BAB I

PENDAHULUAN

A. Latar Belakang

Perkembangan teknologi telah membawa keuntungan yaitu dengan dipermudahnya hidup manusia. Akan tetapi dapat menimbulkan dampak negatif diantaranya munculnya bentuk kejahatan baru seperti, kejahatan penyalahgunaan mengakses komputer secara tidak sah dalam sistem elektronik yang mengakibatkan kerugian bagi orang lain dan disertai pencucian uang dengan menggunakan komputer/jaringan LAN sebagai media untuk melakukan kejahatan, sehingga kejahatan tersebut dinamakan dengan *Cybercrime.*

Cybercrime merupakan keseluruhan bentuk kejahatan yang ditujukan terhadap komputer, jaringan komputer, dan para penggunanya, dan bentuk-bentuk kejahatan konvensional yang menggunakan atau dengan bantuan peralatan komputer.[1] Dimana kejahatan itu sendiri telah ada dan sudah muncul sejak permulaan zaman sampai sekarang.

Dewasa ini penyalahgunaan komputer atau kejahatan komputer berawal dari akses komputer secara illegal, yaitu merupakan suatu perbuatan yang secara sengaja dan tidak sah (tanpa hak) memasuki komputer atau sistem atau jaringan komputer milik pihak lain yang bukan difungsikan sebagai akses publik.

Agus Raharjo mengatakan bahwa cara memasuki sistem atau jaringan komputer tersebut dilakukan dengan memanfaatkan bahasa pemrograman sehingga harus melalui proses pengungkapan kode akses tertentu. Perbuatan berupa penyusupan ini sudah dikategorikan

[1] Widodo, 2011, ***Hukum Pidana di Bidang Teknologi Informasi (Cyber Crime Law) Telaah Teoritik dan Bedah Kasus***, penerbit : Aswaja Pressindo, Yogyakarta, hlm 12.

sebagai kejahatan perbuatan melawan hukum.[2] Sebagai contoh diambil dari putusan yang diangkat oleh penulis yaitu suatu perbuatan yang dilakukan oleh saudara LUKMAN dengan menggunakan komputer sebagai media untuk melakukan perbuatan tindak pidana yaitu mengakses komputer dan/atau sistem elektronik milik orang lain dengan APN (*Akses Point Name*) *campina* terhadap kartu telkomsel (simpati) dilakukan secara tanpa hak, dan melawan hukum karena tidak memiliki kewenangan/izin mengakses APN PT. Telkomsel, Tbk yang seharusnya khusus diberikan kepada PT. CAMPINA ICE CREAM INDUSTRI dan terdakwa tidak mendaftarkan secara resmi kepada pihak provider telkomsel, namun hanya merubah pengisian form aplikasi APN milik PT. Telkomsel, Tbk sehingga seolah-olah terdakwa bertindak sebagai pengguna dari PT. CAMPINA ICE CREAM INDUSTRI.

Dengan memakai nama perusahaan secara tidak sah, sehingga mengakibatkan kerugian kepada pihak perusahaan. Contoh tersebut merupakan salah satu perbuatan / sifat melawan hukum, karena unsur ini merupakan unsur yang harus ada atau mutlak dalam suatu tindak pidana agar sipelaku atau terdakwa dapat dilakukan penuntutan dan pembuktian di pengadilan.[3]

Selanjutnya menurut pendapat Widodo, bahwa akses tidak sah terhadap sistem atau jaringan komputer merupakan langkah awal dari perbuatan yang mengarah pada bentuk – bentuk *cybercrime* lainnya, misalnya pemalsuan dan penipuan melalui komputer, *Denial Of Service Attack* (DOS), dan *Phreaking*.[4] Sehingga akses tidak sah terhadap sistem komputer atau jaringan komputer dapat digolongkan menjadi bentuk tindak pidana *Cybercrime.*

Cybercrime, terjadi kali pertama di Amerika Serikat pada tahun 1960-an. Pada tahun 1970 di Amerika Serikat terjadi kasus manipulasi data nilai akademik mahasiswa di Brooklyn College New York, kasus penyalahgunaan komputer perusahaan untuk kepentingan karyawan, kasus pengkopian data untuk sarana kejahatan penyeludupan narkotika, kasus penipuan melalui kartu kredit. Selain itu, terjadi pula akses tidak sah terhadap database security Pasific National

---

[2] *Ibid*, hlm 50.
[3] Teguh Prasetyo, 2010, ***Hukum Pidana***, penerbit : PT. RajaGrafindo Persada, Jakarta, hlm 67.
[4] *Op.cit.* hlm 53.

Bank yang mengakibatkan kerugian sebesar $10,2 juta US pada tahun 1978. Selanjutnya kejahatan serupa terjadi juga disejumlah negara antara lain Jerman, Australia, Inggris, Finlandia, Swedia, Austria, Jepang, Swiss, Kanada, Belanda, dan Indonesia. Kejahatan tersebut menyerang terhadap harta kekayaan, kehormatan, sistem dan jaringan komputer.[5]

Cybercrime yang terjadi di Indonesia sudah ada sejak tahun 1983, terutama di bidang perbankan. Dalam tahun-tahun berikutnya sampai saat ini, di Indonesia banyak terjadi *cybercrime*, misalnya pembajakan program komputer, cracking, penggunaan kartu kredit pihak lain secara tidak sah (*carding*), pembobolan bank (*banking fraud*), pornografi, termasuk kejahatan terhadap nama domain (*domain name*). Selain itu, kasus kejahatan lain yang menggunakan komputer di Indonesia antara lain penyeludupan gambar-gambar porno melalui internet (*cybersmuggling*), pagejacking (*moustrapping*), spam (*junk mail*), *intercepting, cybersquatting, typosquatting*. Sedangkan kasus kejahatan terhadap sistem atau jaringan komputer antara lain *cracking*, *defacing*, *Denial Of Attack*(DOS), *Distributed Denial Of Service Attack*(DDOS), penyebaran virus (*worm*), dan pemasangan logic bomb.[6]

Dampak dari tumbuh dan berkembangnya teknologi komputer dan sistem elektronik lainnya tersebut, mengharuskan adanya peran hukum positif (hukum pidana) di Indonesia. Namun dalam kaitannya dengan *cyber crime*, undang-undang atau hukum positif di Indonesia belum sepenuhnya mengatur mengenai hal tersebut. Ketiadaan hukum positif atau undang-undang yang mengatur secara khusus dan menyeluruh tentang *cyber crime* ini menjadikan setiap kegiatan atau aktivitas kejahatan di dunia maya semakin banyak dan tidak terkendali yang pada akhirnya menyebabkan kekacauan di masyarakat.

Hal inilah yang tidak dikehendaki oleh masyarakat yang menjadi korban dari kemajuan teknologi. Berkaitan dengan hal itu, maka pada *era digital* seperti saat ini, ketentuan hukum pidana (hukum positif) tersebut sudah harus diubah dengan menghadirkan ketentuan hukum pidana baru yang berbasis pada rezim hukum *cyber* agar dapat menyentuh aktifitas *cyber.* Hukum ini lah yang akan mengatur aktifitas dalam dunia maya (*cyberlaw)* baik dalam aspek hukum administrasi, perdata dan pidana.

---

[5] *Ibid.* hlm. 44
[6] *Ibid.*

Oleh karena dibutuhkan suatu hukum yang baru untuk mengatur aktifitas dunia maya, maka dibentuk lah *Convention On Cybercrime* yang sudah disepakati oleh mayoritas negara dan organisasi internasional sebagai acuan aturan minimum (*minimum rule*) untuk pengaturan *Cybercrime* dalam hukum pidana di negara masing-masing. Berpijak pada rasa keterikatan Indonesia dengan konvensi tersebut, maka Indonesia meratifikasi isi dari *Convention On Cybercrime* ini melalui legislator dengan memberlakukan Undang – Undang ITE.

Tindak pidana yang diatur didalam UU–ITE ini adalah : akses tidak sah (*illegal access),* penyadapan atau interepsi tidak sah (*intercepting)* gangguan terhadap data komputer (*data interefence),* gangguan terhadap sistem komputer (*sistem interference),* penyalahgunaan perangkat lunak komputer (*missuse of device),* pemalsuan melalui komputer (*computer – related forgery),* pornografi melalui komputer (*pornography),* kejahatan" konvensional atau tradisional " yang menggunakan komputer. [7]

Dengan adanya Undang – Undang ITE ini, diharapkan dapat mampu mengurangi terjadinya kejahatan terhadap penyalahgunaan komputer.

Berdasarkan hal-hal yang telah diuraikan diatas, maka penulis tertarik menyusun skripsi yang bejudul : **PENYALAHGUNAAN KOMPUTER SEBAGAI PERBUATAN MELAWAN HUKUM (Studi Kasus Putusan No. 132/PID.B/2012/ PN.PWK).**

B. Rumusan Masalah

Adapun yang menjadi rumsan masalah yang diteliti adalah:

Bagaimanakah bentuk penyalahgunaan komputer yang dapat dinyatakan sebagai perbuatan melawan hukum dalam Putusan No. 132/PID/B/2012/PN.PWK?

C. Tujuan Penelitian

[7] *Ibid*, hlm 83.

Tujuan penelitian adalah untuk mengetahui bagaimana bentuk penyalahgunaan komputer yang dapat dinyatakan sebagai perbuatan melawan hukum dalam Putusan No. 132/PID/B/2012/PN.PWK.

D. Manfaat Penelitian

Adapun manfaat dari penelitian ini adalah sebagai berikut :

1. Manfaat Teoritis

Secara teoritis, penelitian ini diharapkan dapat memberikan sumbangan pemikiran dalam usaha untuk mengembangkan pengetahuan Ilmu Hukum Pidana, khusus Tindak Pidana Komputer dan Pencucian Uang serta sebagai referensi bagi kepentingan akademis serta tambahan bagi kepustakaan di bidang Ilmu Hukum.

2. Manfaat Praktis

Secara praktis, penelitian ini diharapkan mampu memberikan sumbangan pemikiran bagi praktisi dan para penegak hukum agar dapat menjadikannya sebagai pedoman didalam menegakkan keadilan bagi para pencari keadilan.

3. Bagi Penulis

Untuk memenuhi salah persyaratan mendapatkan gelar Sarjana Hukum pada Fakultas Hukum Universitas HKBP Nommensen Medan.

BAB II

TINJAUAN PUSTAKA

A. Tinjauan Umum Tentang Tindak Pidana

1. Pengertian Tindak Pidana

Istilah tindak pidana berasal dari istilah dalam hukum pidana Belanda yaitu *strafbaar feit.* Istilah ini terdapat dalam *wet boek van strafrecht* (WvS) Belanda, akan tetapi tidak ada penjelasan resmi tentang apa yang dimaksud dengan *strafbaar feit* itu. Oleh karena itu, para ahli hukum berusaha untuk memberikan arti dan isi dari istilah itu, sayangnya sampai kini belum ada keseragaman pendapat.[8]

Pidana berasal dari kata *straf* (Belanda), disebut dengan istilah hukuman. Pidana lebih tepat didefenisikan sebagai suatu penderitaan yang sengaja dijatuhkan/diberikan oleh negara kepada seseorang atau beberapa orang sebagai akibat hukum (sanksi) bagiannya atau perbuatannya yang telah melanggar larangan hukum pidana. Secara khusus larangan hukum pidana ini disebut tindak pidana (*strafbaar feit).*[9]

---

[8] Adami Chazawi, 2001, ***Pelajaran Hukum Pidana Bagian Pertama.,*** PT. Raja Grafindo Persada, Jakarta, hlm. 67

[9] *Ibid,* hlm. 24

Istilah-istilah yang pernah digunakan, baik dalam perundang-undangan yang ada maupun dalam berbagai literatur hukum sebagai terjemahan dari istilah *strafbaar feit* adalah sebagai berikut:

a. Tindak pidana
b. Peristiwa pidana
c. Delik
d. Pelanggaran pidana
e. Perbuatan yang boleh dihukum
f. Perbuatan yang dapat dihukum
g. Perbuatan pidana[10]

Beberapa pakar hukum mengemukakan mengenai pengertian tindak pidana antara lain:

a. Simon telah merumuskan "*strafbaar feit*" itu sebagai suatu tindakan melanggar hukum yang telah dilakukan dengan sengaja ataupun tidak dengan sengaja oleh seseorang yang dapat dipertanggung jawabkan atas tindakannya, dan yang oleh undang-undang telah dinyatakan sebagai suatu tindakan yang dapat dihukum.[11]

b. Pompe merumuskan bahwa suatu "*strafbaar feit*" itu sebenarnya adalah tidak lain dari pada suatu tindakan yang menurut suatu rumusan undang-undang telah dinyatakan sebagai tindakan yang dapat dihukum.[12]

c. J.E Jonkers, merumuskan peristiwa pidana ialah perbuatan yang melawan hukum (*wederrechttelijk)* yang berhubungan dengan kesengajaan atau kesalahan yang dilakukan oleh orang yang dapat dipertanggung jawabkan.[13]

d. Wirjono Prodjodikoro, menyatakan bahwa tindak pidana itu adalah suatu perbuatan yang pelakunya dapat dikenakan hukuman pidana.[14]

---

[10] *Ibid,* hlm. 67

[11] P.A.F. Lamintang, 1997, ***Dasar-Dasar Hukum Pidana Indonesia***, Penerbit: PT. Citra Aditya Bakti, Bandung, hlm. 181.

[12] Adami Chazawi , *Op.cit,* hlm. 72

[13] *Ibid,* hlm. 75

[14] *Ibid,* hlm. 75

2. Unsur-unsur Tindak Pidana

Dari uraian diatas, dimana setiap tindak pidana yang terdapat didalam kitab undang-undang hukum pidana itu pada umumnya dapat dijabarkan ke dalam unsur-unsur yang dapat dibagi menjadi dua macam unsur, yakni unsur-unsur subjektif dan unsur-unsur objektif.

Unsur-unsur subjektif adalah unsur-unsur yang melekat pada diri sipelaku atau yang berhubungan dengan diri sipelaku dan termasuk kedalamnya yaitu yang terkandung dalam hatinya.

Unsur-Unsur subjektif dari tindak pidana adalah: [15]

1. Kesengajaan atau ketidaksengajaan (*dolus* atau *culpa).*
2. Maksud atau *voornemen* pada suatu percobaan atau *pogging*.
3. Macam-macam maksud atau *oogmerk* seperti yang terdapat pada tindak pidana pencurian.
4. Merencanakan terlebih dahulu, misalnya terdapat pada pasal 340 KUHP.
5. Perasaan takut, misalnya yang terdapat dalam pasal 308 KUHP.

Sedangkan Unsur objektif adalah unsur-unsur yang ada hubungannya dengan keadaan, yaitu dalam keadaan-keadaan mana tindakan-tindakan dari si pelaku itu harus dilakukan.

Unsur objektif dari tindak pidana adalah:

1. Sifat melanggar hukum atau *wederrechtelijkheid.*
2. Kualitas si pelaku, misalnya keadaan sebagai seorang pegawai swasta dalam kejahatan menurut pasal 451 KUHP. Dalam pasal 451 KUHP antara lain ditegaskan: “keadaan sebagai pengurus atau komisaris dari suatu perseroan terbatas” di dalam kejahatan menurut pasal 398 KUHP.
3. Causalitas, yakni hubungan antar sesuatu tindakan sebagai penyebab dengan kenyataan sebagai akibat.

[15] http://raypratama.blogspot.com/2013/06/pengertian-hukum-pidana-unsur-unsur_1348. html diakses pada tanggal 29 Juni 2014

Sifat dari tindak pidana (*strafbaar feit)* adalah *onrechtmatigheid* atau sifat melanggar hukum dari tindak pidana. Adanya hukum pidana dengan tindak pidana yang dirumuskan didalamnya, bersumber pada pelanggaran-pelanggaran hukum. Dengan sendirinya dalam tiap tindak pidana harus ada sifat melanggar hukum atau *onrechtmatigheid.*[16]

B. Penyalahgunaan Komputer

1. Pengertian Tindak Pidana Komputer

Istilah komputer mempunyai arti dan makna yang luas dimana keberadaannya sebenarnya diambil dari bahasa latin *computare* yang berarti menghitung(*to compute)*. Secara *lexycography*, maka komputer berarti adalah si penghitung atau subjek yang melakukan suatu komputasi, dalam hal ini dapat diartikan si orangnya (*some one who computes)* ataupun perangkat pengolah komputasi itu sendiri (*a computing machine)*. Jika dicermati lebih dalam sepatutnya istilah komputer tidak hanya diartikan dalam artian perangkatnya saja melainkan juga keberadaan subjek pelakunya. Dalam konteks ini, maka keberadaan komputer tidak dapat dilepaskan dari keberadaan orangnya, karena tidak lain komputer sebagai perangkat adalah untuk membantu keperluan dari si orangnya untuk melakukan komputasi.[17]

Pada masa awalnya, *cybercrime* didefinisikan sebagai kejahatan komputer. Mengenai definisi kejahatan komputer sendiri, sampai sekarang para sarjana belum sependapat mengenai pengertian atau definisi dari kejahatan komputer. Bahkan penggunaan istilah tindak pidana untuk kejahatan komputer dalam bahasa Inggris pun masih belum seragam. Beberapa sarjana menggunakan istilah "*computer misuse*", "*computer abuse*", "*computer fraud*", "*computer-related crime*", "*computer-assisted crime*", atau "*computer crime*". Namun para sarjana pada umumnya lebih menerima pemakaian istilah "*computer crime*" oleh karena dianggap lebih luas dan biasa dipergunakan dalam hubungan internasional.[18]

Mandell membagi "*computer crime*" atas dua kegiatan, yaitu:

1. Penggunaan komputer untuk melaksanakan perbuatan penipuan, pencurian atau penyembunyian yang dimaksud untuk memperoleh keuntungan keuangan, keuntungan bisnis, kekayaan atau pelayanan;

---

[16] Wirjono Prodjodikoro,2003, ***Asas-asas Hukum Pidana di Indonesia,*** Bandung, Refika Aditama, hlm. 64.

[17] Edmon Makarim, 2003, ***KOMPILASI HUKUM TELEMATIKA,*** Jakarta, PT. Raja Grafindo Persada, hlm. 53

[18] Budi Suhariyanto, 2013, ***Tindak Pidana Teknologi Informasi (Cybercrime)***, Jakarta, Rajawali Pers, hlm. 9

2. Ancaman terhadap komputer itu sendiri, seperti pencurian perangkat keras atau lunak, sabotase dan pemerasan.

Kejahatan Komputer adalah perbuatan melawan hukum yang dilakukan memakai komputer sebagai sarana/alat atau komputer sebagai objek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain. Kejahatan yang berhubungan erat dengan penggunaan teknologi yang berbasis utama komputer dan jaringan telekomunikasi.[19]

Menurut Andi Hamzah dalam bukunya yang berjudul "Aspek-aspek Pidana di Bidang Komputer", mengemukakan bahwa pengertian kejahatan komputer adalah segala aktifitas tidak sah yang memanfaatkan komputer untuk tindak pidana. Sekecil apapun dampak atau akibat yang ditimbulkan dari penggunaan komputer secara tidak sah atau ilegal merupakan suatu kejahatan. Dan dalam arti sempit kejahatan komputer adalah suatu perbuatan melawan hukum yang dilakukan dengan teknologi komputer yang canggih.[20]

Semua perbuatan hukum yang dilakukan di dalam dunia maya, adalah perbuatan-perbuatan hukum yang dilakukan oleh manusia-manusia yang berada di dunia nyata, dan dilakukan di lokasi tertentu di dunia nyata. Hanya perbuatan tersebut dilakukan menggunakan sarana media atau sarana internet (menggunakan komputer yang berada didunia nyata).[21]

2. Unsur-unsur Tindak Pidana Komputer

Di Indonesia tindak pidana dengan menggunakan komputer sejak dahulu masih sulit untuk dinyatakan atau dikategorikan sebagai tindak pidana, karena terbentur dengan asas legalitas (Pasal 1 ayat (1) KUHP), *Tiada suatu perbuatan yang dapat dipidana jika suatu peraturan belum ada ketentuannya. Adagium* tersebut cenderung sangat membatasi penegak

[19] http://supeeerblog.blogspot.com/2013/01/kejahatan-komputer.html, diakses pada tanggal 29 Juni 2014, pukul. 15:30

[20] Andi Hamzah, 1989, ***Aspek-Aspek Pidana di Bidang Komputer,*** Jakarta, Sinar Grafika, hlm. 26

[21] Niniek Suparni, 2009, ***CYBER SPACE: Problematika dan Antisipasi Pengaturannya,*** Jakarta, Sinar Grafika, hlm. 36

hukum di Indonesia untuk melakukan penyelidikan dan atau penyidik guna mengungkap perbuatan tersebut.[22]

Jika tetap berpatokan pada asas legalitas, maka akan sulit untuk menerapkan peraturan yang ada di dalam KUHP terhadap kasus kejahatan penyalahgunaan komputer ini. Berkaitan dengan hal itu maka perlu suatu penafsiran terhadap undang-undang sehingga suatu perbuatan yang tidak diatur di dalam undang-undang tidak begitu saja dikesampingkan karena alasan tidak ada peraturan atau ketentuannya. Keberanian hakim untuk menafsirkan undang-undang merupakan bentuk antisipasi terhadap kejahatan penyalahgunaan komputer(*cybercrime).*

Dalam hukum pidana dikenal adanya suatu suatu pendekatan dalam menerapkan suatu ketentuan pidana yang biasa dikenal sebagai penafsiran. Penafsiran yang dapat digunakan atas perbuatan atau tindakan tersebut adalah penafsiran *ekstensif;* yang merupakan suatu metode penafsiran dimana hakim memperluas arti atau maksud sebenarnya dari suatu ketentuan undang-undang. Dikaitkan dengan penerapan KUHP terhadap kejahatan penyalahgunaan komputer perlu dipilah-pilah perbuatan mana yang substansinya hampir sama dengan rumusan tindak pidana biasa (dalam KUHP).[23]

Kemudian lahirlah suatu rezim hukum baru yang dikenal dengan hukum siber atau hukum telematika. Hukum siber (*cyber law*), secara internasional digunakan untuk istilah hukum yang terkait dengan pemanfaatan teknologi informasi dan komunikasi. Demikian pula hukum telematika yang merupakan perwujudan dari konvergensi hukum telekomunikasi, hukum media, dan hukum informatika.

Istilah lain juga yang digunakan adalah hukum teknologi informasi (*law of information tecnology)*, hukum dunia maya (*virtual world law)* dan hukum mayantara. Istilah-istilah tersebut lahir mengingat kegiatan yang dilakukan melalui jaringan sistem komputer dan sistem komunikasi baik dalam lingkup lokal maupun global (*internet)* dengan memanfaatkan teknologi informasi berbasis sistem komputer yang merupakan sistem elektronik yang dapat dilihat secara virtual.[24]

---

[22] Edmon Makarim, *Op.cit.*, hlm.53
[23] *Ibid,* hlm. 406
[24] Budi suhariyanto, *Op.cit,* hlm.2

Perbuatan melawan hukum *cyber* sangat tidak mudah diatasi dengan mengandalkan hukum positif konvensional karena berbicara mengenai kejahatan, tidak dapat dilepaskan dari lima faktor yang saling kait-mengkait, yaitu pelaku kejahatan, modus kejahatan, korban kejahatan, reaksi sosial atas kejahatan dan hukum.[25]

Namun akhirnya, pada bulan Maret 2008 disahkanlah Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik oleh pemerintah. Di dalam undang-undang tersebut diatur mengenai beberapa kriminalisasi perbuatan pidana yang sebelumnya bukanlah tindak pidana melalui beberapa terobosan dan perluasan dalam hal asas-asasnya beserta sanksi pidananya. Selain itu aturan pidana substantif, dalam undang-undang ini juga mengatur mengenai prosedur dan alat bukti yang mengalami perluasan, yaitu dimasukkannya alat bukti baru yang berkaitan dengan media elektronik.[26]

Klasifikasi perbuatan yang dilarang dalam UU ITE dijelaskan dalam Pasal 27 sampai dengan Pasal 37. Konstruksi pasal-pasal tersebut mengatur secara lebih detail tentang pengembangan modus-modus kejahatan tradisional sebagaimana tercantum dalam Kitab Undang-undang Hukum Pidana (KUHP). Sebagai contoh dalam kasus yang penulis akan angkat, dimana terdakwa dikenakan beberapa pasal dalam UU ITE yatu Pasal 30 ayat (1), Pasal 36 dan Pasal 51 ayat (2) UU ITE yang berbunyi sebagai berikut:

Pasal 30

1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik orang lain dengan cara apa pun.
2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektonik dengan cara apapun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.
3) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

Pasal 36

[25] *Ibid,* hlm.4
[26] *Ibid,* hlm.6

Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 34 yang mengakibatkan kerugian bagi Orang lain.

Pasal 51
1) Setiap orang yang memenuhi unsur sebgaimana dimaksud dalam Pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp. 12.000.000.000,00 (dua belas miliar rupiah).
2) Setiap orang yang memenuhi unsur sebagaimana yang dimaksud dalam Pasal 36 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp. 12.000.000.000,00 (dua belas miliar rupiah).

Berdasarkan rumusan pasal diatas, perbuatan yang dilarang dan dianggap perbuatan melawan hukum adalah mengakses komputer dan/atau sistem elektronik yang bertentangan dengan hukum. Pengertian tentang perbuatan yang dapat dihukum atau perbuatan melawan hukum, dengan mengikuti pendapat Van Hammel dan Hoge Raad (HR) tentang unsur melawan hukum atau *wederrechttelijk*, yakni tanpa hak atau wewenangnya (*zonder eigenrecht of zonder eigen bevoegheid).*[27]

Unsur-unsur pada Pasal 30 ayat (1), Pasal 36 dan Pasal 51 ayat (2) adalah:

a. Setiap orang;

b. Dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik;
   1. Milik orang lain dengan cara apapun;
   2. Dengan cara apapun dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen elektronik;
   3. Dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan;

c. Yang mengakibatkan kerugian bagi orang lain.

[27] Siswanto Sunarso, 2009, ***HUKUM INFORMASI DAN TRANSAKSI ELEKTRONIK:*** *STUDI KASUS PRITA MULYASARI*, Penerbit: Rineka Cipta, Jakarta, hlm. 69

Pengertian orang disini, selain ditafsirkan sebagai individu juga badan hukum yang berbadan hukum sesuai ketentuan perundang-undangan. Pengetian dengan sengaja dan tanpa hak dapat ditafsirkan sebagai perbuatan yang bertentangan dengan undang-undang dan tindakan melalaikan yang diancam hukuman.

Pengertian mengakses komputer dan/atau sistem elektronik adalah kegiatan melakukan interaksi dengan sistem elektronik yang beridiri sendiri atau dalam jaringan, melalui perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik.[28]

Adapun perbuatan yang dilarang oleh undang-undang (*wederrechttelijk)* ini, adalah mengakses komputer dan/atau sistem elektronik tersebut adalah milik orang lain dengan cara apapun, atau bertujuan untuk memperoleh informasi elektronik dan/atau dokumen elektronik dengan cara apapun, atau dengan melanggarar, memerobos, melampaui, atau menjebol sistem pengamanan dengan cara apapun.

Delik ini adalah delik formil atau delik dengan perumusan formil, yakni delik yang dianggap telah sepenuhnya terlaksana dengan dilakukannya suatu perbuatan yang dilarang tersebut.[29]

Delik yang dimaksud dengan Pasal 36 adalah delik materiil atau delik dengan perumusan materiil, yakni delik yang baru dianggap terlaksana penuh dengan timbulnya akibat yang dilarang. Dengan demikian akibat dari perbuatan yang dilarang undang-undang sebagaimana dimaksud diatas, yang mengakibatkan kerugian bagi orang lain harus dapat dibuktikan.[30]

---

[28] *Ibid,* hlm. 103
[29] *Ibid.*
[30] *Ibid,* hlm. 112

Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik ini jika ditinjau dalam perspektif kebijakan pidana, secara umum dalam hal perumusan tindak pidana, perumusan sanksi pidana dan prosedur atau mekanisme sistem peradilan pidana. Peninjauan masalah kebijakan kriminalisasi dalam Udang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik ini merupakan tahap yang paling strategis dari keseluruhan perencanaan proses fungsionalisasi hukum pidana atau proses penegakan hukm pidana dalam rangka penanggulangan kejahatan *cybercrime.* Perencanaan atau kebijakan penanggulangan kejahatan yang dituangkan dalam peraturan perundang-undangan, secara garis besar meliputi:[31]

1. Perencanan atau kebijakan tentang perbuatan-perbuatan terlarang apa yang akan ditanggulangi karena dipandang membahayakan atau merugikan;
2. Perencanaan atau kebijakan tentang sanksi apa yang dapat dikenakan terhadap pelaku perbuatan terlarang itu (baik berupa pidana atau tindakan) dan sistem penerapannya;
3. Perencanaan atau kebijakan tentang prosedur atau mekanisme sistem peradilan pidana dalam rangka proses penegakan hukum pidana;

Dengan demikian, peninjauan kembali *(review)* terhadap kebijakan kriminalisasi kejahatan teknologi informasi (*cybercrime)* dalam Undang-undang ITE ini harus pula difokuskan pada ketiga bidang kebijakan diatas. Dengan meninjau ketiga hal tersebut dalam undang-undang ini, diharapkan dapat menganalisis fungsionalisasi hukum pidana dalam tahap formulasi sehingga dapat mengetahui dasar pertimbangan pembuat undang-undang dalam menyusun kebijakan kriminalisasi. Selain itu, juga dapat mengetahui letak kelemahan-kelemahan kriminalisasi *cybercrime* dalam UU ITE yang perlu diperhatikan oleh aparat penegak hukum yang mengimplementasikan undang-undang ini.

3. Pengaturan Hukum Positif Mengenai Tindak Pidana Komputer

Penyalahgunaan komputer dalam perkembangannya menimbulkan permasalahan yang sangat rumit, terutama kaitannya dengan proses pembuktian tindak pidana (faktor yuridis). Apalagi penggunaan komputer untuk tindak kejahatan itu memiliki karakteristik tersendiri atau berbeda dengan kejahatan yang dilakukan tanpa menggunakan komputer (konvensional). Perbuatan atau tindakan, pelaku, alat bukti ataupun barang bukti dalam tindak pidana biasa dapat

[31] *Op.cit*, Budi Suhariyanto, hlm. 8

dengan mudah diidentifikasi, tidak demikian halnya untuk kejahatan yang dilakukan dengan menggunakan komputer.

Pengaturan *cyberlaw* Indonesia jauh tertinggal jika dibandingkan dengan negara-negara lain. Seperti Asia Tenggara misalnya, Indonesia merupakan negara yang tidak memiliki perundangan (peraturan) yang khusus mengenai *cyberlaw*. Salah satu isu dari *cyberlaw* yang semakin marak akhir-akhir ini adalah *cybercrime* atau kejahatan yang memiliki keterkaitan erat dengan teknologi informasi. Kejahatan yang terjadi melalui jaringan publik (internet) merupakan suatu konsekuensi negatif dari suatu dunia yang tidak mengenal batas yurisdiksi.

Kejahatan yang dikenal sebagai *cybercrime* ataupun *computer crime* di Indonesia, sebenarnya masih dapat ditangani dengan perturan perundang-undangan pidana Indonesia yang masih berlaku (e.g. KUHP, dan sebagainya), namun seringkali timbul pertanyaan mengenai relevansi pengaturan tersebut dengan jenis kejahatan yang berkembang sekarang.[32]

Sistem hukum Pidana di Indonesia memperkenalkan dua pundi utama dalam mendeskripsikan tindakan yang dianggap melanggar hukum (melawan undang-undang) yaitu, tindakan yang dianggap sebagai suatu pelanggaran dan tindakan yang dianggap sebagai kejahatan.

Kemudian, trend kejahatan dengan memanfaatkan teknologi informasi semakin marak dilakukan. Sementara, para pakar pidana ataupun masyarakat belum juga mencapai titik temu dalam hal penyebutan atau pendefinisiannya. Hingga kemudian masyarakat menilai bahwa sampai saat ini belum ada kejelasan hukum (legalitas) tentang kejahatan ini. Kerugian yang ditimbulkannya akibat kejahatan ini pun tidak sedikit. Sehingga atas dasar itulah, timbul kepentingan beberapa pihak, baik pemerintah maupun masyarakat untuk mengatur kejahatan tersebut dalam hukum positif.[33]

Menjawab tuntutan dan tantangan komunikasi global melalui komputer dengan sarana internet, Undang-Undang yang diharapkan (*ius konstituendum*) adalah perangkat hukum yang akomodatif terhadap perkembangan serta antisipatif terhadap permasalahan, termasuk dampak negatif penyalahgunaan komputer dan Internet dengan berbagai motivasi yang dapat

[32] Edmon Makarim, *Op.cit.*, hlm. 407
[33] *Ibid.*

menimbulkan korban-korban seperti kerugian materi dan non materi. Saat ini, Indonesia belum memiliki Undang – Undang khusus/ *cyber law* yang mengatur mengenai *cybercrime.* Tetapi, terdapat beberapa hukum positif lain yang berlaku umum dan dapat dikenakan bagi para pelaku *cybercrime* terutama untuk kasus-kasus yang menggunakan komputer sebagai sarana, antara lain:[34]

a. Kitab Undang Undang Hukum Pidana

Dalam upaya menangani kasus-kasus yang terjadi para penyidik melakukan analogi atau perumpamaan dan persamaaan terhadap pasal-pasal yang ada dalam KUHP. Pasal-pasal didalam KUHP biasanya digunakan lebih dari satu Pasal karena melibatkan beberapa perbuatan sekaligus pasal-pasal yang dapat dikenakan dalam KUHP pada *cybercrime* antara lain :

1) Pasal 362 KUHP (Pencurian)

Dapat dikenakan untuk kasus *carding* dimana pelaku mencuri nomor kartu kredit milik orang lain walaupun tidak secara fisik karena hanya nomor kartunya saja yang diambil dengan menggunakan *software card generator* di Internet untuk melakukan transaksi di *e-commerce*. Setelah dilakukan transaksi dan barang dikirimkan, kemudian penjual yang ingin mencairkan uangnya di bank ternyata ditolak karena pemilik kartu bukanlah orang yang melakukan transaksi.

2) Pasal 378 KUHP (Penipuan)

Dapat dikenakan untuk penipuan dengan seolah olah menawarkan dan menjual suatu produk atau barang dengan memasang iklan di salah satu *website* sehingga orang tertarik untuk membelinya lalu mengirimkan uang kepada pemasang iklan. Tetapi, pada kenyataannya, barang tersebut tidak ada. Hal tersebut diketahui setelah uang dikirimkan dan barang yang dipesankan tidak datang sehingga pembeli tersebut menjadi tertipu.

3) Pasal 335 KUHP (Kejahatan terhadap kemerdekaan orang)

[34] http://ndutkugaadaygpunya.wordpress.com/2013/11/08/keamanan-ketat-untuk-seorang-cyber-crime, diakses 25/07/2014, pukul. 19.30

Dapat dikenakan untuk kasus pengancaman dan pemerasan yang dilakukan melalui *e-mail* yang dikirimkan oleh pelaku untuk memaksa korban melakukan sesuatu sesuai dengan apa yang diinginkan oleh pelaku dan jika tidak dilaksanakan akan membawa dampak yang membahayakan. Hal ini biasanya dilakukan karena pelaku biasanya mengetahui rahasia korban.

4) Pasal 311 KUHP (Pencemaran nama baik)

Dapat dikenakan untuk kasus pencemaran nama baik dengan menggunakan media Internet. Modusnya adalah pelaku menyebarkan *email* kepada teman-teman korban tentang suatu cerita yang tidak benar atau mengirimkan *email* ke suatu *mailing list* sehingga banyak orang mengetahui cerita tersebut.

5) Pasal 303 KUHP (Perjudiaan)

Dapat dikenakan untuk menjerat permainan judi yang dilakukan secara *online* di Internet dengan penyelenggara dari Indonesia.

6) Pasal 282 KUHP (Kejahatan Pornografi)

Dapat dikenakan untuk penyebaran pornografi maupun *website* porno yang banyak beredar dan mudah diakses di Internet. Walaupun berbahasa Indonesia, sangat sulit sekali untuk menindak pelakunya karena mereka melakukan pendaftaran domain tersebut diluar negri dimana pornografi yang menampilkan orang dewasa bukan merupakan hal yang ilegal.

7) Pasal 282 dan 311 KUHP

Dapat dikenakan untuk kasus penyebaran foto atau film pribadi seseorang yang vulgar di Internet , misalnya kasus Sukma Ayu-Bjah.

8) Pasal 378 dan 262 KUHP

Dapat dikenakan pada kasus *carding*, karena pelaku melakukan penipuan seolah-olah ingin membeli suatu barang dan membayar dengan kartu kreditnya yang nomor kartu kreditnya merupakan curian.

9) Pasal 406 KUHP (Menghancurkan atau Merusakkan barang)

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.

b. Undang-Undang No 36 Tahun 1999 tentang Telekomunikasi

Menurut Pasal 1 angka (1) Undang – Undang No 36 Tahun 1999, Telekomunikasi adalah setiap pemancaran, pengiriman, dan/atau penerimaan dan setiap informasi dalam bentuk tanda-tanda, isyarat, tulisan, gambar, suara, dan bunyi melalui sistem kawat, optik, radio, atau sistem elektromagnetik lainnya. Dari definisi tersebut, maka Internet dan segala fasilitas yang dimilikinya merupakan salah satu bentuk alat komunikasi karena dapat mengirimkan dan menerima setiap informasi dalam bentuk gambar, suara maupun film dengan sistem elektromagnetik. Penyalahgunaan Internet yang mengganggu ketertiban umum atau pribadi dapat dikenakan sanksi dengan menggunakan Undang- Undang ini, terutama bagi para *hacker* yang masuk ke sistem jaringan milik orang lain sebagaimana diatur pada Pasal 22, yaitu Setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah, atau memanipulasi:

a) Akses ke jaringan telekomunikasi

b) Akses ke jasa telekomunikasi

c) Akses ke jaringan telekomunikasi khusus

Apabila anda melakukan hal tersebut seperti yang pernah terjadi pada website KPU www.kpu.go.id, maka dapat dikenakan Pasal 50 yang berbunyi “Barang siapa yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 22, dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp600.000.000,00 (enam ratus juta rupiah)”.

c. Undang-Undang No 25 Tahun 2003 tentang Perubahan atas Undang-Undang No. 15 Tahun 2002 tentang Tindak Pidana Pencucian Uang

Undang-Undang ini merupakan Undang-Undang yang paling ampuh bagi seorang penyidik untuk mendapatkan informasi mengenai tersangka yang melakukan penipuan melalui Internet, karena tidak memerlukan prosedur birokrasi yang panjang dan memakan waktu yang lama, sebab penipuan merupakan salah satu jenis tindak pidana yang termasuk dalam pencucian uang (Pasal 2 Ayat (1) Huruf q). Penyidik dapat meminta kepada bank yang menerima transfer untuk memberikan identitas dan data perbankan yang dimiliki oleh tersangka tanpa harus mengikuti peraturan sesuai dengan yang diatur dalam Undang-Undang Perbankan. Dalam Undang-Undang Perbankan identitas dan data perbankan merupakan bagian dari kerahasiaan bank sehingga apabila penyidik membutuhkan informasi dan data tersebut, prosedur yang harus dilakukan adalah mengirimkan surat dari Kapolda ke Kapolri untuk diteruskan ke Gubernur Bank Indonesia. Prosedur tersebut memakan waktu yang cukup lama untuk mendapatkan data dan informasi yang diinginkan. Dalam Undang-Undang Pencucian Uang proses tersebut lebih cepat karena Kapolda cukup mengirimkan surat kepada Pemimpin Bank Indonesia di daerah tersebut dengan tembusan kepada Kapolri dan Gubernur Bank Indonesia, sehingga data dan informasi yang dibutuhkan lebih cepat didapat dan memudahkan proses penyelidikan terhadap pelaku, karena data yang diberikan oleh pihak bank, berbentuk: aplikasi pendaftaran, jumlah rekening masuk dan keluar serta kapan dan dimana dilakukan transaksi maka penyidik dapat

menelusuri keberadaan pelaku berdasarkan data– data tersebut. Undang-Undang ini juga mengatur mengenai alat bukti elektronik atau *digital evidence* sesuai dengan Pasal 38 huruf b yaitu alat bukti lain berupa informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu.

d. Undang-Undang No 15 Tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme

Selain Undang-Undang No. 25 Tahun 2003, Undang-Undang ini mengatur mengenai alat bukti elektronik sesuai dengan Pasal 27 huruf b yaitu alat bukti lain berupa informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu. *Digital evidence* atau alat bukti elektronik sangatlah berperan dalam penyelidikan kasus terorisme, karena saat ini komunikasi antara para pelaku di lapangan dengan pimpinan atau aktor intelektualnya dilakukan dengan memanfaatkan fasilitas di Internet untuk menerima perintah atau menyampaikan kondisi di lapangan karena para pelaku mengetahui pelacakan terhadap Internet lebih sulit dibandingkan pelacakan melalui handphone. Fasilitas yang sering digunakan adalah *e-mail* dan *chat room* selain mencari informasi dengan menggunakan *search engine* serta melakukan propaganda melalui *bulletin board* atau *mailing list*.

Sesungguhnya segala sesuatu perkembangan apapun yang terjadi di masyarakat Indonesia sesuai tujuan negara maka prospeknya adalah untuk memajukan kesejahteraan umum. Hal ini demi pengamalan nilai-nilai Pancasila yang dikristalisasi dalam Undang-Undang Dasar Negara Republik Indonesia tahun 1945 (UUD RI 1945). Tujuan negara tersebut tertuang dalam pembukaan UUD RI 1945 paragraf ke empat. Untuk mencapai tujuan negara tersebut hukum pidana memiliki peran penting sebagai *ultimum remidium* terhadap kejahatan dan pelanggaran. Kemajuan dan perkembangan teknologi, khususnya telekomunikasi dan teknologi informasi

dapat merubah tatanan organisasi dan hubungan sosial setiap individu di masyarakat. Maka diperlukan langkah konkret untuk mengatasi fenomena tersebut.

Hukum dalam hal ini hukum pidana dibutuhkan oleh masyarakat untuk menjadi lawan utama kejahatan. Fungsi preventif dan represif dari hukum itu harus berlaku secara bersamaan demi mendapatkan penegakan hukum yang lebih baik. Kejahatan dunia maya yang sudah menjadi bahasa sehari-hari disebut *cyber crime atau computer crime* adalah bentuk baru kejahatan dengan lahirnya *virtual reality*. Untuk itu bentuk-bentuk perbuatan hukum itu perlu mendapatkan penyesuaian, seperti melakukan harmonisasi terhadap beberapa perundang-undangan yang sudah ada, mengganti jika tidak sesuai lagi dan membentuk ketentuan hukum baru. Selain adanya upaya penanggulangan dengan cara, proses, pembuatan menangani kejahatan (*cyber crime*) dengan hukum pidana.

4. Jenis-Jenis Tindak Pidana Penyalahgunaan Komputer

Perkembangan internet dan umumnya dunia *cyber* tidak selamanya menghasilkan hal-hal yang positif. Salah satu hal negatif yang merupakan efek sampingnya antara lain adalah kejahatan di dunia *cyber* atau *cybercrime*. Hilangnya batas ruang dan waktu di internet mengubah banyak hal.

Kejahatan komputer adalah kejahatan yang ditimbulkan karena penggunaan komputer secara ilegal. Kejahatan komputer terus berkembang seiring dengan kemajuan teknologi komputer saat ini. Kejahatan yang berhubungan erat dengan penggunaan teknologi yang berbasis utama komputer dan jaringan telekomunikasi ini dalam beberapa literatur dan prakteknya dikelompokkan dalam beberapa jenis, antara lain:[35]

***1. Illegal Access* / Akses Tanpa Ijin ke Sistem Komputer**

[35] http://wahyu410.wordpress.com/2011/11/12/tugas-makalah-kejahatan-komputer/kamis, 24/04/2014 pukul. 12:40

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.

2. ***Illegal Contents* / Konten Tidak Sah**

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.

3. ***Data Forgery* / Pemalsuan Data**

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.

4. ***Spionase Cyber* / Mata-mata**

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.*

5. ***Data Thieft* / Mencuri Data**

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.

6. Misuse of devices / **Menyalahgunakan Peralatan Komputer**

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. Contoh penyalahgunaan peralatan computer : Pemalsuan kartu kredit, perjudian melalui komputer, pelanggan terhadap hak cipta.

BAB III

METODE PENELITIAN

A. Ruang Lingkup

Metode penelitian yang dilakukan dalam penelitian ini adalah dengan menggunakan metode yuridis normatif. Penelitian hukum normatif bisa juga disebut sebagai penelitian hukum doktrinal. Pada penelitian ini, sering kali hukum dikonsepsikan sebagai apa yang tertulis dalam peraturan perundang-undangan (Law in book) atau hukum yang dikonsepsikan sebagai kaidah atau norma yang merupakan patokan berperilaku masyarakat terhadap apa yang dianggap pantas. Namun sesungguhnya hukum juga dapat dikonsepkan sebagai apa yang ada dalam tindakan (Law in action). Law in book adalah hukum yang seharusnya berjalan sesuai harapan, keduanya seiring berbeda, artinya hukum dalam buku sering berbeda dengan hukum dalam kehidupan masyarakat.[36]

[36] http://koffieenco.blogspot.com/2013/08/penelitian-hukum-normatif.html, 5 Mei 2014, 18:33 Wib.

Ruang lingkup penelitian bertujuan untuk membatasi permasalahan dalam penelitian ini sehingga pembahasannya akan menjadi terarah. Dimana penulis akan memfokuskan penelitian dengan menganalisis putusan Pengadilan Negeri Purwakarta: No.132/PID/B/2012 mengenai Dengan Sengaja dan Melawan Hukum Mengakses Komputer dan Sistem Elektronik Orang Lain Dengan Cara Apapun Yang Mengakibatkan Kerugian Bagi Orang Lain dan Pencucian Uang.

B. Metode Pendekatan

Dalam penelitian ini, penulis menggunakan metode pendekatan secara yuridis normatif antara lain :

1. Metode pendekatan kasus *(case approach)* yaitu dengan cara menganalisis putusan Pengadilan Negeri Purwakarta Nomor: 132/PID/B/2012. Pada putusan tersebut terdakwa dijatuhi Pidana atas tindak pidana Dengan Sengaja dan Melawan Hukum Mengakses Komputer dan Sistem Elektronik Orang Lain Dengan Cara Apapun Yang Mengakibatkan Kerugian Bagi Orang Lain dan Pencucian Uang.
2. Metode pendekatan perundang-undangan *(statute approach)* yaitu dilakukan dengan menelaah ketentuan Perundang-undangan yang berlaku dalam kasus tersebut yaitu KUHP (Kitab Undang-undang Hukum Pidana), KUHAP (Kitab Undang-undang Hukum Acara Pidana), Undang-undang RI. Nomor 36 Tahun 1999 Tentang Telekomunikasi, Undang-undang RI. Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, dan Undang-undang RI. Nomor 8 Tahun 2010 Tentang Pencegahan Dan Pemberantasan Tindak Pidana Pencucian Uang.

C. Bahan Hukum dan Sumbernya

Bahan hukum yang digunakan dalam penelitian ini adalah:

1. Bahan Hukum Primer

Merupakan Bahan Hukum yang mengikat seperti peraturan Perundang-undangan, dalam hal ini penulis akan menggunakan KUHP (Kitab Undang-undang Hukum Pidana), KUHAP (Kitab Undang-undang Hukum Acara Pidana), Undang-undang RI. Nomor 36 Tahun 1999 Tentang Telekomunikasi, Undang-undang RI. Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, dan Undang-undang RI. Nomor 8 Tahun 2010 Tentang Pencegahan Dan Pemberantasan Tindak Pidana Pencucian Uang.

2. Bahan Hukum Sekunder

Merupakan bahan-bahan hukum yang diperoleh melalui Buku-buku hukum, Literatur hukum, hasil-hasil penelitian, jurnal hukum, kamus-kamus hukum dan komentar-komentar atas putusan yang telah berkekuatan hukum tetap.

3. Bahan Hukum Tersier

Merupakan bahan hukum yang memberikan petunjuk atau penjelasan terhadap bahan-bahan hukum primer dan bahan hukum sekunder. Dalam hal ini terdiri dari Kamus Hukum Bahasa Indonesia.

D. Metode Analisa

Analisa yang digunakan dalam penelitian adalah yuridis normatif yaitu dengan mempergunakan Perundang-undangan yang berlaku kemudian membandingkannya.