

### **BAB III**

#### **TINJAUAN UMUM *CYBER CRIME***

##### **A. Pengertian Kejahatan**

Berbicara tentang kejahatan sebenarnya tidak lepas dari dunia nyata dalam kehidupan masyarakat itu berada. Kejahatan merupakan cap atau sebutan yang digunakan oleh masyarakat dalam menilai suatu perbuatan seseorang. Dalam mendefinisikan kejahatan, ada beberapa pandangan mengenai perbuatan apakah yang dapat dikatakan sebagai kejahatan. Dalam KBBI kejahatan mempunyai pengertian perilaku yang bertentangan dengan nilai dan norma yang berlaku yang telah disahkan oleh hukum tertulis.<sup>51</sup> Sedangkan secara empiris, definisi kejahatan dalam pengertian yuridis tidak sama dengan pengertian kejahatan dalam kriminologi yang dipandang secara sosiologis.

Secara yuridis, kejahatan dapat didefinisikan sebagai suatu tindakan yang melanggar undang-undang atau ketentuan yang berlaku dan diakui secara legal. Secara kriminologi yang berbasis sosiologis kejahatan merupakan suatu pola tingkah laku yang merugikan masyarakat (dengan kata lain terdapat korban) dan suatu pola tingkah laku yang mendapatkan reaksi sosial dari masyarakat.<sup>52</sup>

Sedangkan Bonger menyatakan bahwa kejahatan adalah merupakan perbuatan anti sosial yang secara sadar mendapat reaksi dari negara berupa

---

<sup>51</sup> Departemen Pendidikan Nasional, *op.cit.* h. 450

<sup>52</sup> Abdul Wahid dan Muhammad Labib, *Kejahatan Mayantara (Cyber Crime)*, Bandung: PT Refika Aditama, 2005, h.37

berupa pemberian derita dan kemudian sebagai reaksi terhadap rumusan-rumusan hukum (*legal definitions*) mengenai kejahatan.<sup>53</sup>

J.E. Sahetapy dan B. Marjono Reksodiputro dalam bukunya “Paradoks Dalam Kriminologi” yang dikutip oleh Syahrudin Husein menyatakan bahwa, kejahatan mengandung konotasi tertentu, merupakan suatu pengertian dan penamaan yang relatif, mengandung variabilitas dan dinamik serta bertalian dengan perbuatan atau tingkah laku (baik aktif maupun pasif), yang dinilai oleh sebagian mayoritas atau minoritas masyarakat sebagai suatu perbuatan anti sosial, suatu perkosaan terhadap skala nilai sosial dan atau perasaan hukum yang hidup dalam masyarakat sesuai dengan ruang dan waktu.<sup>54</sup>

Dari beberapa pengertian yang telah disebutkan dapat disimpulkan bahwa unsur penting dari pengertian kejahatan adalah perbuatan yang merugikan dan menimbulkan ketidaktenangan masyarakat dan bertentangan dengan kepentingan umum. Seiring berjalannya waktu, cara pandang terhadap nilai dan moral pun akan berubah yang merupakan salah satu tolak ukur terhadap suatu perbuatan itu dianggap jahat atau tidak.

## **B. Kejahatan Mayantara (*Cyber Crime*)**

Istilah *cyber crime* banyak bermunculan seiring dengan berkembangnya teknologi. *Cyber crime* lebih sering disebut dengan tindak kejahatan yang berhubungan dengan dunia maya (*cyber space*) atau tindak

---

<sup>53</sup> Nasrulloh, Pengertian Kejahatan, <http://nasrullaheksplorier.blogspot.com/2008/10/pengertian-kejahatan.html> diakses pada tanggal 29 Juli 2011 pukul 11.21 WIB

<sup>54</sup> Syahrudin Husein, “Kejahatan dalam Masyarakat dan Penanggulangannya”, Sumatera Utara: Universitas Sumatera Utara, 2003, h.1, t.d.

kejahatan menggunakan komputer. Ada beberapa pendapat yang menyamakan antara tindak pidana kejahatan komputer dengan *cyber crime*, dan ada pendapat yang membedakan antara keduanya. Meskipun belum ada kesepakatan mengenai definisi kejahatan teknologi informasi, namun ada kesamaan pengertian mengenai kejahatan komputer.

Dalam laporan kongres PBB X/2000 dinyatakan *cyber crime* atau *computer-related crime*, mencakup keseluruhan bentuk-bentuk baru dari kejahatan yang ditujukan pada komputer, jaringan komputer dan para penggunanya, dan bentuk-bentuk kejahatan tradisional yang sekarang dilakukan dengan menggunakan atau dengan bantuan peralatan komputer.<sup>55</sup>

Pengertian lainnya diberikan oleh *Organization of European Community Development*, yaitu “*any illegal, unethical or unauthorized behavior relating to the automatic processing and/or the transmission of data*”.<sup>56</sup>

Didik M.Arief Mansur dan Elisatris Gultom dalam bukunya *Cyber Law-Aspek Hukum Teknologi Informasi* menyatakan bahwa “secara umum yang dimaksud kejahatan komputer atau kejahatan di dunia *cyber* (*cybercrime*) adalah upaya memasuki dan atau menggunakan fasilitas komputer atau jaringan komputer tanpa ijin dengan melawan hukum dengan

---

<sup>55</sup> Barda Nawawi Arief, *loc.cit.* h.259

<sup>56</sup> Mas Wigrantoro Roes Setiyadi dan Mirna Dian Avanti Siregar, Naskah Akademik Rancangan Undang-Undang Tindak Pidana di Bidang Teknologi Informasi, November, 2003, h.25 dalam <http://www.gipi.or.id/download/Naskah%20Akademik> diakses pada tanggal 30 Juli 2011 pukul 19.01 WIB

atau tanpa menyebabkan perubahan dan atau kerusakan pada fasilitas komputer yang dimasuki atau digunakan tersebut”.<sup>57</sup>

Indra Safitri mengemukakan, kejahatan dunia maya (*cyber crime*) adalah jenis kejahatan yang berkaitan dengan pemanfaatan sebuah teknologi informasi tanpa batas serta memiliki karakteristik yang kuat dengan sebuah rekayasa teknologi yang mengandalkan kepada tingkat keamanan yang tinggi dan kredibilitas dari sebuah informasi yang disampaikan dan diakses oleh pelanggan internet.<sup>58</sup>

Menurut Andi Hamzah, *cyber crime* merupakan kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara ilegal.<sup>59</sup>

Dari semua perumusan atau batasan yang diberikan mengenai *cyber crime* dapat disimpulkan bahwa karakteristik *cyber crime* adalah:

- a) Perbuatan anti sosial yang muncul sebagai dampak negatif dari pemanfaatan teknologi informasi tanpa batas.
- b) Memanfaatkan rekayasa teknologi yang mengandalkan kepada tingkat keamanan yang tinggi dan kredibilitas dari sebuah informasi. Salah satu rekayasa teknologi yang dimanfaatkan adalah internet.
- c) Perbuatan tersebut merugikan dan menimbulkan ketidaktenangan di masyarakat, serta bertentangan dengan moral masyarakat

---

<sup>57</sup> Didik M.Arief Mansur dan Elisatris Gultom, *Cyber Law-Aspek Hukum Teknologi Informasi*, Bandung: PT Refika Aditama, 2009, h.8

<sup>58</sup> Indra Safitri, Tindak Pidana di Dunia Cyber, 1999 dalam [http://business.fortunecity.com/buffett/842/art180199\\_tindakpidana.htm](http://business.fortunecity.com/buffett/842/art180199_tindakpidana.htm) diakses pada tanggal 13 Juli 2011 pukul 20.05 WIB

<sup>59</sup> Andi Hamzah, *Hukum Pidana Yang Berkaitan Dengan Komputer*, Jakarta: Sinar Grafika, 1996, h.10

- d) Perbuatan tersebut dapat terjadi lintas negara. Sehingga melibatkan lebih dari satu yurisdiksi hukum.

### C. Klasifikasi dan Jenis-Jenis *Cyber Crime*

#### 1. Klasifikasi *Cyber crime*

*Cyber crime* dapat diklasifikasikan menjadi tiga, yaitu:

- a. *Cyberpiracy* yaitu penggunaan teknologi komputer untuk mencetak ulang software atau informasi, lalu mendistribusikan informasi atau *software* tersebut lewat teknologi komputer misalnya pembajakan *software*.
- b. *Cybertrespass* yaitu penggunaan teknologi komputer untuk meningkatkan akses pada sistem komputer suatu organisasi atau individu misalnya *hacking exploit sytem* dan seluruh kegiatan yang berhubungan dengannya.
- c. *Cyber vandalism* yaitu penggunaan teknologi komputer untuk *membuat* program yang mengganggu proses transmisi elektronik, dan menghancurkan data di sistem komputer misalnya virus, *trojan*, *worm*, metode DoS, *http attack*, *BruteForce Attack* dan lain sebagainya.<sup>60</sup>

#### 2. Jenis-Jenis *Cyber Crime*

Dari klasifikasi kejahatan dunia maya di atas dapat diketahui jenis-jenis *cybercrime* berdasarkan jenis aktivitasnya dan tentunya

---

<sup>60</sup> Poni, Kejahatan Internet (*Cyber Crime*) dan Pernak-Perniknya, <http://haifani.wordpress.com/2009/08/13/kejahatan-internetcybercrime-dan-segala-macam-pernak-perniknya/> diakses tanggal 26 Juni 2011 pukul 16.50 WIB

kegiatan ini yang marak di lakukan baik di Indonesia sendiri atau di negara lain,yaitu:<sup>61</sup>

- a. *Cyber Espionage* ialah kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (*computer network system*) pihak sasaran
- b. *Data Forgery* ialah kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai *scriptless document* melalui internet.
- c. *Data Theft* ialah kejahatan memperoleh data komputer secara tidak sah baik untuk digunakan sendiri ataupun untuk diberikan kepada orang lain.
- d. *Cyber Sabotage and Extortion* ialah kejahatan yang paling mengesankan. Kejahatan ini dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet.
- e. *Unauthorized Access to Computer System and Service* ialah Kejahatan yang dilakukan dengan memasuki/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau

---

<sup>61</sup> Mas Wigrantoro Roes Setiyadi dan Mirna Dian Avanti Siregar, Naskah Akademik Rancangan Undang-Undang Tindak Pidana di Bidang Teknologi Informasi, 2003, h.17 dalam <http://www.gipi.or.id/download/Naskah%20Akademik> diakses pada tanggal 30 Juli 2011 pukul 19.01 WIB

tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya.

*f. Offense against Intellectual Property* ialah Kejahatan ini ditujukan terhadap hak atas kekayaan intelektual yang dimiliki pihak lain di internet.

*g. Illegal Contents* ialah kejahatan dengan memasukkan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum.

*h. Carding* ialah Kejahatan dengan menggunakan teknologi computer untuk melakukan transaksi dengan menggunakan *card credit* orang lain sehingga dapat merugikan orang tersebut baik materil maupun non materil

*i. Cracking* ialah kejahatan yang paling mengesankan. Kejahatan ini dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet

Dalam skripsi ini penulis membatasi permasalahan pada tiga kasus yaitu pengaksesan sistem elektronik milik orang lain tanpa izin, pencurian dokumen elektronik, dan perusakan sistem elektronik. Selanjutnya kasusnya akan penulis paparkan dalam uraian berikut:

### 1. *Unauthorized Access to Computer System and Service*

Kejahatan yang dilakukan dengan memasuki/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya.<sup>62</sup> Biasanya pelaku kejahatan (*hacker*) melakukannya dengan maksud sabotase ataupun pencurian informasi penting dan rahasia. Namun begitu, ada juga yang melakukan hanya karena merasa tertantang untuk mencoba keahliannya menembus suatu sistem yang memiliki tingkat proteksi tinggi. Kejahatan ini semakin marak dengan berkembangnya teknologi internet/intranet. Bagi yang belum pernah dengar, beberapa *website* milik pemerintah RI dirusak oleh *hacker*. Kisah seorang mahasiswa FISIPOL (Fakultas Ilmu Sosial dan Politik) yang ditangkap gara-gara mengacak-acak data milik KPU (Komisi Pemilihan Umum) dan masih banyak contoh lainnya.

Perbuatan ini merupakan kejahatan *illegal access* yaitu melakukan akses secara tidak sah. Perbuatan ini sudah diatur dalam pasal 30 Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi elektronik disebutkan, bahwa:

“setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain (

---

<sup>62</sup> Mas Wigrantoro Roes Setiyadi dan Mirna Dian Avanti Siregar, *op.cit*, h.17 dalam <http://www.gipi.or.id/download/Naskah%20Akademik> diakses pada tanggal 30 Juli 2011 pukul 19.01 WIB

ayat (1)) dengan cara apapun, (ayat (2)) dengan cara apa pun dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen elektronik, (ayat (3)) dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.”<sup>63</sup>

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

Untuk ayat (3), ketentuan pidananya adalah pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah).

## 2. *Data Theft*

Merupakan kejahatan memperoleh data komputer secara tidak sah baik untuk digunakan sendiri ataupun untuk diberikan kepada orang lain.<sup>64</sup> *Identity theft* merupakan salah satu jenis kejahatan ini yang sering diikuti dengan kejahatan penipuan (*fraud*). Kejahatan ini juga sering diikuti dengan kejahatan *data leakage* (membocorkan data rahasia).

---

<sup>63</sup> *ibid*, h.237

<sup>64</sup> Dwi Eka Wiratama, *op.cit*, t.d, h.36

Pencurian data merupakan perbuatan yang telah mengganggu hak pribadi seseorang, terutama jika si pemilik data tidak menghendaki ada orang lain yang mengambil atau bahkan sekedar membaca datanya tersebut. Pasal 32 ayat (2) Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik dapat digunakan menjerat pelaku.

“Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak.”<sup>65</sup>

Dapat dipidana dengan ketentuan pidana sebagaimana diatur dalam pasal 48 ayat (2), yaitu dipidana penjara paling lama 9 (sembilan) tahun dan/atau denda paling banyak Rp 3.000.000.000,00 (tiga miliar rupiah).

### 3. *Cyber Sabotage and Extortion*

Merupakan kejahatan yang paling mengesankan. Kejahatan ini dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet.<sup>66</sup> Biasanya kejahatan ini dilakukan dengan menyusupkan suatu *logic bomb*, virus komputer ataupun suatu program tertentu, sehingga data, program komputer atau sistem jaringan komputer tidak dapat digunakan, tidak berjalan sebagaimana mestinya, atau berjalan

---

<sup>65</sup> *ibid*, h.238

<sup>66</sup> *ibid*

sebagaimana yang dikehendaki oleh pelaku. Dalam beberapa kasus setelah hal tersebut terjadi, maka pelaku kejahatan tersebut menawarkan diri kepada korban untuk memperbaiki data, program komputer atau sistem jaringan komputer yang telah disabotase tersebut, tentunya dengan bayaran tertentu. Kejahatan ini sering disebut sebagai *cyber-terrorism*.

Untuk perusakan atau penghancuran terhadap suatu sistem atau pun data dari komputer. Dasar hukum nya diatur dalam pasal 33 Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, yaitu:

“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.”<sup>67</sup>

Kemudian ketentuan pidananya diatur dalam pasal 49 Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, yaitu pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp 10.000.000.000.00 (sepuluh milyar rupiah).

#### 4. *Cracking*

Kejahatan dengan menggunakan teknologi komputer yang dilakukan untuk merusak sistem keamanan suatu sistem komputer dan biasanya melakukan pencurian, tindakan anarkis begitu mereka mendapatkan akses. Biasanya kita sering salah

---

<sup>67</sup> *ibid*, h.238

menafsirkan antara seorang *hacker* dan *cracker* dimana *hacker* sendiri identik dengan perbuatan negatif, padahal *hacker* adalah orang yang senang memprogram dan percaya bahwa informasi adalah sesuatu hal yang sangat berharga dan ada yang bersifat dapat dipublikasikan dan rahasia. Sedangkan *cracker* identik dengan orang yang mampu merubah suatu karakteristik dan properti sebuah program sehingga dapat digunakan dan disebarluaskan sesuka hati padahal program itu merupakan program legal dan mempunyai hak cipta intelektual.

Dasar hukum nya diatur dalam pasal 33 Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, yaitu:

“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.”<sup>68</sup>

Kemudian ketentuan pidananya diatur dalam pasal 49 Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, yaitu pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp 10.000.000.000.00 (sepuluh milyar rupiah).

---

<sup>68</sup> *ibid*, h.238