KEJAHATAN KOMPUTER MENURUT KITAB UNDANG-UNDANG HUKUM PIDANA DAN UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK

SKRIPSI

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

Oleh:

TATIPATTO NAOMI YUANITA

NIM 0510110183

DEPARTEMEN PENDIDIKAN NASIONAL

UNIVERSITAS BRAWIJAYA

FAKULTAS HUKUM

MALANG

2009

LEMBAR PERSETUJUAN

SKRIPSI

KEJAHATAN KOMPUTER MENURUT KITAB UNDANG-UNDANG HUKUM PIDANA DAN UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK

Oleh:
TATIPATTO NAOMI YUANITA
NIM.0510110183

Disetujui pada tanggal:

Pembimbing Utama	Pembimbing Pendamping
Prof. Dr. I Nyoman Nurjaya SH.MH	Eny Haryati, SH. MH
NIP: 130 819 381	NIP: 131 573 925

Mengetahui
Ketua Bagian Hukum Pidana

Setiawan Nurdayasakti, SH, MH
NIP: 131 839 360

LEMBAR PENGESAHAN

KEJAHATAN KOMPUTER MENURUT KITAB UNDANG-UNDANG HUKUM PIDANA DAN UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK

Disusun Oleh:

TATIPATTO NAOMI YUANITA
NIM. 0510110183

Skripsi ini telah disahkan oleh Dosen Pembimbing pada tanggal:

Pembimbing Utama,	Pembimbing Pendamping,
Prof. Dr. I Nyoman Nurjaya SH.MH NIP:130 819 381	Eny Haryati, SH. MH NIP:131 573 925
Ketua Majelis Penguji,	Ketua Bagian Hukum Pidana
Prof. Dr. Koesno Adi SH. MS NIP: 130 531 853	Setiawan Nurdayasakti, SH, MH NIP: 131 839 360

Mengetahui
Dekan,

Herman Suryokumoro, SH. MS.
NIP. 131 472 741

KATA PENGANTAR

Puji dan syukur senantiasa Penulis haturkan kepada Tuhan Yesus Kristus yang selama ini sudah memberi kekuatan, bimbingan dan perlindungan kepada penulis sehingga penulis dapat menyelesaikan skripsi ini.

Penulis menyadari bahwa tanpa bantuan dari berbagai pihak mustahil rasanya skripsi ini dapat terselesaikan. Dalam kesempatan ini penulis ingin menyampaikan rasa terima kasih yang sebesar-besarnya kepada:

1. Bapak Herman Suryokumoro,SH.MS selaku Dekan Fakultas Hukum Universitas Brawijaya
2. Bapak Setiawan Nurdayasakti, SH. MH selaku Ketua Bagian Hukum Pidana, terima kasih Bapak atas semua bimbingan dan ilmu yang dibagikan sejak semester 1 sampai semester 8 ini.
3. Bapak Prof. Dr. I Nyoman Nurjaya SH.MH selaku Dosen Pembimbing Utama, terima kasih Bapak atas setiap saran, kesabaran dan motivasi yang Bapak berikan dalam membimbing penulis sehingga skripsi ini dapat diselesaikan indah pada waktunya.
4. Ibu Eny Haryati SH. MH selaku Dosen Pembimbing Pendamping, terima kasih Ibu buat setiap saran, bimbingan dan motivasinya. Mohon maaf juga kalau saya sering SMS ibu sebelum konsultasi.

5. Kedua Orang Tuaku, Bapak Izak Johnny Tatipatta dan Ibu Hari Mulyani. Papa dan Mama terimakasih buat setiap semangat, saran dan omelannya sehingga Penulis bisa menyelesaikan skripsi ini indah tepat pada waktunya.
6. Ketiga saudaraku, Kakak Andry Lauda SH, Mas Onie dan Mbak Virna. Terima kasih ya buat setiap sumbangan dananya buat beli kertas, tinta dan printer. Senangnya punya saudara seperti kalian.
7. Persekutuan Mahasiswa Kristen Deifilii FH UB. Terima kasih buat dukungan dan doanya. Khusus buat Theo, Dewi, Indah, Hizka, Yesi, Ferdi, Gita, Mery dan Kiki, terima kasih ya udah temani dan kasih semangat kakak tiap kali kakak bingung buat skripsi ini. Kakak sayang kalian semua. Semangat ya Pelayanannya.
8. Teman-teman Gelap Gulita (Ocie, Acie, Via, Kiki, Ratih, Iid). Suka, duka dan rembug desa kita jalani bersama, tetap semangat teman-temanku. Naomie sayang sama kalian semua. Kapan, dimana kita rembug desa lagi?
9. Teman-teman sepelayanan di KPPM GKJW Jemaat Malang dan PS MUSA (Mbak Santi, Mas Sinung, Mbak Nova, Mbak Putri, Patrice, Iprit, Getsi,Wara, Vian, dan semuanya). Terimakasih buat doa dan bimbingan rohaninya.
10. Teman-temanku (Mas Mahendra SH. MH, Mas Irwan SH, Mbak Caterin, Riska Yourina, Chandra Phils, Paulina). Terima kasih buat ide skripsi dan motivasinya buat aku.
11. Teman-teman KKN Tumpang I dan D'Firm. Terima kasih buat dukungannya. Kapan kita ke Tumpang dan kapan buat acara lagi?

12. Buat semua pihak yang telah secara langsung maupun tidak langsung membantu penulis dalam penyelesaian skripsi ini

Penulis yakin bahwa skripsi ini masih sangat jauh dari sempurna, tetapi penulis berharap skripsi ini bermanfaat bagi semua. Akhir kata penulis mohon maaf apabila dalam proses pembuatan skripsi ini, penulis melakukan kesalahan baik yang disengaja maupun yang tidak disengaja. Kiranya Tuhan yang mengampuni setiap kesalahan kita. Amien. Tuhan Memberkati kita semua.

Malang, Maret 2009

Penulis

DAFTAR ISI

DAFTAR TABEL

ABSTRAKSI

TATIPATTO NAOMI YUANITA, Hukum Pidana, Fakultas Hukum Universitas Brawijaya, April 2009, *Kejahatan Komputer Menurut Kitab Undang-Undang Hukum Pidana dan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik,* Prof. Dr. I Nyoman Nurjaya SH.MH; Eny Haryati, SH. MH

Dalam skripsi ini penulis membahas mengenai masalah Kejahatan Komputer Menurut Kitab Undang-Undang Hukum Pidana dan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Hal ini dilatarbelakangi karena perkembangan kejahatan komputer semakin tinggi dan sulit untuk ditanggulangi dengan menggunakan KUHP sehingga dibuat dan diberlakukannya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Penulis mengkaji tentang pengaturan kualifikasi perbuatan dalam hubungannya dengan kebijakan kriminal dari kejahatan komputer menurut KUHP dan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik serta pengaturan ancaman pidana sebagai bentuk kebijakan penal dari kejahatan komputer menurut KUHP dan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Untuk memperoleh bahan hukum tentang pengaturan perbuatan dan ancaman pidananya, maka metode yang digunakan adalah jenis penelitian yuridis normatif. Pendekatannya menggunakan pendekatan perundang-undangan. Jenis dan sumber bahan hukum yang digunakan adalah primer, sekunder, dan tersier. Setelah seluruh jenis dan sumber bahan hukum lengkap, maka dilakukan analisa bahan hukum dengan menggunakan metode interpretasi atau penafsiran pasal-pasal dalam KUHP dan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Berdasarkan hasil penelitian, penulis memperoleh jawaban atas permasalahan yang ada, bahwa unsur perbuatan dalam KUHP terkait dengan kejahatan komputer kurang lengkap dan perlu adanya penafsiran ekstensif untuk menafsirkan bentuk perbuatan dan objek agar dapat dikenakan pada kejahatan komputer, sedangkan unsur perbuatan dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dirasa sudah cukup kuat mengatur karena unsur perbuatan dan objeknya sudah diatur secara tegas dan jelas. Terkait dengan sanksi pidananya, maka sanksi pidana dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik lebih berat daripada sanksi pidana dalam KUHP. Selain itu, dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sistem perumusannya menggunakan sistem perumusan pidana alternatif kumulatif dengan ancaman pidana penjara dan/atau denda, sedangkan KUHP menggunakan sistem perumusan pidana tunggal dan sistem perumusan pidana alternatif yaitu pidana penjara atau denda.

BAB I

PENDAHULUAN

A. LATAR BELAKANG

Pembangunan Nasional di Indonesia telah mencapai era tinggal. Hal ini ditengarai oleh semakin meningkatnya dua faktor utama yang dianggap sebagai kunci keberhasilan pembangunan dalam rangka memenuhi tuntutan era globalisasi yaitu pertumbuhan ekonomi dan perkembangan ilmu pengetahuan dan teknologi atau IPTEK. Salah satu perkembangan dalam teknologi di masyarakat saat ini adalah kecanggihan teknologi komputer.

Kecanggihan teknologi komputer telah memberikan fasilitas serta kemudahan dalam membantu pekerjaan manusia. Perpaduan antara teknologi komputer dengan teknologi telekomunikasi telah mampu menciptakan jaringan-jaringan yang bersifat mendunia.

Penggunaan komputer dan internet sebagai sarana informasi terlihat nyata telah menjadi sarana kebutuhan masyarakat untuk melakukan berbagai aktifitas dalam pergaulan hidupnya di masyarakat, bahkan teknologi ini sering dikatakan oleh sebagian orang sebagai media tanpa batas atau dunia maya. Hal demikian didasarkan atas pengetahuan kita bahwa dimensi ruang, birokrasi dan waktu dalam hubungan sesama subjek hukum yang selama ini dilakukan berada di dunia nyata telah dengan mudah ditembus oleh teknologi informasi. Fakta demikian dapat kita lihat misalnya kebebasan dan kemudahan berbicara, keterbukaan, dan tukar menukar informasi

dalam dan lintas batas wilayah suatu negara, dan perdagangan bebas atau transaksi-transaksi melalui media elektronik. Dalam kenyataan demikian, perkembangan teknologi informasi patut disadari memiliki dampak bagi hukum yang telah ada dan memerlukan penyesuaian pengaturan lebih lanjut, sehingga penggunaan teknologi sebagai sarana komunikasi global dalam pergaulan masyarakat regional, nasional dan internasional tetap berada dalam landasan legalitas hukum yang benar.

Kemajuan teknologi yang ada pada masyarakat selain membawa dampak positif, dalam arti dapat didayagunakan untuk kepentingan umat manusia juga membawa dampak yang negatif terhadap perkembangan manusia dan peradabannya. Dampak negatif yang dimaksud adalah yang berkaitan dengan dunia kejahatan. Menurut J.E Sahetapy suatu kejahatan erat kaitannya dan bahkan menjadi sebagian dari hasil budaya itu sendiri. Ini berarti semakin tinggi tingkat budaya dan semakin modern suatu bangsa, maka semakin modern pula kejahatan itu dalam bentuk, sifat dan cara pelaksanaannya.[1]

Salah satu kejahatan yang ditimbulkan oleh perkembangan dan kemajuan teknologi informasi atau telekomunikasi adalah kejahatan dengan memanfaatkan teknologi komputer sebagai modus operandinya yaitu yang dikenal dengan istilah kejahatan komputer. Kejahatan ini dalam istilah asing sering disebut dengan *cybercrime*. Istilah *cybercrime* saat ini merujuk pada suatu tindakan kejahatan yang berhubungan dengan dunia maya dan tindakan kejahatan yang menggunakan

1 Abdul Wahid, *Kejahatan Mayantara*, PT.Refika Aditama, Bandung, 2002,hal 26

komputer. Ada ahli yang menyamakan antara tindak kejahatan *cyber (cybercrime*) dengan tindak kejahatan komputer tetapi beberapa ahli membedakan diantara keduanya.[2] Meskipun belum ada kesepahaman mengenai definisi kejahatan teknologi informasi, namun ada kesamaan pengertian universal mengenai kejahatan komputer. Secara umum yang dimaksud dengan kejahatan komputer adalah:

> Upaya memasuki dan atau menggunakan fasilitas komputer atau jaringan komputer tanpa izin dan dengan melawan hukum dengan atau tanpa menyebabkan perubahan dan atau kerusakan pada fasilitas komputer yang dimasuki atau digunakan tersebut.[3]

Secara umum, bentuk-bentuk aktivitas kejahatan komputer dapat dikelompokkan dalam dua golongan yaitu penipuan data dan penipuan program. Dalam penipuan data, suatu data yang tidak sah dimasukkan kedalam sistem atau jaringan komputer yang diubah menjadi data yang sah. Fokus perhatiannya adalah adanya pemalsuan data *input* dengan maksud untuk mengubah *output*.[4]

Bentuk kejahatan yang kedua relatif lebih canggih dan lebih berbahaya karena modus penipuan programnya yaitu seseorang mengubah program komputer baik dilakukan langsung di tempat komputer maupun dilakukan melalui jaringan komunikasi data. [5] Pada kasus ini penjahat melakukan aplikasi kedalam suatu sistem komputer dan selanjutnya mengubah susunan program dengan tujuan menghasilkan

---

2 Didik M. Arief & Elisatris Gultom, *Cyber Law*, PT. Refika Aditama, Bandung, 2005,hal 7

3 Merry Magdalena & Maswigrantoro Roes Setiyadi, *Cyberlaw, Tidak Perlu Takut*,C.V Andi Offset, Yogyakarta, 2007,hal 37

4 *Ibid*, hal 38

5 *Ibid*

keluaran (*output*) yang berbeda dari seharusnya, meski program tersebut memperoleh masukan (*input*) yang benar.

Dalam masyarakat saat ini, banyak dijumpai kejahatan komputer atau *cybercrime*, mulai dari kejahatan umum yang difasilitasi dengan teknologi informasi antara lain penipuan kartu kredit, penipuan bursa efek, penipuan perbankan, pornografi, perdagangan narkoba, terorisme bahkan sampai kejahatan seperti *cracking* yang memiliki lingkup yang sangat luas mencangkup pembajakan situs web, *probing*, menyebarkan virus hingga melumpuhkan target sasaran.

Di Indonesia, penyalahgunaan kejahatan komputer sudah mencapai tingkat yang memprihatinkan. Bahkan pada tahun 2004, Indonesia pernah menduduki peringkat pertama dalam *cybercrime* atau kejahatan komputer tersebut. Pada awal Mei 2008, Mabes Polri berhasil menangkap *hacker* bernama Iqra Syafaat di satu warnet di Batam, Riau, setelah melacak *IP addressnya* dengan nick name Nogra alias Iqra. Pemuda tamatan SMA tersebut dinilai polisi berotak encer dan cukup dikenal di kalangan hacker. Dia pernah menjebol data sebuah website lalu menjualnya ke perusahaan asing senilai 600 ribu dolar atau sekitar Rp 6 miliar.[6]

Kasus lain yang terkait dengan kejahatan komputer adalah kasus yang telah diputus di Pengadilan Negeri Sleman dengan terdakwa Petrus Pangkur alias Bonny Diobok-Obok. Kasus tersebut disidangkan oleh majelis hakim yang terdiri dari Hakim Ketua Cicut Sutiarso SH, dengan Anggota Sarjiman SH dan Jupiyadi SH.

6 PosKota, Dedemit Dunia Maya Acak Situs- Situs Penting, http://www.postkotanews_baca.asp.htm. Diakses 30 September 2008

Selaku Jaksa Penuntut Umum adalah Oemar Dhani SH. Dalam kasus tersebut terdakwa didakwa melakukan kejhatan komputer. Dalam amar putusannya, majelis hakim berkeyakinan bahwa Petrus telah membobol kartu kredit milik warga AS, hasil kejahatannya digunakan untuk membeli barang-barang seperti helm, sarung tangan merk AGV. Total harga barang yang dibelinya mencapai Rp 4 juta.

Sementara itu, penasihat hukum terdakwa, dalam pembelaannya menyatakan secara hukum putusan hukuman selama 18 bulan itu tidak adil. Alasannya dalam perkara tersebut belum ada aturan hukum yang menjangkau perbuatan yang dilakukan kliennya. Bahkan unsur Pasal 378 KUHP, tidak terbukti secara sah dan meyakinkan. Oleh karena itu, terdakwa harus dibebaskan dari segala tuntutan. [7]

Berdasarkan data di Mabes Polri, dari sekitar 200 kasus *cybercrime* yang ditangani hampir 90 persen didominasi carding dengan sasaran luar negeri. Aktivitas internet memang lintas negara dan yang paling sering menjadi sasaran adalah Amerika Serikat, Australia serta Kanada. Pelaku kejahatanpun berasal dari kota-kota besar seperti Yogyakarta, Bandung, Jakarta, Semarang, Medan serta Riau. Motif utama adalah ekonomi.

Peringkat kedua adalah *hacking* yaitu dengan merusak dan menjebol *website* pihak lain dengan tujuan beragam, mulai dari membobol data lalu menjualnya atau iseng merusak situs tertentu. Berdasarkan beberapa contoh kasus yang ada, penanganan masalah kejahatan komputer tersebut masih dengan menggunakan dasar

7 Pikiran Rakyat, http://www.pikiran-rakyat.com/cetak/1102/02/0304.htm. Diakses pada 26 Maret 2009

hukum Kitab Undang-Undang Hukum Pidana. Adapun pasal-pasal yang sering dijatuhkan berkaitan dengan kejahatan komputer seperti *hacking, carding*, penipuan maupun kejahatan-kejahatan umum yang menggunakan media komputer adalah sebagai berikut:

1. Ketentuan berkaitan dengan pembocoran rahasia

   Delik pembocoran rahasia dalam kejahatan komputer diatur dalam Pasal 112, 113, 114 KUHP dan apabila menyangkut dengan pembocoran rahasia profesi maka diatur dalam Pasal 322-323 KUHP dan apabila menyangkut pembocoran rahasia tertentu diatur dalam Pasal 431 KUHP.

2. Ketentuan berkaitan dengan perbuatan memasuki atau melintasi wilayah orang lain

   Kejahatan komputer jenis hacking adalah dengan memasuki wilayah komputer milik orang lain tanpa ijin terlebih dahulu. Kejahatan komputer jenis hacking ini cukup berbahaya karena apabila ia berhasil masuk ke sistem jaringan orang lain, maka implikasi hukumnya ia mungkin saja dapat membaca dan menyalin informasi yang rahasia atau mungkin pula menghapus atau mengubah informasi maupun program yang tersimpan pada sistem komputer tersebut. [8]

   Perbuatan mengakses ke suatu sistem jaringan tanpa ijin dapat dikategorikan sebagai perbuatan tanpa wewenang masuk dengan memaksa kedalam rumah

8 *Ibid*

atau ruangan yang tertutup atau pekarangan tanpa hak berjalan diatas milik orang lain. Sehingga pelaku dapat diancam pidana berdasarkan Pasal 167 KUHP dan Pasal 551 KUHP

3. Ketentuan yang berkaitan dengan perbuatan pemalsuan

   Dalam delik pemalsuan, seringkali adanya perubahaan data dengan cara mengubah data valid atau sah dengan melawan hukum yaitu dengan mengubah input data maupun output data sehingga data tersebut seolah-olah data autentik. Berkaitan dengan perbuatan pemalsuan surat ini diatur dalam Pasal 263 KUHP

4. Ketentuan yang berkaitan dengan delik pencurian

   Delik pencurian dalam dunia maya tidaklah diartikan secara konvensional karena barang yang dicuri adalah berupa data digital, baik yang berisikan data transaksi keuangan maupun data yang menyangkut software atau program ataupun data yang menyangkut hal-hal yang bersifat rahasia.[9] Delik pencurian diatur dalam Pasal 362 KUHP dan variasinya diatur dalam Pasal 363 KUHP yakni pencurian dengan pemberatan, Pasal 364 KUHP pencurian ringan, Pasal 365 KUHP tentang pencurian yang disertai dengan kekerasan dan Pasal 367 KUHP pencurian di lingkungan keluarga.

5. Ketentuan yang berkaitan dengan penggelapan

---

9 Suhartono, *Penanggulangan Kejahatan Hacking di Indonesia*,http://www.google.com. Diakses tanggal 16 Oktober 2008

Penggelapan merupakan salah satu kejahatan konvensional yang juga dapat dilakukan dengan menggunakan sarana internet. Perbuatan penggelapan dengan memanfaatkan internet erat kaitannya dengan perbuatan memanipulasi data atau program pada suatu sistem jaringan komputer. Perbuatan ini dapat dijerat dengan Pasal 372 KUHP

6. Ketentuan yang berkaitan dengan kejahatan perusakan dan penghancuran barang

   Ketentuan ini erat kaitannya dengan kejahatan hacking. Dalam kejahatan komputer perbuatan perusakan dan penghancuran barang tidak hanya ditujukan untuk merusak atau menghancurkan media disket atau media penyimpan sejenisnya, namun juga merusak suatu data. Delik ini juga termasuk didalam perbuatan merusak barang-barang milik publik.[10] Ketentuan mengenai perbuatan perusakan dan penghancuran barang diatur dalam Pasal 406 KUHP

Dengan semakin berkembang dan kompleknya kejahatan komputer di Indonesia saat ini sehingga diperlukan peraturan khususnya hukum pidana yang tepat. Dalam hal ini peraturan perundang-undangan hukum pidana yang berlaku di Indonesia saat ini dirasa sudah tidak memadai lagi dalam rangka menanggulangi penyalahgunaan komputer.[11] Hal tersebut sesuai dengan pendapat beberapa sarjana

10 *Ibid*

11 Al.Wisnubroto, *Kebijakan Hukum Pidana Dalam Penanggulangan Penyalahgunaan Komputer,* Universitas Atmajaya Yogyakarta, 1999, hal 2

seperti J.E Sahetapy yang berpendapat bahwa hukum pidana yang ada tidak siap untuk menghadapi kejahatan komputer, karena tidak mudah untuk menganggap pencurian data di kejahatan komputer sebagai pencurian yang biasa. Sulitnya masalah pembuktian dan kerugian besar yang mungkin terjadi melatarbelakangi perlunya ada produk hukum yang baru untuk menangani kejahatan komputer agar dakwaan terhadap pelaku kejahatan tidak meleset.[12]

Selain itu, J. Sudama Sastroandjojo menghendaki perlu adanya ketentuan baru yang mengatur permasalahan tindak pidana komputer. Hal ini berkaitan dengan unsur kebijakan kriminal dari suatu bentuk kejahatan komputer. Tindak pidana yang menyangkut komputer haruslah ditangani secara khusus, karena cara-caranya, lingkungan, waktu dan letak dalam melakukan kejahatan komputer adalah berbeda dengan tindak pidana lain.[13]

Dengan semakin berkembangnya kejahatan komputer, aparat kepolisian sempat dibuat kebingungan dengan penerapan hukuman atau kebijakan penal bagi pelaku kejahatan komputer ini. Bahkan berdasarkan data yang diperoleh, jumlah kasus kejahatan komputer yang berhasil diputus dipengadilan sangatlah minim dan mengkhawatirkan. Berdasarkan data tahun 2002-2005 dari 71 kasus kejahatan komputer, hanya sebanyak 35 kasus saja yang dinyatakan P21 oleh jaksa penuntut

12 **Teguh Arifiyadi, SH (Inspektorat Jenderal Depkominfo),** *Menjerat Pelaku Cyber Crime dengan KUHP*,http://www.google.com. Diakses tanggal 4 September 2008

13 *Ibid*

umum.[14] Hal ini disebabkan karena kurang adanya aturan yang khusus untuk mengatur masalah teknologi informatika khususnya terkait dengan kejahatan komputer. Berdasarkan atas berbagai macam pertimbangan tersebut maka pada bulan April tahun 2008 pemerintah Republik Indonesia mengeluarkan Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik.

Dalam Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) berisi tentang aturan-aturan yang menjamin keamanan dan kepastian hukum dalam pemanfaatan teknologi, media dan komunikasi agar dapat berkembang secara optimal di masyarakat. Dalam Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik terdapat juga beberapa pasal yang mengatur secara khusus terkait dengan kejahatan komputer. Adapun pasal- pasal dalam Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik yang mengatur tentang kejahatan komputer adalah sebagai berikut:

1. Ketentuan yang berkaitan dengan mengakses komputer milik orang lain dengan cara melawan hukum

   Kejahatan komputer yang mengakses komputer milik orang lain termasuk dalam jenis *hacking*. Kejahatan ini cukup berbahaya karena apabila ia berhasil masuk kewilayah komputer milik orang lain dengan sengaja untuk tujuan memperoleh sesuatu atau dengan menjebol sistem pengamanan maka ia dapat mengambil informasi yang ada dalam komputer tersebut. Perbuatan mengakses sistem

14 *Lima Tahun Polri Tangani 71 Kejahatan 'Cyber Crime'*,http://www.kapanlagi.com. Diakses, 14 Mei 2007

komputer milik orang lain ini diatur dalam Pasal 30 Undang-Undang ITE dengan ancaman pidana yang diatur dalam Pasal 46 Undang-Undang ITE.

2. Ketentuan yang berkaitan dengan tindakan penyadapan atas informasi elektronik dan/ atau dokumen elektronik dalam suatu komputer tertentu milik orang lain

   Dalam Undang-Undang ITE terdapat juga pasal yang mengatur tentang perbuatan secara sengaja dan tanpa hak melakukan intersepsi atau penyadapan informasi elektronik dalam suatu komputer milik orang lain yang tidak menyebabkan perubahan apapun maupun yang menyebabkan adanya perubahan, penghilangan dan/ atau penghentian informasi elektronik dan/atau dokumen elektonik yang sedang ditransmisikan. Perbuatan yang berkaitan dnegan tindakan penyadapan ini diatur dalam Pasal 31 ayat 1 dan 2 dengan ancaman pidana yang diatur dalam Pasal 47 Undang-Undang ITE

3. Ketentuan yang berkaitan dengan pengubahan dan pemindahan informasi elektronik dan dokumen elektronik milik orang lain

   Dalam Undang-Undang ITE terdapat juga pasal yang mengatur secara lebih rinci mengenai kejahatan yang berkaitan dengan pengubahan, pemindahan, pengurangan, perusakan, penghilangan suatu sistem elektronik milik orang lain secara melawan hukum yang mana akibat dari perbuatan tersebut adalah dapat terbukanya suatu informasi elektronik atau dokumen elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya. Perbuatan tersebut diatur dalam Pasal 32 Undang-Undang ITE dengan ancaman pidana yang diatur dalam Pasal 48 Undang-Undang ITE

4. Ketentuan yang berkaitan dengan terganggunya sistem elektronik

   Dalam Undang-Undang ITE diatur juga tentang tindakan yang dapat mengakibatkan terganggunya sistem elektronik atau mengakibatkan sistem elektronik tersebut bekerja tidak sebagaimana mestinya. Perbuatan tersebut diatur dalam Pasal 33 Undang-Undang ITE dengan ancaman pidana yang diatur dalam Pasal 49 Undang-Undang ITE.

5. Ketentuan yang berkaitan dengan perbuatan manipulasi, penciptaan, penghilangan, pengrusakan informasi elektronik dengan tujuan agar informasi elektronik tersebut seolah-olah data yang otentik.

   Ketentuan yang berkaitan dengan perbuatan tersebut diatur secara jelas dalam Pasal 35 Undang-Undang ITE dengan ancaman pidana yang diatur dalam Pasal 51 Undang-Undang ITE.

Berdasarkan uraian latar belakang yang telah dipaparkan, maka penulis merasa bahwa perlu adanya suatu pembahasan yang membahas tentang bentuk perbuatan dan sanksi yang diterapkan dari KUHP dan Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik terkait dengan kejahatan komputer. Maka dari itulah, penulis mengangkat suatu penulisan yang berjudul "Kejahatan Komputer Menurut Kitab Undang-Undang Hukum Pidana dan Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik."

B. RUMUSAN MASALAH

Beberapa masalah yang hendak ditelaah dalam penelitian ini adalah:

1. Bagaimana pengaturan kualifikasi perbuatan dalam hubungan dengan kebijakan kriminal dari kejahatan komputer menurut Kitab Undang-Undang Hukum Pidana dan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik?
2. Bagaimana pengaturan ancaman pidana sebagai bentuk kebijakan penal dari kejahatan komputer menurut Kitab Undang-Undang Hukum Pidana dan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik?

C. TUJUAN PENELITIAN

Adapun yang menjadi tujuan dari penelitian ini adalah:

1. Untuk mengetahui dan menganalisis pengaturan kualifikasi perbuatan dalam hubungan dengan kebijakan kriminal dari kejahatan komputer menurut Kitab Undang-Undang Hukum Pidana dan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

2. Untuk mengetahui dan menganalisis pengaturan ancaman pidana sebagai bentuk kebijakan penal dari kejahatan komputer menurut Kitab Undang-Undang Hukum Pidana dan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

D. MANFAAT PENELITIAN

Adapun manfaat penelitian ini dapat dibagi sebagai berikut :

a. **Manfaat teoritis**

Bagi penelitian selanjutnya, hasil penelitian ini ditujukan untuk pengembangan ilmu hukum pada umumnya dan untuk mengetahui kebijakan kriminal dan penal dari kejahatan komputer menurut Kitab Undang-Undang Hukum Pidana dan Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik

b. Manfaat Praktis

1. Bagi peneliti

Hasil penelitian ini dapat digunakan sebagai bahan untuk menambah wawasan tentang kebijakan kriminal dan penal dari kejahatan komputer menurut Kitab Undang-Undang Hukum Pidana dan Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik

2. Bagi mahasiswa Fakultas Hukum

Hasil penelitian ini diharapkan dapat menjadi landasan untuk lebih mengetahui tentang kebijakan kriminal dan penal dari kejahatan komputer menurut Kitab Undang-Undang Hukum Pidana dan Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik

3. Bagi masyarakat

   Hasil penelitian ini diharapkan untuk menambah pengetahuan masyarakat mengenai perlindungan hukum terkait dengan dengan kejahatan komputer.

E. SISTEMATIKA PENULISAN

Dalam penelitian ini akan dibagi dalam bab-bab yang didalam masing-masing bab akan dibahas mengenai beberapa hal sebagai berikut:

BAB I : PENDAHULUAN

Bab ini merupakan pendahuluan sebagai pengantar dari keseluruhan penelitian ini yang memuat tentang alasan pemilihan judul, perumusan masalah, tujuan penelitian, manfaat penelitian, dan sistematika pembahasan setiap bab.

BAB II : KAJIAN PUSTAKA

Bab ini menjelaskan tentang tinjauan umum mengenai pengertian komputer, pengertian kejahatan komputer, jenis-jenis kejahatan komputer, sistem hukum Indonesia, kebijakan hukum pidana,

ketentuan pidana berdasarkan Kitab Undang-Undang Hukum Pidana terkait dengan kejahatan komputer, ketentuan pidana berdasarkan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik terkait dengan kejahatan komputer.

BAB III : METODE PENELITIAN

Bab ini membahas tentang metode pendekatan yang digunakan, data yang digunakan teknik penelusuran data dan teknik analisa data.

BAB IV : PEMBAHASAN

Bab ini hukum antara Kitab Undang-Undang Hukum Pidana dengan membahas permasalahan yang diangkat yaitu unsur perbuatan dan sanksi dari kejahatan komputer menurut Kitab Undang-Undang Hukum Pidana dan Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik

BAB V : PENUTUP

Bab ini berisi kesimpulan tentang uraian yang telah dibahas serta saran-saran yang diberikan oleh penulis. Harapan penulis dapat memberikan manfaat atau kontribusi mengenai unsur perbuatan dan sanksi dari kejahatan komputer menurut Kitab Undang-Undang Hukum Pidana dan Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik

BAB II

KAJIAN PUSTAKA

A Pengertian Komputer

Istilah komputer diambil dari bahasa latin *computare* yang berarti menghitung (*to compute*). Secara *lexicography,* maka komputer adalah si penghitung atau subyek yang melakukan suatu komputasi. Menurut Andi Hamzah, mengemukakan 2 (dua) definisi dari komputer yang merupakan ciri-ciri dari komputer: [15]

1. Serangkaian atau kumpulan mesin elektronika yang bekerja bersama-sama; dan dapat melakukan rentetan atau rangkaian pekerjaan secara otomatis melalui instruksi atau program yang diberikan kepadanya;
2. Suatu rangkaian peralatan-peralatan dan fasilitas yang bekerja secara elektronis, bekerja dibawah kontrol suatu sistem operasional, melaksanakan pekerjaan berdasarkan rangkaian instruksi-instruksi yang disebut program, serta mempunyai penyimpan data yang digunakan untuk menyimpan sistem operasional, program dan data yang diolah.

Dari kedua ciri tersebut, komputer dapat dibagi menjadi beberapa bagian: [16]

15 Andi Hamzah, *Aspek- Aspek Pidana Dibidang Komputer*, Sinar Grafika, Jakarta, 1987,hal 14

16 Iwan Winarso, "Aspek Yuridis-Kriminologis Penerapan Pasal-Pasal KUHP Terhadap Pelaku Kejahtan yang menggunakan Sarana Komputer", Tesis tidak diterbitkan, Malang, Fakultas Hukum Universitas Brawijaya, 2004, hal 27

1. Komputer merupakan suatu sistem, yaitu serangkaian atau kelompok peralatan yang bekerja bersama secara elektronis;
2. Komputer itu mempunyai suatu alat penyimpan data dan program yang disebut dengan memori komputer;
3. Komputer bekerja dibawah kontrol sistem operasi dan melaksanakan tugas berdasarkan instruksi-instruksi yang disebut program.

Dalam suatu komputer terdapat sistem elektronik yang terdiri atas perangkat keras elektronik (*hardware*), perangkat lunak program komputer (*software*), prosedur-prosedur dan cara penggunaannya (*brainware*) serta data atau informasi itu sendiri (*content*).

Suatu komputer dapat menjalankan fungsinya yaitu dengan menggunakan suatu program. Menurut David I. Bainbridge program komputer adalah serangkaian instruksi yang mengendalikan atau mengubah operasi-operasi komputer.[17] Menurut pasal 1 ayat 8 undang-undang nomor 19 tahun 2002 tentang hak cipta,program komputer adalah

> "Program Komputer adalah sekumpulan instruksi yang diwujudkan dalam bentuk bahasa, kode, skema, ataupun bentuk lain, yang apabila digabungkan dengan media yang dapat dibaca dengan komputer akan mampu membuat komputer bekerja untuk melakukan fungsi-fungsi khusus atau untuk mencapai hasil yang khusus, termasuk persiapan dalam merancang instruksi- instruksi tersebut ."

Program komputer merupakan instruksi-intruksi yang berupa kode-kode numerik yang berada di dalam memori komputer untuk memberitahukan pekerjaan

17 Edmon Makarim, *Kompilasi Hukum Telematika*, PT. RajaGrafindo Persada, Jakarta, 2003,hal 71

yang harus diselesaikan oleh komputer tersebut. Komputer merupakan benda mati sehingga komputer hanya dapat mengerjakan sesuai dengan instruksi yang diberikan kepadanya.[18]

Komputer juga disebut sebagai suatu sistem informasi. Sistem adalah jaringan dari elemen-elemen yang saling berhubungan membentuk satu kesatuan untuk melaksanakan suatu tujuan pokok dari sistem tersebut. Tujuan pokok dari suatu sistem komputer adalah untuk mengolah data yang diperoleh guna menghasilkan suatu informasi.

B. Pengertian Kejahatan Komputer

Hingga saat ini masih banyak pandangan yang berbeda mengenai pengertian atau definisi kejahatan komputer. Perbedaan pendapat ini disebabkan karena sudut pandang para ahli yang mencoba mendefinisikan kejahatan komputer belum terdapat satu kesatuan.

Pemakaian istilah kejahatan komputer atau yang dalam beberapa sumber disebut sebagai penyalahgunaan komputer sebenarnya menunjuk pada sifat dan hakekat yang sama dalam pengertian atau definisinya.[19]

Penulis sendiri dalam penulisan skripsi ini memilih menggunakan istilah kejahatan komputer dengan alasan: *Pertama*, meskipun Kitab Undang-Undang

18 *Ibid*, hal 72

19 Harun Al Rasyid, "Tinjauan Yuridis Kriminologis Penerapan Pasal-Pasal KUHP dan Pasal-Pasal Undang-Undang Di Luar KUHP Terhadap Kejahatan Komputer", Tesis tidak diterbitkan, Malang Fakultas Hukum Universitas Brawijaya, 1999, hal 16

Hukum Pidana (KUHP) belum mengatur tentang kejahatan komputer namun KUHP hanya mengenal istilah kejahatan dan pelanggaran. Jadi istilah kejahatan lebih cocok dipakai untuk menyebut tindak pidana dibidang komputer ini dibandingkan dengan istilah lainnya. *Kedua*, penyalahgunaan komputer merupakan penyebab timbulnya kejahatan komputer atau dengan kata lain kejahatan komputer itu timbul karena adanya penggunaan komputer yang disalahgunakan untuk melakukan kejahatan. Agar tidak menimbulkan salah tafsir, sebaiknya dipahami atau disepakati lebih dahulu definisi kejahatan komputer. Berikut ini beberapa pengertian yang diberikan oleh beberapa ahli mengenai kejahatan komputer:

a. Menurut departemen Kehakiman Amerika seperti yang dikutip Edmon Makarim menyatakan bahwa:

> *"...any illegal act requiring knowlegde of computer technology for its perpretation investigation, or prosecution. It has two main categories. First, computer as a tool of crime, such as found, an theaf property.... Second, computer is the object of crime such sabotage, theaf or alteration data,..."* [20]

Dari definisi ini, penyalahgunaan komputer dibagi menjadi dua bidang utama yaitu:

1. penggunaan komputer sebagai alat untuk melakukan kejahatan
2. komputer merupakan objek atau sasaran dari tindak kejahatan

b. Menurut National Police Agency (NPA) seperti yang dikutip Edmon Makarim

" Computer crime is crime toward to computer." [21]

---

20 Edmon Makarim, *op cit* hal 394

21 *Ibid*, hal 395

Kejahatan komputer adalah kejahatan yang ditujukan pada komputer. Dari batasan yang diberikan NPA, pengertian tentang kejahatan komputer menjadi lebih luas lagi yaitu segala aktivitas yang ditujukan, baik terhadap komputer itu ataupun dengan menggunakan komputer adalah suatu kejahatan.

c. Menurut Andi Hamzah

"Kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara ilegal."[22]

Dari pengertian tersebut, Andi Hamzah memperluas pengertian kejahatan komputer yaitu segala aktivitas tidak sah yang memanfaatkan komputer untuk tindak pidana. Sekecil apapun dampak atau akibat yang ditimbulkan dari penggunaan komputer secara tidak sah merupakan suatu kejahatan.[23]

d. Menurut David I. Bainbridge seperti yang dikutip Edmon Makarim

Kejahatan komputer akan dibatasi dalam pengertian:[24]

1. Kejahatan yang memanfaatkan kemampuan komputer dalam memproses data dan kemudian memanipulasi data tersebut dengan akibat timbulnya kerugian bagi pihak lain

---

22 Andi Hamzah, *op cit* hal 26

23 Edmon Makarim, *op cit*, hal 395

24 Syahnan, Landasan Teori Sistem Informasi, http://www.google.com. Diakses 16 Oktober 2008

2. Kejahatan yang dilakukan dengan cara memasuki sistem komputer orang lain, baik komputer pribadi ataupun komputer yang terhubung ke dalam satu jaringan komputer tanpa ijin.

Secara umum semua batasan tentang kejahatan komputer atau *computer crime* adalah suatu perbuatan atau tindakan yang dilakukan dengan menggunakan komputer sebagai alat atau sarana untuk melakukan tindak pidana atau menggunakan komputer sebagai objek tindak pidana. Secara khusus, kejahatan komputer adalah suatu perbuatan melawan hukum yang dilakukan dengan teknologi komputer yang canggih sebagai objek dengan tujuan untuk memperoleh keuntungan ataupun tidak yang dapat merugikan orang lain.[25]

Seandainya kejahatan komputer diartikan sebagai kejahatan yang menyangkut komputer dan peralatan-peralatan yang berhubungan dengannya atau sarana-sarana penunjangnya, maka sebenarnya tidak semua "kejahatan komputer" merupakan kejahatan komputer. Sebagai gambaran dapat diilustrasikan sebagai berikut: bilamana ada seseorang mencuri *floppy disk* yang "kosong" (tidak memuat data atau program) dan bermaksud untuk dimilikinya sendiri atau dijual kepada orang lain, maka kiranya perbuatan orang tersebut belum dapat digolongkan sebagai kejahatan komputer. Perbuatan tersebut lebih tepat disebut sebagai pencurian biasa seperti diatur pasal 362 KUHP. Berbeda dengan jika seseorang tersebut mencuri *floppy disk* itu dengan mengetahui atau setidak-tidaknya menduga bahwa didalam *floppy disk* tersebut

25 Harun Al Rasyid, *op cit* hal 20

terdapat program atau data komputer dan orang tersebut bermaksud memiliki atau menjual kepada orang lain data atau program yang terdapat dalam disk tersebut atau punya maksud lain misalnya untuk balas dendam atau untuk memperoleh imbalan yang tidak wajar dengan "menyandera" benda-benda vital tersebut agar suatu pusat komputer tidak dapat menjalankan operasinya, maka kiranya perbuatan ini baru pantas bila disebut sebagai kejahatan komputer.[26]

Andi Hamzah berpendapat bahwa kejahatan yang terjadi di bidang komputer itu sangat berkaitan erat dengan faktor manusia di belakang pengoperasian peralatan komputer. Komputer akan melaksanakan tugas yang dibebankan kepadanya baik yang bersifat curang maupun yang tidak curang. Maka dari itu kejahatan komputer dapat diklasifikasikan berdasarkan: [27]

1. Kejahatan terhadap sistem komputer
   a. Pada masukan (*input*), dengan penghapusan, penambahan bahan-bahan masukan dan sebagainya
   b. Pada pengolahan data, dengan perubahan, pengrusakan dan sebagainya
   c. Pada program komputer, dengan pencurian dan penjualan program, pengrusakan program, memasukkan instruksi yang bersifat curang dan sebagainya.
   d. Pada pengeluaran (*output)* dengan pemalsuan dan sebagainya.[28]

26 Al. Wisnubroto, *opcit* hal 25

27 Andi Hamzah, *Hukum Pidana yang Berkaitan dengan Komputer*, Sinar Grafika, Jakarta, 1996, hal 42

28 Harun Al Rasyid, *op cit* hal 23

2. Kejahatan terhadap peralatan komputer

Perbuatan yang dimaksukkan disini misalnya kecurangan pada dana pembelian peralatan komputer dan sebagainya, disamping kecurangan yang dilakukan merusak peralatan komputer (*hardware*) dengan tujuan menghancurkan prestasi dan reputasi pihak lawan.

C. Jenis- Jenis Kejahatan Komputer

Kejahatan yang berhubungan dengan komputer adalah setiap aktivitas seseorang, sekelompok orang, badan hukum yang menggnakan komputer sebagai sarana melakukan kejahatan dan komputer sebagai sasaran kejahatan. Kejahatan tersebut adalah bentuk-bentuk kejahatan yang bertentangan dengan peraturan perundang-undangan.

Menurut J. Sudama Sastraandaja yang dikutip oleh Widodo mengatakan bahwa dalam studi di Kongres Amerika Serikat disimpulkan ada 4 bentuk kejahatan yang berhubungan dengan komputer, yaitu: [29]

1. Pemasukan data yang tidak benar ke dalam komputer;
2. Pemakaian fasilitas-fasilitas yang berhubungan dengan komputer secara tidak sah;
3. Merubah atau merusak suatu arsip;

---

29 Widodo, "Kebijakan Kriminal Terhadap Kejahatan Yang Berhubungan Dengan Komputer Di Indonesia, Disertasi tidak diterbitkan, Program Pasca Sarjana Universitas Brawijaya, 2006.

4. Pencurian yang dilakukan secara elektronis atau dengan cara-cara lain yang berobjek pada uang, benda atau fasilitas-fasilitas dan data yang berharga.

Menurut J. Sudara Sastraandjaja menyatakan bahwa kejahatan yang berhubungan dengan komputer dapat diklasifikasikan dalam 5 bentuk yaitu: [30]

1. Kejahatan-kejahatan yang menyangkut data atau informasi komputer
2. Kejahatan-kejahatan yang menyangkut program atau *software* komputer
3. Pemakaian fasilitas-fasilitas komputer tanpa wewenang untuk kepentingan-kepentingan yang tidak sesuai dengan tujuan pengelolaan operasinya
4. Tindakan-tindakan yang menganggu operasi komputer
5. Tindakan merusak peralatan komputer atau peralatan yang berhubungan dengan komputer atau sarana penunjangnya.

Menurut Donn Parker seperti yang dikutip oleh Edmon Makarim menyatakan bahwa suatu kejahatan komputer dapatlah ditinjau dari empat sudut peranan komputer dalam suatu kejahatan komputer. Yaitu: [31]

1. Komputer sebagai obyek

   Dalam hal ini berkaitan dengan kasus-kasus perusakan terhadap komputer, data atau program yang terdapat didalamnya atau perusakan sarana-sarana

30 *Ibid,* hal 61

31 Edmon Makarim,*op cit* hal 66

komputer seperti *Air Conditioning* (AC) dan peralatan listrik yang menunjang pengoperasian komputer.

2. Komputer sebagai subjek

   Komputer dapat menimbulkan suatu kejahatan seperti pencurian, penipuan, pemalsuan yang tidak tradisional akan tetapi menyangkut harta-harta benda dalam bentuk baru misalnya pulsa elektronik

3. Komputer sebagai alat

   Dalam beberapa kejahatan, komputer digunakan sebagai alat untuk membantu kejahatan tersebut, sehingga kejahatan itu menjadi kompleks dan susah diketahui.

4. Komputer sebagai simbol

   Suatu komputer dapat digunakan sebagai simbol untuk melakukan penipuan atau ancaman. Misalnya, penipuan melalui iklan dari suatu "biro jodoh" yang menyatakan bahwa biro jodoh tersebut memakai komputer untuk membantu si korban mencari jodoh, akan tetapi ternyata biro jodoh itu sama sekali tidak memakai komputer untuk keperluan tersebut.

Menurut Andi Hamzah, bentuk-bentuk kejahatan yang berhubungan dengan komputer diatas dapat dikaitkan dengan ketentuan-ketentuan dalam Buku II KUHP Indonesia. Jika dibuat perbandingan maka akan diperoleh deskripsi sebagai berikut: [32]

32 Andi Hamzah (certakan kedua), *opcit* hal 21-42

1. Data Leakage

Data leakage adalah tindakan pembocoran data rahasia yang dilakukan dengan cara menulis data-data rahasia tersebut kedalam kode-kode tertentu sehingga data dapat dibawa keluar sistem komputer tanpa diketahui oleh pihak yang bertanggungjawab terhadap data tersebut. Tindakan ini dapat dikategorikan sebagai tindak pidana terhadap keamanan negara maupun pembocoran rahasia perusahaan dan profesi (Pasal 112, Pasal 113, Pasal 114, Pasal 322, 323 dan Pasal 431 KUHP).[33]

2. *Hacking*

Hacking adalah perbuatan berupa penyambungan saluran, yaitu dengan cara menambah terminal komputer baru pada sistem jaringan komputer tanpa ijin atau dilakukan dengan melawan hukum dari pemilik sah jaringan komputer. Tindakan ini dapat dikategorikan sebagai tindak pidana yaitu perbuatan tanpa wewenang masuk dengan memaksa ke dalam rumah atau ruang yang tertutup atau pekarangan atau tanpa haknya berjalan di atas tanah milik orang lain (Pasal 167 dan Pasal 551 KUHP).[34]

Proses penyusupan dalam dunia *hacker* dapat dilakukan melalui beberapa tahap, yaitu:[35]

---

33 Widodo, *op cit* hal 62

34 *Ibid*, hal 61

35 Edmon Makari, o*p cit* hal 404

a. Mengumpulkan dan mempelajari informasi mengenai sistem operasi komputer yang dipakai pada target sasaran. Cara memperoleh informasi ini dapat diperoleh dari orang dalam atau dengan cara menggunakan komputer yang tersambung ke internet. Untuk memperlancar digunakan program tertentu seperti *prefix scanner, port scanner.*

b. Menyusup dan mengakses jaringan komputer target

   Hal ini dapat dilakukan dengan menipu atau menaklukkan sistem yang ada pada jaringan komputer. Caranya adalah dengan menebak *password* atau kata kunci, menyadap *password* dan mengeksploitasi kelemahan sistem sasaran.

c. Menjelajahi sistem komputer

   Metode yang dilakukan yaitu dengan cara menyadap dan memeriksa paket-paket data yang melintas di dalam jaringan. Dalam memeriksa sistem tersebut, seorang *hacker* juga mencari kelemahan suatu sistem. Dalam suatu penjelajahan, seorang *hacker* akan memanfaatkan data atau informasi yang ada dalam jaringan tersebut. Cara lain untuk memperoleh suatu akses sehingga seolah-olah *hacker* tersebut memiliki kewenangan yaitu dengan menggunakan *trojan horse.* Setelah hacker melakukan aksinya biasanya mereka akan menghilangkan jejak. Seorang *hacker* akan memperkecil kemungkinan terdeteksi oleh orang lain. Cara ini biasanya memanfaatkan *trojan* atau program *finger.*

d. Membuat backdoor dan menghilangkan jejak

Suatu penyamaran atau penghilangan jejak agar tak terdeteksi. Cara yang paling umum adalah mengedit file-file log pada sistem yang dimasukinya dan menghilangkan semua entry yang berkaitan dengan dirinya. *Backdoor* adalah jalan tembus yang dibuat oleh *hacker* jika suatu saat ia kembali.

3. *Data Diddling*

Data diddling adalah suatu perbuatan yang mengubah data yang sah diubah dengan cara yang tidak sah. Modusnya yaitu mengubah data *input* yang dilakukan seseorang dengan cara memasukkan data yang menguntungkan diri sendiri secara melawan hukum. Mengubah *print-out* atau *out-put* dengan maksud menyembunyikan data atau informasi dengan itikad tidak baik. Penggelapan, pemalsuan, dan atau pemberian informasi melalui komputer yang merugikan pihak lain dan menguntungkan diri sendiri. Dengan sengaja merusak sistem komputer. Apabila dikaitkan dengan delik-delik yang tercantum didalam KUHP, maka perbuatan berupa mengubah data *input*, mengubah *print out* atau *out-put* dengan maksud mengaburkan, menyembunyikam data melakukan penggelapan, pemalsuan data di KUHP dapat dikategorikan sebagai perbuatan tanpa wewenang memalsukan surat.[36] Tindakan tersebut dapat dikategorikan sebagai perbuatan pemalsuan data dan diancam pidana berdasarkan Pasal 263 KUHP.[37]

36 Al Wisnubroto, *loc cit*

37 Iwan Winarso,*op cit* hal 49

4. *Joy computing*

Joy computing adalah perbuatan seseorang yang menggunakan komputer secara tidak sah atau tanpa ijin dan penggunaannya melampaui kewenangan yang dimiliki. Tindakan ini dapat dikategorikan sebagai tindakan pencurian. (Pasal 362 KUHP).[38]

5. The Trojan Horse

Suatu prosedur menambah atau mengurangi data atau instruksi suatu program, sehingga program tersebut selain menjalankan tugas sebenarnya juga akan melaksanakan tugas lain yang tidak sah, juga membuat data atau instruksi pada sebuah program menjadi tidak terjangkau (menghilangkan data atau instruksi pada sebuah program dengan tujuan untuk kepentingan pribadi atau kelompok)[39]

Cara atau modus operandinya :

Mengubah data atau program yang ada sehingga program tersebut akan melakukan penghitungan pembulatan yang salah. Sering terjadi pada pembobolan kartu kredit atau pada rekening tabungan nasabah yang ada pada Bank. Mengubah program yang ada untuk memasukkan transaksi-transaksi tertentu, sehingga transaksi

38 Widodo, *op cit* hal 62

39 Iwan Winarso, *op cit* hal 48

tersebut dikenal oleh spesifikasi sistem, sedangkan untuk transaksi yang tidak dikenal dapat dimasukkan bersama-sama dengan transaksi lainnya. [40]

Memasukkan instruksi yang tidak sah dapat dilakukan baik oleh yang berwenang maupun tidak yang dapat mengakses suatu sistem dan memasukkan instruksi untuk keuntungan sendiri dengan melawan hukum. Apabila data dipandang sebagai suatu benda dalam arti seperti delik harta benda, maka pengubahan, penambahan atau penghapusan akan lebih cenderung ke pengertian delik klasik yaitu perusakan barang sesuai pasal 406 ayat 1 KUHP.[41]

6. Penyia-nyiaan Data Komputer

Penyia-nyiaan data komputer diartikan sebagai suatu perbuatan yang dilakukan dengan sengaja untuk merusak atau menghancurkan media disket dan media penyimpanan sejenis lainnya (*misalnya hardisc*) yang berisi data atau program komputer sehingga data atau program tersebut tidak berfungsi sebagaimana mestinya. Perusakan atau penghancuan media tersebut dapat dilakukan secara fisik maupun non fisik dengan tujuan agar data atau program komputer tidak berfungsi lagi.[42]

Tindakan yang dilakukan secara fisik misalnya membakar, memotong, mengolesi dengan zat kimia atau membuang media disket yang dimaksud hingga

40 Al. Wisnubroto, *op cit* hal 36

41Iwan Winarso, *loc cit*

42 Al. Wisnubroto, *op cit* hal 38

menjadi rusak dan tidak dapat dipakai lagi atau tidak dapat menjalankan fungsinya lagi. Tindakan yang dilakukan secara non fisik misalnya:

a. Dengan menyisipan sebuah *logic bomb*

Ini adalah program yang dengan sengaja dibuat untuk melakukan tindakan yang tidak sah sewaktu-waktu apabila dikehendaki oleh pelakunya

b. Dengan memasukkan "virus"

Ini merupakan "penyakit baru" di dunia komputer. Program virus merupakan program pendek yang bertingkah laku mirip virus penyakit pada tubuh manusia, yang mana bila program ini telah menyusup pada suatu sistem komputer, apabila dibiarkan maka program ini akan merekam dirinya hingga tersebar pada seluruh program. Pada waktu yang ditentukan oleh programer, virus tersebut dapat keluar dari persembunyiannya secara serentak dan membuat data ter "infeksi" tersebut menjadi tidak terbaca atau rusak.[43]

Tindakan ini dapat dikategorikan sebagai tindak pidana perusakan barang (Pasal 406 KUHP)[44]

D. Sistem Hukum Indonesia

Kebijakan hukum pidana, terutama kebijakan aplikatif sangat erat dengan sistem hukum yang dipengaruhi oleh tradisi hukum tertentu. Sistem hukum Indonesia nampak sebagai gabungan dari sistem *civil law* dengan hukum Islam dan hukum adat,

43 *Ibid*, hal 38-39

44 Widodo, *op cit* hal 63

namun tak dapat disangkal bahwa tradisi hukum *civil law* telah mengakar kuat dalam sistem hukum formal di Indonesia terutama dalam bidang hukum pidana.[45]

Penentuan politik hukum yang cenderung mengarah pada tradisi hukum *civil law* tersebut mengandung konsekuensi-konsekuensi tertentu yaitu:

1. Peraturan perundang-undangan harus dirumuskan secara teliti dan lengkap sehingga diharapkan mampu menjangkau semua permasalahan yang timbul.
2. Asas legalitas ditempatkan sebagai landasan yang bersifat fundamental dan dalam pelaksanaannya harus dijunjung tinggi tanpa terkecuali
3. Operasionalisasi peraturan perundang-undangan diupayakan seoptimal mungkin untuk menangani berbagai kasus yang bervariasi dengan pendekatan penafsiran.[46]

Sebagaimana diketahui bahwa tradisi hukum *civil law* menempatkan perundang-undangan sebagai sumber hukum yang paling utama. Ciri-ciri negara yang menganut sistem hukum ini nampak dengan kebijakan kodifikasi dan unifikasinya. Hal ini nampak pada perundang-undangan yang diatur secara cermat, terperinci, abstrak dan sistematis yang tidak sekedar kumpulan peraturan tetapi memuat pula asas-asas hukum. Oleh sebab itu, kebijakan hukum pidana khususnya yang berkaitan dengan kebijakan aplikatif sangat terkait erat dengan asas legalitas dan metode penafsiran.

1. Metode Interpretasi

45 Al. Wisnubroto, *op cit* hal 55

46 *Ibid,* hal 56

Makna isi dari undang-undang sering tidak jelas susunan kata-katanya atau dapat diartikan lebih dari satu kata. Pembuat undang-undang sengaja merumuskan kata-kata dalam setiap pasalnya dengan sedemikian rupa agar undang-undang tersebut dapat selalu *up to date* dan senantiasa relevan seiring dengan perkembangan jaman sehingga undang-undang tersebut dapat digunakan dalam kurun waktu yang lama.

Dalam prakteknya, sekalipun undang-undang disusun sedemikian rupa, seringkali ketentuan-ketentuan dalam undang-undang tersebut sulit untuk langsung bisa diterapkan dalam kasus-kasus konkret yang bervariasi bentuknya. Apalagi saat ini perkembangan pada ilmu pengetahuan dan teknologi semakin berkembang lebih pesat dibandingkan dengan perkembangan dibidang hukumnya. Oleh sebab itu untuk mengatasi hal tersebut diperlukan adanya interpretasi atau penafsiran hukum terhadap rumusan undang-undang yang ada.

Dalam ilmu hukum dikenal berbagai macam interpretasi yang lazim digunakan, antara lain adalah:[47]

a. Penafsiran gramatikal

Penafsiran gramatikal adalah penafsiran secara tata bahasa artinya hanya mengingat bunyi kata-kata dalam arti kalimat itu saja.

b. Penafsiran autentik atau resmi

47 *Ibid*, hal 57-59

Penafsiran autentik adalah memberi interpretasi yang pasti seperti yang ditentukan dalam undang-undang tersebut

c. Penafsiran extensif atau luas

Penafsiran extensif adalah memberikan penafsiran dengan memperluas kata-kata dalam ketentuan undang-undang sehingga peristiwa tersebut dapat dimasukkan.

d. Penafsiran analogi

Penafsiran analogi ini sebenarnya sudah tidak termasuk dalam interpretasi, karena analogi sama dengan *qiyas* yaitu memberi ibarat pada kata-kata tersebut sesuai dengan azas hukumnya, sehingga suatu peristiwa yang sebenarnya tidak dapat dimasukkan lalu dianggap sesuai dengan bunyi peraturan tersebut. Penggunaan penafsiran analogi tidak diperbolehkan dalam hukum pidana, hal ini disebabkan karena penafsiran analogi tidak sesuai dengan asas legalitas.

E. Kebijakan Hukum Pidana

Kebijakan hukum pidana didefinisikan sebagai usaha mewujudkan peraturan perundang-undangan pidana yang sesuai dengan keadaan dan situasi pada suatu waktu dan untuk masa yang akan datang. [48] Menurut A. Mulder mengemukakan bahwa kebijakan hukum pidana adalah garis kebijakan yang menentukan:

48 Abdul Wahid, *op cit* hal 53

1. seberapa jauh ketentuan-ketentuan pidana yang berlaku perlu diperbaharui
2. apa yang dapat diperbuat untuk mencegah terjadinya tindak pidana
3. cara bagaimana penyidikan, penuntutan, peradilan dan pelaksanaan pidana harus dilaksanakan. [49]

Dari definisi tersebut tampak bahwa Mulder memandang hukum pidana sebagai sebuah sistem dan yang menjadi objek kebijakan hukum pidana mencakup hukum pidana dalam arti formil dan materiil.[50]

Menurut Barda Nawawi yang dikutip oleh Abdul Wahid menjelaskan bahwa pada hakekatnya kebijakan untuk membuat peraturan hukum pidana menjadi lebih baik merupakan bagian dari upaya dalam penanggulangan kejahatan. Dengan demikian kebijakan hukum pidana hakekatnya merupakan bagian dari kebijakan penanggulangan kejahatan atau politik kriminal. Dalam perspektif politik kriminal, kebijakan hukum pidana identik dengan pengertian kebijakan penanggulangan kejahatan dengan hukum pidana. [51]

Kebijakan hukum pidana bukan merupakan suatu kebijakan yang berdiri sendiri. Sebagai suatu bagian dari upaya untuk menanggulangi kejahatan dalam rangka mensejahterakan masyarakat dan untuk melindungi masyarakat, maka tindakan untuk mengatur masyarakat dengan sarana hukum pidana terkait erat dengan

---

49 Al. Wisnubroto,*op cit* hal 10

50 Abdul Wahid, *loc cit*

51 *Ibid*, hal 54 (dikutip dari Barda Nawawi Arief, 2002, *Bunga Rampai Kebijakan Hukum Pidana*, Citra Aditya Bakti, Bandung)

berbagai bentuk kebijakan dalam suatu proses kebijakan sosial yang mengacu pada tujuan yang lebih luas yaitu kebijakan kriminal.

Kebijakan kriminalisasi merupakan suatu kebijakan dalam menetapkan suatu perbuatan yang semula bukan tindak pidana atau tidak dipidana menjadi suatu tindak pidana atau perbuatan yang dapat dipidana.[52] Oleh karena itu, dengan perkataan lain kebijakan penanggulangan kejahatan dengan hukum pidana dapat disebut dengan kebijakan kriminalisasi yang mana dalam proses kriminalisasi menggunakan sarana pidana.

Dalam rangka penanggulangan kejahatan secara terpadu maka kebijakan penanggulangan kejahatan dalam pengembangannya dapat menggunakan 2 (dua) alternatif kebijakan yaitu kebijakan non penal dan kebijakan penal.

1. Kebijakan nonpenal

Kebijakan non-penal merupakan suatu upaya untuk menanggulangi kejahatan dengan mempergunakan sarana lain selain hukum pidana. Upaya non-penal cenderung merupakan upaya *preventif*. Usaha-usaha non-penal misalnya pemberian sosialiasi tentang adanya undang-undang ITE sehingga masyarakat mengetahui tentang adanya peraturan tersebut, pembentukan tim khusus dalam kepolisian yang

52 *Ibid*, hal 54

mengatur tentang informasi teknologi dan lain sebagainya. Tujuan utama dari usaha-usaha non-penal adalah memperbaiki kondisi-kondisi sosial tertentu.[53]

2. Kebijakan penal

Kebijakan penal merupakan suatu kebijakan penanggulangan kejahatan dengan menggunakan sarana hukum pidana atau sanksi. Dua masalah sentral dalam kebijakan kriminal dengan menggunakan sarana penal adalah masalah penentuan perbuatan apa yang seharusnya dijadikan tindak pidana dan sanksi apa yang sebaiknya digunakan atau dikenakan pada si pelanggar. Pendekatan penal cenderung mengarah pada upaya *represif* yang dalam pelaksanaannya mengandung keterbatasan. Namun hal ini bukan berarti upaya penal dikesampingkan melainkan upaya penal merupakan sarana yang sangat vital dalam proses penegakan hukum dalam menanggulangi kejahatan. Dalam penjatuhan sanksi pidana sebagai sarana penal yang pada umumnya dicantumkan dalam perumusan delik menurut pola KUHP, menggunakan sembilan bentuk perumusan ancaman pidana, yaitu: [54]

a. Diancam dengan pidana mati atau penjara seumur hidup atau penjara tertentu;

b. Diancam dengan pidana penjara seumur hidup atau penjara tertentu;

c. Diancam dengan pidana penjara;

---

53 Muladi & Barda Nawawi, *Teori-Teori dan Kebijakan Pidana*, PT. Alumni, Bandung, 2005, hal 159

54 Sholehuddin, *Sistem Sanksi Dalam Hukum Pidana*, PT. RajaGrafindo Persada, Jakarta, 2004, hal 189

d. Diancam dengan pidana penjara atau kurungan;

e. Diancam dengan pidana penjara atau kurungan atau denda;

f. Diancam dengan pidana penjara atau denda;

g. Diancam dengan pidana kurungan;

h. Diancam dengan pidana kurungan atau denda; dan

i. Diancam dengan pidana denda.

Dalam sistem perumusan sanksi pidana terdapat beberapa macam yaitu:[55]

a. Sistem tunggal yaitu pidana penjara dirumuskan sebagai satu-satunya jenis sanksi pidana. Misalnya "...diancam dengan pidana penjara paling lama tujuh tahun."

b. Sistem kumulatif/ alternatif yaitu dengan menggunakan kata "...dan/atau..." Sistem penjatuhan pidananya dapat dijatuhi dengan pidana penjara saja atau denda saja atau dapat kedua-duanya yaitu pidana penjara dan denda. Misalnya "...dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 600.000.000,00 (enam ratus juta rupiah)." Maka penjatuhan pidananya dapat dipidana penjara paling lama 6 tahun atau denda paling banyak Rp 600.000.000,00 (enam ratus juta rupiah) atau dapat dipidana dengan pidana penjara paling lama 6 tahun dan denda paling banyak Rp 600.000.000,00 (enam ratus juta rupiah).

55 Dwidja Priyatno, *Sistem Pelaksanaan Pidana Penjara di Indonesia*, PT. Refika Aditama, Bandung, 2006, hal 77

c. Sistem alternatif yaitu dengan menggunakan kata "...atau..." Artinya pidana penjara atau denda dialternatifkan dengan jenis pidana pokok yang lain. Misalnya "...dengan pidana penjara paling lama lima tahun atau denda paling banyak enam puluh rupiah."

d. Sistem kumulatif yaitu dengan menggunakan kata "...dan..." Artinya pidana penjara atau dikumulatifkan dengan jenis pidana pokok yang lain. Misalnya "...dengan pidana penjara paling lama lima tahun dan denda paling banyak enam puluh rupiah."

Kebijakan kriminal yang dilakukan secara penal maupun nonpenal sebagai sarana untuk melindungi masyarakat (*Social Defence*) terhadap kejahatan merupakan bagian integral dari kebijaksanaan sosial yang bersama-sama untuk mensejahterakan masyarakat (*social welfare policy*) mengupayakan suatu tujuan akhir yang lebih luas yaitu perlindungan masyarakat untuk kesejahteraan masyarakat.[56]

Dari uraian tersebut nampak bahwa kebijakan hukum pidana merupakan bagian integral dari kebijakan-kebijakan yang lain terutama kebijakan kriminal dan kebijakan sosial yang dapat digambarkan dalam bagan sebagai berikut

Bagan 2.1

56 Al Wisnubroto, *op cit* hal 14

Berdasarkan bagan tersebut maka upaya penanggulangan kejahatan perlu ditempuh dengan pendekatan kebijakan secara terpadu dalam arti bahwa adanya keterpaduan antara kebijakan kriminal dengan kebijakan sosial serta ada keterpaduan antara upaya penanggulangan dengan sarana penal dan non-penal. Selanjutnya upaya penanggulangan kejahatan yang terintegrasi dalam kebijakan sosial perlu diintegrasikan pula dalam perencanaan pembangunan nasional guna mencapai tujuan nasional.[57]

Dalam penganalisaan hukum pidana tidak dapat dilepaskan dari konsepsi integral dalam kebijakan nasional yaitu masalah penentuan perbuatan dan sanksi adalah sebagai berikut:

1. Perbuatan apa yang seharusnya dijadikan tindak pidana. Dalam penentuan perbuatan yang harus dijadikan tindak pidana harus mempertimbangkan beberapa faktor yaitu: [58]

   a. Teknologi komputer merupakan aset pembangunan nasional yang sangat besar. Dengan kata lain komputer merupakan salah satu teknologi strategis dalam rangka pembangunan menuju ke kemajuan bangsa dan negara dalam menghadapi era globalisasi. Oleh sebab itu pengaturan delik komputer harus

57 *Ibid*, hal 15

58 *Ibid*, hal 64

dipertimbangkan secara utuh jangan sampai menimbulkan akibat yang dapat menghambat pengembangan teknologi komputer beserta pengapilikasiannya dan perkembangan industri komputer yang ditujukan pada kemajuan bangsa dan negara.

b. Pemilihan dan penetapan perbuatan penyalahgunaan komputer yang akan diatur dan dijadikan delik harus dilakukan secara selektif dan limitatif. Artinya perbuatan penyalahgunaan komputer yang benar-benar tidak dikehendaki, tidak disukai atau dibenci oleh warga masyarakat yaitu perbuatan yang merugikan baik secara materiil maupun imateriil atau dapat merugikan, mendatangkan korban atau dapat mendatangkan korban. Selain itu dipertimbangkan sejauhmana perbuatan-perbuatan penyalahgunaan komputer tersebut bertentangan dengan nilai-nilai fundamental yang berlaku dimasyarakat.

c. Perlu diperhitungkan apakah biaya yang harus dikeluarkan (*cost*) dalam pembuatan undang-undang yang memuat delik komputer yang sangat rumit dan komplek, *cost* untuk pengawasan dan penegakan hukum yang memerlukan fasilitas atau sarana teknologi tinggi. Serta beban yang dipikul oleh korban dan kejahatan akan seimbang dengan hasilnya yaitu situasi tertib hukum yang akan dicapai. Jangan sampai biaya penuntutan lebih besar daripada besarnya kerugian yang ditimbulkan akibat penyalahgunaan komputer, atau jangan sampai terjadi biaya yang diperlukan untuk penuntutan sangat besar namun pengaruhnya terhadap pencapaian situasi tertib hukum sangat kecil.

d. Perlu dipertimbangkan struktur kapasitas aparat penegak hukum di Indonesia dalam menegakkan ketentuan-ketentuan yang mengatur masalah delik komputer

e. Akibat sosial dari pengkriminalisasian atau pendekriminalisasian dari penyalahgunaan komputer.

2. Bertolak dari pendekatan nilai masyarakat, maka dalam menetapkan sanksi pidana terhadap pelaku penyalahgunaan komputer harus disepadankan dengan kebutuhan untuk melindungi dan mempertahankan kepentingan-kepentingan sosial yaitu:[59]

a. Pemeliharaan tertib masyarakat dan perlindungan warga masyarakat dari kejahatan, kerugian atau bahaya-bahaya lain yang tidak dapat dibenarkan. Dalam hal ini faktor-faktor yang perlu diperhitungkan berkaitan dengan karakteristik yang bersifat khas dari penyalahgunaan komputer adalah:

1) Penyalahgunaan komputer menyangkut sesuatu yang sangat peka seperti data, program, sistem dan informasi, serta fasilitas-fasilitas lainnya yang dihasilkan komputer. Hal ini menimbulkan berbagai kerawanan-kerawanan yang mengganggu, merugikan dan membahayakan masyarakat.

2) Penyalahgunaan komputer membuka kemungkinan mengeruk hasil dalam jumlah yang sangat besar dengan cara yang "aman".

59 *Ibid*, hal 66-67

b. Memelihara atau mempertahankan integritas pandangan-pandangan dasar tertentu mengenai keadilan sosial, martabat kemanusiaan dan keadilan individu. Dalam hal ini faktor-faktor yang perlu diperhatikan berkaitan dengan karakteristik yang bersifat khas dari penyalahgunaan komputer adalah penyalahgunaan komputer tidak selalu mengarah pada tujuan atau maksud yang bersifat materiil namun seringkali berorientasi pada tujuan yang bersifat tantangan dari pelakunya. Apabila dilihat perbuatan tersebut secara materi tidak merugikan namun dilihat dari aspek sosial, kultural dan politis bertentangan dengan nilai etika, moral dan pandangan politik suatu pemerintah.

c. Memasyarakatkan kembali (resosialisasi) para pelanggar hukum

Pemberian sanksi pidana harus disesuaikan dengan kebutuhan untuk melindungi dan mempertahankan kepentingan-kepentingan tersebut. Pidana hanya dibenarkan apabila terdapat suatu kebutuhan yang berguna bagi masyarakat. Suatu pidana yang tidak diperlukan, tidak dapat dibenarkan dan berbahaya bagi masyarakat.[60] Selain itu, batas-batas sanksi pidana yang ditetapkan harus berdasarkan pada kepentingan-kepentingan dan nilai-nilai yang mewujudkan.

F. Ketentuan Pidana berdasarkan Kitab Undang-Undang Hukum Pidana Terkait dengan Kejahatan Komputer

60 Muladi & Barda Nawawi, *op cit* hal 166

1. Ketentuan yang berkaitan dengan perbuatan pembocoran rahasia

Data, dokumen, *file* atau berbagai bentuk informasi lainnya seringkali harus dijaga kerahasiaannya. Hal ini dimaksudkan untuk mencegah pemanfaatan data atau informasi tersebut oleh pihak-pihak yang tidak bertanggung jawab, atau untuk menghindari penyalahgunaan data atau informasi tersebut untuk tujuan yang merugikan baik bagi pemilik data, pihak-pihak tertentu atau masyarakat pada umumnya. Berkaitan dengan hal tersebut maka perlindungan terhadap kerahasiaan data atau informasi perlu dilakukan dengan menetapkan ancaman pidana bagi pelaku perbuatan pembocoran rahasia.

Dalam KUHP telah diatur delik mengenai pembocoran rahasia yaitu dalam Pasal 112 KUHP tentang pembocoran rahasia negara, Pasal 113 dan 114 KUHP tentang pembocoran rahasia pertahanan dan keamanan negara.

Pasal 112 KUHP berbunyi:

> "Barangsiapa dengan sengaja mengumumkan surat-surat atau benda-benda atau keterangan-keterangan yang diketahuinya bahwa harus dirahasiakan untuk kepentingan negara atau dengan sengaja memberitahukan atau memberikannya kepada negara asing, diancam dengan pidana penjara paling lama tujuh tahun."

Pasal 113 KUHP berbunyi:

(1) "Barangsiapa dengan sengaja, untuk seluruhnya atau sebagian mengumumkan, atau memberitahukan maupun menyerahkan kepada orang yang tidak berwenang mengetahui, surat-surat, peta-peta, rencana-rencana, gambar-gambar atau benda-benda yang bersifat rahasia dan bersangkutan dengan pertahanan atau keamanan Indonesia (negara) terhadap serangan dari luar, yang daripadanya atau isinya, bentuk atau susunannya benda-benda itu diketahui olehnya, diancam dengan pidana penjara paling lama empat tahun."

(2) "Jika adanya surat-surat atau benda-benda pada yang bersalah, atau pengetahuannya tentang itu karena pencahariannya, pidananya dapat ditambah sepertiga."

Pasal 114 KUHP berbunyi:

" Barangsiapa karena kealpaanya menyebabkan bahwa surat-surat atau benda-benda rahasia tersebut dalam Pasal 113 yang tentang menyimpan atau menaruhnya menjadi tugasnya, diketahui oleh umum, mengenai bentuk dan susunannya, untuk seluruhnya dan sebagian atau oleh orang yang tidak wenang mengetahui, ataupun jatuh dalam tangannya, diancam dengan pidana penjara paling lama satu tahun enam bulan atau kurungan paling lama satu tahun atau denda paling banyak empat ribu limaratus rupiah."

Dalam KUHP juga mengatur tentang pembocoran rahasia yang menyangkut profesi atau jabatan seseorang. Pasal-pasal yang berkaitan dengan delik tersebut adalah Pasal 322 KUHP mengatur tentang pembocoran rahasia yang menyangkut profesi atau jabatan seseorang, Pasal 323 KUHP menyangkut pembocoran rahasia perusahaan dan Pasal 431 KUHP menyangkut pembocoran rahasia dalam situasi tertentu.

Pasal 322 KUHP berbunyi:

(1) "Barangsiapa dengan sengaja membuka rahasia yang wajib disimpannya karena jabatan atau pencahariannya, baik yang sekarang, maupun yang terdahulu, diancam dengan pidana penjara paling lama sembilan bulan atau denda paling banyak sembilan ribu rupiah."
(2) "Jika kejahatan dilakukan terhadap seseorang yang tertentu, maka perbuatan itu hanya dapat dituntut atas pengaduan orang itu."

Pasal 323 KUHP berbunyi:

(1) " Barangsiapa dengan sengaja memberitahukan hal-hal khusus tentang suatu perusahaan dagang, kerajinan atau pertanian dimana ia bekerja atau dahulu bekerja, yang olehnya supaya dirahasiakan, diancam dengan pidana penjara paling lama sembilan bulan atau denda paling banyak sembilan ribu rupiah."
(2) " Kejahatan ini hanya dituntut atas pengaduan pengurus perusahaan itu."

Pasal 431 KUHP

> "Seorang pejabat suatu lembaga pengangkutan umum yang dengan sengaja dan melawan hukum membuka suatu surat, barang tertutup atau paket yang diserahkan kepada lembaga itu, memriksa isinya, atau memberitahukan isinya kepada orang lain, diancam dengan pidana penjara paling lama dua tahun."

Penerapan ketentuan-ketentuan pasal-pasal KUHP tersebut dapat diterapkan dalam kasus-kasus pembocoran data komputer yang bersifat rahasia. Hal tersebut tentu saja bergantung dari jenis kerahasiaan data komputer yang dibocorkan.

2. Ketentuan yang berkaitan dengan perbuatan memasuki atau melintasi wilayah orang tanpa hak

Dalam kitab undang-undang hukum pidana yang berlaku sekarang ini telah diatur tentang perbuatan memasuki atau melintasi wilayah tanpa hak. Ketentuan ini diatur dalam Pasal 167 KUHP yaitu tanpa hak memasuki rumah, ruangan atau pekarangan tertutup yang ditempati orang lain dan ketentuan Pasal 551 KUHP yaitu tanpa hak melintasi tanah orang lain.[61]

Pasal 167 KUHP berbunyi:

(1) "Barangsiapa memaksa masuk ke dalam rumah, ruangan atau pekarangan tertutup yang dipakai orang lain dengan melawan hukum atau berada di situ dengan melawan hukum, dan atas permintaan yang berhak atau suruhannya tidak pergi dengan segera, diancam dengan pidana penjara paling lama sembilan bulan atau denda paling banyak empat ribu lima ratus rupiah."
(2) "Barangsiapa masuk dengan merusak atau memanjat, dengan menggunakan anak kunci palsu, perintah palsu atau pakaian jabatan palsu atau barangsiapa

61 Al. Wisnubroto, *op cit* hal 76

tidak setahu yang berhak lebih dulu serta bukan karena kekhilafan masuk dan kedapatan di situ pada waktu malam, dianggap memaksa masuk."

(3) "Jika mengeluarkan ancaman atau menggunakan sarana yang dapat menakutkan orang, diancam dengan pidana penjara paling lama satu tahun empat bulan."

(4) "Pidana tersebut dalam ayat (1) dan(3) ditambah sepertiga jika yang melakukan kejahatan dua orang atau lebih dengan bersekutu."

Pasal 551 KUHP berbunyi

"Barangsiapa tanpa wewenang berjalan atau berkendaraan di atas tanah yang oleh pemiliknya dengan cara jelas dilarang memasukinya, diancam dengan pidana denda paling banyak dua ratus dua puluh lima rupiah."

Dalam rumusan pasal-pasal tersebut nampak bahwa wilayah yang tidak boleh dimasuki atau dilalui tanpa hak tersebut merupakan wilayah "fisik" seperti rumah, ruangan, atau pekarangan tertutup sehingga sulit untuk diterapkan pada perbuatan tanpa hak yang memasuki sistem komputer yang dapat dianggap sebagai wilayah "non fisik."

Sebagaimana diketahui bahwa dalam perkembangannya teknologi komputer yang "dikawinkan" dengan teknologi komunikasi telah memunculkan suatu sistem yang disebut sistem jaringan komputer. Sistem jaringan ini biasanya bersifat eksklusif dalam arti tidak setiap orang dapat memasukinya tanpa ijin atau tanpa menjadi peserta jaringan komputer tersebut. Apabila terjadi pelanggaran terhadap jaringan komputer tersebut yang mana telah terjadi perbuatan menyambung terminal komputer pada jaringan komputer tersebut secara ilegal atau dikenal dengan istilah *hacking*, maka terhadap *hacker* dapat diterapkan ketentuan Pasal 167 atau 551 KUHP.[62]

62 *Ibid*, hal 77

3. Ketentuan yang berkaitan dengan perbuatan pemalsuan

Delik pemalsuan dalam KUHP dimaksudkan sebagai pemalsuan surat. Lazimnya surat atau data atau informasi ditulis atau dicetak di atas media kertas yang dapat dipakai sebagai alat bukti secara tertulis misalnya akte, sertifikat, ijasah dan lain sebagainya. Kini dengan hadirnya teknologi komputer, maka sistem penyimpanan yang konvensional tersebut dialihkan ke dalam media penyimpanan seperti disket, *flashdisk* dan media penyimpanan yang sejenisnya.

Dengan pengalihan data atau keterangan ke dalam media disket atau sejenisnya ternyata masih belum menjamin data atau informasi tersebut menjadi aman dari kejahatan pemalsuan. Ternyata data atau keterangan tersebut masih dapat dipalsu dengan cara yang canggih yaitu dengan memanfaatkan teknologi komputer yang merupakan perkembangan dari bentuk kejahatan pemalsuan surat.

Kejahatan pemalsuan surat bentuk baru tersebut disebut *data diddling* yaitu kejahatan yang berupa perbuatan mengubah data valid atau sah dengan cara melawan hukum yaitu dengan mengubah *input* data maupun *output* data dengan memakai sarana komputer.[63] Dalam KUHP pemalsuan surat diatur dalam Pasal 263 KUHP.

Pasal 263 KUHP berbunyi:

> (1) "Barangsiapa membuat secara tidak benar atau memalsu surat yang dapat menimbulkan sesuatu hak, perikatan atau pembebasan hutang, atau yang diperuntukkan sebagai bukti daripada sesuatu hal, dengan maksud untuk memakai atau menyuruh orang lain pakai surat tersebut seolah-olah isinya

63 *Ibid*, hal 79

benar dan tidak dipalsu, diancam, jika pemakaian tersebut dapat menimbulkan kerugian karena pemalsuan surat, dengan pidana pejara paling lama enam tahun."

(2) "Diancam dengan pidana yang sama, barang siapa dengan sengaja memakai surat yang sisinya tidak benar atau yang dipalsu, seolah-olah benar dan tidak dipalsu, jika pemakaian surat dapat menimbulkan kerugian."

Dalam komentar Pasal 263 KUHP disebutkan bahwa yang diartikan dengan surat dalam bab ini adalah segala surat yang ditulis dengan tangan, dicetak, maupun ditulis memakai mesin tik dan lain-lainnya. Kalimat "dan lain-lain" dalam komentar Pasal 263 KUHP mempunyai pengertian yang cukup luas yang memungkinkan surat otentik yang dibuat atau ditulis melalui proses komputer, sehingga data atau keterangan dalam disket atau sejenisnya dapat dimasukkan dalam pengertian surat, asalkan data atau informasi atau keterangan yang tersimpan dalam media disket dan sejenisnya tersebut sudah dituangkan dalam bentuk tulisan. Dengan demikian data informasi tersebut dapat dipakai sebagai bahan informasi tertulis.[64]

4. Ketentuan yang berkaitan dengan pencurian

Dalam KUHP tindak pidana pencurian diatur dalam Pasal 362 KUHP, sedang variasinya diatur dalam Pasal 363 KUHP yaitu pencurian dengan pemberatan, Pasal 364 KUHP yaitu pencurian ringan, Pasal 365 KUHP yaitu pencurian yang disertai dengan kekerasan atau ancaman kekerasan dan Pasal 367 KUHP yaitu pencurian di lingkungan keluarga. Pencurian yang berkaitan dengan kejahatan komputer adalah:

64 *Ibid*, hal 80

a. Pencurian terhadap data atau program komputer, yaitu data atau program yang tersimpan didalam media disket, *floppy disk, magnetic tape* dan media penyimpan sejenisnya.[65]

b. Pencurian terhadap waktu pemakaian komputer, yaitu bentuk kejahatan yang oleh Nico Keijzer disebut dengan istilah *"Joycomputing"*.

Pasal 362 KUHP berbunyi:

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

Apabila dijabarkan maka unsur-unsur yang terdapat di dalam pasal 362 KUHP adalah:

a. Unsur objektif:

- mengambil
- barang sesuatu
- barang tersebut seluruhnya atau sebagian kepunyaan orang lain

b. unsur subjektifnya

- dengan maksud untuk memiliki
- secara melawan hukum

5. Ketentuan yang berkaitan dengan perbuatan penggelapan

65 *Ibid,* hal 81

Dalam KUHP delik penggelapan (*verduistering*) diatur dalam Pasal 372 KUHP, sedangkan variasinya diatur dalam Pasal 373 KUHP yaitu penggelapan ringan, Pasal 374 KUHP yaitu penggelapan yang dilakukan atas hubungan kerja, Pasal 375 KUHP yaitu penggelapan dengan pemberatan dan Pasal 376 KUHP yaitu penggelapan di lingkungan keluarga. [66]

Pasal 372 berbunyi:

> "Barangsiapa dengan sengaja dan melawan hukum mengaku sebagai milik sendiri (*zich toeeigenen*) barang sesuatu yang seluruhnya atau sebagian adalah kepunyaan orang lain, tetapi yang ada dalam kekuasaannya bukan karena kejahatan, diancam karena penggelapan, dengan pidana penjara paling lama empat tahun atau denda paling banyak enam puluh rupiah."

Adapun unsur-unsur dari pasal tersebut adalah sebagai berikut:

a. Unsur objektif

- mengaku sebagai milik sendiri atau memiliki
- barang sesuatu
- barang tersebut sebagaian atau seluruhnya adalah
- kepunyaan orang lain
- barang tersebut ada dalam kekuasaannya bukan karena kejahatan

b. Unsur subjektif

- dengan sengaja
- melawan hukum [67]

---

66 *Ibid*, hal 85

67 *Ibid*, hal 86

Apabila kepercayaan untuk memegang barang dalam hal ini adalah komputer beserta sarana-sarana penunjangnya berdasarkan hubungan karena pekerjaan atau jabatan atau karena upah, maka terhadap pelaku manipulasi data atau *the trojan horse* dapat diancam pidana berdasarkan Pasal 374 KUHP yang berbunyi:

> "Penggelapan yang dilakukan oleh orang yang penguasaannya terhadap barang disebabkan karena ada hubungan kerja atau karena pencariannya atau karena mendapatkan upah untuk itu, diancam dengan pidana penjara paling lama lima tahun."

Pengertian "mengaku sebagai milik sendiri" atau "memiliki" pada Pasal 372 KUHP, pada dasarnya mempunyai pengertian yang mirip dengan pengertian "mengambil" pada Pasal 362 KUHP yang mana maksud memiliki adalah seseorang yang ingin menguasai atau ingin mempunyai hak atas suatu barang.

6. Ketentuan yang berkaitan dengan perbuatan penghancuran atau perusakan barang

Pengertian mengenai penghancuran atau perusakan barang (*vernieling of beschadiging van goederen*) diatur dalam Pasal 406 KUHP sedang variasinya diatur dalam Pasal 407-412 KUHP

Pasal 406 berbunyi:

a. "Barangsiapa dengan sengaja dan melawan hukum menghancurkan, merusakkan, membikin tak dapat dipakai atau menghilangkan barang sesuatu yang seluruhnya atau sebagian adalah kepunyaan orang lain, diancam dengan pidana penjara paling lama dua tahun delapan bulan atau denda paling banyak empat ribu lima ratus rupiah."
b. "Dijatuhkan pidana yang sama terhadap orang yang dengan sengaja dan melawan hukum membunuh, merusakkan, membikin tak

dapat digunakan atau menghilangkan hewan, yang seluruhnya atau sebagian adalah kepunyaan orang lain.

Beberapa pengertian dalam pasal 406 ayat 1 KUHP adalah: [68]

a. Pengertian "menghancurkan" (*vernielen*)

Menghancurkan atau membinasakan dimaksudkan sebagai merusak sama sekali sehingga barang tersebut tidak dapat berfungsi sebagaimana mestinya, misalnya membanting gelas, piring, vas bunga dan sebagainya sehingga hancur berkeping-keping.

b. Pengertian "merusakkan"

Merusakkan dimaksudkan sebagai memperlakukan suatu barang sedemikian rupa namun kurang daripada membinasakan (*beschadigen*), misalnya memukul cangkir atau vas bungan tetapi tidak sampai hancur, melainkan hanya pecah sedikit atau retak.

c. Pengertian "membikin (membuat) tidak dapat dipakai lagi"

Disini tindakan itu harus sedemikian rupa, sehingga barang itu tidak dapat diperbaiki lagi.

d. Pengertian "menghilangkan"

Menghilangkan dimaksudkan dengan membuat sehingga barang itu tidak ada lagi, misalnya dibakar sampai habis, dibuang di laut atau di sungai sehingga tidak bisa ditemukan lagi.

---

68 *Ibid,* hal 88

G. Ketentuan Pidana berdasarkan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik Terkait dengan Kejahatan Komputer

1. *Ketentuan yang berkaitan dengan mengakses komputer milik orang lain dengan cara melawan hukum*

Kejahatan komputer yang mengakses komputer milik orang lain termasuk dalam jenis *hacking*. Kejahatan ini cukup berbahaya karena apabila ia berhasil masuk ke wilayah komputer milik orang lain dengan sengaja untuk tujuan memperoleh sesuatu atau dengan menjebol sistem pengamanan maka ia dapat mengambil informasi yang ada dalam komputer tersebut. Perbuatan mengakses sistem komputer milik orang lain ini diatur dalam Pasal 30 Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) dengan ancaman pidana yang diatur dalam Pasal 46 Undang-Undang ITE.

Pasal 30 undang-undang ITE berbunyi

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

Apabila dijabarkan maka unsur-unsur yang terdapat dalam pasal 30 UU ITE adalah:

a. Unsur objektif ayat 1

- mengakses komputer dan/ atau sistem elektronik
- milik orang lain
- dengan cara apapun

b. Ayat 2

- mengakses komputer dan/ atau sistem elektronik
- milik orang lain
- dengan cara apapun
- tujuan untuk memperoleh informasi elektronik dan/ atau dokumen elektronik

c. Ayat 3

- mengakses komputer dan/ atau sistem elektronik
- milik orang lain
- dengan cara apapun
-dengan melanggar,
- menerobos, sistem pengamanan
- melampaui,
- atau menjebol

b. Unsur subjektif

- setiap orang dengan sengaja dan tanpa hak atau melawan hukum

Sanksi pidana yang diberikan apabila melanggar Pasal 30 ini adalah pasal 46 Undang-Undang ITE yang berbunyi

Pasal 46

(1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp600.000.000,00 (enam ratus juta rupiah).
(2) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp700.000.000,00 (tujuh ratus juta rupiah).
(3) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah).

2. Ketentuan yang berkaitan dengan tindakan penyadapan atas informasi elektronik dan/ atau dokumen elektronik dalam suatu komputer tertentu milik orang lain

Dalam Undang-Undang ITE terdapat juga pasal yang mengatur tentang perbuatan secara sengaja dan tanpa hak melakukan intersepsi atau penyadapan informasi elektronik dalam suatu komputer milik orang lain yang tidak menyebabkan perubahan apapun maupun yang menyebabkan adanya perubahan, penghilangan dan/ atau penghentian informasi elektronik dan/atau dokumen elektonik yang sedang ditransmisikan. Perbuatan yang berkaitan dnegan tindakan penyadapan ini diatur dalam Pasal 31 ayat 1 dan 2 dengan ancaman pidana yang diatur dalam Pasal 47 Undang-Undang ITE.

Pasal 31 ayat 1 dan 2 berbunyi

(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain.
(2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan,

penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan.

Apabila dijabarkan unsur-unsurnya adalah sebagai berikut:

a. Unsur objektif ayat 1

- melakukan intersepsi atau penyadapan
- atas informasi elektronik dan/atau dokumen elektronik
- dalam suatu komputer dan/atau sistem elektronik tertentu
- milik orang lain

b. Ayat 2

- melakukan intersepsi
- atas transmisi Informasi Elektronik dan/atau Dokumen Elektronik
- tidak bersifat publik
- dari, ke, dan di dalam suatu komputer dan/ atau sistem elektronik tertentu
- milik orang lain
- baik yang tidak menyebabkan perubahan apapun
- maupun yang menyebabkan perubahan, penghilangan, dan/atau penghentian informasi elektronik dan/atau dokumen elektronik
- yang sedang ditransmisikan

c. Unsur subjektif

- setiap orang dengan sengaja dan tanpa hak atau melawan hukum

Ketentuan pidana Pasal 31 ayat 1 dan 2, diatur dalam Pasal 47 Undang-Undang ITE. Adapun isi dari Pasal 47 adalah

Pasal 47

Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 31 ayat (1) atau ayat (2) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah).

3. Ketentuan yang berkaitan dengan pengubahan dan pemindahan informasi elektronik dan dokumen elektronik milik orang lain

Dalam Undang-Undang ITE terdapat juga pasal yang mengatur secara lebih rinci mengenai kejahatan yang berkaitan dengan pengubahan, pemindahan, pengurangan, perusakan, penghilangan suatu sistem elektronik milik orang lain secara melawan hukum yang mana akibat dari perbuatan tersebut adalah dapat terbukanya suatu informasi elektronik atau dokumen elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya. Perbuatan tersebut diatur dalam Pasal 32 Undang-Undang ITE dengan ancaman pidana yang diatur dalam Pasal 48 Undang-Undang ITE.

Pasal 32 Undang-Undang ITE berbunyi

(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik.
(2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak.
(3) Terhadap perbuatan sebagaimana dimaksud pada ayat (1) yang mengakibatkan terbukanya suatu Informasi Elektronik dan/atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya.

Unsur-unsur dalam Pasal 32 Undang-Undang ITE adalah sebagai berikut:

a. Unsur objektif ayat 1

-dengan cara apapun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan

- suatu informasi elektronik dan/atau dokumen elektronik

- milik orang lain atau

- milik publik

b. Ayat 2

- dengan cara apapun memindahkan atau menstransfer

- Informasi elektronik dan/atau dokumen elektronik

- kepada sistem elektronik orang lain

- yang tidak berhak

c. Ayat 3

- mengakibatkan terbukanya

- informasi elektronik dan/atau dokumen elektronik

- bersifat rahasia

- menjadi dapat diakses

- oleh publik

- dengan keutuhan data yang tidak sebagaimana mestinya

d. Unsur subjektif

- setiap orang dengan sengaja dan tanpa hak atau melawan hukum

Ketentuan pidana Pasal 32 diatur dalam Pasal 48 Undang-Undang ITE. Adapun isi dari Pasal 48 adalah

Pasal 48

(1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (1)dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp2.000.000.000,00 (dua miliar rupiah).
(2) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (2) dipidana dengan pidana penjara paling lama 9 (sembilan) tahun dan/ atau denda paling banyak Rp3.000.000.000,00 (tiga miliar rupiah).
(3) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (3) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/ atau denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah).

4. Ketentuan yang berkaitan dengan terganggunya sistem elektronik

Dalam Undang-Undang ITE diatur juga tentang tindakan yang dapat mengakibatkan terganggunya sistem elektronik atau mengakibatkan sistem elektronik tersebut bekerja tidak sebagaimana mestinya. Perbuatan tersebut diatur dalam Pasal 33 Undang-Undang ITE dengan ancaman pidana yang diatur dalam Pasal 49 Undang-Undang ITE.

Pasal 33 berbunyi

> Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya.
> Unsur-unsur dari Pasal 33 tersebut adalah

a. Unsur objektif

- melakukan tindakan apapun
- berakibat terganggunya Sistem Elektronik
- dan/atau mengakibatkan Sistem elektronik menjadi tidak bekerja

- sebagaimana mestinya

b. Unsur subjektif

- Setiap orang dengan sengaja dan tanpa hak atau melawan hukum

Ketentuan pidana dari Pasal 33 tersebut diatur dalam Pasal 49 Undang-Undang ITE. Adapun isi dari Pasal 49 tersebut adalah

Pasal 49 Undang-Undang ITE

> Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 33, dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp10.000.000.000,00 (sepuluh miliar rupiah).

5. Ketentuan yang berkaitan dengan perbuatan manipulasi, penciptaan, penghilangan, perusakan informasi elektronik dan/atau dokumen elektronik dengan tujuan agar informasi elektronik tersebut seolah-olah data yang otentik.

Ketentuan yang berkaitan dengan perbuatan tersebut diatur secara jelas dalam Pasal 35 Undang-Undang ITE dengan ancaman pidana yang diatur dalam Pasal 51 ayat 1 Undang-Undang ITE.

Pasal 35 Undang-Undang ITE berbunyi

> Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik.

Unsur-unsur dalam Pasal 35 Undang-Undang ITE tersebut adalah sebagai berikut

a. Unsur objektif

- melakukan manipulasi
- penciptaan — informasi elektronik dan/atau dokumen
- perubahan — elektronik
- pengrusakan
- tujuan agar informasi elektronik dan/atau dokumen elektronik
- dianggap seolah-olah data yang otentik

b. Unsur subjektif

- Setiap orang dengan sengaja dan tanpa hak atau melawan hukum

Ketentuan pidana dari Pasal 35 tersebut diatur dalam Pasal 51 ayat 1 yang berisi sebagai berikut

Pasal 51
(1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp12.000.000.000,00 (dua belas miliar rupiah)

Untuk memperjelas gambaran mengenai operasionalisasi Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, maka penulis menampilkan sebuah tabel tentang perbuatan dan ketentuan pidana yang terkait dengan kejahatan komputer.

Tabel 2.1

Perbuatan dan ketentuan pidana Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik terkait dengan kejahatan komputer

No	Perbuatan	Pasal	Sanksi	Ancaman Pidana	
				Penjara	Denda
1	Secara sengaja dan tanpa hak mengakses komputer milik orang lain dengan cara apapun	30 ayat 1	46 ayat 1	6 tahun	Rp 600.000.000
2	Secara sengaja dan tanpa hak mengakses komputer milik orang lain dengan cara apapun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau dokumen elektronik	30 ayat 2	46 ayat 2	7 tahun	Rp 700.000.000
3	Secara sengaja dan tanpa hak mengakses komputer milik orang lain dengan cara apapun dengan melanggar, menerobos, melampaui atau menjebol sistem pengaman	30 ayat 3	46 ayat 3	8 tahun	Rp 800.000.000
4	Secara sengaja dan tanpa hak melakukan intersepsi atau penyadapan atas informasi elektronik dan/ atau dokumen elektronik dalam suatu komputer dan/atau sistem elektronik tertentu milik orang lain	31 ayat 1	47	10 tahun	Rp 800.000.000
5	Secara sengaja dan tanpa hak melakukan intersepsi yang tidak bersifat publik dari, ke, dan di dalam suatu komputer milik orang lain yang	31 ayat 2	47	10 tahun	Rp 800.000.000

	tidak menyebabkan perubahan atau adanya perubahan, dan/atau penghentian informasi elektronik yang sedang ditransmisikan				
6.	Secara sengaja dan tanpa hak mengubah, menambah, mengurangi,menghilangkan, memindahkan suatu informsi elektronik dan/atau dokumen elektronik milik orang lain atau publik	32 ayat 1	48 ayat 1	8 tahun	Rp 2 M
7	Secara sengaja dan tanpa hak memindahkan informasi elektronik dan/ atau dokumen elektronik kepada sistem elektronik orang lain yang tidak berhak	32 ayat 2	48 ayat 2	9 tahun	Rp 3 M
8	Sebagaimana ayat 1 dan 2 yang berakibat terbukanya suatu informasi elektronik dan/ atau dokumen elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya	32 ayat 3	48 ayat 3	10 tahun	Rp 5 M
9	Secara sengaja dan tanpa hak melakukan tindakan yang berakibat terganggunya sistem elektronik dan/atau mengakibatkan sistem elektronik menjadi tidak bekerja sebagaimana mestinya	33	49	10 tahun	Rp 10 M
10	Secara sengaja dan tanpa hak melakukan	35	51 ayat 1	12 tahun	Rp 12 M

	manipulasi, penciptaan, perubahan, penghilangan, pengrusakan informasi elektronik dan/atau dokumen elektronik dengan tujuan agar informasi elektronik dan/ atau dokumen elektronik tersebut dianggap seolah-olah data otentik

Sumber: Bahan Hukum Primer Diolah, 2009

BAB III

METODE PENELITIAN

A Jenis Penelitian

Penelitian ini menggunakan tipe penelitian yuridis normatif yaitu penelitian yang difokuskan untuk mengkaji penerapan kaidah-kaidah atau norma-norma dalam hukum positif.[69] Dalam penelitian ini, peneliti mengkaji masalah pengaturan kualifikasi perbuatan dalam hubungan dengan kebijakan kriminal dan pengaturan ancaman pidana dalam hubungan dengan kebijakan penal dari kejahatan komputer menurut Kitab Undang-Undang Hukum Pidana dan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

B. Pendekatan Penelitian

Pendekatan yang digunakan dalam menganalisa penelitian ini adalah dengan menggunakan pendekatan perundang-undangan atau *statute approach*.

Pendekatan perundang-undangan adalah pendekatan yang melakukan pengkajian peraturan perundang-undangan yang berhubungan dengan sentral penelitian.[70] Dalam penelitian ini, penulis menggunakan pendekatan perundang-undangan karena dalam penelitian tentang kejahatan komputer ini penulis akan

---

69 Johnny Ibrahim, *Teori dan Metodologi Penelitian Hukum Normatif*, Bayumedia, Malang, 2007, hal 295

70 *Ibid*, hal 295

melakukan analisa terkait dengan pengaturan kualifikasi perbuatan dalam hubungan dengan kebijakan kriminal dari kejahatan komputer menurut KUHP dan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik serta melakukan analisa terkait dengan pengaturan ancaman pidana sebagai bentuk kebijakan penal dari kejahatan komputer menurut Kitab Undang-Undang Hukum Pidana dan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

C. Jenis dan Sumber Bahan Hukum

1. Jenis bahan hukum

Jenis bahan hukum menitikberatkan pada data sekunder. Data sekunder dalam penelitian ini terdiri dari bahan hukum primer, sekunder dan tersier.

a. Bahan hukum primer

Bahan hukum primer adalah bahan hukum yang terdiri dari aturan hukum yang diurut berdasarkan hierarki. Adapun yang menjadi bahan hukum primer adalah:

1) Undang-Undang Dasar 1945
2) Kitab Undang-Undang Hukum Pidana yang terdiri dari Pasal 112, 113, 114, 167, 263, 322, 323, 362, 372, 406, 431, dan 551 KUHP
3) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang terdiri dari Pasal 30, 31 ayat 1 dan 2, 32,

33, dan Pasal 35. Ketentuan pidana diatur dalam Pasal 46, 47, 48, 49 dan 51 ayat 1

4) Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi

5) Undang-Undang Nomor 20 tahun 2001 yang merupakan perubahan dari Undang-Undang Nomor 31 tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi

6) Undang-Undang Nomor 19 Tahun 2002 tentang Hak Cipta

b. Bahan hukum sekunder

Bahan hukum sekunder adalah bahan hukum yang merupakan penunjang dari penelitian yaitu:

1) Penjelasan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

2) Buku literatur terkait dengan kejahatan komputer

3) Makalah, skripsi, tesis, disertasi yang terkait dengan kejahatan komputer

4) Pendapat para ahli

c. Bahan hukum tersier

Bahan hukum tersier adalah bahan hukum yang memberikan pertunjuk atau penjelasan yang bermakna terhadap bahan hukum primer dan sekunder. Bahan hukum yang digunakan adalah:

1) Kamus hukum

2) Kamus besar Bahasa Indonesia

3) Internet

2. Sumber Bahan Hukum

Sumber bahan hukum dalam penelitian ini terdiri dari bahan hukum primer, sekunder dan tersier, yaitu:

a. Bahan hukum primer

Bahan hukum primer adalah bahan hukum yang terdiri dari aturan hukum yang diurut berdasarkan hierarki. Adapun yang menjadi bahan hukum primer adalah:

1) Undang-Undang Dasar 1945
2) Kitab Undang-Undang Hukum Pidana yang terdiri dari Pasal 112, 113, 114, 167, 263, 322, 323, 362, 372, 406, 431, dan 551 KUHP
3) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang terdiri dari Pasal 30, 31 ayat 1 dan 2, 32, 33, dan Pasal 35. Ketentuan pidana diatur dalam Pasal 46, 47, 48, 49 dan 51 ayat 1
4) Undang-Undang Nomor 36 Tahun1999 tentang Telekomunikasi
5) Undang-Undang Nomor 20 tahun 2001 yang merupakan perubahan dari Undang-Undang Nomor 31 tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi
6) Undang-Undang Nomor 19 Tahun 2002 tentang Hak Cipta

b. Bahan hukum sekunder

Bahan hukum sekunder adalah bahan hukum yang merupakan penunjang dari penelitian yaitu:

1) Penjelasan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
2) Buku literatur yang terkait dengan kejahatan komputer
3) Makalah, skripsi, tesis, disertasi yang terkait dengan kejahatan komputer
4) Pendapat para ahli

c. Bahan hukum tersier

Bahan hukum tersier adalah bahan hukum yang memberikan pertunjuk atau penjelasan yang bermakna terhadap bahan hukum primer dan sekunder. Bahan hukum yang digunakan adalah:

1) Kamus hukum
2) Kamus besar Bahasa Indonesia
3) Internet

D. Teknik Penelusuran Bahan Hukum

Teknik penelusuran bahan hukum penelitian dilakukan melalui studi kepustakaan dan dokumentasi. Studi kepustakaan dan dokumentasi dilakukan dengan

menggunakan inventarisasi dari bahan hukum primer yang ditunjang dengan beberapa bahan hukum sekunder dan tersier.

Adapun studi kepustakaan yang dilakukan dari bahan hukum primer, sekunder maupun tersier adalah dengan mencari dan mengumpulkan buku-buku, literatur, artikel, tesis, disertasi, pendapat para ahli, browsing internet serta dokumen yang relevan dengan pokok masalah dari penelitian yaitu tentang kejahatan komputer. Setelah penelusuran pustaka dilakukan, penulis melanjutkan dengan melakukan pengkajian terhadap undang-undang yang berkaitan dengan penulisan yang kemudian dilakukan analisis terhadap undang-undang yang berkaitan dengan kejahatan komputer tersebut.

E. Teknik Analisa Bahan Hukum

Teknik analisa bahan hukum dalam penelitian ini ialah menggunakan metode interpretasi atau penafsiran pasal-pasal dalam KUHP dan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik terkait dengan pengaturan kualifikasi perbuatan dan pengaturan ancaman pidana dalam kejahatan komputer. Analisa bahan hukum yang dilakukan melalui beberapa tahap yaitu:

1. Tahap identifikasi

   Dalam tahap ini yang dilakukan adalah mengiventarisasi bahan-bahan hukum tentang kejahatan komputer.

2. Tahap deskripsi

Dalam tahap ini yang dilakukan adalah melakukan penganalisaan terkait dengan pengaturan kualifikasi perbuatan dalam hubungan dengan kebijakan kriminal dan pengaturan ancaman pidana dalam hubungan dengan kebijakan penal dari kejahatan komputer menurut Kitab Undang-Undang Hukum Pidana dan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

3. Tahap analisis fungsional

   Dalam tahap ini yang dilakukan adalah melakukan penarikan kesimpulan dari tahapan-tahapan yang sebelumnya.

BAB IV

PEMBAHASAN

A. Pengaturan Kualifikasi Perbuatan Berkaitan dengan kebijakan Kriminal dari Kejahatan Komputer menurut KUHP dan Undang-Undang ITE

Dalam pembahasan yang berkaitan dengan rumusan masalah yang pertama yaitu tentang pengaturan kualifikasi perbuatan dalam hubungan kebijakan kriminal terkait dengan kejahatan komputer menurut KUHP dan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), maka terlebih dahulu penulis mengambil pengertian dari kejahatan komputer. Dalam kajian pustaka telah dipaparkan beberapa pengertian dari kejahatan komputer, akan tetapi sampai saat ini belum ada kesepakatan yang pasti tentang pengertian kejahatan komputer akan tetapi ada kesamaan pengertian universal mengenai kejahatan komputer. Dari beberapa pengertian kejahatan komputer yang ada, penulis menggunakan pendapat dari Andi Hamzah.

Menurut Andi Hamzah yang dimaksud dengan kejahatan komputer adalah kejahatan di bidang komputer secara umum yang dapat diartikan sebagai penggunaan komputer secara ilegal.[71] Dari pengertian tersebut, Andi Hamzah memperluas pengertian kejahatan komputer yaitu sebagai aktivitas tidak sah yang memanfaatkan

---

71 Andi Hamzah, *loc cit*

komputer untuk tindak pidana. Sekecil apapun dampak atau akibat yang ditimbulkan dari suatu penggunaan komputer yang tidak sah merupakan suatu kejahatan.

Dari pengertian kejahatan komputer tersebut, saat ini penulis akan memaparkan beberapa bentuk kejahatan komputer yang akan dibahas kualifikasi perbuatannya menurut KUHP dan UU ITE. Adapun bentuk dari kejahatan komputer yaitu:

a) *Data leakage*
b) *Hacking*
c) Data *diddling*
d) *Joy Computing*
e) *The Trojan Horse*
f) Penyia-nyiaan data komputer.

1. *Data Leakage*

Data leakage merupakan suatu tindakan membocorkan data rahasia yang dilakukan dengan cara menulis data-data rahasia dalam kode-kode tertentu sehingga data tersebut dapat dibawa keluar dari sistem komputer tanpa diketahi oleh pihak yang bertanggungjawab terhadap data tersebut.

Data, dokumen atau berbagai bentuk informasi lainnya seringkali harus dijaga kerahasiaannya. Hal ini dimaksudkan untuk mencegah pemanfaatan data atau informasi oleh pihak-pihak yang tidak bertanggungjawab. Berkaitan dengan hal tersebut, maka perlindungan terhadap kerahasiaan data atau informasi perlu dilakukan

dengan menetapkan ancaman pidana bagi pelaku pembocoran. Pembocoran data komputer dapat berupa rahasia negara, rahasia perusahaan, data yang dipercayakan kepada seseorang dan data dalam situasi tertentu.

a) Ketentuan menurut KUHP

Dalam KUHP, bentuk kejahatan *data leakage* dapat dikategorikan dalam tindak pidana terhadap keamanan negara yaitu Pasal 112 KUHP tentang pembocoran rahasia negara, Pasal 113 dan 114 KUHP pembocoran rahasia pertahanan dan keamanan negara.

Dalam menerapkan Pasal 112, 113 dan 114 KUHP terkait dengan pembocoran rahasia negara, maka terlebih dahulu penulis akan menyusun unsur obyektif dan subyektif dari ketiga pasal tersebut.

a. Unsur objektif Pasal 112 KUHP

- mengumumkan
- surat-surat atau benda-benda atau keterangan-keterangan
- yang diketahui bahwa harus dirahasiakan
- untuk kepentingan negara
- memberitahukan kepada negara asing
- memberikan

b. Unsur subjektif

- dengan sengaja

c. Unsur objektif Pasal 113 KUHP

- mengumumkan
- memberitahukan kepada orang yang tidak berwenang mengetahui
- menyerahkan
- surat-surat
- peta-peta
- rencana-rencana
- gambar-gambar
- benda-benda
- yang bersifat rahasia
- bersangkutan dengan pertahanan atau keamanan Indonesia
- terhadap serangan dari luar
- yang isinya, bentuk atau susunan benda-benda diketahui olehnya

d. Unsur subjektif

- dengan sengaja

e. Unsur objektif Pasal 114 KUHP

- menyebabkan surat-surat atau benda-benda rahasia
- yang tersebut Pasal 113
- menyimpan menjadi tugasnya
- menaruh
- diketahui oleh umum

- mengenai bentuk dan susunan

- untuk seluruh dan sebagian atau oleh orang yang tidak wenang mengetahui

f. Unsur subjektif

- kealpaan

Dalam rumusan suatu tindak pidana yang terdapat dalam Pasal 112, 113 dan Pasal 114 KUHP, disebutkan adanya kata "barangsiapa". Rumusan kata "barangsiapa" tersebut memiliki maksud bahwa rumusan tindak pidana itu berlaku pada setiap orang. Jadi siapapun yang melanggar ketentuan dalam Pasal 112, 113 dan 114 KUHP dapatlah dikenakan pasal tersebut.

Selain unsur subjek hukum, dalam rumusan tindak pidana terdapat juga unsur tingkah laku atau perbuatan. Unsur tingkah laku merupakan unsur mutlak tindak pidana. Tingkah laku dalam tindak pidana terdiri dari tingkah laku aktif yaitu suatu bentuk tingkah laku yang untuk mewujudkannya diperlukan wujud gerakan tubuh, misalnya mengambil atau memalsu. Selain itu, terdapat juga tingkah laku pasif. Tingkah laku pasif merupakan tingkah laku yang membiarkan atau suatu bentuk tingkah laku yang tidak melakukan aktivitas tertentu, misalnya tidak memberikan pertolongan, membiarkan.

Berdasarkan atas pembagian dalam unsur objektif dan subjektif dalam Pasal 112, 113 dan 114 KUHP, maka dapat disusun unsur tingkah laku atau perbuatan yang dilakukan yaitu:

- Memberitahukan
- Memberikannya

- Mengumumkan
- Menyerahkan
- Menyimpan
- Menaruhnya

Dari beberapa tingkah laku atau perbuatan yang dituliskan dalam ketiga pasal tersebut, dapat diketahui bahwa tingkah laku yang dilakukan termasuk dalam tingkah laku aktif. Artinya perbuatan yang dilakukan itu sudah merupakan suatu tindakan yang berwujud aktif.

Selain unsur objektif, dalam pembagian rumusan terdapat unsur subjektif yang artinya berkaitan dengan sikap batin seseorang dalam melakukan suatu perbuatan. Sesuai dengan Pasal 112 dan Pasal 113 KUHP yang menjadi unsur subjektifnya adalah adanya kesengajaan. Dalam doktrin hukum pidana, dikenal adanya tiga bentuk kesengajaan yaitu:[72]

1) kesengajaan sebagai maksud atau tujuan

   Adalah dengan menghendaki untuk mewujudkan suatu perbuatan atau tindak pidana aktif, menghendaki untuk tidak berbuat dan atau juga menghendaki timbulnya akibat dari perbuatan itu

2) kesengajaan sebagai kepastian

   Adalah kesadaran seseorang terhadap suatu akibat yang menurut akal orang pada umumnya pasti terjadi oleh dilakukannya suatu perbuatan

72 Adami Chazawi, *Pelajaran Hukum Pidana*, PT. RajaGrafindo Persada, Jakarta, 2005, hal 96

tertentu. Apabila perbuatan tertentu disadarinya pasti menimbulkan akibat yang tidak dituju tetap dilakukan juga, maka disini terjadi kesengajaan sebagai kepastian.

3) kesengajaan sebagai kemungkinan

Adalah kesengajaan untuk melakukan perbuatan yang diketahuinya bahwa ada akibat lain yang mungkin dapat timbul yang ia tidak inginkan dari perbuatan, namun begitu besarnya kehendak untuk mewujudkan perbuatan, ia tidak mundur dan siap mengambil risiko untuk melakukan perbuatan itu.

Kesengajaan sebagai kepastian dan kesengajaan sebagai kemungkinan berhubungan erat dengan pengetahuan seseorang tentang sekitar perbuatan yang akan dilakukan beserta akibatnya. Secara logika maka unsur kesengajaan yang terdapat dalam Pasal 112 dan Pasal 113 KUHP merupakan suatu unsur kesengajaan sebagai kepastian dan kemungkinan. Hal ini berarti, dengan sengaja melakukan perbuatan mengumumkan, memberitahukan, menyerahkan dan memberikan surat-surat, berita-berita atau keterangan-keterangan kepada negara asing yang seharusnya dirahasiakan. Dari unsur kesengajaan tersebut, maka secara pasti negara asing dapat mengetahui isi dari surat-surat, berita-berita atau keterangan-keterangan tersebut.

Selain itu, akibat lain dari kesengajaan melakukan perbuatan mengumumkan, memberitahukan, menyerahkan dan memberikan surat-surat, berita-berita atau keterangan-keterangan kepada negara lain yang seharusnya dirahasiakan juga dapat muncul. Artinya dari kesengajaan tersebut dapat timbul kemungkinan akibat lain yang

tidak diinginkan, misalnya dengan adanya perbuatan mengumumkan surat-surat itu, maka negara lain dapat mengambil suatu informasi dari isi surat itu yang dapat digunakan untuk menghancurkan bangsa Indonesia.

Dalam Pasal 114 KUHP, yang menjadi unsur subjektifnya adalah karena kealpaannya dalam menyimpan atau menaruh benda-benda rahasia yang tersebut dalam Pasal 113 KUHP menyebabkan dapat diketahui oleh umum mengenai bentuk dan susunannya untuk seluruh atau sebagian. Dalam pandangan yang subjektif mengenai suatu kealpaan atau kelalaian menitikbertakan pada syarat adanya sikap batin seseorang dalam hubungannya dengan perbuatan dan akibat perbuatan yang dapat dipersalahkan sehingga ia dapat dibebani tanggung jawab atas perbuatan itu.[73]

Kelalaian dalam Pasal 114 KUHP merupakan suatu hubungan batin dengan akibat yang ditimbulkan. Sikap batin dalam kelalaian yang hubungannya dengan akibat perbuatan dapat terletak dalam dua hal yaitu:[74]

1) terletak pada ketiadaan pikir sama sekali

   Artinya alam batin orang tersebut sama sekali tidak memikirkan bahawa dari perbuatan yang hendak dilakukan itu dapat menimbulkan suatu akibat yang dilarang undang-undang

2) terletak pada pemikiran bahwa akibat tidak akan terjadi

   Artinya kesalahan tersebut terletak pada sikap batin yang sudah memikirkan tentang kemungkinan timbulnya akibat terlarang, namun

73 *Ibid*, hal 100

74 *Ibid*, hal 101-102

dalam alam batinnya begitu percaya bahwa akibat itu tidak akan timbul. Ternyata setelah mewujudkan perbuatan, akibat itu benar-benar timbul. Jadi dalam hal ini merupakan kesalahan dalam berpikir.

Berkaitan dengan Pasal 114 KUHP, maka kealpaan tersebut termasuk dalam kealpaan yang terletak pada pemikiran bahwa akibat tidak akan terjadi. Artinya seseorang tersebut sebenarnya sudah mengetahui bahwa apabila ia melakukan suatu kesalahaan atau kelalaian atau kealpaan dalam menjaga surat-surat, benda-benda atau keterangan-keterangan yang seharusnya dijaga, maka surat, benda atau keterangan tersebut akan dapat diketahui oleh umum dan akibat dari kelalaian tersebut ia dapat dikenakan ancaman pidana.

Dalam rumusan pasal KUHP yang berkaitan dengan kejahatan komputer dalam hal pembocoran data atau *data leakage*, tidak disebutkan kata "data komputer" atau informasi yang dihasilkan oleh komputer akan tetapi yang menjadi objek dalam tindak pidana adalah surat-surat, berita-berita atau keterangan-keterangan. Berdasarkan atas objek tersebut, maka dalam hal kebijakan penerapan hukum yang dilakukan adalah dengan menggunakan pendekatan interpretasi ekstensif. Penafsiran ekstensif adalah memberikan penafsiran dengan memperluas kata-kata dalam ketentuan undang-undang sehingga peristiwa tersebut dapat dimasukkan.

Dalam melakukan penafsiran ektensif tersebut, penafsiran yang diperluas adalah dengan memperluas pengertian "benda-benda" dalam rumusan pasal tersebut. Perluasan kata "benda-benda" tersebut meliputi juga data komputer. Selain itu cara lain adalah dengan melakukan penafsiran terhadap kata "keterangan-keterangan"

yang meliputi informasi yang dihasilkan oleh komputer. Dengan melakukan penafsiran terhadap beberapa kata yang terdapat dalam pasal tersebut, maka Pasal 112, 113 dan 114 KUHP dapatlah dimasukkan dalam pasal yang terkait dengan kejahatan komputer.

Selain dengan melakukan penafsiran dalam beberapa kata, perlu juga dilakukan pembuktian dalam kasus pembocoran data atau data *leakage* tersebut. Pembuktian yang perlu dilakukan dalam kasus tersebut adalah sejauh mana bocornya data atau informasi yang disampaikan kepada pihak-pihak yang tidak berwenang.

Suatu data tertentu dapat menjadi kepentingan ekonomi artinya apabila data-data yang berkaitan dengan rahasia suatu perusahaan jatuh pada pihak ketiga atau saingannya, maka hal itu akan merugikan salah satu pihak. Berkaitan dengan pembocoran rahasia perusahaan, dalam KUHP diatur di Pasal 323 KUHP. Berkaitan dengan kebocoran data yang menyangkut profesi atau jabatan, misal: dokter,advokat, notaris diatur dalam Pasal 322 KUHP.

Menurut Kalpersen dan Keijezer yang dikutip oleh Andi Hamzah, menyatakan bahwa dalam Pasal 323 KUHP terkait dengan pembukaan rahasia perusahaan dirasa kurang lengkap. Hal ini disebabkan karena:[75]

1) Dalam rumusan pasal tersebut, yang diancam pidana hanya perbuatan memberitahukan data, bukan mencari tahu data bagi yang tidak berwenang.

75 Andi Hamzah, cetakan kedua, *op cit*, hal 37

2) Mencari tahu dengan mengumumkan oleh pihak ketiga di luar perusahaan atau spionage tidak termasuk dalam pasal ini

3) Perbuatan yang diancam dengan pidana hanya yang disengaja, sedangkan perbuatan yang culpa atau karena kealpaan berakibat terbukanya rahasia tidak diancam dengan pidana.

Dalam hal pembocoran data suatu perusahaan yang menjadi rahasia perusahaan, seperti karyawan perusahaan atau mantan karyawan perusahaan membuka file perusahaan dan memberitahukan pada pihak lain yang tidak wenang mengetahui, maka ketentuan Pasal 323 KUHP dapat diterapkan. Unsur perbuatan yang dapat dikenakan pidana adalah memberitahukan hal-hal khusus yang menjadi rahasia dari perusahaan tersebut.

Dalam Pasal 322 KUHP yang terkait dengan rahasia profesi, maka unsur-unsur objektif dan subjektif adalah sebagai berikut:

a. Unsur objektif

- membuka rahasia
- yang wajib disimpannya
- karena jabatan atau pencahariannya
- baik sekarang, maupun yang terdahulu

b. Unsur subjektif

- dengan sengaja

Unsur perbuatan yang terdapat dalam Pasal 322 KUHP yang dapat dikenai ancaman pidana hanyalah perbuatan membuka rahasia yang dilakukan dengan

sengaja, artinya apabila perbuatan tersebut dilakukan dengan kealpaan maka tidak dikenai ancaman pidana. Selain itu, perbuatan lain seperti menyimpan, mengumumkan atau mengetahui secara tidak sah data yang bersifat pribadi tidak diatur dalam hukum pidana. Apabila penyimpanan data pribadi yang seharusnya tidak diketahui oleh pihak ketiga akan tetapi dapat diketahui oleh pihak ketiga yang tidak berwenang, maka perbuatan tersebut dapat diajukan oleh pihak yang dirugikan melalui jalur hukum perdata.[76]

Dalam Pasal 322 dan 323 KUHP dalam ayat ke-2 menyebutkan bahwa kejahatan pembocoran rahasia profesi dan rahasia perusahaan hanya dapat dituntut apabila ada pengaduan dari orang atau pengurus perusahaan yang merasa dirugikan. Berkaitan dengan hal ini, maka Pasal 322 dan 323 KUHP merupakan suatu delik aduan, artinya apabila tidak ada aduan dari pihak-pihak tersebut, maka perbuatan membocorkan rahasia tidak dapat dituntut.

Dalam kasus pembocoran data, masih terdapat satu bentuk kasus pembocoran data namun dalam suasana atau situasi tertentu. Menurut Nico Keijzer yang dikutip oleh Andi Hamzah berpendapat bahwa yang dimaksud dengan kebocoran data dalam situasi tertentu adalah

> suatu perbuatan yang tanpa wewenangnya berusaha memperoleh data dari pihak lain yang bersifat rahasia dengan jalan menghalangi atau merintangi atau tidak menyampaikan data yang dimaksud yang seharusnya diserahkan kepada pihak yang berhak atas data tersebut.[77]

76 *Ibid*, hal 38

77 *Ibid*, hal 38

Hal tersebut dapat terjadi pada data komputer yang tersimpan dalam berbagai media penyimpanan, misalnya seorang ekspeditur biro pengiriman barang mendapat tugas untuk mengirim paket yang berisi data penting dan bersifat rahasia pada suatu instansi, namun sebelum disket tersebut sampai pada pihak yang dituju, petugas tersebut membuka *file-file* yang ada dalam disket tersebut untuk mengetahui isinya. Terhadap kasus tersebut dapat diterapkan ketentuan Pasal 431 KUHP dengan menafsirkan *file* sebagai surat atau disket sebagai barang tertutup.

Rumusan dalam Pasal 431 KUHP, merupakan rumusan pasal yang ditujukan pada seorang pejabat suatu lembaga pengangkutan umum. Artinya, rumusan tindak pidana ini tidak ditujukan untuk semua orang melainkan hanya kepada orang tertentu saja yaitu pejabat suatu lembaga angkutan umum. Hal itu terbukti dengan adanya pencantuman kualitas subjek hukum tindak pidana.

Dalam Pasal 431 KUHP, penerapan unsur perbuatan yang diatur adalah membawa paket atau surat yang tertutup, memeriksa isinya atau memberitahukan isinya kepada orang lain. Berdasarkan atas ketiga bentuk perbuatan itu, maka dapat diketahui bahwa perbuatan yang dilakukan termasuk dalam tingkah laku aktif.

Selain unsur perbuatan atau tingkah laku, dalam unsur subjektif mencantumkan adanya unsur kesengajaan dan melawan hak. Pencantuman secara tegas unsur sifat melawan hukum dalam suatu rumusan tindak pidana didasarkan pada suatu alasan tertentu seperti yang dijelaskan dalam penjelasan WvS Belanda yaitu adanya kekhawatiran bagi pembentuk undang-undang apabila tidak dimuatnya unsur melawan hukum, maka akan dapat dipidana pula perbuatan lain yang sama,

namun tidak bersifat melawan hukum.[78] Melawan hukum merupakan suatu sifat tercela atau terlarang yang mana sifat tercela tersebut bersumber dari undang-undang atau melawan hukum formil dan bersumber dari masyarakat atau melawan hukum materiil.

Berdasarkan atas penjelasan yang ada, maka unsur melawan hukum dalam rumusan Pasal 431 KUHP ini menekankan pada perbuatan dengan sengaja dan melawan hukum secara formil atau tercantum dalam undang-undang membuka paket atau surat yang tertutup itu dan memeriksa isinya atau memberitahukan isinya kepada orang lain yang tidak berwenang. Perbuatan memeriksa isi surat atau paket ini juga dapat dikatakan bukan suatu perbuatan melawan hukum apabila dilaksanakan sesuai dengan aturan yang benar, misalnya memeriksa isi paket tersebut apakah membahayakan bagi keselamatan orang lain atau tidak atau isinya berupa bom atau benda-benda yang berbahaya. Dalam pelaksaanaan pemeriksaan paket tentulah harus dilakukan oleh pejabat yang berwenang.

Atas perbuatan lain yang sama itulah, maka dalam rumusan Pasal 431 KUHP mencantumkan unsur melawan hukum, agar pejabat yang melakukan kewajiban memeriksa isi paket atau surat yang menjadi kewajibannya itu tidak dipidana. Perlu ditekankan bahwa yang dapat dipidana adalah pejabat yang secara sengaja dan melawan hukum. Pejabat atau petugas yang melakukan tugas serta kewajibannya sesuai dengan undang-undang dan tidak melawan hukum tidak dapat dipidana.

78 Adami Chazawi, *op cit* hal 87

b) Ketentuan menurut Undang-Undang ITE

Dalam KUHP telah dirumuskan beberapa pasal yang berkaitan dengan kejahatan komputer tentang pembocoran rahasia. Dalam Undang-Undang ITE, terdapat juga pasal yang mengatur tentang perbuatan yang mengakibatkan terbukanya suatu informasi elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya. Perbuatan tersebut diatur dalam Pasal 32 ayat 3.

Unsur-unsur perbuatan yang terdapat dalam Pasal 32 ayat 3 adalah sebagai berikut:

a. Unsur objektif

- perbuatan yang dimaksud pada ayat 1
- mengakibatkan terbukanya
- informasi elektronik dan/atau dokumen elektronik
- bersifat rahasia
- menjadi dapat diakses
- oleh publik
- dengan keutuhan data yang tidak sebagaimana mestinya

b. Unsur subjektif

- setiap orang dengan sengaja dan tanpa hak atau melawan hukum

Dilihat dari unsur kualitas subjek hukum tindak pidana, rumusan Pasal 32 ayat 3 ini diberlakukan kepada semua orang tanpa terkecuali. Hal ini terbukti dengan adanya

pencantuman kata "setiap orang". Kata "setiap orang" sering digunakan dalam tindak pidana khusus yang memiliki arti yang sama dengan "barangsiapa".

Ketentuan tentang jenis perbuatan *data leakage* dalam Undang-Undang ITE diatur dalam Pasal 32 ayat 3, yang mana dalam rumusannya disebutkan adanya suatu tindakan yang mengakibatkan terbukanya informasi elektronik tersebut. Dalam rumusan tindak pidana terdapat unsur akibat konstitutif. Unsur akibat konstitutif terdapat pada:[79]

1. Tindak pidana yang akibat menjadi syarat selesainya tindak pidana

   Artinya, suatu akibat timbul bukan untuk menjadi alasan pemberat pidana melainkan syarat selesainya tindak pidana. Apabila unsur akibat tidak muncul, maka tindak pidana itu tidak terjadi yang terjadi hanyalah percobaan.
2. Tindak pidana yang mengandung unsur akibat sebagai syarat pemberat pidana

   Artinya apabila syarat akibat tidak timbul, maka tidak terjadi percobaan tindak pidana melainkan terjadinya pidana selesai.
3. Tindak pidana yang mana akibat merupakan syarat dipidananya pembuat

   Artinya tanpa timbulnya akibat maka perbuatan yang dirumuskan dalam undang-undang tidak dipidana. Pidana akan dilakukan apabila akibat terlarang telah timbul.

Dilihat dari beberapa rumusan unsur akibat konstitutif, maka rumusan Pasal 32 ayat 3 Undang-Undang ITE termasuk dalam unsur akibat konstitutif yang kedua

79 *Ibid,* hal 104

yaitu tindak pidana yang mengandung unsur akibat sebagai syarat pemberat pidana. Unsur akibat dalam Pasal 32 ayat 3 mengandung unsur pemberat pidana karena apabila akibat terbukanya suatu informasi elektronik dan/atau dokumen eletronik yang bersifat rahasia kepada publik dengan keutuhan data yang tidak sebagaimana mestinya itu tidak muncul, maka tindak pidana pembocoran suatu data bukan merupakan suatu percobaan untuk membocorkan suatu data, melainkan tindak pidana lain yang muncul yaitu tindak pidana yang sesuai dengan rumusan Pasal 32 ayat 1.

Penerapan Pasal 32 ayat 3 merupakan suatu unsur pemberat pidana karena dengan perbuatan yang dilakukan dalam Pasal 32 ayat 1 yang diantaranya adalah menambah, menghilangkan, menyembunyikan suatu informasi elektronik dan/atau dokumen elektronik yang mana akibat yang ditimbulkan adalah terbukanya suatu informasi elektronik dan/atau dokumen elektronik yang bersifat rahasia sehingga dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya berakibat pemberatan pidana dalam kebijakan penal. Selain itu, apabila unsur akibat pemberat pidana itu muncul maka jenis kejahatan *data leakage* dapat dikenai dengan Pasal 32 ayat 3.

Dalam rumusan Pasal 32 ayat 3 Undang-Undang ITE, jenis kejahatan *data leakage* bukan berasal dari perbuatan yang secara aktif atau sengaja dilakukan seperti dalam beberapa pasal dalam KUHP, melainkan akibat dari perbuatan itulah yang menyebabkan terjadinya pembocoran suatu data atau terbukanya suatu data. Adapun perbuatan yang berakibat terbukanya suatu informasi elektronik dan/atau dokumen elektronik adalah:

- mengubah
- menambah
- mengurangi
- melakukan transmisi
- merusak
- menghilangkan
- memindahkan
- menyembunyikan

Dari kedelapan unsur perbuatan yang ada, perbuatan dalam Undang-Undang ITE termasuk dalam jenis perbuatan atau tingkah laku yang aktif.

Berkaitan dengan objek hukum tindak pidana, dalam Pasal 32 ayat 3 disebutkan bahwa yang menjadi objek adalah informasi elektronik dan/atau dokumen eletronik. Menurut Pasal 1 ayat 1 yang dimaksud dengan informasi elektronik adalah

> "Satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, electronic data interchange (EDI), surat elektronik (electronic mail), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya."

Menurut Pasal 1 ayat 4 yang dimaksud dokumen elektronik adalah

> "Setiap informasi elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya yang dapat dilihat, ditampilkan, dan/atau didengar melalui komputer atau sistem elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, kode akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya."

Dengan rumusan objek yang sudah dituliskan dalam Pasal 1 ayat 1 dan 4, maka dapat diketahui bahwa data-data komputer jenis apapun sudah tercantum didalamnya. Tidak hanya yang berbentuk tulisan atau yang terlihat saja melainkan bentuk-bentuk lain seperti suara, gambar maupun simbol apapun yang memiliki arti sudah termasuk dalam pasal tersebut. Jadi dalam penafsiran rumusan pasal dapat langsung dilakukan dengan menggunakan penafsiran autentik atau resmi sesuai dengan kata-kata yang terdapat dalam undang-undang tersebut.

2. Hacking

Dalam kajian pustaka telah dipaparkan tentang pengertian dari jenis kejahatan hacking dan proses atau cara penyusupan yang dilakukan oleh *hacker*. Dalam KUHP jenis kejahatan *hacking* dimasukkan dalam Pasal 167 dan Pasal 551 KUHP sedangkan dalam Undang-Undang ITE dimasukkan dalam Pasal 30 dengan ketentuan pidana yang diatur dalam Pasal 46 KUHP.

a. Ketentuan menurut KUHP

Menurut KUHP, jenis kejahatan *hacking* termasuk dalam rumusan Pasal 167 dan 551 KUHP yang mana rumusan pasal ini ditujukan bagi setiap orang tanpa ada kecuali. Hal ini terlihat dalam rumusan pasal dicantumkan kata-kata “barangsiapa” yang berarti ditujukan kepada siapapun juga.

Dalam Pasal 167 KUHP dan Pasal 551 KUHP, melihat dari unsur tingkah laku atau perbuatan yang dilakukan dapat diketahui bahwa perbuatan yang tercantum dalam kedua pasal itu adalah:

a. Pasal 167 ayat 1

- masuk dengan memaksa;
- ke dalam rumah atau ruangan yang tertutup atau pekarangan yang dipakai oleh orang lain;
- atau sedang di situ dengan tidak ada haknya;
- tidak segera pergi dari tempat itu;
- atas permintaan orang yang berhak atau atas nama orang yang berhak

b. ayat 2

- barangsiapa;
- masuk;
- dengan memecah atau memanjat, memakai kunci palsu, perintah palsu, atau pakaian dinas palsu;
- atau barangsiapa;
- dengan tidak setahu yang berhak;
- masuk ketempat yang tersebut

c. Pasal 551

- berjalan;
- berkendaraan
- di atas tanah yang oleh pemiliknya jelas dilarang untuk masuk

Dari kedua rumusan pasal tersebut, sebenarnya penggunaan Pasal 167 dan 551 KUHP kurang tepat untuk jenis kejahatan *hacking* sehingga tidak mutlak untuk

digunakan. Hal ini disebabkan karena dalam penafsiran bentuk perbuatan maupun objek adalah dengan menggunakan penafsiran analogi yang mana dalam melakukan suatu penafsiran tidaklah boleh dengan menggunakan penafsiran analogi.[80]

Penafsiran analogi dilakukan dalam menafsirkan beberapa perbuatan dan objek yang terdapat dalam kedua pasal ini. Unsur objek yang dianalogikan dalam rumusan pasal ini salah satunya adalah "rumah". Suatu bentuk kejahatan komputer adalah memasuki wilayah komputer orang lain yang mana dunia dalam komputer termasuk dalam dunia maya, sementara pengertian rumah merupakan suatu ruangan yang ada dalam kehidupan nyata atau terlihat oleh mata. Berkaitan dengan objek yang diatur dalam Pasal 167 dan 551 KUHP tersebut, tampak adanya usaha untuk memperluas pengertian dari rumah, pekarangan, ruangan atau tanah dengan melakukan penafsiran analogi.[81] Dalam penerapannya, penafsiran analogi sulit untuk diterapkan. Hal ini disebabkan karena dalam kejahatan komputer semua model kejahatannya adalah kejahatan yang bersifat maya atau tidak dapat terlihat oleh mata sehingga untuk menerapkan kedua pasal tersebut dalam jenis kejahatan *hacking* ini cukuplah sulit.

Selain dari unsur objek, dalam unsur perbuatan juga dilakukan penafsiran secara analogi, misalnya dalam Pasal 551 KUHP tentang berjalan atau berkendaraan di atas tanah orang lain. Penafsiran analogi dilakukan dalam menafsirkan kata "berjalan" yang disamakan dengan mengakses. Hal ini dirasa tidak sesuai karena

80 Al. Wisnubroto, *op cit* hal 77

81 Al. Wisnubroto, *op cit* hal 77

dalam dunia nyata perbuatan memasuki wilayah orang lain dapatlah dilihat dengan mata akan tetapi dalam dunia maya perbuatan mengakses atau memasuki wilayah orang lain atau sistem komputer orang lain semuanya serba maya.[82] Jadi dalam penafsirannya menggunakan penafsiran analogi yang sebenarnya kurang tepat dilakukan.

Berdasarkan atas penjelasan yang ada tentang penerapan pasal dalam KUHP tentang jenis kejahatan *hacking,* maka dapat dilihat bahwa sebenarnya dalam KUHP untuk tipe kejahatan *hacking* ini masih belum diatur secara jelas. Hal ini terbukti bahwa dalam penafsiran yang dilakukan baik dalam unsur perbuatan maupun objek menggunakan penafsiran secara analogi yang mana penafsiran analogi bukanlah suatu penafsiran yang benar dan tidak sesuai dengan asas legalitas yang terdapat dalam Pasal 1 ayat 1 KUHP.

b. Ketentuan menurut Undang-Undang ITE

Kejahatan komputer jenis *hacking* dalam Undang-Undang ITE diatur dalam Pasal 30 ayat 1 dan 3. Dalam unsur subjek hukumnya, rumusan pasal dalam Undang-Undang ITE dirumuskan untuk semua orang atau setiap orang tanpa terkecuali. Berkaitan dengan unsur melawan hukumnya, dalam Pasal 30 ini dirumuskan secara bersama unsur melawan hukum dan unsur kesengajaan. Hal dimaksudkan bahwa

82 *Ibid,* hal 77

unsur melawan hukum yang digunakan adalah unsur melawan hukum secara formil yang harus dibuktikan unsur melawan hukum dari perbuatan tersebut.

Berkaitan dengan kebijakan kriminal yang mana dalam kajian pustaka telah dipaparkan tentang pengertian kebijakan kriminal, maka dalam Undang-Undang ITE ini sudah muncul adanya unsur perbuatan baru yang lebih spesifik atau lebih jelas yang mana dalam KUHP belum diterapkan yaitu perbuatan mengakses komputer dan/ atau sistem elektronik. Dalam Pasal 1 ayat 15 dijelaskan bahwa yang dimaksud dengan akses adalah "Kegiatan melakukan interaksi dengan sistem elektronik yang berdiri sendiri atau dalam jaringan." Berdasarkan dari bentuk perbuatan itu, maka sudah dapat dilihat bahwa perbuatan yang dilakukan adalah secara nyata melakukan suatu kegiatan interaksi atau hubungan dalam suatu sistem elektronik. Jadi unsur perbuatan sudah dirumuskan secara jelas tanpa perlu adanya penafsiran analogi melainkan penafsiran yang digunakan adalah penafsiran autentik atau resmi.

Cara mengakses suatu komputer dan/atau sistem elektronik yang secara melawan hukum juga telah diatur dalam Pasal 30 ayat 3, yaitu dengan cara melanggar, menerobos, melampaui atau menjebol sistem pengaman. Jadi unsur cara untuk mewujudkan tindak pidana *hacking* pun juga sudah dicantumkan dalam rumusan pasal ini. Dengan rumusan yang lengkap diharapkan agar pelaku kejahatan komputer tidak dapat lepas dari ancaman pidana.

Dalam sistem objek suatu tindak pidana, Pasal 30 ayat 1 dan 3 mencantumkan bahwa yang menjadi objek dari kejahatan ini adalah komputer dan/atau sistem

elektronik. Dalam kajian pustaka telah dipaparkan tentang pengertian dari komputer sedangkan sistem elektronik menurut Pasal 1 ayat 5 adalah

> "Serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik."

Dengan pengertian yang ada maka dapat dilihat bahwa komputer dan/atau sistem elektronik merupakan objek yang dapat menjadi sasaran perangkat untuk dirusak atau dijebol dengan cara *hacking* tersebut. Dalam hal ini, objek dari suatu tindak pidana lebih terlihat secara khusus dan nyata yaitu komputer dan/atau sistem elektronik. Dengan adanya suatu bentuk objek yang dirumuskan secara nyata, maka tidak perlu adanya penafsiran secara analogi lagi yang mana akibat dari penafsiran tersebut adalah sulitnya untuk menjatuhkan suatu pidana pada kejahatan tersebut. Dengan adanya pencantuman objek secara khusus, maka jenis kejahatan *hacking* dapat dikenai Pasal 30 ayat 1 dan 3 Undang-Undang ITE karena dalam kejahatan *hacking* yang menjadi objek dari kejahatan tersebut adalah komputer dengan perbuatan menyambung atau menambah terminal baru secara melawan hukum. Jenis kejahatan ini sesuai dengan Pasal 30 ayat 1 dan 3 yang mana perbuatan yang dilakukan adalah mengakses komputer dan/atau sistem elektronik milik orang lain secara melawan hukum. Unsur perbuatan melawan hukum dilakukan dengan cara apapun maupun dengan cara melanggar, menerobos, melampaui atau menjebol sistem pengaman.

Selain Pasal 30 ayat 1 dan 3, dalam Undang-Undang ITE juga diatur rumusan pasal tentang penyadapan atas informasi elektronik dan/atau dokumen elektronik. Rumusan pasal tentang perbuatan tersebut diatur dalam Pasal 31 ayat 1 dan 2. Jenis perbuatan yang diatur dalam Pasal 31 ayat 1 dan 2 adalah melakukan intersepsi atau penyadapan atas informasi elektronik dan/atau dokumen elektronik. Menurut penjelasan Undang-Undang ITE, yang dimaksud dengan intersepsi atau penyadapan adalah

> "kegiatan untuk mendengarkan, merekam, membelokkan, mengubah, menghambat, dan/atau mencatat transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik, baik menggunakan jaringan kabel komunikasi maupun jaringan nirkabel, seperti pancaran elektromagnetis atau radio frekuensi."

Berdasarkan atas pengertian dari intersepsi atau penyadapan tersebut, maka penulis mengkategorikan Pasal 31 ayat 1 dan 2 ini termasuk dalam kejahatan *hacking*. Hal ini disebabkan karena dalam proses penyusupan dalam dunia *hacker* terdapat proses menjelajahi sistem komputer dengan cara menyadap paket-paket data komputer tersebut untuk mencari kelemahan dalam sistem itu. Dalam penjelajahannya seorang hacker akan memanfaatkan data atau informasi yang ada dalam sistem komputer itu. Berkaitan dengan proses dalam dunia *hacker* itu, maka dalam Undang-Undang ITE diatur dalam rumusan Pasal 31 ayat 1 dan 2.

Dalam KUHP, rumusan delik yang berkaitan dengan perbuatan mendengarkan pembicaraan orang lain tanpa seizin pemiliknya dengan menggunakan alat bantu elektronik belumlah diatur.[83] Hal itu yang menyebabkan banyak dari pelaku kejahatan

83 Andi Hamzah, *op cit* hal 13

komputer sulit untuk ditangani atau dijatuhi pidana. Dalam paparan yang ada diatas telah dipaparkan bahwa penggunaan Pasal 167 dan 551 KUHP kurang tepat untuk menjerat pelaku kejahatan komputer. Berdasarkan atas hal tersebut, maka pemerintah mengeluarkan rumusan pasal yang berkaitan dengan kejahatan komputer yang mana dalam KUHP belum diatur.

Sebelum dikeluarkannya Undang-Undang ITE dengan adanya salah satu pasal yang mengatur tentang perbuatan penyadapan, pemerintah sudah mengeluarkan Undang-Undang No 36 Tahun 1999 tentang telekomunikasi yang dalam Pasal 40 berisi tentang larangan untuk melakukan kegiatan penyadapan informasi. Adapun bunyi dari Pasal 40 adalah sebagai berikut

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

Dalam rumusan pasal tersebut, larangan yang dikeluarkan sebenarnya sudah cukup kuat untuk menjerat pelaku penyadapan suatu informasi, akan tetapi dengan semakin berkembangnya teknologi sehingga kejahatan juga semakin berkembang, sehingga pemerintah merasa bahwa perlu adanya pengaturan yang lebih khusus dan lebih kuat yang mengatur tentang suatu informasi elektronik agar tujuan dari kebijakan kriminal yaitu mensejahterakan masyarakat dapat terwujud.

Berkaitan dengan kebijakan kriminal itulah maka perbuatan menyadap atau mendengarkan, merekam suatu sistem secara melawan hukum diatur dalam Undang-Undang ITE. Dalam Pasal 31 ayat 1 dan 2 unsur perbuatan yang diatur adalah melakukan intersepsi atau penyadapan, dengan objeknya adalah informasi elektronik

dan/atau dokumen elektronik dalam suatu komputer dan/atau sistem elektronik milik orang lain baik dilakukan dengan sengaja maupun secara melawan hukum. Dalam Undang-Undang ITE, objek dari rumusan pasal tersebut lebih lengkap dengan jenis data elektronik yang lebih banyak. Selain itu rumusan pasal dalam Undang-Undang ITE mengatur bahwa perbuatan penyadapan itu dilakukan baik saat informasi elektronik tersebut dalam keadaan diam maupun dalam keadaan sedang ditransmisikan atau sedang dikirimkan. Dengan adanya rumusan yang semakin lengkap diharapkan agar pelaku dari kejahatan komputer dapat dikenai pidana sesuai dengan kejahatan yang dilakukan.

3. *Data Diddling*

Data diddling merupakan suatu kejahatan yang berupa perbuatan mengubah data valid atau sah dengan cara melawan hukum yaitu dilakukan dengan mengubah *input* data maupun *output* data dengan memakai sarana komputer. Perbuatan mengubah *input* maupun *output* dilakukan dengan adanya maksud untuk mengaburkan atau menyembunyikan data dengan cara memalsukan data tesebut sehingga isinya diubah seolah-olah menjadi data yang autentik.

a. Ketentuan menurut KUHP

Dalam KUHP, jenis kejahatan *data diddling* dikategorikan dalam delik perbuatan pemalsuan data yang diatur dalam Pasal 263 KUHP. Dalam rumusan Pasal 263 KUHP, unsur perbuatan yang dilakukan adalah:

- membuat secara tidak benar atau

memalsukan surat

Dengan demikian yang dimaksud dengan "perbuatan memalsu surat" adalah mengubah data atau surat sedemikian rupa, sehingga isinya menjadi lain daripada yang asli. Cara untuk mengubah data bermacam-macam diantaranya dapat dengan cara mengurangi, menambah atau mengubah sesuatu dari surat tersebut.

Dalam kajian pustaka berkaitan dengan Pasal 263 KUHP telah dipaparkan tentang pengertian kata "dan lain-lain" yang dapat memungkinkan data atau keterangan dalam media disket atau *flashdisk* dapat dimasukkan dalam pengertian surat, asalkan data atau keterangan yang tersimpan dalam media disket itu dituangkan dalam bentuk tulisan, dengan demikian data informasi tersebut dapat dipakai sebagai bahan informasi tertulis.

Saat ini timbul suatu permasalahan yaitu apabila data atau keterangan yang terdapat dalam media penyimpanan tersebut tidak dicetak kedalam kertas, maka harus ada keberanian dari aparat penegak hukum untuk dapat menerapkan ketentuan Pasal 263 KUHP dengan melakukan pendekatan dengan cara memperluas kata-kata dalam undang-undang untuk dapat menafsirkan angka-angka, huruf-huruf yang terdapat dalam media komputer sehingga dapat dianggap sebagai surat.[84] Berdasarkan atas pemaparan ini, maka dapat dilihat bahwa ketentuan Pasal 263 KUHP dapatlah digunakan apabila data atau keterangan tersebut dicetak atau tertuang dalam media kertas sehingga dapat diketahui adanya pemalsuan data, akan tetapi apabila data yang

84 *Ibid,* hal 79

dipalsu itu tidak dicetak melainkan tetap berada dalam komputer, maka penerapan Pasal 263 ini cukup sulit untuk diterapkan.

b. Ketentuan berdasarkan Undang-Undang ITE

Jenis kejahatan *data diddling* atau perbuatan mengubahan data seolah-olah menjadi data yang valid dengan merubah *input* maupun *output* data, dalam Undang-Undang ITE diatur dalam Pasal 35. Unsur perbuatan yang diatur dalam Pasal 35 tersebut adalah:

- Melakukan manipulasi;
- Penciptaan;
- Perubahan;
- Penghilangan;
- Perusakan;

Dalam ketentuan Undang-Undang ITE, rumusan unsur perbuatan sudah dicantumkan secara lebih rinci yaitu dengan cara-cara yang telah dipaparkan. Hal ini bertujuan agar tidak adanya penafsiran secara analogi lagi sehingga berakibat sulitnya untuk menerapkan pidana seperti dalam beberapa rumusan pasal di KUHP. Dalam Pasal 263 KUHP, tidak dicantumkan bentuk-bentuk perbuatan memalsu, sehingga harus adanya penafsiran secara ekstensif maupun secara analogi. Hal ini berbeda dengan Pasal 35 Undang-Undang ITE yang merinci bentuk-bentuk atau cara-cara untuk melakukan perubahan data atau informasi elektronik tersebut.

Dalam bentuk-bentuk yang dirinci tersebut, diharapkan agar pelaku-pelaku kejahatan komputer tidak dapat lepas dari sanksi pidana yang seharusnya ia terima. Dengan adanya bentuk-bentuk perbuatan yang dicantumkan dalam rumusan pasal ini, maka kebijakan kriminal sudah dimasukkan atau sudah ada. Dalam kajian pustaka telah dipaparkan bahwa tujuan dari adanya kebijakan kriminal adalah menciptakan kesejahteraan masyarakat. Atas dasar tujuan itulah, maka unsur-unsur perbuatan yang dalam KUHP belum ada, maka dalam Undang-Undang ITE dimasukkan untuk tujuan menciptakan kesejahteraan masyarakat tersebut.

Pasal 35 Undang-Undang ITE menyebutkan bahwa unsur kesengajaan dan melawan hukum dari perbuatan manipulasi, penciptaan, perubahan suatu informasi elektronik dan/atau dokumen elektronik memiliki suatu tujuan yaitu agar informasi elektronik dan/atau dokumen elektronik dianggap seolah-olah data otentik. Dilihat dari tujuannya itu, maka unsur kesengajaan dari perbuatan itu dapat dikategorikan sebagai kesengajaan sebagai maksud atau tujuan. Artinya adalah untuk mewujudkan unsur tingkah laku yang aktif tersebut, sudah ada maksud untuk timbulnya suatu akibat dari perbuatan itu yaitu perubahan data menjadi seolah-olah data yang autentik. Unsur perbuatan manipulasi dalam Undang-Undang ITE tidak harus diwujudkan dalam media kertas, melainkan perubahan data atau manipulasi data dalam komputer pun dapat dikenai dengan pasal ini. Hal ini disebabkan karena objek dari perbuatan manipulasi sudah disebutkan secara jelas yaitu informasi elektronik dan dokumen elektronik yang mana bentuk dari informasi elektronik dan/atau dokumen elektronik tidak dalam bentuk tulisan yang harus tertuang dalam kertas saja

melainkan dalam bentuk-bentuk lain yang memiliki arti sehingga dapat dipahami oleh orang lain meskipun tidak dicetak.

4. *Joycomputing*

Dalam KUHP kejahatan komputer jenis *joycomputing* atau menggunakan komputer secara tidak sah melampaui batas kewenangannya dikategorikan dalam tindak pidana pencurian yang diatur dalam Pasal 362 KUHP dan Pasal 30 ayat 2 dalam Undang-Undang ITE.

a. Ketentuan menurut KUHP

Dalam KUHP kejahatan *joycomputing* dikategorikan dalam tindak pidana pencurian yang diatur dalam Pasal 362 KUHP yang dalam kajian pustaka telah dirumuskan dan dibagi unsur subjektif dan objektif dari Pasal 362 KUHP ini. Dari pembagian unsur tersebut, terdapat unsur perbuatan dari Pasal 362 KUHP yaitu perbuatan mengambil. Unsur "mengambil" dan "barang sesuatu" apabila dihubungkan dengan perbuatan imateriil dalam bentuk penyalahgunaan komputer dapat diartikan sebagai berikut:[85]

a. Pengertian "mengambil"

Dalam komentar Pasal 362 KUHP disebutkan bahwa yang dimaksud dengan "mengambil" adalah mengambil untuk dikuasainya dan pengambilan itu sudah dapat dikatakan selesai apabila barang tersebut sudah berpindah

85 Al. Wisnubroto, *op cit* hal 82

tempat. Sedangkan yang dimaksud dengan "mengambil" dalam penyalahgunaan komputer adalah:

1) Mengambil dalam arti nyata atau secara fisik yaitu mengambil disket, *floppy disk* yang berisikan data atau program komputer.

2) Mengambil dalam arti tidak nyata atau secara nonfisik yaitu:

a) Mengkopi atau merekam data atau program yang tersimpan di dalam suatu disket dan sejenisnya kedalam disket atau media lainnya dengan cara memberikan instruksi-instruksi tertentu pada komputer.

b) Memanfaatkan "waktu" atau "jasa" penggunaan komputer melampaui batas wewenangnya.

Apabila dikaitkan dengan komentar Pasal 362 KUHP, untuk bentuk mengambil yang pertama tidak menjadi masalah, yang menjadi masalah adalah pengertian mengambil dalam bentuk yang kedua yaitu 2a. Dalam perbuatan mengambil data karena sekalipun barang (data atau program) sudah diambil baik dengan cara mengkopi atau menstransfer, namun barang yang asli masih tetap utuh dan tidak berubah posisi. Artinya yang berpindah adalah turunannya atau hasil kopiannya. Hal ini dapat diartikan bahwa perlu adanya suatu penafsiran dari perbuatan "mengambil" tersebut. Apabila tidak dilakukan suatu penafsiran maka suatu bentuk tingkah laku mengambil dalam arti mengambil suatu data sulit untuk diterapkan. Hal ini disebabkan karena barang yang diambil adalah barang yang berbentuk maya dan barang aslinya

masih ada. Hal ini tentu berbeda dengan pengertian mengambil yang berarti mengambil untuk dikuasainya dan pengambilan itu sudah dapat dikatakan selesai apabila barang tersebut sudah berpindah tempat. Akan tetapi, selain dengan melihat unsur perbuatan mengambil perlu juga melihat unsur yang lainnya yaitu melihat unsur adanya maksud untuk memiliki, yang berarti bahwa adanya suatu unsur kesengajaan untuk memiliki sehingga perbuatan mengkopi data atau program yang dilakukan dengan sengaja dan tanpa ijin dari pemiliknya. Bentuk perbuatan itu dapat dikategorikan "mengambil" sebagaimana yang dimaksud dalam Pasal 362 KUHP

b. Pengertian "barang" atau "benda"

Barang atau benda dalam kejahatan komputer adalah data atau program yang tersimpan dalam media disket, *floppy disk* dan sejenisnya dalam perbuatan merekam atau mengkopi. Benda-benda tersebut secara fisik tidak dapat terlihat wujudnya. Data atau program komputer baru dapat dilihat wujudnya apabila ditampilkan pada layar monitor komputer atau dicetak pada alat cetak yang dihubungkan dengan komputer.

Melalui pengalaman kepustusan Hoge Raad der Nederland tentang Arest listrik, maka agar perbuatan mengkopi data atau program komputer secara melawan hukum dan perbuatan *joycomputing* dapat dikenai Pasal 362 KUHP diperlukan adanya perluasan dalam pengertian "benda" sehingga data dan program komputer

yang terdapat dalam media komputer serta "waktu" atau "jasa" yang merupakan benda tak berwujud dapat dikategorikan sebagai benda atau barang.

Unsur-unsur dalam Pasal 362 KUHP yang lain seperti milik orang lain dan secara melawan hukum, pada dasarnya cukup sesuai apabila dikaitkan dengan kejahatan komputer. Dengan demikian pada prinsipnya Pasal 362 KUHP yang mengatur tentang pencurian dapat diterapkan dalam perbuatan mengkopi data atau program komputer, dengan catatan bahwa pengertian "mengambil" dalam pasal tersebut diperluas sebagai perbuatan "mengkopi" atau "merekam" dan pengertian "barang" atau "benda" diperluas menjadi data atau program komputer yang terdapat dalam media komputer

b. Ketentuan menurut Undang-Undang ITE

Ketentuan Pasal 30 ayat 2 dapat dikategorikan dengan sebagai perbuatan *joycomputing*. Hal ini didasarkan pada adanya suatu maksud untuk memperoleh suatu informasi elektronik dan/atau dokumen elektronik dengan cara mengakses komputer dan/atau sistem elektronik secara sengaja dan melawan hukum. Dalam rumusan Pasal 362 KUHP tentang pencurian, terdapat salah satu unsur yang menguatkan bahwa perbuatan tersebut adalah suatu pencurian yaitu adanya maksud untuk memiliki. Apabila melihat rumusan Pasal 30 ayat 2, maka unsur pencurian suatu informasi elektronik dan/atau dokumen elektronik adalah ada yaitu adanya tujuan untuk memperoleh suatu informasi dan/atau dokumen elektronik.

Dalam Pasal 30 ayat 2 Undang-Undang ITE telah disebutkan bahwa pelaku memiliki suatu maksud atau tujuan untuk memiliki objek dari suatu kejahatan yaitu informasi elektronik dan/atau dokumen elektronik atau secara khusus data komputer. Rumusan Pasal 30 ayat 2 ini merupakan suatu unsur kesengajaan dengan adanya maksud yang jelas yaitu memperoleh suatu informasi elektronik dan/atau dokumen elektronik.

Selain adanya suatu maksud, unsur lain yang perlu untuk diketahui adalah unsur perbuatannya. Dari unsur perbuatan dapat diketahui bahwa perbuatan yang dilakukan adalah mengakses suatu komputer atau sistem elektronik. Perbuatan mengakses adalah suatu bentuk kegiatan dalam berinteraksi dengan suatu sistem elektronik. Hal ini berarti sudah adanya suatu kegiatan interaksi dalam jaringan komputer tersebut yang dapat berupa pentransferan data ataupun bentuk lain yang berakibat adanya suatu interaksi antara sistem elektronik tersebut. Dengan adanya suatu rumusan perbuatan yang jelas, diharapkan mempermudah aparat penegak hukum untuk dapat menerapkan pasal ini tanpa perlu adanya penganalogian kata-kata dalam pasal tersebut.

Selain Pasal 30 ayat 2, kejahatan *joycomputing* dapat juga dikenai Pasal 32 ayat 2. Apabila melihat pengertian dari kejahatan *joycomputing* yaitu menggunakan komputer melebihi batas kewenangannya, maka Pasal 32 ayat 2 dapat diterapkan. Hal ini disebabkan karena dalam Pasal 32 ayat 2 dicantumkan adanya suatu perbuatan yaitu mentransfer atau memindahkan informasi elektronik kepada sistem elektronik orang lain yang tidak berhak. Hal ini berarti pelaku melakukan suatu perbuatan yang

melibihi dari kewenangan dia yaitu dia memindahkan suatu informasi elektronik pada sistem elektronik milik orang lain yang tidak berhak mendapatkannya.

Apabila dalam KUHP perlu adanya suatu penafsiran dengan cara perluasan kata-kata untuk menafsiran perbuatan mengambil yang diperluas sebagai perbuatan mentransfer atau mengkopi data, maka dalam Pasal 32 ayat 2 sudah dicantumkan secara jelas bahwa perbuatan yang dilakukan adalah memindahkan atau mentransfer Informasi Elektronik dan/atau dokumen elektronik. Dengan adanya rumusan yang jelas tersebut, maka tidak diperlukan lagi suatu penafsiran dengan memperluas kata yang kadang menyulitkan untuk dilakukan pembuktiannya.

5. The Trojan Horse

Jenis kejahatan *the trojan horse* merupakan suatu bentuk kejahatan komputer dengan cara mengurangi data atau instruksi suatu program, sehingga program tersebut selain menjalankan tugas sebenarnya juga akan melaksanakan tugas lain yang tidak sah. Dalam kajian pustaka telah dipaparkan unsur-unsur dalam Pasal 372 KUHP terkait dengan *the trojan horse*. Diantara unsur Pasal 372 KUHP terdapat unsur "barang yang ada dalam kekuasaannya bukan karena kejahatan." Dalam unsur tersebut memiliki arti bahwa adanya suatu kepercayaan dari pemilik barang terhadap pelaku untuk memakai, membawa atau menyimpan barang tersebut.

Menurut Andi Hamzah yang telah dipaparkan dalam kajian pustaka dijelaskan bahwa kejahatan yang terjadi di bidang komputer sangat berkaitan erat dengan faktor manusia dibelakang pengoperasian komputer.[86] Dengan demikian perbuatan manipulasi data ini dilakukan oleh pihak-pihak yang diberi kepercayaan untuk memegang atau mengelola peralatan komputer beserta perlengkapannya, termasuk juga data atau program komputer tersebut. Selain adanya suatu kepercayaan, apabila kepercayaan untuk memegang barang dalam hal ini komputer beserta perangkatnya berdasarkan atas adanya hubungan karena pekerjaan atau jabatan, maka terhadap pelaku manipulasi data dapat diancam pidana Pasal 374 KUHP

Berkaitan dengan perbuatan mengubah data, perlu diketahui bahwa apabila perbuatan tersebut terdapat unsur lain yaitu untuk memperkaya diri sendiri secara melawan hukum atau unsur penyalahgunaan kewenangan dan perbuatan tersebut dipandang merugikan keuangan negara dan/atau perekonomian negara sehingga dapat dikategorikan sebagai tindak pidana korupsi, yang dapat juga dikenai dengan Pasal 3 Undang-Undang Nomor 20 Tahun 2001 tentang Perubahan atas Undang-Undang Nomor 31 Tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi. Adapun bunyi Pasal 3 tersebut adalah sebagai berikut:

> Pasal 3
>
> Setiap orang yang dengan tujuan menguntungkan diri sendiri atau orang lain atau suatu korporasi, menyalahgunakan kewenangan, kesempatan atau sarana yang ada padanya karena jabatan atau kedudukan yang dapat merugikan keuangan negara atau perekonomian negara, dipidana dengan pidana penjara

86 Andi Hamzah (cetakan kedua), *op cit* hal 42

seumur hidup atau pidana penjara paling singkat 1 (satu) tahun dan paling lama 20 (dua puluh) tahun dan atau denda paling sedikit Rp50.000.000,00 (lima puluh juta rupiah) dan paling banyak Rp1.000.000.000,00 (satu milyar rupiah).

Menurut Andi Hamzah, perlu adanya suatu penafsiran secara ekstensif untuk menafsirkan benda tidak berwujud sehingga meliputi juga data atau program komputer seperti yang dilakukan oleh Hoge Raad yang menafsirkan aliran listrik sebagai suatu barang sehingga dapat menjadi objek delik kekayaan.[87] Jadi selain dapat dikenai dengan Pasal 372 KUHP dan 374 KUHP, dapat juga dikenai dengan Pasal 3 Undang-Undang Pemberantasan Tindak Pidana Korupsi apabila unsur dari memperkaya diri dapat dipenuhi.

b. Ketentuan berdasarkan Undang-Undang ITE

Berdasarkan atas pengertian dari jenis kejahatan *the trojan horse* yang telah dipaparkan dalam kajian pustaka, bahwa perbuatan yang dilakukan adalah memanipulasi suatu program dengan cara menambah atau mengurangi program tersebut sehingga selain menjalankan tugas sebenarnya juga akan melaksanakan tugas lainnya. Berdasarkan atas pengertian itu, maka menurut Undang-Undang ITE, kejahatan ini dapat dikenai Pasal 33, apabila perbuatan untuk mengurangi data atau memanipulasi program ditujukan pada sistem elektroniknya atau pada perangkatnya

87 *Ibid*, hal 26

sehingga perangkat tersebut tidak bekerja sebagaimana mestinya. Jadi yang diubah adalah perangkatnya untuk menghasilkan suatu informasi elektronik yang tidak sebenarnya yang mana akibat dari perubahan sistem itu adalah adanya perubahan pada datanya.

Dalam pasal 33 yang diatur adalah unsur perubahan atas suatu sistem elektronik atau perangkatnya, akan tetapi apabila secara melawan hukum yang diubah adalah data atau informasi elektronik tersebut, maka dalam Undang-Undang ITE diatur dalam Pasal 32 ayat 1. Unsur-unsur perbuatan yang diatur dalam Pasal 32 ayat 1 adalah

- mengubah
- menambah
- merusak
- menghilangkan
- memindahkan
- menyembunyikan

Dengan objeknya adalah informasi elektronik dan/atau dokumen elektronik. Jadi apabila *the trojan horse* ditujukan pada perubahan di sistem elektroniknya sehingga bekerja tidak sebagaimana mestinya, maka pasal yang digunakan adalah Pasal 33. Hal ini berbeda apabila yang diubah adalah informasi elektroniknya maka dapat dikenai Pasal 32 ayat 1.

6. Penyia-nyiaan Data Komputer

a. Ketentuan Menurut KUHP

Dalam kajian pustaka telah dipaparkan secara umum tentang unsur perbuatan menghancurkan, merusakkan, membikin tidak dapat dipakai dan menghilangkan yang diatur dalam Pasal 406 ayat 1 KUHP. Adapun unsur-unsur perbuatan tersebut apabila dikaitkan dengan kejahatan komputer adalah sebagai berikut:[88]

a. Pengertian dari tindakan "menghancurkan" pada kejahatan komputer adalah suatu perbuatan menghancurkan disket dan sejenisnya yang berisikan data atau program komputer sehingga mengakibatkan disket dan sejenisnya beserta data atau program didalamnya menjadi hancur dan tidak dapat dimanfaatkan.
b. Pengertian dengan tindakan "merusak" pada kasus kejahatan komputer adalah perbuatan merusak isi disket dan media penyimpan lainnya. Misalnya merusak data atau program yang terdapat dalam *floppydisk* atau disket dengan cara menghapus data atau program tersebut.
c. Pengertian "membuat tidak dapat dipakai lagi" pada kejahatan komputer adalah perbuatan yang dilakukan sedemikian rupa sehingga tidak dapat dimanfaatkan sesuai dengan fungsinya. Hal tersebut disebabkan karena data atau program telah dirubah sehingga penggunaan data atau program komputer tersebut terhalangi dan tidak dapat diperbaiki lagi.
d. Pengertian "menghilangkan" pada kejahatan komputer adalah suatu perbuatan menghilangkan atau menghapus data atau program yang tersimpan dalam

88 Al. Wisnubroto, *op cit* hal 89-90

disket atau media yang sejenisnya sehingga mengakibatkan semua data atau program yang disimpan menjadi hapus sama sekali.

Berdasarkan atas penjelasan unsur perbuatan dalam kejahatan komputer, nampak bahwa adanya kesesuaian antara pengertian perusakkan barang dengan pengertian perusakkan data atau program komputer yang pada intinya perbuatan tersebut menyebabkan fungsi dari barang yang dalam hal ini data atau program komputer menjadi terganggu. Berdasarkan atas kesesuaian pengertian itulah, maka terhadap perbuatan penyia-nyiaan data komputer yang pada hakekatnya adalah perbuatan menghancurkan atau merusakkan data, pada pelakunya dapat dikenakan ketentuan Pasal 406 ayat 1 KUHP.

b. Ketentuan Menurut Undang-Undang ITE

Melihat pengertian dari penyia-nyiaan data komputer yang telah dipaparkan dalam kajian pustaka, dapat kita lihat bahwa perbuatan yang dilakukan adalah merusak atau menghancurkan media penyimpanan atau *hardisc* yang berisikan data atau program komputer sehinggga data atau program komputer itu tidak berfungsi sebagaimana mestinya. Dilihat dari pengertiannya, maka objek dari perbuatan merusak, menghilangkan atau apapun itu adalah terletak pada alat atau sistem sehingga data yang terdapat dalam alat atau sistem elektronik itu menjadi tidak berfungsi.

Berdasarkan atas pemaparan itu, maka Pasal 33 Undang-Undang ITE dapat dijatuhkan pada jenis kejahatan penyia-nyiaan komputer. Hal ini disebabkan karena

dalam Pasal 33 telah dicantumkan objek yang dirusak yaitu sistem elektroniknya. Akibat dari perusakkan objek itu adalah tidak bekerja sistem elektronik sebagaimana mestinya. Sistem elektronik adalah suatu perangkat yang berfungsi untuk menyimpan, mengolah, menampilkan, mengumumkan suatu informasi elektronik atau suatu data elektronik, sehingga apabila sistem elektronik ini dirusak dengan cara yang non-fisik seperti dengan menyisipkan *logic bomb* atau virus, maka akibat dari rusaknya sistem tersebut adalah data atau informasi elektronik itu menjadi tidak bisa berfungsi dengan baik atau mengalami kerusakkan. Jadi yang menjadi sasaran dari pelaku untuk merusak suatu data adalah dengan cara merusak sistemnya yang mana akibat dari rusaknya sistem itu adalah data menjadi tidak berfungsi sebagaimana mestinya atau bahkan dapat hilang.

Dilihat dari objek yang dirusak, apabila yang dirusak bukan suatu sistem elektronik melainkan yang dirusak adalah langsung pada datanya atau informasi elektronik, maka dalam Undang-Undang ITE diatur dalam Pasal 32. Dalam Pasal 32, dijelaskan unsur perbuatannya diantaranya adalah melakukan perbuatan untuk merusak, menghilangkan, menyembunyikan suatu informasi elektronik milik orang lain atau milik publik. Hal ini berarti dalam rumusan Pasal 32 ayat 1 yang menjadi objek untuk dirusak adalah langsung pada data atau informasi elektronik atau dokumen elektronik tanpa harus merusak sistemnya terlebih dahulu.

Dilihat antara bentuk kejahatan penyia-nyiaan data komputer dan the trojan horse memiliki kesamaan perbuatan, akan tetapi ada perbedaannya yaitu pada unsur objek dan akibat yang ditimbulkan. Apabila dalam Pasal 32 ayat 1, yang menjadi

objek adalah informasi elektronik sedangkan Pasal 33, yang menjadi objeknya adalah sistem elektroniknya. Selain itu, dalam Pasal 33 dijelaskan bahwa akibat dari tindakan apapun menyebabkan atau berakibat sistem elektronik tidak bekerja sebagaimana mestinya. Sedangkan Pasal 32 ayat 1, akibat yang ditimbulkan berada pada Pasal 32 ayat 2 yaitu dapat diaksesnya informasi elektronik dan.atau dokumen elektronik sehingga dapat diketahui oleh publik dengan keutuhan data yang tidak sebagaimana mestinya.

7. Kejahatan Terhadap Pembajakan Perangkat Lunak *(software)*

Kejahatan komputer selain diatur dalam KUHP dan Undang-Undang ITE, juga diatur dalam Undang-Undang Nomor 19 Tahun 2002 tentang Hak Cipta. Sebagaimana diketahui bahwa peralatan komputer terdiri dari perangkat keras yang terdiri dari CPU, *keyboard*, layar monitor yang dapat dilindungi dengan hak paten. Sedangkan perangkat lunak seperti program komputer dan pengembangannya dilindungi dalam hak cipta. Alasan mengapa program komputer yang termasuk hak milik intelektual perlu dilindungi oleh hak cipta adalah karena pada dasarnya program komputer merupakan karya cipta di bidang ilmu pengetahuan.[89]

Dalam Undang-Undang Nomor 19 tahun 2002 tentang Hak cipta yang disebut dengan UUHC terdapat beberapa ketentuan yang mengatur masalah program komputer dan perlindungannya terhadap upaya penyalahgunaan ciptaan. Apabila

89 Al. Wisnubroto, *op cit* hal 109

terjadi penyalahgunaan komputer yang berupa pelanggaran hak cipta di bidang program komputer, misalnya dengan cara mengkopi atau menggandakan program komputer secara tidak sah atau tanpa ijin pemegang hak cipta, maka terhadap pelaku dapat diancam dengan ketentuan Pasal 72 ayat 3 UUHC yang berbunyi:

> (3) "Barangsiapa dengan sengaja dan tanpa hak memperbanyak penggunaan untuk kepentingan komersial suatu Program Komputer dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau denda paling banyak Rp 500.000.000,00 (lima ratus juta rupiah)."

Pada ketentuan tersebut nampak bahwa pada hakekatnya menggandakan dengan cara mengkopi program komputer yang bukan miliknya sendiri, merupakan suatu pelanggaran hak cipta. Namun dalam Pasal 15 poin e dicantumkan bahwa apabila penggandaan program komputer ditujukan untuk pendidikan dan pusat dokumentasi bukan untuk komersil, maka perbuatan itu diperbolehkan. Jadi kaitannya dengan mengkopi program komputer secara ilegal dan untuk kepentingannya sendiri tentu sudah melanggar hak cipta dan dapat dikenai ancaman Pasal 72 ayat 3 UUHC.

Dilihat dari unsur kesengajaan dan unsur melawan hukumnya, maka dalam Undang-Undang ITE selalu dicantumkan kedua unsur tersebut. Hal ini berarti bahwa unsur kesengajaan itu harus ditujukan dengan unsur melawan hukum yang ada di belakang kata sengaja yang dikuasai unsur sengaja tersebut.[90]

B. Pengaturan Sanksi berkaitan dengan Kebijakan Penal dari Kejahatan Komputer Menurut KUHP dan Undang-Undang ITE

90 Masruchin Rubai, *Asas-Asas Hukum Pidana*, Kerjasama antara UM PRESS dan FH UB, Malang, 2001, hal 54

Berkaitan dengan rumusan masalah yang kedua yaitu tentang kebijakan penal dari kejahatan komputer menurut KUHP dan Undang-Undang ITE, maka dalam pemaparan ini akan dibagi sanksi yang dikenakan sesuai dengan jenis kejahatan menurut KUHP dan Undang-Undang ITE.

1. Data Leakage

Dalam jenis kejahatan *data leakage* atau pembocoran rahasia, menurut KUHP apabila berkaitan dengan pembocoran rahasia negara maka dapat dikenai dengan Pasal 112, 113 dan 114 KUHP. Apabila pembocoran rahasia profesi Pasal 322 dan pembocoran rahasia perusahaan 323 KUHP. Pembocoran rahasia dalam situasi tertentu dikenai dengan Pasal 431 KUHP.

Ancaman sanksi yang dikenai pada keenam pasal ini adalah sebagai berikut:

a. Pasal 112 : ancaman hukuman penjara paling lama 7 (tujuh) tahun

b. Pasal 113 : (1) ancaman hukuman penjara paling lama 4 (empat) tahun

(2) ditambah 1/3 apabila adanya surat atau benda yang bersalah karena pencarian

c. Pasal 114 :- ancaman hukuman pidana penjara paling lama 1 (satu) tahun atau;

- denda paling banyak Rp 300

d. Pasal 322 : (1) - ancaman hukuman pidana penjara paling lama 9 (sembilan) bulan atau;

- denda paling banyak Rp 600

(2) dituntut atas adanya pengaduan

e. Pasal 323 : (1) - ancaman hukuman pidana penjara paling lama 9 (sembilan) bulan atau;

- denda paling banyak Rp 600

(2) dituntut atas adanya pengaduan

f. Pasal 431 : - diancam pidana penjara paling lama 2 (dua) tahun

Menurut Undang-Undang ITE, maka bentuk perbuatan dari Pasal 32 ayat 3, dapat dikenai sanksi yaitu Pasal 48 ayat 3 dengan ancaman pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp 5 M.

Berdasarkan atas pemaparan sanksi yang dikenakan sesuai pasal-pasal yang ada baik sesuai dengan KUHP maupun Undang-Undang ITE, maka dapat diketahui bahwa sesuai dengan jenis sanksi yang sudah dipaparkan dalam kajian pustaka, jenis pidana menurut KUHP menggunakan sistem perumusan tunggal yaitu pidana penjara. Apabila ada pidana lain selain pidana penjara, maka sistem yang digunakan adalah dengan menggunakan sistem perumusan alternatif yaitu pidana penjara atau denda. Berbeda dengan Pasal 48 ayat 3 Undang-Undang ITE, sistem perumusan yang digunakan adalah sistem perumusan secara alternatif. Artinya adalah apabila pelaku mendapatkan sanksi sesuai dengan Pasal 48 ayat 3, maka pelaku dapat dikenai dengan pidana penjara saja atau pidana denda saja atau bahkan pidana penjara dan pidana denda. Itulah yang disebut dengan sistem pemidanaan kumulatif dan/atau alternatif.

Selain itu, berkaitan dengan perbuatan pembocoran rahasia atau *data leakage*, apabila dilihat menurut KUHP, maka untuk kasus pembocoran rahasia perusahaan

dan rahasia profesi adalah merupakan delik aduan yang mana baru dapat dijatuhi penuntutan apabila ada yang mengadukan perbuatan tersebut. Hal ini berbeda dengan Undang-Undang ITE yang mana merupakan delik umum, sehingga langsung dapat dilakukan penuntutan apabila diketahui adanya perbuatan yang melawan hukum sesuai dengan Pasal 32 ayat 3 Undang-Undang ITE.

2. Hacking

Berkaitan dengan jenis kejahatan *hacking*, menurut KUHP dapat dikenai dengan Pasal 167 dan 551 KUHP. Menurut Undang-Undang ITE, jenis kejahatan yang melanggar Pasal 30 ayat 1 dan 3 dapat dikenai Pasal 46 ayat 1 dan 3.

Ancaman pidana untuk jenis kejahatan *hacking* menurut Pasal 167 dan 551 KUHP adalah

a. Pasal 167 : (1) - diancam pidana penjara paling lama 9 (sembilan) bulan atau;

- denda paling banyak Rp 300

(3) – jika mengeluarkan ancaman, pidana penjara paling lama 1 (satu) tahun 4 (empat) bulan

(4) – ditambah 1/3 apabila perbuatan dilakukan dengan bersekutu

b. Pasal 551 : - diancam dengan denda paling banyak Rp 15

Ancaman pidana menurut Pasal 46 ayat 1 dan 3 Undang-Undang ITE adalah:

a. Pasal 46 : (1) – diancam pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 600 juta

(3) – diancam dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp 800 juta

Selain itu, dalam kejahatan *hacking* ini juga mengatur tentang penyadapan yang merupakan perbuatan yang melanggar Pasal 31 ayat 1 dan 2 serta Pasal 40 Undang-Undang Telekomunikasi. Untuk perbuatan penyadapan dalam Undang-Undang ITE, sanksi pidana diatur dalam Pasal 47 dengan ancaman hukuman sebagai berikut

a. Pasal 47 : - dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp 800 juta

Untuk perbuatan penyadapan atas informasi yang disalurkan melalui jaringan komunikasi dalam Undang-Undang Telekomunikasi diancam dengan Pasal 56 Undang-Undang Telekomunikasi yaitu:

a. Pasal 56 : - dipidana dengan pidana penjara paling lama 15 (lima belas) tahun

Berdasarkan atas pemberian pidana, maka dapat diketahui bahwa dalam Undang-Undang ITE, penjatuhan ancaman pidana baik secara pidana penjara maupun pidana denda sangatlah besar dan berat ancamannya. Hal ini tentu harus sesuai dengan tujuan dari kebijakan penal yang sudah dipaparkan di kajian pustaka dan harus diperhitungkan setiap biaya dari kerugian yang dialami dari perbuatan kejahatan komputer tersebut.

Untuk perbuatan yang melanggar Pasal 40 Undang-Undang Telekomunikasi, maka ancaman hukumannya adalah pidana penjara paling lama 15 tahun. Jadi

penjatuhan pidananya hanya menggunakan pidana penjara saja tanpa adanya pidana denda.

3. Data Diddling

Jenis kejahatan perbuatan mengubah data valid dengan cara yang tidak sah yaitu dengan mengubah input dan output data atau jenis kejahatan *data diddling* menurut KUHP dapat dikenai dengan delik pemalsuan surat yaitu Pasal 263 KUHP. Menurut Undang-Undang ITE, jenis perbuatan yang melanggar Pasal 35 dapat dikenai dengan sanksi pidana menurut Pasal 51 ayat 1.

Ancaman pidana menurut Pasal 263 KUHP adalah sebagai berikut

a. Pasal 263 : (1) diancam dengan pidana penjara paling lama 6 (enam) tahun

(2) diancam dengan pidana penjara paling lama 6 (enam) tahun apabila pemakaian surat menimbulkan kerugian

Ancaman pidana menurut Pasal 51 ayat 1 Undang-Undang ITE adalah sebagai berikut

b. Pasal 51 : (1) diancam dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp 12 M

Dalam KUHP, terkait dengan perbuatan dalam Pasal 263 KUHP pidana yang dijatuhkan adalah sistem perumusan tunggal yaitu hanya pidana penjara saja tanpa

adanya pidana denda. Hal ini berbeda dengan Pasal 51 ayat 1 Undang-Undang ITE yang pidananya dengan pidana penjara dan/atau pidana denda.

4. Joycomputing

Perbuatan menggunakan komputer secara tidak sah ini menurut KUHP termasuk dalam Pasal 362 dan menurut Undang-Undang ITE termasuk dalam perbuatan yang melanggar Pasal 30 ayat 2 dengan sanksi pidana Pasal 46 ayat 2. Ancaman pidana menurut KUHP adalah sebagai berikut:

a. Pasal 362 : diancam dengan pidana penjara paling lama 5 (lima) tahun atau denda paling banyak Rp 60

Menurut Pasal 46 ayat 2 Undang-Undang ITE, ancaman pidana yang dijatuhkan adalah sebagai berikut:

a. Pasal 46 : (2) diancam dengan pidana penjara paling lama 7 (tujuh) tahun dan/ atau denda paling banyak Rp 700 juta.

b. Pasal 48 : (2) diancam dengan pidana penjara paling lama 9 (sembilan) tahun dan/atau denda paling banyak Rp 3 M

Penjatuhan ancaman pidana menurut KUHP dan Undang-Undang khususnya dalam penjatuhan pidana penjara lebih berat pada Undang-Undang ITE. Dalam Pasal 362 KUHP selain pidana penjara, juga digunakan penjatuhan pidana denda. Jadi sistem perumusan yang digunakan adalah sistem perumusan alternatif sedangkan dalam Undang-Undang ITE menggunakan sistem perumusan alternatif kumulatif

5. The Trojan Horse

Jenis kejahatan dengan cara mengubah data sehingga data yang muncul menjadi data yang manipulasi dengan tujuan kepentingan pribadi, menurut KUHP termasuk dalam Pasal 372 dan 374 yaitu tentang penggelapan. Selain itu apabila perbuatan tersebut merugikan keuangan negara maka termasuk delik korupsi yang melanggar Pasal 3 Undang-Undang Pemberantasan Tindak Pidana Korupsi. Menurut Undang-Undang ITE, perbuatan tersebut dapat dikenai dengan dua pasal, tergantung pada jenis objek perbuatan mengubah data tersebut. Apabila yang diubah adalah sistem elektronik, maka dapat dikenai dengan sanksi Pasal 49, melainkan apabila yang diubah adalah informasi elektroniknya maka dapat dikenai Pasal 48 ayat 1.

Ancaman pidana menurut Pasal 372 KUHP adalah sebagai berikut

a. Pasal 372 : - diancam pidana penjara paling lama 4 (empat) tahun atau;

- denda paling banyak Rp 60

b. Pasal 374 :- diancam pidana penjara paling lama 5 (lima) tahun

Ancaman pidana menurut Undang-Undang Pemberantasan tindak pidana korupsi terkait dengan perbuatan penggelapan yang dilakukan oleh jabatannya maka sanksi pidananya adalah

a. Pasal 3 : - dipidana dengan pidana penjara seumur hidup atau pidana penjara paling singkat 1 (satu) tahun dan paling lama 20 (duapuluh) tahun dan/atau

- denda paling sedikit Rp 50.000.000,00 (lima puluh juta rupiah) dan paling banyak Rp 1.000.000.000,00 (satu miliar rupiah)

Ancaman pidana menurut Pasal 48 ayat 1 dan 49 Undang-Undang ITE

a. Pasal 48 : (1) – diancam pidana penjara paling lama 8 (delapan) tahun dan/atau
- denda paling banyak Rp 2 M

b. Pasal 49 : - diancam dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp 10 M

Dalam penjatuhan pidana, maka dapat diketahui bahwa untuk Undang-Undang Pemberantasan Tindak Pidana Korupsi menggunakan sistem perumusan kumulatif yaitu pidana penjara dan denda. Hal ini berbeda dengan sistem perumusan menurut Undang-Undang ITE yang menggunakan sistem perumusan kumulatif dan/atau alternatif.

6. Penyia-nyiaan Data Komputer

Perbuatan penyia-nyiaan data komputer, termasuk dalam perbuatan yang merusak, menghilangkan, menghancurkan dan membuat tidak dapat dipakai yang dalam KUHP diatur dalam Pasal 406 ayat 1 terkait dengan bentuk perusakkan barang. Adapun bentuk ancaman pidana yang dijatuhkan menurut Pasal 406 ayat 1 adalah

a. Pasal 406 : (1) diancam dengan pidana penjara paling lama 2 (dua) tahun 8 (delapan) bulan atau denda paling banyak Rp 300

Dalam Undang-Undang ITE, apabila penyia-nyiaan data komputer pada sistem komputernya, maka dapat dikenai dengan Pasal 49, melainkan apabila yang dirusak adalah data, maka dapat dikenai dengan Pasal 48 ayat 1. Dilihat dari penjatuhan sanksi pidana antara perbuatan penyia-nyiaan data komputer dan *the trojan horse*, dapat diketahui bahwa sebenarnya unsur perbuatan dan sanksinya sama, yang membedakan adalah objek dan akibat yang ditimbulkan. Artinya dalam Pasal 32 ayat 1, unsur akibat dalam Pasal 32 ayat 3 merupakan syarat tambahan yang memperberat pidana. Hal ini berbeda dengan Pasal 33 yang mana akibat yang timbul berada langsung dalam pasal tersebut yaitu sistem yang bekerja tidak sebagaimana mestinya.

7. Pembajakan Perangkat Lunak

Dalam Undang-Undang Hak Cipta, telah dicantumkan ketentuan pidana yaitu dalam Pasal 72 ayat 3 yang mana diatur bahwa ketentuan pidana dari perbuatan memperbanyak suatu program komputer untuk tujuan komersil dapat dijatuhi dengan pidana penjara selama 5 tahun dan/atau pidana denda Rp 500 juta.

Dalam pemaparan terkait dengan penjatuhan sanksi pidana dengan kebijakan penal. Maka dapat diketahui bahwa dalam penjatuhan pidana terhadap kejahatan komputer menurut KUHP banyak menggunakan sistem perumusan alternatif yaitu dengan penjatuhan pidana penjara atau pidana denda. Hal ini tentu berbeda dengan penjatuhan sanksi pidana menurut Undang-Undang ITE yang menggunakan sistem perumusan kumulatif alternatif.

Dalam kajian pustaka telah dipaparkan tentang sistem kumulatif alternatif dan seringkali sistem perumusan ini digunakan pada tindak pidana khusus seperti Undang-Undang ITE maupun UUHC. Dengan sistem perumusan alternatif kumulatif, maka pelaku dari kejahatan komputer tidak hanya dapat dikenai pidana penjara saja atau denda saja, melainkan dapat langsung dikenai pidana penjara dan denda sesuai dengan ketentuan maksimal dari masing-masing pasal.

Tujuan dari suatu penjatuhan sanksi pidana yang berat dan besar merupakan suatu bentuk penyesuaian atas bentuk perbuatan kejahatan komputer yang mana akibat dari perbuatan itu adalah merugikan dan membahayakan keselamatan masyarakat. Selain itu, suatu informasi elektronik dan/atau dokumen dapat diartikan juga sebagai suatu karya cipta yang wajib dilindungi oleh pemerintah. Dengan adanya suatu karya cipta yang dilindungi tersebut, maka diharapkan adanya suatu perlindungan yang memiliki kepastian hukum agar suatu karya cipta seperti informasi elektronik dan/atau dokumen elektronik tidak diambil atau diakses secara melawan hukum.

Penjatuhan pidana haruslah diberikan dan disesuaikan dengan kebutuhan masyarakat. Suatu penjatuhan pidana hanya dibenarkan apabila terdapat suatu kebutuhan yang berguna bagi masyarakat. Berdasarkan atas itulah, pemberian pidana yang berat dan maksimal diberikan yaitu dengan tujuan untuk melindungi masyarakat sesuai dengan tujuan dari kebijakan kriminal dan penal adalah untuk mencapai suatu tujuan yaitu mensejahterakan dan melindungi masyarakat.

3. Penerapan Undang-Undang ITE

Berdasarkan atas pemaparan tentang kejahatan komputer menurut KUHP dan Undang-Undang ITE maka dapat kita perhatikan bahwa dengan adanya Undang-Undang ITE saat ini berarti kejahatan komputer ini sudah memiliki suatu aturan yang mana apabila dilanggar maka akan ada sanksi yang dikenakan. Dalam penerapan suatu aturan, kita dapat melaksanakan suatu aturan hukum berdasarkan atas asas *lex specialis derogat les generalis* yang berarti bahwa hukum yang khusus lebih didahulukan daripada hukum yang umum. Hal Dengan adanya asas tersebut maka dapat diketahui bahwa apabila terjadi suatu kejahatan komputer maka aturan yang digunakan adalah dengan menggunakan Undang-Undang ITE.

Dengan adanya Undang-Undang ITE, maka salah satu hambatan dari sulitnya penanganan kejahatan komputer sudah sedikit berkurang, akan tetapi masih perlu adanya pembinaan terhadap aparat penegak hukum agar memiliki kesamaan dalam mengartikan suatu bentuk kejahatan komputer tersebut. Dengan adanya Undang-Undang ITE tersebut, maka jenis-jenis kejahatan komputer yang sebelumnya oleh KUHP sulit untuk dikenai sanksi karena belum adanya aturan yang jelas mengatur, maka saat ini setelah adanya Undang-Undang ITE dapat langsung ditangani secara khusus.

Berdasarkan beberapa contoh kasus yang ada seperti kasus Petrus Pangkur yang membobol kartu kredit milik warga AS yang mana dia bisa dibebaskan karena pasal dalam KUHP yang dikenakan padanya tidak sesuai dengan kejahatan yang ia lakukan dan tidak dapat dibuktikan kesalahannya, maka dengan adanya Undang-

Undang ITE bentuk kejahatan pembobolan kartu kredit dapat dikenai dengan Pasal 30 ayat 2 atau j*oycomputing* karena melakukan perbuatan dengan adanya tujuan untuk memperoleh informasi elektronik dan/atau dokumen elektronik.

Dalam penerapan Undang-Undang ITE, agar memiliki dampak pada masyarakat maka diperlukan adanya kerja keras dalam tubuh aparat penegak hukum. Dalam suatu sistem hukum yang menekankan pada substansi, struktur dan kultur, saat ini yang perlu dikerjakan adalah kesiapan dari struktur dalam menangani kejahatan komputer tersebut. Kesiapan struktur dalam hal ini berarti kesiapan aparat dalam melakukan penyelidikan, penyidikan, penuntutan, pembuktian dan putusan hakim harus dilakukan dengan baik karena bentuk kejahatan ini adalah suatu kejahatan maya yang mana sulit untuk pembuktian *locus delicti* atau tempat, pelaku, waktu dan lain sebagainya

Pemerintah telah mengeluarkan suatu peraturan baru yaitu Undang-Undang ITE. Agar sistem hukum berjalan dengan baik maka perlu kesiapan dari aparat untuk menjalankan aturan tersebut sehingga kejahatan komputer yang saat ini sudah menjadi budaya dalam masyarakat Indonesia bisa dihilangkan atau dihapuskan. Pelaksanaan ini tidak dapat berhasil apabila hanya dilakukan oleh salah satu pihak saja, melainkan semua pihak termasuk masyarakat juga wajib membantu terlaksananya penerapan Undang-Undang ITE. Dengan dapat diterapkannya Undang-Undang ITE dengan baik, maka kejahatan komputer dapat sedikit demi sedikit berkurang sehingga tujuan dari kebijakan kriminal yaitu mensejahterakan dan melindungi masyarakat dapat terwujud.

Tabel 4.1

Perbandingan KUHP dan Undang-Undang ITE

No	Jenis Kejahatan	KUHP	Undang-Undang ITE
1	*Data Leakage*	- Pasal 112, 113, 114, 322, 323, 431	- Pasal 32 ayat 3
		- Perbuatan yang dilakukan adalah mengumumkan, memberitahukan, memberikan, menyerahkan, membuka rahasia kepada negara lain atau orang lain	- Perbuatannya adalah mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan
		- Objeknya adalah surat-surat yang diperluas pengertiannya sebagai suatu data komputer	- Objeknya adalah informasi elektronik dan/atau dokumen elektronik

		- Secara sengaja, melawan hukum dan kealpaan	- Berakibat dapat terbukanya informasi elektronik sehingga dapat diakses oleh publik dengan keutuhan data yang tidak sebenarnya
2	*Hacking*	- Pasal 167 dan 551	- Pasal 30 ayat 1 dan 3, Pasal 31 ayat 1 dan 2, Pasal 40 Undang-Undang Telekomunikasi
		- Masuk dengan paksa, menggunakan kunci palsu ke rumah atau ruangan orang lain	- Bentuk perbuatannya adalah mengakses dengan cara melanggar, menerobos, melampaui atau menjebol sistem pengaman.
		- Adanya beberapa penafsiran yang diperluas dalam pasal tersebut. Misalnya berjalan diperluas menjadi mengakses	- Melakukan suatu penyadapan - Objeknya adalah informasi elektronik dan/atau dokumen elektronik
3	*Data Diddling*	- Pasal 263 KUHP	- Pasal 35, sanksi pidana Pasal 51 ayat 1
		- Adanya perluasan pengertian dalam mengartikan kata surat-surat yang memiliki arti sebagai angka-angka dalam media komputer	-Perbuatannya adalah melakukan manipulasi, penciptaan, perubahan, penghilangan, perusakan informasi elektronik dan/atau dokumen elektronik
		- Cukup sulit diterapkan, karena data yang diubah harus dicetak dalam kertas	- Tidak perlu diwujudkan dalam media kertas terlebih dahulu
4	*Joycomputing*	- Pasal 362 KUHP	- Pasal 30 ayat 2 dan 32 ayat 2. Sanksi pidana Pasal 46 ayat 2 dan Pasal 47 ayat 2
		- Perbuatan mengambil dapat diartikan dan sebagai mengambil secara fisik dan	- Tujuan perbuatannya adalah untuk memperoleh informasi elektronik dan/atau

		non fisik seperti mengkopi data	dokumen elektronik
		- Kata “benda” diperluas pengertiannya sebagai data atau program komputer	- Dengan cara mentransfer atau memindahkan informasi elektronik dan/atau dokumen elektronik ke sistem elektronik orang lain yang tidak berhak
5	*The Trojan Horse*	-Pasal 372 KUHP dan 374 KUHP - Pasal 3 Undang-Undang Pemberantasan Tipikor apabila perbuatan itu diketahui merugikan keuangan negara	- Pasal 32 ayat 1 dan sanksi pidana Pasal 48 ayat 1 - Pasal 33 dan sanksi pidana Pasal 49
		- Manipulasi data dilakukan atas dasar kepercayaan, adanya manusia dibelakang pengoperasian komputer	- Perbuatannya adalah mengubah, menambah, merusak, menghilangkan, memindahkan, menyembunyikan suatu informasi elektronik dan/atau dokumen elektronik. Jadi yang diubah adalah langsung pada informasi elektroniknya - Pasal 33 perbuatannya adalah melakukan perbuatan perubahan terhadap sistem elektroniknya sehingga menghasilkan suatu informasi elektronik yang tidak sebenarnya
6	Penyia-nyiaan data komputer	- Pasal 406 ayat 1 KUHP	- Pasal 32 ayat 1 dan sanksi pidana Pasal 48 ayat 1 -Pasal 33 dan sanksi pidana Pasal 49
		- Unsur perbuatannya adalah menghancurkan, merusak, membikin tidak	- Pasal 32 ayat 1 yang dirusak langsung pada informasi eletronik dan/atau

		dapat dipakai dan menghilangkan	dokumen elektronik. Jadi yang dirusak adalah langsung pada informasi elektroniknya - Pasal 33 perbuatannya adalah melakukan perbuatan apapun yang berakibat sistem elektronik tidak bisa bekerja sebagaimana mestinya.
7	Pembajakan perangkat lunak		- Diatur dalam Pasal 72 ayat 3 UUHC -Perbuatannya adalah memperbanyak program komputer untuk tujuan komersil

Sumber: Bahan Hukum Primer diolah, 2009

Tabel 4.2

Perbedaan Pengaturan Ancaman Pidana antara KUHP dan Undang-Undang ITE

No	Jenis Kejahatan	KUHP	Undang-Undang ITE
1	*Data Leakage*	- Pasal 112, 113, 114, 322, 323, 431 KUHP - Pasal 112 dipidana paling lama 7 tahun penjara - Pasal 113 dipidana paling lama 4 tahun penjara - Pasal 114 dipidana penjara paling lama 1 tahun 6 bulan atau kurungan paling lama 1 tahun atau denda paling banyak Rp 300	- Pasal 32 ayat 3 - Sistem penjatuhan pidana menggunakan alternatif kumulatif yaitu pidana penjara paling lama 10 tahun dan/atau denda paling banyak Rp 10 M

		- Pasal 322 dipidana paling lama 9 bulan penjara atau denda paling banyak Rp 6 - Pasal 323 dipidana paling lama 9 bulan penjara atau denda paling banyak Rp 6 - Pasal 431 dipidana paling lama 2 tahun penjara - Sistem penjantuhan pidana ada yang menggunakan sistem tunggal yaitu penjara saja tetapi ada juga yang menggunakan sistem alternatif yaitu pidana penjara atau denda. - Pasal 322&323 dituntut atas adanya pengaduan	
2	*Hacking*	- Pasal 167 dan 551 KUHP	- Pasal 30 ayat 1 dan 3 dengan sanksi Pasal 46 ayat 1 dan 3, Pasal 31 ayat 1 dan 2 dengan sanksi Pasal 47, Pasal 40 Undang-Undang Telekomunikasi
		- Pasal 167 menggunakan sistem perumusan alternatif yaitu pidana penjara paling lama 9 bulan atau denda paling banyak Rp 300	-Undang-Undang ITE menggunakan sistem perumusan alternatif kumulatif yaitu pidana penjara dan/atau denda
		- Pasal 551 menggunakan sistem perumusan tunggal yaitu pidana denda paling banyak Rp 15	- Ps 46 (1) pidana penjara maksimal 6 tahun dan/atau denda paling banyak Rp 600 juta

			- Ps 46 (3) pidana penjara maksimal 8 tahun dan/atau denda paling banyak Rp 800 juta - Pasal 47 dipidana dengan pidana penjara paling lama 10 (sepuluh tahun) dan/atau denda paling banyak Rp 800 juta - Pasal 56 Undang-Undang Telekomunikasi menggunakan sistem tunggal yaitu pidana penjara maksimal 15 tahun.
3	*Data Diddling*	- Pasal 263 KUHP	- Pasal 35, sanksi pidana Pasal 51 ayat 1
		- Sistem perumusan tunggal yaitu pidana penjara paling lama 6 tahun	- Sistem perumusan menggunakan sistem perumusan alternatif kumulatif dengan ancaman pidana penjara paling lama 12 tahun dan/atau denda paling banyak Rp 12 M
4	*Joycomputing*	- Pasal 362 KUHP	- Pasal 30 ayat 2 dan 32 ayat 2. Sanksi pidana Pasal 46 ayat 2 dan Pasal 48 ayat 2
		- Sistem perumusan pidana menggunakan sistem perumusan alternatif yaitu pidana penjara paling lama 5 tahun atau denda paling banyak Rp 60	- Sistem perumusan menggunakan sistem alternatif kumulatif dengan ancaman pidana penjara dan/atau denda. - Pasal 46 (2) pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp

			700 juta
			- Pasal 48 (2) pidana penjara paling lama 9 (sembilan tahun) dan/atau denda paling banyak Rp 3M
5	*The Trojan Horse*	-Pasal 372 KUHP dan 374 KUHP	- Pasal 32 ayat 1 dan sanksi pidana Pasal 48 ayat 1, Pasal 33 dan sanksi pidana Pasal 49
		- Pasal 372 menggunakan sistem perumusan alternatif dengan ancaman pidana penjara paling lama 4 (empat tahun) atau denda paling banyak Rp 60	- Sistem perumusan sanksinya adalah alternatif kumulatif
			- Pasal 48 (1) pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp 2M
		- Pasal 374 sistem perumusan tunggal yaitu pidana penjara paling lama 5 (lima) tahun	
		- Pasal 3 Undang-Undang Pemberantasan Tindak Pidana Korupsi pidana penjara seumur hidup atau pidana penjara paling singkat 1 (satu) tahun dan paling lama 20 (duapuluh) tahun dan/atau denda paling sedikit Rp 50.000.000,00 (lima puluh juta rupiah) dan paling banyak Rp 1.000.000.000,00 (satu miliar rupiah)	- Pasal 49 pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp 10 M
6	Penyia-nyiaan Data Komputer	- Pasal 406 ayat 1 KUHP	- Pasal 32 ayat 1 dan sanksi pidana Pasal 48 ayat 1 - Pasal 33 dan sanksi

			pidana Pasal 49
		-Sistem perumusan pidananya adalah alternatif dengan ancaman pidana penjara paling lama 2 (dua) tahun 8 (delapan) bulan atau denda paling banyak Rp 300	- Sistem perumusan sanksinya adalah alternatif kumulatif - Pasal 48 (1) pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp 2M - Pasal 49 pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp 10 M
7	Pembajakan Perangkat Lunak		- Sistem perumusannya adalah alternatif kumulatif dengan pidana penjara paling lama 5 (lima) tahun dan/atau denda paling banyak Rp 500 juta.

Sumber: Bahan Hukum Primer diolah, 2009

BAB V

PENUTUP

A. KESIMPULAN

1. Pengaturan Kualifikasi Perbuatan dalam Hubungannya dengan Kebijakan Kriminal

Berdasarkan hasil pembahasan yang telah dipaparkan, maka dapat disimpulkan bahwa bentuk-bentuk perbuatan yang diatur dalam Undang-Undang ITE lebih jelas dan terperinci. Dalam Undang-Undang ITE lebih diatur secara rinci bentuk-bentuk perbuatannya seperti merusak, menghilangkan, menyembunyikan, mengakses dan lain sebagainya yang mana dalam KUHP belum diatur secara jelas. Dengan aturan perbuatan yang lebih rinci tersebut, maka aparat penegak hukum dapat lebih mudah menafsirkan bentuk-bentuk perbuatan terkait dengan kejahatan komputer.

Selain itu, terkait dengan kebijakan kriminal yang mengatur suatu perbuatan yang semula bukan tindak pidana menjadi suatu perbuatan yang dapat dipidana, maka Undang-Undang ITE memenuhi rumusan ini. Hal ini disebabkan karena dalam KUHP belum adanya aturan yang mengatur secara tegas terkait dengan kejahatan komputer sehingga bentuk perbuatan dan objeknya perlu dilakukan suatu penafsiran yang memperluas pengertian dari rumusan pasal tersebut yang mana akibat dari perluasan tersebut seringkali sulit untuk menjatuhkan pidana terkait dengan kejahatan komputer. Dengan adanya Undang-Undang ITE, maka kejahatan komputer yang semula sulit untuk dikenai sanksi pidana karena belum adanya aturan yang mengatur,

maka saat ini sudah dapat dikenai sanksi karena telah ada aturan yang mengatur yaitu adanya Undang-Undang ITE.

Dalam Undang-Undang ITE, objek dari rumusan pasal yang diatur jelas yaitu informasi elektronik dan/atau dokumen elektronik serta sistem elektronik dan/atau komputer sehingga tidak diperlukan lagi penafsiran yang justru menyulitkan aparat penegak hukum. Selain perbedaan, antara KUHP dan Undang-Undang ITE juga terdapat persamaannya yaitu subjek hukum dari aturan tersebut yang sama-sama ditujukan kepada semua orang kecuali dalam Pasal 431 KUHP yang ditujukan pada lembaga pejabat pengangkutan umum.

2. Pengaturan Ancaman Pidana sebagai Bentuk Kebijakan Penal

Dalam kesimpulan yang kedua dapat disimpulkan bahwa bentuk ancaman pidana dalam KUHP lebih sering menggunakan sistem perumusan tunggal atau sistem perumusan alternatif. Dalam sistem perumusan tunggal maupun alternatif, yang sering digunakan yaitu pidana penjara atau denda.

Dalam Undang-Undang ITE, sistem perumusan sanksi yang digunakan yaitu sistem perumusan alternatif kumulatif yaitu pidana penjara dan/atau denda. Dalam Undang-Undang ITE, Undang-Undang Pemberantasan Tindak Pidana Korupsi, dan Undang-Undang Hak Cipta seluruhnya menggunakan sistem perumusan alternatif kumulatif. Hal ini disebabkan karena tindak pidana yang dilakukan adalaha tindak pidana khusus. Penggunaan sistem alternatif kumulatif yang ancaman pidananya berat tersebut memiliki tujuan yaitu untuk melindungi dan mensejahterakan

masyarakat yang sudah dirugikan dari adanya kejahatan komputer ini sesuai dengan tujuan awal kebijakan sosial masyarakat Dengan ancaman yang berat tersebut diharapkan agar masyarakat tidak melakukan suatu bentuk kejahatan komputer.

B. SARAN

1. Bagi Aparat Penegak Hukum

Berkaitan dengan kejahatan komputer, maka bagi aparat penegak hukum disarankan untuk menggunakan Undang-Undang ITE dalam menangani kasus kejahatan komputer maupun kejahatan lain yang terkait dengan informasi elektronik. Rumusan pasal yang terdapat dalam Undang-Undang ITE dirasa sudah cukup lengkap dan tegas sehingga dapat langsung diterapkan tanpa perlu adanya suatu penganalogian dalam menafsirkan rumusan pasal yang terdapat dalam Undang-Undang ITE.

Selain itu, dengan adanya Undang-Undang ITE, disarankan kepada seluruh aparat penegak hukum untuk mulai menyamakan suatu pandangan tentang bentuk kejahatan komputer sehingga mempermudah untuk melakukan suatu penyelidikan, penyidikan, pembuktian sampai pada putusan hakim. Dalam usaha non-penal, diharapkan bahwa aparat penegak hukum juga melakukan suatu sosialisasi tentang Undang-Undang ITE, sehingga masyarakat dapat mengetahui dan dapat menjahui bentuk-bentuk kejahatan komputer tersebut.

2. Bagi Masyarakat

Saat ini sudah ada suatu undang-undang baru yang mengatur tentang suatu bentuk informasi elektronik yang mana selama ini sulit untuk diselesaikan dengan menggunakan KUHP yaitu Undang-Undang ITE. Dengan adanya Undang-Undang ITE yang mengatur segala hal terkait dengan kejahatan komputer ataupun kejahatan lainnya yang berkaitan dengan informasi elektronik, maka disarankan kepada masyarakat untuk tidak lagi melakukan suatu bentuk kejahatan komputer atau kejahatan lainnya yang berkaitan dengan informasi elektronik tersebut. Hal ini disebabkan karena pengaturan dalam Undang-Undang ITE cukup jelas dan tegas mengatur tentang kejahatan komputer yang mana ancaman hukuman yang diberikan juga berat.

DAFTAR PUSTAKA

Buku

Arief, Didik M. & Elisatris Gultom, 2005, *Cyber Law*, PT. Refika Aditama, Bandung

Chazawi, Adami, 2005, *Pelajaran Hukum Pidana*, PT. RajaGrafindo Persada, Jakarta

Hamzah, Andi, 1987, *Aspek-Aspek Pidana Dibidang Komputer*, Sinar Grafika, Jakarta

----------, 1996, *Hukum Pidana yang Berkaitan dengan Komputer*, Sinar Grafika, Jakarta

Ibrahim, Johnny, 2007**,** *Teori dan Metodologi Penelitian Hukum Normatif*, Bayumedia, Malang

Magdalena, Merry & Maswigrantoro Roes Setiyadi, 2007**,** *Cyberlaw, Tidak Perlu Takut***,** C.V Andi Offset, Yogyakarta

Makarim, Edmon, 2003, *Kompilasi Hukum Telematika*, PT. RajaGrafindo Persada, Jakarta

Moeljatno, *Kitab Undang-Undang Hukum Pidana*, 1999, cetakan 19, Bumi Aksara, Jakarta

Muladi & Barda Nawawi, 2005, *Teori-Teori dan Kebijakan Pidana*, PT. Alumni, Bandung

Priyatno, Dwidja, 2006, *Sistem Pelaksanaan Pidana Penjara di Indonesia*, PT. Refika Aditama, Bandung

Rubai, Masruchin, 2001, *Asas-Asas Hukum Pidana*, Kerjasama antara UM PRESS dan FH UB, Malang

Sholehuddin, 2004**,** *Sistem Sanksi Dalam Hukum Pidana***,** PT. RajaGrafindo Persada, Jakarta

Wahid, Abdul, 2002, *Kejahatan Mayantara*, PT.Refika Aditama, Bandung

Wisnubroto, Al, 1999, *Kebijakan Hukum Pidana Dalam Penanggulangan Penyalahgunaan Komputer*, Universitas Atmajaya Yogyakarta

Tesis dan Disertasi

Harun Al Rasyid, 1999, "Tinjauan Yuridis Kriminologis Penerapan Pasal-Pasal KUHP dan Pasal-Pasal Undang-Undang Di Luar KUHP Terhadap Kejahatan Komputer**",** Tesis tidak diterbitkan, Malang Fakultas Hukum Universitas Brawijaya

Iwan Winarso, 2004, "Aspek Yuridis-Kriminologis Penerapan Pasal-Pasal KUHP Terhadap Pelaku Kejahtan yang menggunakan Sarana Komputer," Tesis tidak diterbitkan, Malang, Fakultas Hukum Universitas Brawijaya

Widodo, 2006, "Kebijakan Kriminal Terhadap Kejahatan Yang Berhubungan Dengan Komputer Di Indonesia," Disertasi tidak diterbitkan, Program Pasca Sarjana Universitas Brawijaya

Internet

Lima Tahun Polri Tangani 71 Kejahatan 'Cyber Crime',http://www.kapanlagi.com.

PosKota, *Dedemit Dunia Maya Acak situs-Situs Penting*, http;//www.postkotanews baca.asp.htm. Diakses 30 Seotember 2008

Syahnan, *Landasan Teori Sistem Informasi*, http://www.google.com

Suhartono, *Penanggulangan Kejahatan Hacking di Indonesia*. http://www.google.com. Diakses tanggal 16 Oktober 2008

Teguh Arifiyadi, SH (Inspektorat Jenderal Depkominfo), *Menjerat Pelaku Cyber Crime dengan KUHP***,**http://www.google.com.

Undang-Undang

Undang-Undang Nomor 36 Tahun 1999 Telekomunikasi

Undang-Undang Nomor 20 Tahun 2001 yang merupakan perubahan dari Undang-Undang Nomor 31 Tahun 1999 Tentang Pemberantasan Tindak Pidana Korupsi

Undang-Undang Nomor 19 Tahun 2002 Hak Cipta

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik