# ANALISIS YURIDIS TINDAK PIDANA MENGAKSES SISTEM ELEKTRONIK MILIK ORANG LAIN

**(Studi Putusan Nomor : 2.862/Pid.B/2016/PN.MDN)**

**SKRIPSI**

**OLEH :**

**ALEKSANDER GINTING**

**13.840.0081**

**BIDANG HUKUM KEPIDANAAN**

**FAKULTAS HUKUM**

**UNIVERSITAS MEDAN AREA**

**MEDAN**

**2017**

# LEMBAR PENGESAHAN SKRIPSI

Judul Skripsi : Analisis Yuridis Tindak Pidana Mengakses Sistem Elektronik Milik Orang Lain (Studi Putusan Nomor : 2.862/Pid.B/2016/PN.MDN)

Nama : Aleksander Ginting

NPM : 13.840.0081

Bidang Hukum : Ilmu Hukum Kepidanaan

Disetuju Oleh

Komisi Pembimbing

PEMBIMBING I

(Dr. Isnaini,SH,M.Hum)

PEMBIMBING II

(Ridho Mubarak,SH,MH)

DEKAN

(Dr. Utary Maharany Barus,SH,M.Hum)

Tanggal Lulus : 17 Juni 2017

# ABSTRAK
## ANALISIS YURIDIS TINDAK PIDANA MENGAKSES SISTEM ELEKTRONIK MILIK ORANG LAIN
## (Studi Putusan Nomor : 2.862/Pid.B/2016/PN.MDN)

**OLEH**

**ALEKSANDER GINTING**

**NPM : 13.840.0081**

**BIDANG HUKUM KEPIDANAAN**

Komputer merupakan suatu perangkat ataupun sistem elektronik yang mengolah atau memproses data atau informasi sebagaimana yang diperintahkan, terdiri atas perangkat keras elektronik (*hardware*), dan perangkat lunak program komputer(*software*),prosedur-prosedur (*procedures*) dan penggunaannya (*brainware*) serta data atau informasi itu sendiri (*content*). Ketika digunakan untuk pertama kalinya komputer muncul dalam bentuk *mainframe computer* yang berukuran sangat besar, yang dalam perkembangannya ukuran untuk sebuah komputer semakin lama semakin kecildimulai dari PC (*personal computer)* yang berbentuk desktop, menyusul bentuk PC (*personal computer)* lain yangdisebut laptop atau *notebook* sampai jenis handphone tertentu dapat difungsikan sebagai laptop mini. Bagaimana pertanggungjawaban hukum dan sanksi terhadap pelaku tindak pidana mengakses sistem elektronik milik orang lain. Bagaimana perlindungan hukum terhadap korban kejahatan tindak pidana ITE khususnya korban atas kejahatan mengakses sistem elektronik milik orang lain. Bagaimana Pertimbangan hakim dalam penjatuhan putusan terhadap pelaku tindak pidana mengakses sistem elektronik milik orang lain. jenis data dalam penelitian ini adalah secara Yuridis Normatif yaitu merupakan data yang diperoleh langsung dari intansi terkait yaitu di Pengadilan Negeri Medan dan dari bahan perpustakaan. Pertanggungjawaban pidana adalah pertanggungjawaban orang terhadap tindak pidana yang dilakukannya, tegasnya , yang dipertanggungjawabkan orang itu adalah tindak pidana yang dilakukannya, dengan demikian, terjadinya pertanggungjawaban pidana karena telah ada tindak pidana yang dilakukan oleh seseorang. Upaya pencegahan dan penanggulangan tindak pidana *cyber crime* khususnya pada tindak pidana mengakses sitem elektronik milik orang lain sudah diatur dalam pasal 406 KUHP dan pasal 28 ayat (1) Undang-Undang Informasi dan Transaksi Elektronik. Majelis Hakim akan mempertimbangkan apakah perbuatan terdakwa sebagaimana yang diterangkan dalam persidangan telah memenuhi unsur-unsur delik dari pasal-pasal yang didakwakan. Untuk menentukan apakah terdakwa dapat dinyatakan secara sah dan meyakinkan bersalah melakukan tindak pidana sebagaimana didakwakan Jaksa Penuntut Umum dalam surat dakwaan tersebut maka terlebih dahulu dipertimbangkan tentang tindak pidana yang menjadi dasar dakwaan jaksa Penuntut Umum.


**Kata Kunci : *cyber crime***

## *ABSTRACT*

*CRIMINAL JURIDIS ANALYSIS ACCESSING ANY OTHER PEOPLE ELECTRONICS SYSTEM*

*(Study of Decision Number: 2.862 / Pid.B / 2016 / PN.MDN)*

*BY*

ALEKSANDER GINTING

*NPM: 13,840,0081*

*THE FIELD OF THE CRIMINAL LAW*

*A computer is a device or electronic system that processes or processes data or information as instructed, comprising of electronic hardware (hardware), and software of computer programs (software), procedures (procedures) and its use (brainware) and data or The information itself (content). When used for the first time the computer appears in the form of a very large computer mainframe, which in its development size for a computer the more kecildimulai from PC (personal computer) in the form of desktop, following the form of PC (personal computer ) Others are called laptops or notebooks until certain types of mobile phones can function as a mini laptop. How legal liability and sanctions against criminals access electronic systems belonging to others. How is the legal protection of crime victims of the crime of ITE especially the victim for the crime of accessing the electronic system belonging to someone else. How the judge's judgment in the judgment of the offender against the electronic system belongs to another person. The type of data in this study is Juridicai Normative that is the data obtained directly from the relevant institutions in the Medan District Court and from library materials. Criminal liability is the accountability of a person against a crime he committed, strictly speaking, the person responsible is the crime he committed, thus, the occurrence of criminal liability because there has been a crime committed by someone. Efforts to prevent and control criminal acts of cyber crime, especially on the crime of accessing electronic systems belonging to others have been regulated in Article 406 of the Criminal Code and Article 28 paragraph (1) of Information and Electronic Transaction Law. The Panel of Judges will consider whether the act of the defendant as described in the hearing has fulfilled the elements of the offense of the articles being charged. To determine whether the defendant can be declared legally and convincingly guilty of committing a crime as prosecuted by the Public Prosecutor in the indictment, then first consider the offense on which the prosecutor charges.*


***Keywords: cyber crime***

# KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Tuhan Yang Maha Esa yang telah mengkaruniakan kesehatan dan juga kelapangan berpikir kepada penulis sehingga akhirnya tulisan ilmiah dalam bentuk skripsi ini dapat juga terselesaikan.

Penulisan skripsi ini pada dasarnya adalah untuk memenuhi kewajiban akhir dari perkuliahan penulis di Fakultas Hukum Universitas Medan Area dalam Program pendidikan strata satu (S-1),pada bidang hukum kepidanaan.

Adapun judul yang diajukan sehubungan dengan penyusunan skripsi ini adalah **"Analisis yuridis Tindak Pidana Mengakses Sistem Elektronik Milik Orang Lain (Studi kasus Putusan No.2.682/Pid.B/PN.MDN)"**

Dalam penulisan skripsi iniu banyak pihak telah memberikan masukan,saran kepada penulis,maka pada kesempatan ini penulis ingin mengucapkan terimakasih kepada pihak-pihak tersebut terutama kepada:

1. Ibu Dr. Utasry Maharany, S.H,M.Hum selaku dekan Fakultas Hukum Universitas Medan Area.
2. Ibu Anggreni Atmei Lubis, S.H,M.Hum selaku Wakil Dekan Bidang Akademik Universitas Medan Area,
3. Bapak Isnaini, SH, M.Hum selaku Pembimbing I penulis
4. Bapak Ridho Mubarak,SH, M.H selaku Pembimbing II Penulis.
5. Ibu Wessy Trisna, SH,MH selaku Ketua Bidang Hukum Kepidanaan Fakultas Hukum Universitas Medan Area dan selaku Sekretaris Penulis.
6. Bapak dan Ibu Dosen serta seluruh Civitas Akademika Fakultas Hukum Universitas Medan Area

7. Hormat Ginting dan Tio Minar br Sipayung Kedua orang tua yang sudah bersusah payah membesarkan dan mendidik penulis sejak kecil hingga bangku kuliah tanpa rasa pamrih.
8. Veronika Lia Kristina br Ginting,Amd, Delisoviana br Ginting,Amd, Yohana, S.E dan Beltsazar Norman Sqwartz Panjaitan, S.H yang selalu mendukung penulis dengan semua perhatian dan kasih sayangnya.
9. Teman-teman angkatan 2013 Fakultas Hukum Universitas Medan Area.Hadi Sopiyan,SH, Erick Wellington Sirait,SH, Suaridin Lase,SH, Dio Poliando Panggabean,SH, Nyoman Bagus,CSH. Atas segala bantuan dan dorongan dari semua pihak di atas penulis hanya dapat bermohon,hanya Tuhan Yang Maha Esa sajalah yang dapat membalas budi baik dan bantuan mereka tersebut,mudah-mudahan skripsi penulis ini akan memberikan manfaat bagi kita semua.

Medan,17 Juni 2017

Penulis

**ALEKSANDER GINTING**

NPM : 13.840.0081

# DAFTAR ISI

Halaman

**ABSTRAK**

**KATA PENGANTAR** ..... **i**

**DAFTAR ISI** ..... **iii**

**BAB I PENDAHULUAN** ..... 1

1.1 Latar Belakang Masalah ..... 1
1.2 Idantifikasi Masalah ..... 10
1.3 Pembatasan Masalah ..... 11
1.4 Perumusan Masalah ..... 11
1.5 Tujuan dan Manfaat Penelitian ..... 12

**BAB II LANDASAN TEORI** ..... **14**

2.1 Teori Perlindungan Hukum ..... 14
2.2 Teori Penegakan Hukum ..... 16
2.1.1 Pengertian Melawan Hukum ..... 18
2.1.2 Pengertian Tindak Pidana ..... 21
2.1.3 Pengertian *Cyber Crime* ..... 27
2.1.4 Faktor-Faktor yang mempengaruhi tindak pidana ..... 41
*Cyber Crime* khususnya *Cracking*.
2.3 Kerangka Pemikiran ..... 44
2.4 Hipotesis ..... 45

**BAB III METODE PENELITIAN** ..... **48**

3.1 Jenis, Lokasi dan Waktu Penelitian ..... 48
3.2 Teknik Pengumpulan Data ..... 51
3.3 Analisis kualitatif ..... 51

**BAB IV HASIL PENELITIAN DAN PEMBAHASAN** ..... **51**

4.1. Hasil Penelitian ..... 52
4.1.1. Pertanggungjawaban dan sanksi hukum bagi pelaku Tindak Pidana Mengakses Sistem Elektronik Milik Orang Lain ..... 52
4.1.2. Perlindungan hukum bagi korban Tindak Pidana Mengakses Sistem Elektronik Milik Orang Lain ..... 56
4.1.3. Pertimbangan Hakim Dalam Penjatuhan Terhadap Tindak Pidana Mengakses Sistem Elektronik Milik Orang Lain pada Putusan No.2.862/Pid.B/2016?PN.MDN ..... 65

**BAB V SIMPULAN dan SARAN ..... 71**

5.1. Simpulan ..... 71
5.2. Saran ..... 72

**DAFTAR PUSTAKA**

**LAMPIRAN**

# BAB I

# PENDAHULUAN

## 1.1 Latar Belakang Masalah

Pada saat ini kita berada disuatu era yang disebut era teknologi informasi. Era ini dimulai sejak munculnya suatu teknologi baru yang disebut komputer (*computer*).[1]Komputer merupakan suatu perangkat ataupun sistem elektronik yang mengolah atau memproses data atau informasi sebagaimana yang diperintahkan, terdiri atas perangkat keras elektronik (*hardware*), dan perangkat lunak program komputer (*software*), prosedur-prosedur (*procedures*) dan penggunaannya (*brainware*) serta data atau informasi itu sendiri (*content*).[2]Ketika digunakan untuk pertama kalinya komputer muncul dalam bentuk *mainframe computer* yang berukuran sangat besar, yang dalam perkembangannya ukuran untuk sebuah komputer semakin lama semakin kecildimulai dari PC (*personal computer)* yang berbentuk desktop, menyusul bentuk PC (*personal compuier)* lain yangdisebut laptop atau *notebook* sampai jenis handphone tertentu dapatdifungsikan sebagai laptop mini. Dalam perkembangannya, komputer telah memunculkan sesuatu yangbaru di dalam kehidupan kita, yaitu internet.

Internet (*Interconnected Network*) merupakan jaringan *(network)* komputer yang terdiri dari ribuan jaringan komputer independen yang dihubungkan satu dengan yang lainnya. Jaringan komputer ini dapat

---

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

[2]. Edmon Makarim, *Kompilasi Hukum Telematika, (Jakarta : RajaGrafindo Persada), 2003,* halaman 54

digunakan oleh lembaga pendidikan, pemerintahan, militer, organisasi, bisnis dan organisasi lainnya. Internet merupakan jaringan komputer terbesar dunia. Internet sendiri pada dasarnya hanya sebuah media pengantar sebagaimana media-media pengantar dalam bentuk lainnya. Adanya Internet menciptakan jenis dunia baru yang tak lagi dihalangi oleh batas-batas teritorial antara negara yang dahulu ditetapkan. Internet membawa pada dunia tanpa batas dan menembus batas kedaulatan negara yang sebelumnya tidak pernah dikenal oleh manusia, yaitu dunia yang disebut "*virtual world*" yang dalam bahasa Indonesia ada yang menerjemahkannya dengan "dunia maya" atau "mayantara".

Disebut dunia maya oleh karena dunia tersebut tidak seperti dunia dimana kita hidup danmelakukan kegiatan. Dunia dimana kita hidup bersifat *physical* (fisik), sedangkan dunia virtual atau dunia maya bersifat *non-physical* (*non-fisik*). Oleh karena semua yang berkaitan dengan komputer diberi keterangan dengan sebutan "*cyber*" maka untuk ruang lingkup yang berhubungan dengan komputer sering disebut pula "*cyberspace*" (ruang siber).[3]Dunia maya atau *cyberspace* adalah dunia atau ruang tempat beroperasinya kegiatan atau kehidupan internet. Dunia tempat beroperasinya kegiatan atau kehidupan manusia disebut *real world* (dunia nyata) atau *physical world* (dunia fisik). Walaupun peralatan komputer yang disebut perangkat keras *( computer hardware*) berada di dunia nyata, tetapi kegiatan program komputer (yang disebut perangkat lunak komputer atau *computer software*) tidak berlangsung di dunia nyata melainkan di duniamaya.

[3].Sutan Remy Syahdeini, Op.cid, 2009, halaman 8.

Munculnya dunia maya telah mengubah kebiasaan banyak orang terutama yang dalam kehidupannya terbiasa menggunakan internet. Dengan internet, kita dapat melakukan hampir semua kegiatan yang dapat dilakukan didunia nyata *(real world*) dapat dilakukan di dunia maya, dengan kebebasan beraktivitas dan berkreasi yang paling sempurna. Namun dibalik kegemerlapan itu, internet juga menciptakan peluang-peluang baru bagi kejahatan sebagai akibat negatif dari perkembangan teknologi.

Seiring dengan perkembangan teknologi komunikasi yang begitu pesat, orang-orang tertentu dapat juga menyalah gunakan sarana Internet . Salah satu dampak negative teknologi Internet ini adalah munculnya kejahatan melalui media internet yang sudah sering terjadi di masyarakat. Kejahatan dengan menggunakan layanan internet telah banyak memakan korban, pada umumnya yaitu masyarakat pengguna internet itu sendiri. Di dunia *virtual* orang melakukan berbagai kejahatan yang justru tidak dapat dilakukan di dunia nyata. Kejahatan tersebut diiakukan dengan menggunakan *computer* sebagai sarana perbuatannya. Dalam hal ini penulis lebih mengkonsentrasikan penulisan mengenai pelaku kejahatan dunia maya pada tindak pidana melawan hukum dengan sengaja mengakses sisten elektronik milik orang lain atau biasa disebut dengan *cracker. Cracker* biasanya mengacu pada seseorang yang punya minat besar untuk mempelajari sistem komputer secara detail dan bagaimana meningkatkan kapabilitasnya. Boleh dibilang cracker ini sebenarnya adalah *hacker* yang yang memanfaatkan kemampuannya untuk hal-hal yang negatif. Aktivitas *cracking* di internet memiliki lingkup yang sangat luas, mulai dari pembajakan account milik orang lain, pembajakan situs

web, probing, menyebarkan virus, hingga pelumpuhan target sasaran. Tindakan yang terakhir disebut sebagai DoS (*Denial Of Service*). Dos attack merupakan serangan yang bertujuan melumpuhkan target (*hang, crash*) sehingga tidak dapat memberikan layanan. Pada kasus Hacking ini biasanya modus seorang hacker adalah untuk menipu atau mengacak-acak data sehingga pemilik tersebut tidak dapat mengakses web miliknya. Untuk kasus ini Pasal 406 KUHP dapat dikenakan pada kasus *deface* atau *hacking* yang membuat sistem milik orang lain, seperti *website* atau program menjadi tidak berfungsi atau dapat digunakan sebagaimana mestinya.

> "barang siapa dengan sengaja dan dengan hak membinasakan, merusakkan, membuat sehingga tidak dapat dipakai lagi atau menghilangkan suatu barang yang sama sekali atau sebagiannya kepunyaan orang lain, dihukum penjara selama dua tahun delapan bulan atau denda sebanyak-banyaknya Rp 4.500".

Kejahatan yang dilakukan di dunia maya dengan menggunakan *computer* disebut "kejahatan komputer" atau "*cybercrime*". Memang belum ada kesatuan pendapat dikalangan para ahli mengenai definisi *cyber crime*. Hal tersebut disebabkan kejahatan ini ( *cyber crime*) merupakan kejahatan yang relatif baru dibandingkan dengan kejahatan-kejahatan *konvensional*. Ada yang menerjemahkan dengan kejahatan *cyber*, kejahatan di dunia maya, kejahatan *virtual*, bahkan ada yang mempergunakan istilah aslinya yaitu *cyber crime* tanpa menerjemahkannya.

*Cyber crime* merupakan salah satu bentuk atau dimensi baru dari kejahatan masa kini yang mendapat perhatian luas di dunia

internasional.[4]Permasalahan *Cyber crime* harus di tangani secara serius karena dampak dari kejahatan ini sangat luas dan banyak merugikan perekonomian masyarakat sehingga apabila tidak ditanggulangi secara dini akan berkembang dan jika tidak terkendali dampaknya akan sangat fatal bagi kehidupan masyarakat.[5]Di Indonesia sendiri, sampai saat ini tidak ada rumusan baku tentang definisi *cyber crime*. Namun demikian, bukan berarti tidak adanya hukum di Indonesia yang mengatur mengenai *cyber crime*. Saat ini Indonesia telah memiliki UU No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.Sebelum berlakunya Undang-Undang tersebut, tentu saja hal itu hanya dapat dilakukan oleh penegak hukum sepanjang di dalam KUHP memang dapat ditemukan pasal-pasal yang pas untuk dipakai menjatuhkan pidana bagi pelaku kejahatan komputer tersebut.

Undang-Undang ITE boleh disebut sebuah *cyber law* karena muatan dan cakupannya luas membahas pengaturan di dunia maya, meskipun di beberapa sisi ada yang belum terlalu lugas dan juga ada yang sedikit terlewat. Muatan UU ITE adalah sebagai berikut:

1.Tanda tangan elektronik memiliki kekuatan hukum yang sama dengan tanda tangan konvensional (tinta basah dan bermaterai). Sesuai dengan e-ASEAN

2.*Framework Guidelines* (pengakuan tanda tangan digital lintas batas)

3.Alat bukti elektronik diakui seperti alat bukti lainnya yang diatur dalam KUHP

[4] Dikdik M. Arief Mansur, SH, MH ; Elisatris Gultom, SH, MH, *Cyber Law Aspek Hukum*
[5]Volodymyr Golubev, cyber crime and legal problems of Internet usage, dalam Tindak Pidana Mayantara : Perkembangan Kajian Cyber Crime di Indonesia , (Jakarta : RajaGrafindo Persada), hal 1

4.UU ITE berlaku untuk setiap orang yang melakukan perbuatan hukum, baik yang berada di wilayah Indonesia maupun di luar Indonesia yang memiliki akibat hukum di Indonesia[6]

Perbuatan yang dilarang (*cybercrime*) dijelaskan pada Bab VII (pasal 27-37) Undang-undang No. 11 Tahun 2008 Tentang teransaksi dan Transaksi Elektronik:

a) Pasal 27 (Asusila, Perjudian, Penghinaan, Pemerasan)
b) Pasal 28 (Berita Bohong dan Menyesatkan, Berita Kebencian dan Permusuhan)
c) Pasal 29 (Ancaman Kekerasan dan Menakut-nakuti)
d) Pasal 30 (Akses Komputer Pihak Lain Tanpa Izin, Cracking)
e) Pasal 31 (Penyadapan, Perubahan, Penghilangan Informasi)
f) Pasal 32 (Pemindahan, Perusakan dan Membuka Informasi Rahasia)
g) Pasal 33 (Virus(Membuat Sistem Tidak Bekerja)

Semakin berkembangnya kejahatan dalam masyarakat, sehingga hukum juga harus berkembang agar fungsinya sebagai pemberi rasa aman dapat terpenuhi, dengan adanya Undang-undang ini maka diharapkan masyarakat takut untuk melakuakan kesalahan, karna dijelaskan pada pada ayat (1), bertanggung jawab atas segala kerugian dan konsekwensi yang timbul, tetapi dalam Undang-Undang ITE pihak yang bertanggung jawab atas segala akibat hukum dalam pelaksanaan Transaksi Elektronik. Sebagaimana dimaksud pada ayat (1) diatur sebagai berikut:

[6] ,Undang_undang no 11 tahun 2008 tentang Informasi dan Transaksi Elektronik

1. Jika dilakukan sendiri,segala akibat hukum dalam Pelaksanaan Transaksi Elektronik menjadi tanggung jawab para pihak yang bertransaksi.
2. Jika dilakukan melalui pemberi kuasa,segala akibat hukum dalam pelaksanaan Transaksi Elektronik menjadi tanggung jawab pemberi kuasa.
3. Jika dilkukan melaui agen Elektronik,segala akibat hukum dalam pelaksanaan Transaksi Elektronik menjadi tanggung jawab penyelenggara agen elektronik.

Melengkapi Kitab Undang–Undang Hukum Acara Pidana (KUHAP) yang telah ada, UU ITE juga mengatur mengenai hukum acara terkait penyidikan yang dilakukan aparat penegak hukum (kepolisian dan kejaksaan) yang memberi paradigma baru terhadap upaya penegakkan hukum dalam rangka meminimalkan potensi *abuse of power* penegak hukum sehingga sangat bermanfaat dalam rangka memberikan jaminan dan kepastian hukum. "Penyidikan di bidang teknologi informasi dan transaksi elektronik dilakukan dengan memperhatikan perlindungan terhadap privasi, kerahasiaan, kelancaran layanan publik, *integritas* data atau keutuhan data, sesuai ketentuan peraturan perundang-undangan (Pasal 43 ayat (2).Sedangkan Penggeledahan dan/atau penyitaan terhadap sistem elektronik yang terkait dengan dugaan tindak pidana harus dilakukan atas izin ketua pengadilan negeri setempat dan wajib menjaga terpeliharanya kepentingan pelayanan umum Pasal 43 ayat (3).

Namun demikian perlu disikapi bahwa tidak mustahil ada kejahatan komputer tertentu yang ternyata belum dinyatakan sebagai tindak pidana (belum diatur) oleh UU No.11 Tahun 2008 tentang Informasi danTransaksi

Elektronik tersebut.[7] Fenomena *cyber crime* memang harus diwaspadai karena kejahatan iniagak berbeda dengan kejahatan lain pada umumnya. Kejahatan mayantara dapat terjadi tanpa diperlukan interaksi langsung antara pelaku dengan korban kejahatan. Bisa dipastikan dengan global internet, semua negara yang melakukan kegiatan internet hampir pasti akan terkena imbas perkembangan *cyber crime* ini. Modus kejahatan dalam dunia maya memang agak sulit dimengerti oleh orang-orang yang tidak menguasai pengetahuan teknologi informasi.

Sebab,salah satu karakter pokok *cyber crime* adalah penggunaan teknologi informasi dalam modus operandinya.Salah satu ciri *cyber crime* adalah memanfaatkan jaringan teknologi informasi secara global. Aspek global menimbulkan kondisi seakan-akan dunia tidak ada batasnya (*borderless*). Keadaan ini dapat mengakibatkan pelaku, korban serta tempat dilakukannya tindak pidana *( locus delictie*) terjadi di negara yang berbeda-beda. Hukum pidana adalah hukum yang terikat pada ruang dan waktu,sehingga mengenai kapan dan dimana tindak pidana dilakukan harus jelas diketahui. Locus Delictie menurut *Black's Law Dictionary is the placewhere an offense is commiteted: the place where the last event necessaryto make the actor liable occurs.* Terjemahannya adalah *locus delictie* merupakan tempat dimana suatu tindak pidana terjadi tempat dimana kejadian (tindak pidana) dapat menyebabkan pelaku harus bertanggungjawab.[8]

Penentuan *Locus Delictie* menjadi persoalan ketika pembuat dan penyelesaian delik tidak berada di suatu tempat yang sama. Seperti yang

[7] Loc.cit

[8] Bryan A. Garner, Black's Law Dictionary seventh Edition, St. Paul Minn: West Group, 1999, hal. 951

terjadi dalam cyber crime, dimana perbuatan melawan hukum yang dilakukan di suatu tempat dapat berakibat di tempat lain,demikian pula sebaliknya. Untuk menyelesaikan permasalahan ini adalah mengikuti salah satu pola dari empat macam ajaran sebagai berikut :

1. Ajaran tindakan badaniah, untuk menentukan tempat kejadian, pusatperhatian adalah kepada tempat dimana pelaku melakukan suatu tindakpidana, unsur-unsur tindak pidana pada saat itu menjadi sempurna.
2. Ajaran tempat bekerjanya alat, tempat kejadiannya adalah dimana alat yang digunakan bekerja dan telah sempurna atau menimbulkan suatutindak pidana.
3. Ajaran akibat dari tindakan, tempat tindak pidana adalah di tempat terjadinya suatu akibat, yang merupakan penyempurnaan dari tindak pidana yang telah terjadi.
4. Ajaran berbagai tempat tindak pidana, tempat tindak pidana adalah gabungan dari ketiga-tiganya atau dua diantara ajaran-ajaran tersebut diatas.[9]

Keempat teori locus delictie ini yang kemudian akan digunakan untuk menentukan kewenangan pengadilan mengadili tindak pidana khususnya yang dilakukan dengan memanfaatkan media Internet. Banyak permasalahan yang muncul ketika *cyber crime* dapat diungkapoleh aparat penegak hukum, khususnya apabila dalam kejahatan tersebut terkait unsur-unsur asing, seperti pelakunya orang asing, korbannya orangasing atau tempat terjadinya di luar negeri tetapi pengaruhnya dirasakan diIndonesia. Salah satu permasalahan

[9] E.Y Kanter dan S.R Sianturi, Asas-Asas hukum Pidana di Indonesia dan Penerapannya, (Jakarta : Penerbit Storia Grafika), 2002, halaman 113-115

hukum utama yang muncul bersamaan dengan terungkapnya kejahatan tersebut adalah masalah kerumitan berkenaan dengan *yurisdiksi* hukum karena tidak lengkap dan tidak konsistennya hukum suatu negara.

Dalam hukum Internasional berlaku ketentuan bahwa tidak seorang pun dapat secara sah diekstradisi dari satu negara untuk menghadapi tuntutan dinegara lain kecuali apabila kedua negara tersebut menganut kriminalitas ganda *(dual criminality)*, Artinya suatu tindak pidana harus dianggap diakui oleh bhukum negara tersebut dan sama tingkatannya dalam jenis tindak pidananya (*same level criminality*) sebelum ekstradisi tersebut dipertimbangkan oleh pengadilan.

Berdasarkan latar belakang di atas sangat menarik sekali bagi penulis untuk mencoba melakukan pembahasan tantang kejahatan dunia maya (*Cyber Crime*) terutama tentang tindakan melawan hukum dengan sengaja mengakses system elektronik milik orang lain yang terjadi dalam dunia maya dan meneliti upaya penanggulangannya dengan judul "*Analisis Yuridis Tindak Pidana Melawan hukum Dengan Sengaja Telah Mengakses Sistem Elektronik Milik Orang Lain*".

## 1.2 Identifikasi Masalah

Secara Umum permasalah dalam penelitian ini adalah tentang Kajian Hukum Tindak Pidana Melawan Hukum Dengan Sengaja Mengakses Sistem Elektronik Milik Orang Lain Ditinjau dari Undang-Undang No.11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, maka berdasarkan latar belakang dapat di identifikasikan sebagai berikut :

1. Terhadap hal-hal yang menyatakan suatu perbuatan adalah Perbuatan Tindak Pidana Melawan Hukum dengan Sengaja Mengakses Sistem Elektronik Milik Orang Lain Ditinjau dari Undang-Undang No. 11 Tahun 2008.
2. Terhadap Undang-Undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

## 1.3 Pembatasan Masalah

Disebabkan keterbatasan waktu, dan proses yang panjang dalam hal ini penelitian dilakukan hanya tentang dasar suatu perbuatan tindak pidana dapat dinyatakan sebagai tindak pidana dengan sengaja melawan hukum mengakses system elektronik milik orang lain dalam Perkara Putusan No. 2.862/Pid.B/2016/PN.MDN dan melakukan penncegahan serta menanggulangi terjadinya tindak pidana dengan sengaja mengakses system elektronik.

## 1.4 Perumusan Masalah

Adapun permasalahan yang akan diteliti dalam penelitian ini adalah :

1. Bagaimana pertanggungjawaban hukum dan sanksi terhadap pelaku tindak pidana mengakses sistem elektronik milik orang lain ?
2. Bagaimana perlindungan hukum terhadap korban kejahatan tindak pidana ITE khususnya korban atas kejahatan mengakses sistem elektronik milik orang lain ?
3. Bagaimana Pertimbangan hakim dalam penjatuhan putusan terhadap pelaku tindak pidana mengakses sistem elektronik milik orang lain ?

## 1.5 Tujuan dan Manfaat Penelitian

Adapun tujuan secara umum yang hendak di capai dalam penelitian ini adalah sesuai dengan pokok permasalahn yang ada, maka tujuan penulisan skripsi ini adalah :

1. Untuk Mengetahui pertanggungjawaban dan sanksi hukum bagi pelaku tindak pidana dengan sengaja melawan hukum mengakses system elektronik milik orang lain.
2. Untuk mengetahui perlindungan hukum bagi korban tindak pidana dengan sengaja mengakses system elektronk milik orang lain.
3. Untuk mengetahui pendapat hakim bagi pelakuk tindak pidana dengan sengaja mengakses sistem elektronik milik orang lain.

**1. Manfaat Teoritis**

Diharapkan hasil penelitian ini dapat dijadikan sebagai bahan kajian lebih lanjut untuk melahirkan beberapa konsep ilmiah yang pada gilirannya akan memberikan sumbangan pemikiran bagi perkembangan ilmu hukum kepidanaan khususnya mengenai, Putusan No. 2.862/Pid.B/2016/PN.MDN.

**2. Manfaat Praktis**

a. Sebagai pedoman dan masukan bagi semua pihak terutama masyarakat dan para penegak hukum, agar lebih memberikan perhatian dan kebijaksanaan dalam menggunakan media elektronik untuk mencegah terjadinya tindak pidana dengan sengaja melawan hukum mengakses sitem elektronik milik orang lain. Sebagai bahan Informasi semua pihak yang berkaitan dengan perkembangan ilmu hukum kepidanaan.

b. Sebagai bahan kajian lebih lanjut terhadap kalangan akademis untuk menambah wawasan dalam bidang hukum kepidanaan khususnya mengenai kajian hukum tindak pidana dengan sengaja melawan hukum mengakses system elektronik milik orang lain.

# BAB II

# LANDASAN TEORI

## 2.1 Teori Perlindungan Hukum

Manusia merupakan makhluk ciptaan Tuhan yang sejak lahir memiliki hak-hak dasar yaitu hak untuk hidup, hak untuk dilindungi, hak untuk bebas dan hak-hak lainnya. Jadi, pada dasarnya setiap manusia memiliki hak untuk dilindungi termasuk dalam kehidupan bernegara. Dengan kata lain, setiap warganegara akan mendapat perlindungan dari negara. Hukum merupakan sarana untuk mewujudkannya sehingga muncul teori perlindungan hukum. Ini adalah perlindungan akan harkat dan martabat serta hak-hak asasi manusia berdasarkan ketentuan hukum oleh aparatur negara. Dengan begitu, perlindungan hukum merupakan hak mutlak bagi setiap warganegara dan merupakan suatu kewajiban yang harus dilakukan oleh pemerintah, mengingat Indonesia yang dikenal sebagai negara hukum.[10]

Terdapat beberapa teori perlindungan hukum yang diutarakan oleh para ahli, seperti Setiono yang menyatakan bahwa perlindungan hukum merupakan tindakan untuk melindungi masyarakat dari kesewenang-wenangan penguasa yang tidak sesuai dengan aturan yang berlaku untuk mewujudkan ketenteraman dan ketertiban umum. Tetapi yang paling relevan untuk Indonesia adalah teori dari Philipus M.Hadjon. Dia menyatakan bahwa

[10] Maria Alfons, "Implementasi Perlindungan Indikasi Geografis Atas Produk-produk Masyarakat Lokal Dalam Perspektif Hak Kekayaan Intelektual", Ringkasan Disertasi Doktor, (Malang: Universitas Brawijaya, 2010), hal 18.

perlindungan hukum bagi rakyat berupa tindakan pemerintah yang bersifat preventif dan represif. Bersifat preventif artinya pemerintah lebih bersikap hati-hati dalam pengambilan dan pembuatan keputusan karena masih dalam bentuk tindakan pencegahan. Sedangkan bersifat represif artinya pemerintah harus lebih bersikap tegas dalam pengambilan dan pembuatan keputusanatas pelanggaran yang telah terjadi.[11]

Perlindungan hukum preventif merupakan hasil teori perlindungan hukum berdasarkan Philipus. Perlindungan hukum ini memiliki ketentuan-ketentuan dan ciri tersendiri dalam penerapannya. Pada perlindungan hukum preventif ini, subyek hukum mempunyai kesempatan untuk mengajukan keberatan dan pendapatnya sebelum pemerintah memberikan hasil keputusan akhir. Perlindungan hukum ini terdapat dalam peraturan perundang-undangan yang berisi rambu-rambu dan batasan-batasan dalam melakukan sesuatu. Perlindungan ini diberikan oleh pemerintah untuk mencegah suatu pelanggaran atau sengketa sebelum hal tersebut terjadi. Karena sifatnya yang lebih menekankan kepada pencegahan, pemerintah cenderung memiliki kebebasan dalam bertindak sehingga mereka lebih hati-hati dalam menerapkannya. Belum ada peraturan khusus yang mengatur lebih jauh tentang perlindungan hukum tersebut di Indonesia.

Perlindungan hukum represif juga merupakan hasil teori dari Philipus, tetapi ini memiliki ketentuan-ketentuan dan ciri yang berbeda dengan perlindungan hukum preventif dalam hal penerapannya. Pada hukum represif

[11] Phillipus M. Hadjon, "perlindungan hukum Bagi Rakyat Indonesia", (Surabaya: PT. Bina Ilmu, 1987), hal 2 .

ini, subyek hukum tidak mempunyai kesempatan untuk mengajukan keberatan karena ditangani langsung oleh peradilan administrasi dan pengadilan umum. Selain itu, ini merupakan perlindungan akhir yang berisi sanksi berupa hukuman penjara, denda dan hukum tambahan lainnya.Perlindungan hukum ini diberikan untuk menyelesaikan suatu pelanggaran atau sengketa yang sudah terjadi dengan konsep teori perlindungan hukum yang bertumpu dan bersumber pada pengakuan dan perlindungan terhadap hak-hak manusia dan diarahkan kepada pembatasan-pembatasan masyarakat dan pemerintah.

**Teori Penegakan Hukum**

Hukum dan penegakan Hukum adalah satu kesatuan yang tak dapa dipisahkan, keduanya harus bisa berjalan secara sinegis. subtansi (isi) hukum yang termuat dalam berbagai peraturan perundangan hanya akan menjadi sampah tampa ditopang dengan sistem hukum serta budaya hukum yang tumbuh dan berkembang dalam masyarakat. Berbicara hukum secara das sollen , artinya kita sedang berbicara mengenai cita atau keinginan hukum. Nah salah satu yang menjadi cita hukum adalah dengan tegaknya hukum itu sendiri. Penulis sendiri kurang sepakat dalam penggunaan kata penegakan hukum, penulis lebih sepakat dengan kata pengakan keadilan. "Dalam hukum belum tentu ada keadilan, tapi dalam keadilan sudah pasti ada hukum" begitulah kira-kira perkataan Mahfud MD dalam acara seminarnya.[12]

[12] Wignjosoebroto, Soetandyo, Dari Hukum Kolonial ke Hukum Nasional Dinamika Sosial Politik Dalam Perkembangan Hukum di Indonesia, Jakarta: Raja Grapindo Persada, 2009

Teori-teori pengakan Hukum dapat kita jumpai diberbagai literatur, baik itu buku, majalah atau media lain yang tersebar. artikel yang sedang anda baca ini satu dari sekian banyak yang mengulas mengenai teori penegakan Hukum. untuk itu, berikut ini penulis akan membahas dengan bahasa sederhana beberapa teori yang membahas tentang penegakan hukum

Pakar Hukum yang sangat terkenal dengan teorinya adalah Freidmann. menurut Freidmann *Friedman* berhasil atau tidaknya Penegakan hukum bergantung pada: Substansi Hukum,Struktur Hukum/Pranata Hukum dan Budaya Hukum.

Substansi hukum adalah keseluruhan asas-hukum, norma hukum dan aturan hukum, baik yang tertulis maupun yang tidak tertulis, termasuk putusan pengadilan

Struktur Hukum adalah keseluruhan institusi penegakan hukum, beserta aparatnya. Jadi mencakupi: kepolisian dengan para polisinya; kejaksaan dengan para jaksanya; kantor-kantor pengacara dengan para pengacaranya, dan pengadilan dengan para hakimnya

Budaya Hukum adalah kebiasaan-kebiasaan, opini-opini, cara berpikir dan cara bertindak, baik dari para penegak hukum maupun dari warga masyarakat.Substansi dan Aparatur saja tidak cukup untuk berjalannya sistem hukum. oleh karenanya, Lawrence M Friedman menekankan kepada pentingnya Budaya Hukum (Legal Culture).

### 2.1.1 Pengertian Melawan Hukum

Pengertian Perbuatan Melawan Hukum menurut Wiryono Prodjodikoro adalah perbuatan yang mengakibatkan keguncangan dalam kehidupan bermasyarakat dan keguncangan ini tidak hanya terdapat dalam kehidupan bermasyarakat apabila peraturan-peraturan hukum dalam suatu masyarakat dilanggar (langsung). Oleh karena itu, tergantung dari nilai hebatnya keguncangan itu. Meskipun secara langsung hanya mengenai peraturan kesusilaan, keagamaan atau sopan santun, tetapi harus dicegah keras, seperti mencegah suatu perbuatan yang langsung melawan hukum.Perbuatan melawan hukum bukan hanya berupa perbuatan yang langsung melawan hukum, melainkan juga perbuatan yang secara langsung melanggar peraturan lain dari hukum yaitu peraturan di lapangan kesusilaan, keagamaan dan sopan santun.

Menurut Mr. Ter Haar, Pengertian Perbuatan Melawan Hukum ialah tiap-tiap gangguan dari keseimbangan, tian-tiap gangguan pada barang-barang kelahiran dan kerohaniaan dari milik hidup seseorang atau gerombolan orang-orang. Pengertian perbuatan melawan hukum yang dikemukakan Ter Haar mirip sekali dengan sifat suatu perbuatan melawann hukum yang diuraikan Mr. C. Van Vollenhoven. Van Vollenhoen mengusulkan dalam pasal 92 dari "*Adatwetboekje*" itu pemakaian istilah *ongeoorloofde gedraging* (perbuatan yang tidak diperbolehkan), hal ini sama dengan yang dimaksud dalam perbuatan melawan hukum.[13]

[13] http://sosialhukum.blogspot.com/2016/01/perbuatan-melawan-hukum.html diakses pada tanggal 20 Februari 2017 pada pukul 23:15 wib

Di Indonesia hal ini tidak begitu sulit, karena dalam hukum adat ada suatu persamaan corak di antara peraturan-peraturan hukum di satu pihak dan peraturan-peraturan keagamaan, kesusilaan dan sopan santun di lain pihak. Semua peraturan-peraturan tidak termuat dalam suatu undang-undang, sehingga para penguasa dalam hal ini para hakim tidak begitu terikat pada kata-kata yang terpaku dalam suatu undang-undang. Dengan ini para penguasa itu lebih berkesempatan untuk benar-benar memperhatikan rasa keadilan yang tiap waktu berada dalam dada para anggota masyarakat tentang suatu hal yang tertentu. Berbicara mengenai perbutan melawan hukum, maka untuk dapat mengatakan bahwa suatu perbuatan merupakan perbuatan melawan hukum harus dipenuhi unsur-unsur perbuatan melawan hukum, yaitu :

1. Adanya suatu perbuatan yang dilakukan. Suatu perbuatan melawan hukum diawali oleh suatu perbuatan dari si pelaku. Perbuatan disini merupakan perbuatan aktif (melakukan sesuatu) maupun pasif (tidak melakukan sesuatu), namun secara hukum orang tersebut diwajibkan untuk tunduk terhadap perintah undang-undang, kesusilaan dan ketertiban di dalam masyarakat.
2. Perbuatan tersebut melawan hukum jika pelaku tidak melaksanakan apa yang diwajibkan oleh undang-undang, ketertiban umum dan ataupun kesusilaan, maka perbuatan pelaku dalam hal ini dapat dianggap telah melanggar hukum, sehingga memiki konsekuensi tersendiri yang dapat dituntut oleh pihak lain yang merasa telah dirugikan.

3. Dapat dikatakan perbuatan melawan hukum jika, adanya kerugian bagi korban. Yang dimaksud dengan kerugian dalam hal ini, terdiri dari kerugian yang bersifat materil dan kerugian yang bersifat immateril. Akibat dari perbuatan melawan hukum harus menimbulkan adanya kerugian di pihak korban, sehingga hal ini membuktikan adanya suatu perbuatan yang melanggar hukum.
4. Adanya hubungan kausal (sebab akibat) antara perbuatan dengan kerugian. Hubungan kausal merupakan salah satu dari ciri pokok adanya suatu perbuatan melawan hukum. Perbuatan melawan hukum dalam kasus ini harus dilihat secara *materil*. Dikatakan dilihat secara *materil* karena sifat perbuatan melawan hukum harus dilihat sebagai suatu kesatuan tentang akibat yang ditimbulkan olehnya terhadap pihak korban.

Untuk hubungan sebab akibat ada 2 macam teori, yaitu teori hubungan yang nyata dan teori penyebab kira-kira. Hubungan sebab akibat hanyalah merupakan masalah fakta atau apa yang secara nyata telah terjadi. Sedangkan teori penyebab kira-kira lebih menekankan pada penyebab timbulnya kerugian korban, apakah perbuatan pelaku justru bukan dikarenakan suatu perbuatan melawan hukum. Namun dengan adanya kerugian yang ditimbulkan, maka yang harus dibuktikan ialah hubungan antara perbuatan melawan hukum dengan kerugian yang ditimbulkannya.[14]

[14] http://www.pengertianpakar.com/2015/01/pengertian-perbuatan-melawan-hukum-menurut-pakar-hukum.html diakses pada hari Selasa tanggal 29 November Pukul 22: 31 Wib.

### 2.1.2 Pengertian Tindak Pidana.

Pengertian tindak pidana dalam Kitab Undang-undang Hukum Pidana (KUHP)

dikenal dengan istilah *stratbaar feit* dan dalam kepustakaan tentang hukum pidana sering mempergunakan istilah delik, sedangkan pembuat undang-undang merumuskan suatu undang-undang mempergunakan istilah peristiwa pidana atau perbuatan pidana atau tindak pidana. Tindak pidana merupakan suatu istilah yang mengandung suatu pengertian dasar dalam ilmu hukum, sebagai istilah yang dibentuk dengan kesadaran dalam memberikan ciri tertentu pada peristiwa hukum pidana.

Tindak pidana mempunyai pengertian yang abstrak dari peristiwa-peristiwa yang kongkrit dalam lapangan hukum pidana, sehingga tindak pidana haruslah diberikan arti yang bersifat ilmiah dan ditentukan dengan jelas untuk dapat memisahkan dengan istilah yang dipakai sehari-hari dalam kehidupan masyarakat. Seperti yang diungkapkan oleh seorang ahli hukum pidana yaitu Prof. Moeljatno, SH, yang berpendapat bahwa pengertian tindak pidana yang menurut istilah beliau yakni perbuatan pidana adalah:

"Perbuatan yang dilarang oleh suatu aturan hukum larangan mana disertai ancaman (sanksi) yang berupa pidana tertentu, bagi barang siapa melanggar larangan tersebut." [15]

Jadi berdasarkan pendapat tersebut di atas pengertian dari tindak pidana yang dimaksud adalah bahwa perbuatan pidana atau tindak pidana senantiasa merupakan suatu perbuatan yang tidak sesuai atau melanggar suatu aturan

[15] Moeljatno, *Asas-asas Hukum Pidana, Bina Aksara, Jakarta 1987*, hal 54

hukum atau perbuatan yang dilarang oleh aturan hukum yang disertai dengan sanksi pidana yang mana aturan tersebut ditujukan kepada perbuatan sedangkan ancamannya atau sanksi pidananya ditujukan kepada orang yang melakukan atau orang yang menimbulkan kejadian tersebut. Dalam hal ini maka terhadap setiap orang yang melanggar aturan-aturan hukum yang berlaku, dengan demikian dapat dikatakan terhadap orang tersebut sebagai pelaku perbuatan pidana atau pelaku tindak pidana. Akan tetapi haruslah diingat bahwa aturan larangan dan ancaman mempunyai hubungan yang erat, oleh karenanya antara kejadian dengan orang yang menimbulkan kejadian juga mempunyai hubungan yang erat pula.

Sehubungan dengan hal pengertian tindak pidana ini Prof. DR. Bambang Poernomo, SH, berpendapat bahwa perumusan mengenai perbuatan pidana akan lebih lengkap apabila tersusun sebagai berikut:

"Bahwa perbuatan pidana adalah suatu perbuatan yang oleh suatu aturan hukum pidana dilarang dan diancam dengan pidana bagi barang siapa yang melanggar larangan tersebut."[16] Adapun perumusan tersebut yang mengandung kalimat "Aturan hukum pidana" dimaksudkan akan memenuhi keadaan hukum di Indonesia yang masih mengenal kehidupan hukum yang tertulis maupun hukum yang tidak tertulis, Prof.DR. Bambang Poernomo, SH, juga berpendapat mengenai kesimpulan dari perbuatan pidana yang dinyatakan hanya menunjukan sifat perbuatan terlarang dengan diancam pidana.

[16] Poernomo, Bambang. *Asas-asas Hukum Pidana, Ghalia Indonesia, Jakarta, 1992,* hal 130

Maksud dan tujuan diadakannya istilah tindak pidana, perbuatan pidana, maupun peristiwa hukum dan sebagainya itu adalah untuk mengalihkan bahasa dari istilah asing *stafbaar feit* namun belum jelas apakah disamping mengalihkan bahasa dari istilah *sratfbaar feit* dimaksudkan untuk mengalihkan makna dan pengertiannya, juga oleh karena sebagian besar kalangan ahli hukum belum jelas dan terperinci menerangkan pengertian istilah, ataukah sekedar mengalihkan bahasanya, hal ini yang merupakan pokok perbedaan pandangan, selain itu juga ditengan-tengan masyarakat juga dikenal istilah kejahatan yang menunjukan pengertian perbuatan melanggar morma dengan mendapat reaksi masyarakat melalui putusan hakim agar dijatuhi pidana.

Tindak pidana adalah merupakan suatu dasar yang pokok dalam menjatuhi pidana pada orang yang telah melakukan perbuatan pidana atas dasar pertanggung jawaban seseorang atas perbuatan yang telah dilakukannya. tapi sebelum itu mengenai dilarang dan diancamnya suatu perbuatan yaitu mengenai perbuatan pidanya sendiri, yaitu berdasarkan *azas legalitas (Principle of legality)* asas yang menentukan bahwa tidak ada perbuatan yang dilarang dan diancam dengan pidana jika tidak ditentukan terlebih dahulu dalam perundang-undangan, biasanya ini lebih dikenal dalam bahasa latin sebagai *Nullum delictum nulla poena sine praevia lege* (tidak ada delik, tidak ada pidana tanpa peraturan lebih dahulu), ucapan ini berasal dari von feurbach, sarjana hukum pidana Jerman. Asas legalitas ini dimaksud mengandung tiga pengertian yaitu:

Tidak ada perbuatan yang dilarang dan diancam dengan pidana kalau hal itu terlebih dahulu belum dinyatakan dalam suatu aturan undang-undang. Untuk menentukan adanya perbuatan pidana tidak boleh digunakan analogi. Tindak pidana merupakan bagian dasar dari pada suatu kesalahan yang dilakukan terhadap seseorang dalam melakukan suatu kejahatan. Jadi untuk adanya kesalahan hubungan antara keadaan dengan perbuatannya yang menimbulkan celaan harus berupa kesengajaan atau kelapaan. Dikatakan bahwa kesengajaan (*dolus*) dan kealpaan (*culpa*) adalah bentuk-bentuk kesalahan sedangkan istilah dari pengertian kesalahan (*schuld*) yang dapat menyebabkan terjadinya suatu tindak pidana adalah karena seseorang tersebut telah melakukan suatu perbuatan yang bersifat melawan hukum sehingga atas`perbuatannya tersebut maka dia harus bertanggung jawabkan segala bentuk tindak pidana yang telah dilakukannya untuk dapat diadili dan bilamana telah terbukti benar bahwa telah terjadinya suatu tindak pidana yang telah dilakukan oleh seseorang maka dengan begitu dapat dijatuhi hukuman pidana sesuai dengan pasal yang mengaturnya.

**Unsur-unsur Tindak Pidana**

Dalam kita menjabarkan sesuatu rumusan delik kedalam unsur-unsurnya, maka yang mula-mula dapat kita jumpai adalah disebutkan sesuatu tindakan manusia, dengan tindakan itu seseorang telah melakukan sesuatu tindakan yang terlarang oleh undang-undang. Setiap tindak pidana yang terdapat di dalam Kitab Undang-undang Hukum Pidana (KUHP) pada umumnya dapat dijabarkan ke dalam unsur-unsur yang terdiri dari unsur subjektif dan unsur objektif.

Unsur subjektif adalah unsur-unsur yang melekat pada diri si pelaku atau yang berhubungan dengan diri si pelaku, dan termasuk ke dalamnya yaitu segala sesuatu yang terkandung di dalam hatinya. Sedangkan unsur objektif adalah unsur-unsur yang ada hubungannya dengan keadaan-keadaan, yaitu di dalam keadaan-keadaan mana tindakan-tindakan dari si pelaku itu harus di lakukan.[17]

Unsur-unsur subjektif dari suatu tindak pidana itu adalah:

Kesengajaan atau ketidaksengajaan *(dolus* atau *Culpa)*, Maksud atau Voornemen pada suatu percobaan atau pogging seperti yang dimaksud dalam Pasal 53 ayat 1 KUHP;

Macam-macam maksud atau oogmerk seperti yang terdapat misalnya di dalam kejahatan-kejahatan pencurian, penipuan, pemerasan, pemalsuan dan lain-lain; Merencanakan terlebih dahulu atau voorbedachte raad seperti yang terdapat di dalam kejahatan pembunuhan menurut Pasal 340 KUHP; Perasaan takut yang antara lain terdapat di dalam rumusan tindak pidana menurut Pasal 308 KUHP.

Unsur-unsur objektif dari sutau tindak pidana itu adalah:

Sifat melanggar hukum atau *wederrechtelicjkheid*; Kwalitas dari si pelaku, misalnya kedaan sebagai seorang pegawai negeri di dalam kejahatan jabatan menurut pasal 415 KUHP atau keadaan sebagai pengurus atau komisaris dari suatu Perseroan Terbatas di dalam kejahatan menurut Pasal 398

[17] Drs. P.A.F. Lamintang, SH.*Dasar-dasar Hukum Pidana Indonesia; Bandung, PT. Citra Aditya Bakti, 1997,* Hal m193

KUHP. Kausalitas yakni hubungan antara suatu tindak pidana sebagai penyebab dengan sesuatu kenyataan sebagai akibat.

Seorang ahli hukum yaitu simons merumuskan unsur-unsur tindak pidana sebagai berikut :

a. Diancam dengan pidana oleh hukum
b. Bertentangan dengan hukum
c. Dilakukan oleh orang yang bersalah
d. Orang itu dipandang bertanggung jawab atas perbuatannya.[18]

Pengertian Tindak Pidana

Terlebih dahulu penulis akan menguraikan pengertian tentang tindak pidana atau perbuatan pidana. Di dalam Kitab Undang-Undang Hukum Pidana (KUHAP) tidak memberikan penjelasan secara rinci mengenai perkataan strafbaar feit tersebut.

Istilah *strafbaar feit* diterjemahkan oleh pakar hukum pidana Indonesia dengan istilah yang berbeda-beda. Diantaranya ada yang memakai istilah delik, peristiwa pidana, perbuatan pidana, tindak pidana, pelanggaran pidana. perbuatan yang melawan hukum atau bertentangan dengan tata hukum dan diancam pidana apabila perbuatan yang dilarang itu dilakukan oleh orang yang dapat dipertanggungjawabkan.

Pendapat tersebut misalnya menurut Simons (Sianturi, 1996:205) merumuskan bahwa: "*Strafbaar feit* " adalah suatu *handeling* (tindakan/perbuatan) yang diancam dengan pidana oleh undang-undang,

[18] DR. Andi Hamzah, *Asas-Asas Hukum Pidana; PT. Rineka Cipta, Jakarta Tahun 2004*, Hal 88

bertentangan dengan hukum (*onrechtmatig*) dilakukan dengan kesalahan (*schuld*) oleh seseorang yang mampu bertanggungjawab.

Kemudian beliau membaginya dalam 2 (dua) golongan unsur yaitu:

Unsur subyektif yang berupa kesalahan (*schuld*) dan kemampuan bertanggungjawab (*toerekeningsvatbaar*) dari petindak.

Unsur obyektif yang berupa tindakan yang dilarang/diharuskan, akibat keadaan/masalah tertentu.[19]

### 2.1.3 Pengertian *Cyber Crime*

Kejahatan komputer atau kejahatan *cyber* atau kejahatan dunia maya (*cybercrime*) adalah sebuah bentuk kriminal yang mana menjadikan internet dan komputer sebagai medium melakukan tindakan kriminal.Masalah yang berkaitan dengan kejahatan jenis ini misalnya *hacking*, pelanggaran hak cipta, *pornografi* anak, dan eksploitasi anak. Juga termasuk pelanggaran terhadap privasi ketika informasi rahasia hilang atau dicuri, dan lainnya.

Dalam definisi lain, kejahatan dunia maya adalah istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer menjadi alat, sasaran atau tempat terjadinya kejahatan. Termasuk ke dalam kejahatan dunia maya antara lain adalah penipuan lelang secara online, pemalsuan cek, penipuan kartu kredit, *confidence fraud*, penipuan identitas, pornografi anak, dll.Walaupun kejahatan dunia maya atau *cybercrime* umumnya mengacu kepada aktivitas kejahatan dengan komputer atau jaringan

[19] *http://infodanpengertian.blogspot.co.id/2016/02/*pengertian-dan-unsur-tindak-pidana.html diakses pada tanggal 29 November 2016 pada pukul 23: 03 Wib.

komputer sebagai unsur utamanya, istilah ini juga digunakan untuk kegiatan kejahatan tradisional dimana komputer atau jaringan komputer digunakan untuk mempermudah atau memungkinkan kejahatan itu terjadi.[20]

Kejahatan komputer mencakup berbagai potensi kegiatan ilegal. Umumnya, kejahatan ini dibagi menjadi dua kategori: (1) kejahatan yang menjadikan jaringan komputer dan divais secara langsung menjadi target; (2) Kejahatan yang terfasilitasi jaringan komputer atau divais, dan target utamanya adalah jaringan komputer independen atau divais.Contoh kejahatan yang target utamanya adalah jaringan komputer atau *divais* yaitu:

***1) Malware (malicious software / code)***

*Malware* (berasal dari singkatan kata malicious dan *software)* adalah perangkat lunak yang diciptakan untuk menyusup atau merusak sistem komputer, *server* atau jaringan komputer tanpa izin *(informed consent)* dari pemilik.Istilah ini adalah istilah umum yang dipakai oleh pakar komputer untuk mengartikan berbagai macam perangkat lunak atau kode perangkat lunak yang mengganggu atau mengusik.Istilah '*virus computer*' terkadang dipakai sebagai frasa pemikat (*catch phrase*) untuk mencakup semua jenis perangkat perusak, termasuk virus murni (*true virus).*

***2) Denial-of-service (DOS) attacks***

*Denial of service attack* atau serangan DoS adalah jenis serangan terhadap sebuah komputer atau *server* di dalam jaringan internet dengan cara

[20]*http://dutaxp.blogspot.com/2012/06/*pengertian-dan-jenis-jenis-cybercrime.html diakses pada tanggal 29 November 2016 pada pukul 23:12 wib.

menghabiskan sumber *(resource)* yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer yang diserang tersebut.

***3) Computer viruses***

Virus komputer merupakan program komputer yang dapat menggandakan atau menyalin dirinya sendiri dan menyebar dengan cara menyisipkan salinan dirinya ke dalam program atau dokumen lain. Virus murni hanya dapat menyebar dari sebuah komputer ke komputer lainnya (dalam sebuah bentuk kode yang bisa dieksekusi).ketika inangnya diambil ke komputer target, contohnya ketika user mengirimnya melalui jaringan atau internet, atau membawanya dengan media lepas (*floppy disk, cd, dvd, atau usb drive*). Virus bisa bertambah dengan menyebar ke komputer lain dengan mnginfeksi *file* pada *network file system* (sistem file jaringan) atau sistem *file* yang diakses oleh komputer lain.

Contoh kejahatan yang menjadikan jaringan komputer atau divais sebagai alat yaitu:

**1) *Cyber stalking* (Pencurian dunia maya)**

*Cyberstalking* adalah penggunaan internet atau alat elektronik lainnya untuk menghina atau melecehkan seseorang, sekelompok orang, atau organisasi.Hal ini termasuk tuduhan palsu, memata-matai, membuat ancaman, pencurian identitas, pengerusakan data atau peralatan, penghasutan anak di bawah umur untuk seks, atau mengumpulkan informasi untuk mengganggu.

Definisi dari "pelecehan" harus memenuhi kriteria bahwa seseorang secara wajar, dalam kepemilikan informasi yang sama, akan menganggap itu cukup untuk menyebabkan kesulitan orang lain secara masuk akal.[21]

**2) Penipuan dan pencurian identitas**

Pencurian identitas adalah menggunakan identitas orang lain seperti KTP, SIM, atau paspor untuk kepentingan pribadinya, dan biasanya digunakan untuk tujuan penipuan. Umumnya penipuan ini berhubungan dengan Internet, namun sering huga terjadi di kehidupan sehari-hari. Misalnya penggunaan data yang ada dalam kartu identitas orang lain untuk melakukan suatu kejahatan. Pencuri identitas dapat menggunakan identitas orang lain untuk suatu transaksi atau kegiatan, sehingga pemilik identitas yang aslilah yang kemudian dianggap melakukan kegiatan atau transaksi tersebut.

***3) Phishing scam***

Dalam sekuriti komputer, *phising* (Indonesia: pengelabuan) adalah suatu bentuk penipuan yang dicirikan dengan percobaan untuk mendapatkan informasi peka, seperti kata sandi dan kartu kredit, dengan menyamar sebagai orang atau bisnis yang terpercaya dalam sebuah komunikasi elektronik resmi, seperti surat elektronik atau pesan instan. Istilah phishing dalam bahasa Inggris berasal dari kata *fishing* (memancing), dalam hal ini berarti memancing informasi keuangan dan kata sandi pengguna.[22]

---

[21] *http://id.wikipedia.org/wiki/Cyberstalking* diakses pada tanggal 29 November 2016 pada pukul 23:18 Wib.

[22] metadatastudio.com/pengertian-email-phishing diakses pada tanggal 29 November 2016 pada pukul 23:19 Wib.

**4) Perang informasi *(Information warfare)***

Perang Informasi adalah penggunaan dan pengelolaan informasi dalam mengejar keunggulan kompetitif atas lawan.perang Informasi dapat melibatkan pengumpulan informasi taktis, jaminan bahwa informasi sendiri adalah sah, penyebaran propaganda atau disinformasi untuk menurunkan moral musuh dan masyarakat, merusak kualitas yang menentang kekuatan informasi dan penolakan peluang pengumpulan-informasi untuk menentang kekuatan. Informasi perang berhubungan erat dengan perang psikologis.

Contohnya ketika seseorang mencuri informasi dari situs, atau menyebabkan kerusakan computer atau jaringan komputer.Semua tindakan ini adalah virtual (tidak nyata) terhadap informasi tersebut hanya ada dalam dunia digital, dan kerusakannya dalam kenyataan, tidak ada kerusakan fisik nyata kecuali hanya fungsi mesin yang bermasalah.Komputer dapat dijadikan sumber bukti. Bahkan ketika komputer tidak secara langsung digunakan untuk kegiatan kriminal, komputer merupakan alat yang sempurna untuk menjaga record atau catatan, khususnya ketika diberikan tenaga untuk mengenkripsi data. Jika bukti ini bisa diambil dan didekripsi, ini bisa menjadi nilai bagi para investigator criminal.[23]

Jenis Tindak Pidana yang dilakukan dalam dunia maya :

Dalam perembangannya tindak pidana *Cyber Crime* memiliki berbagai jenis modus yang dilakukan dan sering terjadi pada dunia maya:

[23] *http://www.lemhannas.go.id/portal/daftar-artikel/1556-cyber-warfare.html* diakses pada tanggal 29 November 2016 pada pukul 23:21 Wib.

***a. Unauthorized Access to Computer System and Service***

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

Kejahatan ini semakin marak dengan berkembangnya teknologi Internet/intranet.Kita tentu belum lupa ketika masalah Timor Timur sedang hangat-hangatnya dibicarakan di tingkat internasional, beberapa website milik pemerintah RI dirusak oleh hacker (Kompas, 11/08/1999). Beberapa waktu lalu, hacker juga telah berhasil menembus masuk ke dalam data base berisi data para pengguna jasa America Online (AOL), sebuah perusahaan Amerika Serikat yang bergerak dibidang ecommerce yang memiliki tingkat kerahasiaan tinggi (Indonesian Observer, 26/06/2000). Situs Federal Bureau of Investigation (FBI) juga tidak luput dari serangan para hacker, yang mengakibatkan tidak berfungsinya situs ini beberapa waktu lamanya.

**b. *Offense against Intellectual Property.***

Kejahatan ini ditujukan terhadap Hak atas Kekayaan Intelektual yang dimiliki pihak lain di internet. Sebagai contoh adalah peniruan tampilan pada web page suatu situs milik orang lain secara ilegal, penyiaran suatu informasi

di internet yang ternyata merupakan rahasia dagang orang lain, dan sebagainya.Dapat kita contohkan saat ini.Situs mesin pencari bing milik microsoft yang konon di tuduh menyerupai sebuah situs milik perusahaan travel online.

***c. Illegal Contents.***

Merupakan kejahatan dengan memasukkan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum. Sebagai contohnya adalah pemuatan suatu berita bohong atau fitnah yang akan menghancurkan martabat atau harga diri pihak lain, hal-hal yang berhubungan dengan pornografi atau pemuatan suatu informasi yang merupakan rahasia negara, agitasi dan propaganda untuk melawan pemerintahan yang sah, dan sebagainya.Masih ingat dengan kasus prita mulyasari yang sampai saat ini belum selesai.Hanya gara-gara tulisan emailnya yang sedikit merusak nama baik sebuah institusi kesehatan swasta dia di seret ke meja hijau.

***d. Cyberstalking***

Kejahatan jenis ini dilakukan untuk mengganggu atau melecehkan seseorang dengan memanfaatkan komputer, misalnya menggunakan e-mail dan dilakukan berulang-ulang.Kejahatan tersebut menyerupai teror yang ditujukan kepada seseorang dengan memanfaatkan media internet. Hal itu bisa terjadi karena kemudahan dalam membuat email dengan alamat tertentu tanpa harus menyertakan identitas diri yang sebenarnya. Contoh Kasus : Misalnya e-mail yang berisi ajakan bergabung dengan suatu website, email yang berisi

ajakan untuk membeli produk tertentu, mail yang berisi kontes / undian berhadiah. Undang-undang ITE Pasal 25: Penggunaan setiap informasi melalui media elektronik yang menyangkut data tentang hak pribadi seseorang harus dilakukan atas persetujuan dari orang yang bersangkutan, kecuali ditentukan lain oleh peraturan perundang-undangan.

***e. Hacking dan Cracker***

Istilah hacker biasanya mengacu pada seseorang yang punya minat besar untuk mempelajari sistem komputer secara detail dan bagaimana meningkatkan kapabilitasnya. Adapun mereka yang sering melakukan aksi-aksi perusakan di internet lazimnya disebut cracker.Boleh dibilang cracker ini sebenarnya adalah hacker yang yang memanfaatkan kemampuannya untuk hal-hal yang negatif. Aktivitas cracking di internet memiliki lingkup yang sangat luas, mulai dari pembajakan account milik orang lain, pembajakan situs web, probing, menyebarkan virus, hingga pelumpuhan target sasaran. Tindakan yang terakhir disebut sebagai DoS (Denial Of Service). Dos attack merupakan serangan yang bertujuan melumpuhkan target (hang, crash) sehingga tidak dapat memberikan layanan. Contoh Kasus : Pada tahun 1983, pertama kalinya FBI menangkap kelompok kriminal komputer The 414s(414 merupakan kode area lokal mereka) yang berbasis di Milwaukee AS. Kelompok yang kemudian disebut hacker tersebut melakukan pembobolan 60 buah komputer, dari komputer milik Pusat Kanker Memorial Sloan-Kettering hingga komputer milik Laboratorium Nasional Los Alamos.Salah seorang dari antara pelaku tersebut mendapatkan kekebalan karena testimonialnya, sedangkan 5 pelaku lainnya mendapatkan hukuman masa percobaan. Undang-

Undang Pasal 27 (1) Setiap orang dilarang menggunakan dan atau mengakses komputer dan atau sistem elektronik dengan cara apapun tanpa hak, untuk memperoleh, mengubah, merusak, atau menghilangkan informasi dalam komputer dan atau sistem elektronik. (Pidana empat tahun penjara dan denda Rp 1 miliar).

### *f. Cybersquatting and Typosquatting*

*Cybersquatting* merupakan kejahatan yang dilakukan dengan mendaftarkan domain nama perusahaan orang lain dan kemudian berusaha menjualnya kepada perusahaan tersebut dengan harga yang lebih mahal. Adapun typosquatting adalah kejahatan dengan membuat domain plesetan yaitu domain yang mirip dengan nama domain orang lain. Nama tersebut merupakan nama domain saingan perusahaan. Contoh Kasus : Contoh kasus yang beredar di international adalah kasus Yahoo yang menuntut Oniine NIC atas aksi *cybersquatting* pada 500 nama domain yang mirip atau dapat membingungkan para penggunanya termasuk yahoozone.*com*, *yahooyahooligans.com* dan *denverwifesexyahoo.com*. Undang-Undang : Pasal 23 (2): Pemilikan dan penggunaan nama domain sebagaimana dimaksud dalam ayat (1) wajib didasarkan pada itikad baik, tidak melanggar prinsip persaingan usaha secara sehat, dan tidak melanggar hak orang lain. (Tindak pidana sebagaimana dimaksud dalam ayat (1) hanya dapat dituntut atas pengaduan dari orang yang terkena tindak pidana) ( Pidana enam bulan atau denda Rp 100 juta).

### *g. Arp spoofing*

*Arp spoofing* adalah teknik yang cukup populer untuk melakukan penyadapan data, terutama data username/password yang ada di jaringan internal. Intinya adalah dengan mengirimkan paket ARP Reply palsu sehingga merubah data MAC Address:IP yang ada di tabel ARP komputer target. Perubahan data ini menyebabkan pengiriman paket TCP/IP akan melalui attacker sehingga proses penyadapan dapat dilakukan.

### *h. Carding*

Adalah berbelanja mengunakan nomor atau identitas kartu kredit orang lain yang dilakukan secara ilegal. Pelakunya biasa disebut carder. Parahnya indonesia menduduki peringkat kedua dunia setelah Ukraina untuk kasus ini. Tak tanggung-tanggung 20% transaksi internet dari Indonesia adalah dari hasil Carding.Itulah sebabnya banyak situs belanja online yang memblokir ip asal Indonesia. Atau dengan kata lain konsumen Indonesia tidak boleh belanja di situs tersebut. Perkembangan terakhir pelaku carding juga mulai menyusup ke ruang-ruang chat seperti mIRC dengan mengiming-imingi barang berharga "miring", begitu ada yang tertarik si pembeli disuruh membayar via rekening. Begitu uang terkirim barang tak pernah dikirim. Sebagai tambahan, kadang sebagian orang menganggap pelaku carding sama dengan hacker. Hal ini jelas tidak benar karena untuk melakukan carding tidak terlalu memerlukan otak.Mereka cukup mengetahui nomor kartu dan tanggal kadaluwarsa.Sedangkan hacker adalah orang yang sangat paham betul

mengenai sistem keamanan suatu jaringan dan memerlukan waktu yang tidak sebentar untuk menjadi seorang hacker sejati.

**i. *Defacing***

Defacing adalah kegiatan mengubah halaman situs/website pihak lain, seperti yang terjadi pada situs Menkominfo dan Partai Golkar, BI baru-baru ini dan situs KPU saat pemilu 2004 lalu. Tindakan deface ada yang semata-mata iseng, unjuk kebolehan, pamer kemampuan membuat program, tapi ada juga yang jahat, untuk mencuri data dan dijual kepada pihak lain.

***j. Phising***

Phising adalah tindak kejahatan memancing pemakai komputer di internet (user) agar mau memberikan informasi data diri pemakai (username) dan kata sandinya (password) pada suatu website yang sudah di-deface. Phising biasanya diarahkan kepada pengguna online banking. Isian data pemakai dan password yang vital yang telah dikirim akhirnya akan menjadi milik penjahat tersebut dan digunakan untuk belanja dengan kartu kredit atau uang rekening milik korbannya.

***k. Spamming***

Adalah mengirimkan pesan atau iklan yang tidak dikehendaki melalui surat elektronik (E-mail). Pengiriman e-mail dapat hadiah, lotere, atau seseorang yang mengaku mempunyai rekening di Amerika, baghdad dan sebagainya lalu meminta tolong untuk mencairkan. Belakangan ini seorang spammer telah ditangkap dan terancam menghadapi bui karena aksinya yang

menyalahi aturan koneksi Facebook.Perkara tersebut telah ditangani oleh Kejaksaan Agung Amerika Serikat. Sanford Wallace atau yang dikenal dengan nama "Spam King" berhasil digiring oleh Jeremy Fogel, hakim U.S Distric Court for Northern Distric of California atas kasus mail marketing. Jaksa Agung tersebut akan memprosesnya atas tuduhan pencemaran dalam akses Facebook. Dan hasilnya Wallace dikenai sanksi membayar denda sebesar US$ 230 juta.Yang saya pertanyakan apakah inbox berantai di Facebook juga termasuk kejahatan di internet dan bisa di kenai pasal pidana? Soalnya akhir-akhir ini inbox di Akun Facebook saya sering mendapat pesan berantai yang tidak berkesudahan.

***l. Malware***

Adalah program komputer yang mencari kelemahan dari suatu software.Umumnya malware diciptakan untuk membobol atau merusak suatu software atau operating system. Malware terdiri dari berbagai macam, yaitu: *virus, worm, trojan horse, adware, browser hijacker*, dll. Di pasaran alat-alat komputer dan toko perangkat lunak (software) memang telah tersedia antispam dan anti virus, dan anti malware. Meski demikian, bagi yang tak waspadai selalu ada yang kena.Karena pembuat virus dan malware umumnya terus kreatif dan produktif dalam membuat program untuk mengerjai korban-korbannya.

***m. Jamming***

Jamming adalah sebuah bentuk interferensi dengan mengurangi energi frekuensi radio dari sumber energi tertentu dengan karakteristik tertentu untuk

mencegah *receiver* menerima sinyal GPS pada suatu area yang ditargetkan. Karakteristik Sinyal GPS berada bebas diangkasa membuat orang bisa dengan mudah untuk membuat tipuan sinyal sejenis.Hanya dengan sebuah sinyal generator maka frekuensi radio dari oscillator dapat dimodifikasi.Bahkan hal ini bisa dilakukan dengan menggunakan sebuah pesawat Hand Phone. Biasanya para jammer jika takut diketahui didarat umumnya akan melakukannya dari atas pesawat udara atau balon udara.

***n. .Spoofing***

*Spoofing* adalah sebuah teknik yang telah lama digunakan untuk mengelabui wilayah jangkauan operasi radar. Pada kasus GPS, tujuan dari teknik ini adalah untuk membuat receiver aktif GPS terkunci pada sebuah sinyal palsu, dan kemudian secara perlahan – lahan dibelokan menuju target yang lain. *Meaconing* adalah *reception, delay dan rebroadcast* dari radio navigasi yang bertujuan untuk mengelabui sistem navigasi atau penggun.

***o. Cyber Espionage***

Merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (*computer network system*) pihak sasaran. Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen ataupun data-data pentingnya tersimpan dalam suatu sistem yang *computerized*. Biasaynya si penyerang menyusupkan sebuah program mata-mata yang dapat kita sebut sebagai *spyware*.

***p. Infringements of Privacy***

Kejahatan ini ditujukan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia. Kejahatan ini biasanya ditujukan terhadap keterangan pribadi seseorang yang tersimpan pada formulir data pribadi yang tersimpan secara *computerized*, yang apabila diketahui oleh orang lain maka dapat merugikan korban secara materil maupun immateril, seperti nomor kartu kredit, nomor PIN ATM, cacat atau penyakit tersembunyi dan sebagainya.

***q. Data Forgery***

Merupakan kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai scriptless document melalui internet. Kejahatan ini biasanya ditujukan pada dokumen-dokumen *e-commerce* dengan membuat seolah-olah terjadi "salah ketik" yang pada akhirnya akan menguntungkan pelaku.

***r. Cyber Sabotage and Extortion***

Merupakan kejahatan yang paling mengenaskan. Kejahatan ini dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet. Biasanya kejahatan ini dilakukan dengan menyusupkan suatu logic bomb, virus komputer ataupun suatu program tertentu, sehingga data, program komputer atau sistem jaringan komputer tidak dapat digunakan, tidak berjalan sebagaimana mestinya, atau berjalan sebagaimana yang dikehendaki oleh pelaku. Dalam beberapa kasus setelah hal tersebut terjadi, maka pelaku kejahatan tersebut menawarkan diri kepada korban untuk memperbaiki data,

program komputer atau sistem jaringan komputer yang telah disabotase tersebut, tentunya dengan bayaran tertentu.Kejahatan ini sering disebut sebagai cyber-terrorism.

***s. Snifing***

*Snifing* adalah kegiatan menyadap dan/atau menginspeksi paket data menggunakan sniffer software atau hardware di internet. Kegiatan ini sering disebut sebagai serangan sekuriti pasif dengan cara membaca data yang berkeliaran di internet, dan memfilter khusus untuk host tujuan tertentu. Jadi kegiatan ini tidak melakukan apa-apa terhadap data, tidak merubah dan tidak memanipulasi. Cukup menyadap.Ia digunakan untuk mendapatkan informasi seperti password, data-data rahasia dan lainnya. Sering digunakan para *analyst networking,* baik dari kalangan developer maupun *network administrator,* untuk melakukan *troubleshooting.*

### 2.1.4 Faktor –Faktor Yang Menyebabkan Terjadinya Tindak Pidana Dengan Sengaja Mengakses Sistem Elektronik Milik Orang Lain atau *Cracking.*

Era kemajuan teknologi informasi ditandai dengan meningkatnya penggunaan internet dalam setiap aspek kehidupan manusia. Meningkatnya penggunaan internet di satu sisi memberikan banyak kemudahan bagi manusia dalam melakukan aktivitasnya, di sisi lain memudahkan bagi pihak-pihak tertentu untuk melakukan tindak pidana.

Faktor-faktor yang mempengaruhi cyber crime adalah :

1. Faktor Politik.

Mencermati maraknya *cyber crime* yang terjadi di Indonesia dengan permasalahan yang dihadapi oleh aparat penegak, proses kriminalisasi di bidang *cyber* yang terjadi merugikan masyarakat. Penyebaran virus koputer dapat merusak jaringan komputer yang digunakan oleh pemerintah, perbankan, pelaku usaha maupun perorangan yang dapat berdampak terhadap kekacauan dalam sistem jaringan. Dapat dipastikan apabila sistem jaringan komputer perbankan tidak berfungsi dalam satu hari saja akan mengakibatkan kekacauan dalam transaksi perbankan.

Kondisi ini memerlukan kebijakan politik pemerintah Indonesia untuk menanggulangi cyber crime yang berkembang di Indonesia.Aparat penegak hukum telah berupaya keras untuk menindak setiap pelaku cyber crime, tapi penegakkan hukum tidak dapt berjalan maksimal sesuai harapan masyarakat karena perangkat hukum yang mengatur khusus tentang cyber crime belum ada.

Untuk menghindari kerugian yang lebih besar akibat tindakan pelaku cyber crime maka diperlukan kebijakan politik pemerintah Indonesia untuk menyiapkan perangkat hukum khusus (*lex specialist*) bagi *cyber crime*. Dengan perangkat hukum ini aparat penegak hukum tidak ragu-ragu lagi dalam melakukan penegakan hukum terhadap *cyber crime*.

2. Faktor Ekonomi.

Kemajuan ekonomi suatu bangsa salah satunya dipengaruhi oleh promosi barang-barang produksi.Jaringan komputer dan internet merupakan media yang sangat murah untuk promosi.Masyarakat dunia banyak yang menggunakan media ini untuk mencari barang-barang kepentingan perorangan maupun korporasi.Produk barang yang dihasilkan oleh indutri di Indonesia sangat banyak dan digemari oleh komunitas Internasional.Para pelaku bisnis harus mampu memanfaatkan sarana internet dimaksud.Krisis ekonomi yang melanda bangsa Indonesia harus dijadikan pelajaran bagi masyarakat Indonesia untuk bangkit dari krisis dimaksud.Seluruh komponen bangsa Indonesia harus berpartisipasi mendukung pemulihan ekonomi.Media internet dan jaringan komputer merupakan salah satu media yang dapat dimanfaatkan oleh seluruh masyarakat untuk mempromosikan Indonesia.

3. Faktor Sosial Budaya.

Faktor sosial budaya dapat dilihat dari beberapa aspek, yaitu :

Kemajuan teknologi Informasi Dengan teknologi informasi manusia dapat melakukan akses perkembangan lingkungan secara akurat, karena di situlah terdapat kebebasan yang seimbang, bahkan dapat mengaktualisasikan dirinya agar dapat dikenali oleh lingkungannya.

4. Sumber Daya Manusia.

Sumber daya manusia dalam teknologi informasi mempunyai peranan penting sebagai pengendali sebuah alat.Teknologi dapat dimanfaatkan untuk

kemakmuran namun dapat juga untuk perbuatan yang mengakibatkan petaka akibat dari penyimpangan dan penyalahgunaan.Di Indonesia Sumber Daya Pengelola teknologi Informasi cukup, namun Sumber Daya untuk memproduksi masih kurang.Hal ini akibat kurangnya tenaga peneliti dan kurangnya biaya penelitian dan apresiasi terhadap penelitian.Sehingga Sumber Daya Manusia di Indonesia hanya menjadi pengguna saja dan jumlahnya cukup banyak.

5. Komunitas Baru.

Dengan adanya teknologi sebagai sarana untuk mencapai tujuan, di antaranya media internet sebagai wahana untuk berkomunikasi, secara sosiologis terbentuk sebuah komunitas baru di dunia maya. Komunitas ini menjadim populasi gaya baru yang cukup diperhitungkan. Pengetahuan dapat diperoleh dengan cepat.[24]

**2.2 Kerangka Pemikiran**

Dalam hal kerangka pemikiran akan dikaitkan dengan judul isi skripsi ini yaitu Analisis Yuridis Tindak Pidana Mengakses Sistem Elektronik Milik Orang Lain Ditinjau dari Undang-Undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, yaitu membahas apa yang dimaksud dengan tindak pidana kejahatan dunia maya terutama pada tindakan dengan sengaja mengakses system informasi milik orang lain berdasarkan Undang-Undang Nomor 11 Tahun 2008 dalam perkara putusan nomor : 2.862/Pid.B/2016/PN.MDN

[24] *http://dumadia.wordpress.com/2009/04/02/aplikasi-konvensi-cyber-crime-2001-dalam-uu-no-11-tahun-2008-mengenai-informasi-dan-transaksi-elektronik-ite* diakses pada tanggal 29 november 2016 pada pukul 23:48 Wib.

## 2.3 Hipotesis

Hipotesis merupakan jawaban sementara atau dugaan yang dianggap benar, tetapi masih perlu dibuktikan. Hipotesis pada dasarnya dugaan peneliti tentang hasil yang akan dicapai. Tujuan ini dapat diterima apabila ada cukup data untuk membuktikannya.

Dalam system berfikir yang teratur, maka hipotesis sangat perlu dalam melakukan penyidikan suatu penulisan skripsi jika ingin mendapat suatu kebenaran yang hakiki. Hipotesis dapat diartikan suatu yang berupa dugaan-dugaan atau perkiran-perkiraan yang masih harus dibuktikan kebenaran atau kesalahannya, atau berupa pemecahan masalah untuk sementara waktu.[25] Dalam hal ini penulis juga akan membuat hipotesis. Adapun hipotesa penulis dalam permasalahn yang dibahas adalah sebagai berikut :

1. Berdasarkan rumusan masalah pertama bahwa pertanggungjawaban dan sanksi hukum terhadap pelaku tindak pidana mengakses sistem elektronik milik orang lain dampaknya dapat menimbulkan konsekuensi hukum, terlebih jika penggunaan yang dimaksud dilakukan tanpa izin yang bersangkutan dan bertujuan untuk mengirimkan konten seolah-olah atas nama korban dan menimbulkan kerugian pada korban atau pihak ketiga sehingga pelaku dapat diancam pidana berdasarkan pasal 30 ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik ("UU ITE"), yaitu "sengaja dan tanpa hak mengakses Komputer atau Sistem Elektronik Orang lain",ancaman dari pasal 30 ayat (1) tersebut adalah

[25] Samsul Arifin, "*Metode Penulisan Karya Ilmiah dan Penelitian Hukum*", Medan Area University Press,2012, hlm.38.

pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp. 600.000.000,- (enam ratus juta rupiah).

2. Berdasarkan rumusan masalah yang kedua tentang bagaimana perlindungan hukum terhadap korban kejahatan tindak pidana ITE khususnya korban atas kejahatan mengakses sistem elektronik milik orang lain,pemerintah dengan tegas mengeluarkan undang-undang Informasi dan Transaksi Elektronik atau yang disebut dengan *cyber law* yang digunakan untuk mengatur berbagai perlindungan hukum atas kegiatan yang memanfaatkan internet sebagai medianya baik transaksi atau pemanfaatan informasinya, dengan adanya undang undang ITE tersebut diharapkan dapat memberikan rasa aman dan dapat memberikan perlindungan bagi mereka yang menggunakan teknologi,disamping itu dalam keadaan tertentu dan membahayakan bagi mereka yang menjadi korban kejahatan teknologi juga berhak mendapatkan perlindungan hukum hal ini tercantum pada Undang-undang nomor 13 tahun 2006 tentang Perlindungan Saksi dan Korban yang tertuang dalam pasal 5 undang-undang perlindungan saksi dan korban.

3. Berdasarkan rumusan masalah yang ketiga tentang pertimbangan hakim dalam penjatuhan putusan terhadap pelaku tindak piudana mengakses sistem elektronik milik orang lain, Dalam kasus tindak pidana mengakses sitem elektronik milik orang lain telah melalui proses peradilan serta diputuskan berdasarkan undang-undang yang

berlaku serta pertimbangan-pertimbangan hakim sehingga putusan telah mempunyai kekuatan hukum tetap.

Untuk Menyatakan seseorang telah melakukan suatu tindak pidana, maka perbuatan orang tersebut sebagaimana yang terungkap dalam fakta-fakta hukum persidangan haruslah dapat memenuhi seluruh unsur-unsur dari tindak pidana yang didakwakan kepadanya.

Majelis Hakim akan mempertimbangkan apakah perbuatan terdakwa sebagaimana yang diterangkan dalam persidangan telah memenuhi unsur-unsur delik dari pasal-pasal yang didakwakan.

# BAB III

# METODE PENELITIAN

Metode berarti cara yang tepat untuk melakukan sesuatu, sedangkan penelitian berarti suatu kegiatan untuk mencari, mencatat, merumuskan dan menganalisa sampai menyusun laporannya.[26] Dengan menggunakan metode, seseorang diharapkan mampu untuk menemukan dan menganalisis masalah tertentu, sehingga dapat mengungkapkan sesuatu kebenaran, karena metode memberikan pedoman tentang cara bagaimana seorang ilmuwan mempelajari, memahami dan menganalisa permasalahan yang dihadapi.

## 3.1 Jenis, Sifat, Lokasi dan Waktu Penelitian

### 3.1.1. Jenis Penelitian

Adapun jenis data dalam penelitian ini adalah secara Yuridis Normatif yaitu merupakan data yang diperoleh langsung dari intansi terkait yaitu di Pengadilan Negeri Medan dan dari bahan perpustakaan.

### 3.1.2. Sifat penelitian

Sifat penelitian ini dianalisis secara deskriptif sehingga diperoleh gambaran yang jelas dengan pokok permasalahan. Dengan analisis deskriptif maka data yang diperoleh dari responden dan informasi menghasilkan deskriptif analisis sehingga diteliti dan dipelajari sebagai sesuatu yang utuh.

[26] Cholid Narbuko dan H. Abu Achnadi, *Metode penelitian, PT Bumi Aksara, Jakarta, 2002* hal 1

### 3.1.3. Sumber data dari penulisan tersebut didapat melalui pengadilan dan buku:

a. Data Primer

Data primer atau data dasar dalam penelitian ini diperlukan untuk memberi pemahaman secara jelas dan lengkap terhadap data sekunder data mengenai putusan perkara pidana dengan no. 2.862/Pid.B/2016/PN.Mdn. Yang diperoleh atau yang bersumber langsung dari intansi terkait yaitu di Pengadilan Negeri Medan yang merupakan lokasi penelitian.

b. Data Sekunder

Dalam penelitian ini data sekunder merupakan data pokok yang diperoleh dari perpustakaan, terhadap berbagai macam bahan seperti buku-buku, artikel, serta perundang-undangan yang berlaku, maupun sumber lainnya yang berkaitan dengan masalah dan tujuan penelitian.

### 3.1.4. Lokasi Penelitian

Penelitian dilakukan pada Pengadilan Negeri Medan dengan mengambil data riset berupa kasus yang berkaitan dengan judul skripsi yaitu tentang tindak pidana mengakses sistem elektronik milik orang lain Putusan No.2.862/pid.B/2016/PN.MDN.

### 3.1.5. Waktu Penelitian

Waktu penelitian dilaksanakan sekitar bulan Maret 2017 setelah dilakukan seminar proposal dan perbaikan outline.

| o | Kegiatan | Bulan | | | | | | | | | | | | | | | | | | | Keterangan |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Desember 2016 | | | | Januari 2017 | | | | Februari 2017 | | | | Maret 2017 | | | | April 2017 | | | |
| | | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 |
| | Pengajuan judul | | | | | | | | | | | | | | | | | | | | |
| 2 | Seminar Proposal | | | | | | | | | | | | | | | | | | | | |
| 3 | Perbaikan Proposal | | | | | | | | | | | | | | | | | | | | |
| 4 | Penelitian | | | | | | | | | | | | | | | | | | | | |
| 5 | Penulisan Skripsi | | | | | | | | | | | | | | | | | | | | |
| 6 | Bimbingan Skripsi | | | | | | | | | | | | | | | | | | | | |
| 7 | Seminar Hasil | | | | | | | | | | | | | | | | | | | | |
| 8 | Pengajuan Berkas Meja Hijau | | | | | | | | | | | | | | | | | | | | |
| 9 | Meja Hijau | | | | | | | | | | | | | | | | | | | | |

Dalam penelitian diatas Penulis Menganalisis hasil putusan, pengambilan data pada saat melakukan riset sebagai pembahasan untuk melengkapi penulisan skripsi ini.

### 3.2 Teknik Pengumpulan Data

Adapun teknik pengumpulan data dilakukan dengan cara sebagai berikut:

1. Penelitian keperpustakaan (*Library research)*. Metode ini dengan melakukan penelitian terhadap berbagai sumber bacaan tertulis dari para sarjana yaitu buku-buku teori tentang hukum, majalah hukum, jurnal-jurnal hukum dan juga bahan-bahan kuliah seta peraturan-peraturan tentang hukum kepidanaan.
2. Penelitian Lapangan *(Field Research)* yaitu dengan melakukan studi penelitian langsung ke Pengadilan Negeri Medan dengan mengambil putusan yang berhubungan dengan judul skripsi yaitu kasus tentang perbuatan melawan hukum dengan sengaja mengakses system elektronik orang lain No. 2.862/Pid.B/2016/PN.Mdn

### 3.3 Analisis Data

Data sekunder dari bahan hukum primer disusun secara sistematis dan kemudian substansinya dianalisis secara Kualitatif untuk memperboleh gambaran tentang pokok permasalahan.

Sedangkan data-data berupa teori yang diperoleh dikelompokkan sesuai dengan sub bab pembahasan, selanjutnya dianalisis secara kualitatif sehingga diperoleh gambaran yang jelas dengan pokok permasalahan. Dengan analisis kualitatif maka data yang diperoleh dari responden atau informasi menghasilkan data deskriptif analisis sehingga diteliti dan dipelajari sebagai sesuatu yang utuh.

# BAB V

# KESIMPULAN DAN SARAN

## 5.1.Kesimpulan

1. Pertanggungjawaban pelaku tindak pidana mengakses sistem elektronik milik orang lain pada putusan No.2.862/Pid.B/2016/PN.MDN Alex Siregar terbukti bersalah melakukan tindak pidana mengakses sistem elektronik orang lain secara berulang, menjatuhkan pidan penjara selama 3 (tiga) bulan pidana penjara dan denda Rp. 1.000.000,00 (satu juta rupiah) dengan ketentuan apabila denda tersebut tidak dibayar diganti dengan pidana kurungan selama (1) bulan.
2. perlindungan hukum bagi korban tindak pidana mengakses sistem elektronik orang lain pada putusan No.2.862/Pid.B/2016/PN.MDN. Penindakan penyalahgunaan ini terdapat pada kajian UU ITE (Informasi dan Transaksi Eletronik) No. 11 Tahun 2008 pasal 30 dimana pada ayat 3 yaitu : "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan". Dalam kajian ini, suatu bentuk tindakan yang akan di aplikasikan pada suatu tindakan yang dilakukan oleh pihak yang berniat secara jahat bukan dengan maksud untuk hal yang positif. Implementasi dari UU ITE sebagai gerakan yang dicanangkan oleh pemerintah dalam meminimalisir bahkan menghilangkan fenomena yang berkembang ini seperti halnya menjebol sistem pengamanan pada akun pribadi. Dan dari

UU ITE pasal 30 ayat 3 ini terhadap penyalahgunaan hukum akan diberikan sanksi dengan ancaman pidana maksimum 8 tahun denda maksimum Rp.800juta.

3. Pertimbangan hakim dalam menjatuhkan putusan terhadap tindak pidana mengakses sistem elektronik milik orang lain pada putusan No.2.862/Pid.B/2016/PN.MDN. Memperhatikan ketentuan pasal 46 ayat (1) UU RI No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik Jo pasal 64 ayat (1) KUHP. Pasal-pasal dari undang-undang No. 8 Tahun 1981 Tentang Hukum Acara Pidana serta peraturan perundang-undangan. Menimbang, bahwa sebelum menjatuhkan pidana, Maka majelis Hakim mempertimbangkan keadaan yang memberatkan perbuatan terdakwa merugikan pihak Kemenkominfo dan keadaan yang meringankan terdakwa Alex Siregar belum pernah dihukum, terdakwa mengakui perbuatannya secara terus terang dan menyesalinya, terdakwa belaku sopan dalam persidangan, bahwa pihak kemenkominfo telah memaafkan perbuatan terdakwa dan memohon hukuman terdakwa Alex Siregar agar diringankan. Bahwa menurut Majelis hakim putusan yang dijatuhkan telah memenuhi rasa keadilan hukum, sosial dan keadilan masyarakat.

## 5.2. Saran

1. Bahwa pertanggungjawaban pelaku tindak pidana mengakses sistem elektronik orang lain pada putusan No.2.862/Pid.B/2016/PN.MDN. Hukuman yang diberikan kepada terdakwa Alex siregar terlalu ringan

sehingga tidak memberikan efek jera terhadap pelaku tindak pidana *cracking*

2. Perlindungan hukum korban tindak pidana mengakses sistem elektronik milik orang lain tidak adil karena sanksi yang diberikan terlalu ringan sehingga apa yang diterima korban tidak setimpal dengan apa yang dipertanggungjawabkan pelaku tindak pidana cyber cime khususnya cracking.
3. Pertimbangan hakim dalam menjatuhkan putusan terhadap tindak pidana mengakses sistem elektronik milik orang lain. Seharusnya seoarang hakim harus menjatuhkan hukuman yang setimpal kepada pelaku tindak pidana cyber crime karnea seorang hakim menjatuhkian suatu putusan menurut hati nuraninya. Terhadap putusan No.2.862/Pid.B/2016/PN.MDN sangat ringan sehingga tidak memberikan efek jera terhadap pelaku tindak pidana cyber crime karena hukumannya sanggat jauh dari hukuman minimun yang diterapkan pada UU No.11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

# DAFTAR PUSTAKA

## A. Buku-buku

Andi Hamzah, Tahun 2004 Asas-Asas Hukum Pidana;PT. Rineka Cipta, Jakarta

Ayunda, 2013, Cybercrime Fighters, CIS

Ach Tahir, 2013, Cyber Crime, Suka Press

Bryan A. Garner, Black's Law Dictionary seventh Edition, St. Paul Minn: West

Baranda Nawawi Arief, Tahun 2006, Perkembangan Kajian Cyber Crime di Indonesia, RajaGrafindo Persada

Dikdik M. Arief Mansur; Elisatris Gultom, Cyber Law Aspek Hukum

E.Y Kanter dan S.R Sianturi, Asas-Asas hukum Pidana di Indonesia dan

Edmon Makarim, 2003 Kompilasi Hukum Telematika, Jakarta : Raja Grafindo Persada,

Josua Sitompul, Tinjauan aspek Hukun Pidana Cybercimes

Jogja Bangkit Team,Tahun 2009 Undang Undang ITE Etika Berinternet, Jogja Bangkit Publisher, JB Publiser

Jonathan Clough,13 mei 2010 ,Principles of Cybercrime,Cabridge University Press

Lamintang, 1997.Dasar-dasar Hukum Pidana Indonesia; Bandung, PT. Citra Aditya Bakti,

Moeljatno, 1987Asas-asas Hukum Pidana, Bina Aksara, Jakarta

Maskun, 2013, kejahatan Siber,Prenada Media

Poernomo, Bambang. 1992 Asas-asas Hukum Pidana, Ghalia Indonesia, Jakarta,

Samsul Arifin, 2012 "Metode Penulisan Karya Ilmiah dan Penelitian Hukum", Medan Area University Press,

sultan Remy Syahdeini, 2009, Kejahatan dan Tindak Pidana Komputer,grafiti

Sutan Remy Syahdeini, 2009 Kejahatan & Tindak Pidana Komputer : Jakarta, Grafiti,

Volodymyr Golubev, cyber crime and legal problems of Internet usage, dalam Tindak Pidana Mayantara : Perkembangan Kajian Cyber Crime di Indonesia , Jakarta : RajaGrafindo Persada

Budi Suhariyanto, Tahun 2012, Tindak Pidana Teknologi Informasi, Rajagrafindo Indonesia

**B. Undang – undang**

Undang-undang No 11 tahun 2008 tentang Informasi dan Transaksi Elektronik

Kitab Undang-Undang Hukum Pidana

**C. Internet**

http://www.pengertianpakar.com/2015/01/pengertian-perbuatan-melawan-hukum-menurut-pakar-hukum.html diakses pada hari Selasa tanggal 29 November Pukul 22: 31 Wib.

http://infodanpengertian.blogspot.co.id/2016/02/pengertian-dan-unsur-tindak-pidana.html diakses pada tanggal 29 November 2016 pada pukul 23: 03 Wib.

http://dutaxp.blogspot.com/2012/06/pengertian-dan-jenis-jenis-cybercrime.html diakses pada tanggal 29 November 2016 pada pukul 23:12 wib.

http://id.wikipedia.org/wiki/Cyberstalking diakses pada tanggal 29 November 2016 pada pukul 23:18 Wib.

metadatastudio.com/pengertian-email-phishing diakses pada tanggal 29 November 2016 pada pukul 23:19 Wib.

http://www.lemhannas.go.id/portal/daftar-artikel/1556-cyber-warfare.html diakses pada tanggal 29 November 2016 pada pukul 23:21 Wib.

http://vertikalpoint.blogspot.com/2012/10/jenis-jenis-cyber-crime.html diakses pada tanggal 29 November 2016 pada pukul 23:25 Wib.

http://dumadia.wordpress.com/2009/04/02/apliikasi-konvensi-cyber-crime-2001-dalam-uu-no-11-tahun-2008-mengenai-informasi-dan-transaksi-elektronik-ite diakses pada tanggal 29 november 2016 pada pukul 23:48 Wib.