentukan Konsep Kitab Undang-Undang Hukum Pidana Yang Baru

   Perlu adanya konsep KUHP yang baru dalam negara kita, karena perkembangan jaman akan menciptakan kejahatan-kejahatan yang baru pula, sedangkan KUHP lama negara kita sudah tidak layak lagi. Karena sudah tidak mencakup kejahatan-kejahatan baru yang muncul seiring dengan perkembangan jaman.

2. IDCERT (Indonesia Computer Emergency Response Team)

   Salah satu cara untuk mempermudah penanganan masalah keamanan adalah dengan membuat sebuah unit untuk melaporkan kasus keamanan. Masalah keamanan ini di luar negeri mulai dikenali dengan munculnya *"sendmail worm"* (sekitar tahun 1988) yang menghentikan system email Internet kala itu. Kemudian dibentuk sebuah *Computer Emergency Response Team* (CERT). Semenjak itu di negara lain mulai juga dibentuk CERT untuk

menjadi point of contact bagi orang untuk melaporkan masalah kemanan. IDCERT merupakan CERT Indonesia.

3. Sertifikasi Perangkat Keamanan Simtem Komputer

Perangkat yang digunakan untuk menanggulangi keamanan semestinya memiliki peringkat kualitas. Perangkat yang digunakan untuk keperluan pribadi tentunya berbeda dengan perangkat yang digunakan untuk keperluan militer. Namun sampai saat ini belum ada institusi yang menangani masalah evaluasi perangkat keamanan di Indonesia. Di Korea hal ini ditangani oleh *Korea Information Security Agency*.

DAFTAR PUSTAKA

- **Buku**

Abu Bakar Munir, *Cyber Law Policies and Challenges*, 1999.

Adami Chazawi, *Hukum Pembuktian Tindak Pidana Korupsi*, Bandung : PT Alumni, 2006.

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

Ahmad M Ramli, *Prinsip-prisnsip Cyber Law Dan kendala Hukum Positif Dalam Menanggulangi Cyber Crime*, Fakultas Hukum Universitas Padjajaran, Jakarta, Desember 2004.

Ahmad Suwandi dan B. Ryanto Setyo, *"Menabur entuh, Menuai Software Tangguh"*, PC Media 08/2004.

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

Bambang Sunggono, *Metodologi penelitian hukum*, Rajawali Press. Jakarta,2005.

Barda Nawawi Arief, *Beberapa Aspek Kebijakan Penegakan dan Pengembangan Hukum Pidana*, Bandung: PT Citra Aditya Bakti, 1998.

Hari Sasangka dan Lily Rosita, *Hukum Pembuktian Dalam Perkara Pidana*, Mandar Maju. Bandung. 2003

Laporan Akhir Penelitian, Kementrian Komunikasi Dan Informasi, Jakarta, November 2003.

Moch. Safar Hayim, *Mengenali Undang-undang Media Dan Siber*, Refika Aditama.2002.

Moeljatno, *Asas-asas Hukum Pidana*. Bina Aksara, Jakarta.

Peter Mahmud Marzuki, *Penelitian Hukum*, Jakarta : Prenada Media, 2005.

Saifudin Aswar, *Metode Penelitian*, Pustaka Pelajar, Jakarta, 2003.

S'to, "*Seni Internet Hacking Uncencored*",Jasakom, 2004.

_____, *"Kajian Hukum Tentang Kejahatan Di Dunia Maya (Cyber Crime)"*.

_____, *"Naskah Akademik Rancangan Undang-undang Tentang Kejahatan Dunia Maya (Cyber Crime)"*, Seminar Hak Cipta dan Informai, Jakarta, Juni 2003

- **Peraturan Perundang-undangan**

"Garis-garis Besar Haluan Negara GBHN 1999-2004 TAP MPR NO. IV/ MPR/1999", 1999, Sinar Grafika, Jakarta.

Kejaksaan Republik Indonesia, 1998, "Himpunan Peraturan tentang Tugas Dan Wewenang Kejaksaaan", Buku II, diterbitkan oleh Kejaksaan Agung R.I., Jakarta.

Moeljatno, 1994, "Kitab Undang-undang Hukum Pidana", cetakan kesembilanbelas, Bumi Aksara, Jakarta.

Soenarto Soerodibroto, 2000, "KUHP dan KUHAP", Edisi keempat, cetakan kelima, PT RajaGrafindo Persada,Jakarta.

Undang-Undang Nomor 36 tahun 1999 Tentang Telekomunikasi, 2000, cetakan pertama, Sinar Grafika, Jakarta.

Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (ITE), Kementrian Komunikasi dan Informasi Republik Indonesia, 25 Maret 2008.

- **Koran, jurnal, majalah, dan media publikasi lain**

Muladi, 22 Agustus 2002, *"Kebijakan Kriminal terhadap Cybercrime"*, Media Hukum Vol. 1 No. 3, Persatuan Jaksa Republik Indonesia.

Pattiradjawane, Rene L., *"Media Konverjensi dan Tantangan Masa Depan"*, Kompas, 21 Juli 2000.

Yosef Ardi, "*Meroket, Bisnis E-Commerce"*, Kompas, 21 Juli 2000.

- **Website**

http://www.aaxnet.com/news/S000711.html.

http://www.ecorp.com/history.htm.

http://www.msnbc.com/news/471197.asp?cp1=1#BODY

http://www.siliconvalley.com/docs/news/reuters_wire/9004801.htm.

http://www.hukumonline.com/docs/frnt_pg/RUU%21%ITE_2004/htm.

http://www.suaramerdeka.com/harian/0207/24/nas13.htm.

http://business.fortunecity.com/buffett/842/art180199_tindakpidana.htm