

**KEJAHATAN *CYBER CRIME* DALAM PERSPEKTIF HUKUM  
PIDANA**

**Oleh :**

**Helmi Zaki Mardiansyah, S.H., M.H.**

## **a. Pendahuluan**

Globalisasi dan segala perkembangannya menawarkan janji-janji yang sangat menarik manusia. Hal ini dikarenakan globalisasi yang melahirkan ilmu pengetahuan dan teknologi yang amat membantu manusia. Ilmu pengetahuan dan teknologi telah menghasilkan sarana prasarana, piranti-piranti dan alat-alat yang mempermudah manusia dalam berbagai aktifitasnya. Pada intinya ilmu pengetahuan dan teknologi memberikan sesuatu yang memiliki nilai guna kepada manusia.

Perkembangan globalisasi dan era teknologi saat ini membuat segala sesuatunya yang dahulu amat sulit dilakukan menjadi mudah dan serba otomatis. Globalisasi dalam bidang teknologi telekomunikasi telah mempersempit wilayah dunia dan memperpendek jarak komunikasi. Sebagai contoh bahwa media elektronika komputer dengan jejaring internet membuat komunikasi menjadi tanpa batas dan dapat dilakukan oleh siapapun dan dimanapun.

Kemajuan teknologi yang merupakan hasil budaya manusia disamping membawa dampak positif, dalam arti dapat didayagunakan untuk kepentingan umat manusia juga membawa dampak negatif terhadap perkembangan manusia dan peradabannya. Dampak negatif yang dimaksud adalah yang berkaitan dengan dunia kejahatan. J.E Sahetapy menyatakan bahwa 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.<sup>1</sup>

Berbicara mengenai kejahatan, maka secara empiris definisi kejahatan dapat dilihat dari dua perspektif, *pertama* adalah kejahatan dalam perspektif yuridis, kejahatan yang dirumuskan sebagai perbuatan yang oleh negara diberi pidana. Pemberian pidana ini dimaksudkan untuk mengembalikan keseimbangan yang tertanggung akibat perbuatan itu. Perbuatan atau kejahatan yang dalam ilmu hukum pidana biasa disebut dengan tindak pidana (*strafbaarfeit*). *Kedua*, kejahatan dalam arti sosiologis (kriminologis) merupakan suatu perbuatan yang dari sisi

---

<sup>1</sup> Abdul Wahid dan Mohammad Labib, 2005, Kejahatan Mayantara (*cyber crime*), Refika Aditama, Bandung, hal 26.

sosiologis merupakan kejahatan sedangkan dari segi yuridis (hukum positif) bukan merupakan suatu kejahatan. Artinya, perbuatan tersebut oleh negara tidak dijatuhi pidana.<sup>2</sup>

Kejahatan adalah suatu tindakan anti sosial yang merugikan, tidak pantas, tidak dapat dibiarkan, yang dapat menimbulkan kegoncangan dalam masyarakat.<sup>3</sup> Sedangkan Van Bemmelen merumuskan, kejahatan adalah tiap kelakuan yang bersifat tidak susila dan merugikan, dan menimbulkan begitu banyak ketidaktenangan dalam suatu masyarakat tertentu, sehingga masyarakat itu berhak mencelanya dan menyatakan penolakannya atas kelakuan itu dalam bentuk nestapa dengan sengaja diberikan karena kelakuan tersebut. Dari pengertian tersebut dapat disimpulkan bahwa unsur penting dari pengertian kejahatan adalah, perbuatan yang anti sosial, merugikan dan menimbulkan ketidaktenangan masyarakat serta bertentangan dengan moral masyarakat. Namun hal tersebut dapat mengalami pergeseran cara pandang yang dipengaruhi oleh faktor moral masyarakat karena moral masyarakat menjadi tolok ukur perbuatan itu jahat atau tidak.<sup>4</sup>

Salah satu bentuk kejahatan yang ditimbulkan oleh perkembangan dan kemajuan teknologi informasi atau telekomunikasi adalah kejahatan yang berkaitan dengan aplikasi internet. Kejahatan ini dalam istilah asing disebut *Cybercrime*. Barda Nawawi Arief menggunakan istilah tindak pidana mayantara untuk menunjuk jenis kejahatan ini atau identik dengan “tindak pidana siber” (*cyberspace*).<sup>5</sup>

Secara garis besar, kejahatan yang berkaitan dengan teknologi informasi dapat dibagi menjadi dua bagian besar. Pertama, kejahatan yang bertujuan merusak atau menyerang sistem atau jaringan komputer. Dan kedua, kejahatan yang menggunakan komputer dan internet sebagai alat bantu dalam melancarkan kejahatan. Namun, mengingat teknologi informasi (telekomunikasi, komputer dan

---

<sup>2</sup> *Ibid*, hal 37-38.

<sup>3</sup> *Ibid*, hal 38

<sup>4</sup> *Ibid*, hal 39.

<sup>5</sup> Barda Nawawi Arief, 2010, *Kapita Selekta Hukum Pidana*, Citra Aditya Bakti, Bandung, hal 253.

media) dapat berkembang seiring waktu maka kejahatan jenis diatas dapat berkembang menjadi lebih luas lagi.

Dalam beberapa pandangan ahli, terdapat perbedaan dalam menafsirkan tentang *cyber crime*. Muladi dalam “Bunga Rampai Hukum Pidana“ berpendapat bahwa sudut pandang *cyber crime* adalah dengan menggunakan pendekatan *computer crime*. Namun adapula yang berpendapat bahwa sebenarnya *cyber crime* berbeda dengan *computer crime*. Walaupun demikian, sesungguhnya memang ada upaya untuk memperluas pengertian komputer agar dapat melingkupi segala kejahatan di internet dengan peralatan apapun, seperti pengertian komputer dalam *The Proposed West Virginia Computer Crimes Act*:<sup>6</sup>

*“an electronic, magnetic, optical, electrochemical or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typewriter or type-setter, a portable hand-held calculator, or other similiar device”*

Terjemahan bebasnya : peralatan pemrosesan data listrik, magnetik, optik, elektro kimia, atau peralatan kecepatan tinggi lainnya dalam melakukan logika aritmatika, atau fungsi penyimpanan dan memasukkan beberapa fasilitas penyimpanan data atau fasilitas komunikasi yang secara langsung berhubungan dengan operasi tersebut dalam konjungsi dengan peralatan tersebut tidak memasukkan mesin ketik otomatis atau tipe-setter, sebuah kalkulator tangan atau peralatan serupa lainnya.

Dengan demikian pendapat yang mengidentikkan *cyber crime* dengan *computer crime* dapat dipahami dengan menggunakan pendekatan pemaknaan komputer yang diperluas di atas.

Pengertian yang membedakan *cyber crime* dengan *computer crime* juga ada. Bahwa kejahatan komputer dapat melingkupi dalam lingkup luas bermacam-macam pelanggaran, aktifitas atau isu kriminal. Dengan maksud bahwa kejahatan komputer sebagai alat dan melibatkan hubungan langsung antara kriminal dan komputer. Kejahatan *cyber* merupakan kejahatan yang dilakukan secara *virtual*

---

<sup>6</sup> Abdul Wahid dan Mohammad Labib, *Op.cit*, hal 41.

melalui *internet online*. Hal ini berarti bahwa kejahatan yang dilakukan dapat berkembang ke negara lain yang berada diluar yurisdiksi negara yang bersangkutan.<sup>7</sup> Di lihat dari beberapa definisi tersebut tampak bahwa belum ada kesepakatan mengenai definisi *cyber crime* atau kejahatan *cyber*. Bahkan belum ada pengakuan internasional mengenai istilah baku, namun ada yang menyamakan istilah *cyber crime* dengan *computer crime*.

#### **b. Kejahatan Cyber Crime Dalam Perspektif Hukum Pidana**

Dalam hukum pidana, sesuatu yang dikatakan sebagai kejahatan apabila tindakan jahat tersebut dirumuskan dalam suatu delik atau tindak pidana, dan bagi pelanggarnya dapat dijatuhi pidana. Istilah tindak pidana atau *strafbaarfeit* di dalam bahasa Belanda ialah *Strafbaar* “dapat dihukum” dan *Feit* “sebagian dari suatu kenyataan”. Menurut beberapa ahli hukum dapat disebutkan sebagai berikut:<sup>8</sup>

1. HAZEWINKEL SURINGA, *strafbaarfeit* merupakan suatu perilaku manusia yang pada suatu saat tertentu telah ditolak di dalam sesuatu pergaulan hidup tertentu dan dianggap sebagai perilaku yang harus ditiadakan oleh hukum pidana dengan menggunakan sarana-sarana yang bersifat memaksa yang terdapat didalamnya.
2. POMPE, *strafbaarfeit* merupakan suatu tindakan yang menurut sesuatu rumusan Undang-undang telah dinyatakan sebagai tindakan yang dapat dihukum.
3. SIMONS, *strafbaarfeit* merupakan suatu tindakan melanggar hukum yang telah dilakukan dengan sengaja oleh seseorang yang dapat dipertanggungjawabkan atas tindakannya dan yang oleh undang-undang telah dinyatakan sebagai suatu tindakan yang dapat dihukum.

---

<sup>7</sup> *Ibid*, hal 42.

<sup>8</sup> P.A.F Lamintang, 1997, *Dasar-dasar Hukum Pidana Indonesia*, Citra Aditya Bakti, Bandung, hal 182-185.

Menurut SIMONS, bahwa *strafbaarfeit* dirumuskan sebagai berikut :

- a. Untuk adanya suatu *strafbaarfeit* disyaratkan bahwa harus terdapat suatu tindakan yang dilarang ataupun yang diwajibkan oleh undang-undang, dimana pelanggaran terhadap larangan atau kewajiban semacam itu telah dinyatakan sebagai suatu tindakan yang dapat dihukum;
- b. Agar sesuatu tindakan itu dapat dihukum, maka tindakan tersebut harus memenuhi semua unsur dari delik seperti yang dirumuskan dalam undang-undang, dan
- c. Setiap *strafbaarfeit* sebagai pelanggaran terhadap larangan atau kewajiban menurut undang-undang itu, pada hakikatnya merupakan suatu tindakan melawan hukum atau merupakan suatu “*onrechtmatige handeling*”

Pada intinya bahwa suatu perbuatan yang dilakukan serta melawan hukum namun dilanggar oleh seseorang, maka perbuatan yang bersangkutan dapat dikenakan suatu sanksi pidana menurut suatu peraturan yang berlaku.

*Cyber Crime* merupakan jenis baru dalam dunia kriminal. KUHP memiliki yurisdiksi yang jelas bahwa sesuai Pasal 2 KUHP menyebutkan bahwa ketentuan pidana dalam perundang-undangan Indonesia diterapkan bagi setiap orang yang melakukan sesuatu delik di Indonesia. Hal ini menurut saya menjadi hambatan dalam penegakan kejahatan siber (*cyber crime*) karena bisa jadi pelakunya melakukan kejahatan tersebut di luar Indonesia sedangkan korbannya adalah orang Indonesia. Sedangkan apabila sebaliknya, negara kita seakan tidak mampu karena belum adanya perjanjian *mutual legal assistant* dalam bidang hukum pidana (ekstradisi).

Penjelasan di atas merujuk pada definisi bahwa ruang *cyber* bersifat global, tidak terikat pada yurisdiksi nasional suatu negara. Hal ini karena *cyber space* tercipta melalui ruang internet. Pendapat bahwa *cyber crime* sama dengan *computer crime* terkadang tidak relevan lagi karena pelaku dapat menggunakan media atau alat lain dalam melakukan kejahatan tersebut.

Bentuk-bentuk *cyber crime* pada umumnya yang dikenal dalam masyarakat dibedakan menjadi 3 (tiga) kualifikasi umum, yaitu :<sup>9</sup>

1. Delik-delik yang berkaitan dengan kerahasiaan, integritas dan keberadaan data dan sistem komputer.
  - a. *Illegal access* (akses secara tidak sah terhadap sistem komputer)
  - b. *Data interference* (mengganggu data komputer)
  - c. *System interference* (mengganggu sistem komputer)
  - d. *Illegal interception in the computers, systems and computer networks operation* (intersepsi secara tidak sah terhadap komputer, sistem, dan jaringan operasional komputer)
  - e. *Misuse of devices* (menyalahgunakan peralatan komputer)
2. Delik-delik yang berhubungan dengan komputer: pemalsuan dan penipuan (*computer related offences; forgery and fraud*).
3. Delik-delik yang bermuatan pornografi anak (*content-related offences, child phornography*).
4. Delik-delik yang berhubungan dengan hak cipta (*offences-related of infringements of copyright*).

Mengacu pada Kitab Undang-Undang Hukum Pidana (KUHP), pengertian secara luas mengenai tindak pidana siber ialah semua tindak pidana yang menggunakan sarana atau dengan bantuan Sistem Elektronik. Itu artinya semua tindak pidana konvensional dalam Kitab Undang-Undang Hukum Pidana (KUHP) sepanjang dengan menggunakan bantuan atau sarana Sistem Elektronik seperti pembunuhan, perdagangan orang, dapat termasuk dalam kategori tindak pidana siber dalam arti luas.<sup>10</sup> Namun, hukum pidana (KUHP) menurut sebagian berpendapat tidak dapat menjangkau kejahatan ini, sementara sebagian yang lain berpendapat bahwa hukum pidana positif dapat menjangkau kejahatan ini. Untuk membahas *cyber crime* dalam perspektif hukum pidana maka saya akan

---

<sup>9</sup> Abdul Wahid dan Mohammad Labib, Op.cit, hal 74.

<sup>10</sup> "Landasan Hukum Penanganan *Cyber Crime* di Indonesia" – [www.hukumonline.com.htm](http://www.hukumonline.com.htm) diakses tanggal 18 Maret 2013.

mengkaitkan dengan delik yang diatur dalam KUHP. Ada beberapa contoh tindak pidana *cyber crime* yang dapat saya berikan, diantaranya:

### **1. Pencurian**

*Pasal 362*

*Barang siapa 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 pidana denda paling banyak sembilan ratus rupiah.*

Ketentuan Pasal di atas dapat digunakan dalam kasus pencurian nomor kartu kredit orang lain dengan menggunakan internet untuk melakukan transaksi. Setelah barang dikirimkan, penjual tidak dapat mencairkan uangnya karena pemilik kartu bukanlah orang yang melakukan transaksi.

### **2. Penipuan**

*Pasal 378*

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

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

### **3. Pemerasan dan Pengancaman**

*Pasal 335*

*(1) Diancam dengan pidana penjara paling lama satu tahun atau denda paling banyak empat ribu lima ratus rupiah:*

- 1. barang siapa secara melawan hukum memaksa orang lain supaya melakukan, tidak melakukan atau membiarkan sesuatu, dengan memakai kekerasan, sesuatu perbuatan lain maupun perlakuan*



- yang tak menyenangkan, atau dengan memakai ancaman kekerasan, sesuatu perbuatan lain maupun perlakuan yang tak menyenangkan, baik terhadap orang itu sendiri maupun orang lain;*
- 2. barang siapa memaksa orang lain supaya melakukan, tidak melakukan atau membiarkan sesuatu dengan ancaman pencemaran atau pencemaran tertulis.*
- (2) Dalam hal sebagaimana dirumuskan dalam butir 2, kejahatan hanya dituntut atas pengaduan orang yang terkena.*

Ketentuan pasal di atas dapat digunakan dalam kasus pengancaman dan pemerasan yang dilakukan melalui e-mail yang dikirimkan oleh pelaku untuk memaksa korban melakukan sesuatu sesuai dengan apa yang diinginkan oleh pelaku dan jika tidak dilaksanakan akan membawa dampak yang membahayakan. Hal ini biasanya dilakukan karena pelaku mengetahui rahasia korban.

#### **4. Pencemaran nama baik**

*Pasal 311 ayat (1)*

*Jika yang melakukan kejahatan pencemaran atau pencemaran tertulis dibolehkan untuk membuktikan apa yang dituduhkan itu benar, tidak membuktikannya, dan tuduhan dilakukan bertentangan dengan apa yang diketahui, maka dia diancam melakukan fitnah dengan pidana penjara paling lama empat tahun.*

Ketentuan Pasal di atas dapat digunakan pada Kasus pencemaran nama baik dengan menggunakan media Internet. Modusnya adalah pelaku menyebarkan email kepada teman-teman korban tentang suatu cerita yang tidak benar atau mengirimkan email ke suatu *mailing list* sehingga banyak orang mengetahui cerita tersebut.

#### **5. Judi online**

*Pasal 303 ayat (1) butir 1*

*(1) Diancam dengan pidana penjara paling lama sepuluh tahun atau pidana denda paling banyak dua puluh lima juta rupiah, barang siapa tanpa mendapat izin:*

- 1. dengan sengaja menawarkan atau memberikan kesempatan untuk permainan judi dan menjadikannya sebagai pencarian, atau dengan sengaja turut serta dalam suatu perusahaan untuk itu;*

Pasal 303 KUHP dapat dikenakan untuk menjerat permainan judi yang dilakukan secara *online* (ex: judi bola *online*) di Internet dengan penyelenggara dari Indonesia.

## **6. Pornografi**

*Pasal 282*

*Barang siapa menyiarkan, mempertunjukkan atau menempelkan di muka umum tulisan, gambaran atau benda yang telah diketahui isinya melanggar kesusilaan, atau barang siapa dengan maksud untuk disiarkan, dipertunjukkan atau ditempelkan di muka umum, membikin tulisan, gambaran atau benda tersebut, memasukkannya ke dalam negeri, meneruskannya, mengeluarkannya dari negeri, atau memiliki persediaan, ataupun barang siapa secara terang-terangan atau dengan mengedarkan surat tanpa diminta, menawarkannya atau menunjukkannya sebagai bisa diperoleh, diancam dengan pidana penjara paling lama satu tahun enam bulan atau pidana denda paling tinggi empat ribu lima ratus rupiah.*

Dapat dikenakan untuk penyebaran pornografi maupun *website* porno yang banyak beredar dan mudah diakses di Internet. Walaupun berbahasa Indonesia, sangat sulit sekali untuk menindak pelakunya karena mereka melakukan pendaftaran *domain* tersebut diluar negeri dimana pornografi yang menampilkan orang dewasa bukan merupakan hal yang ilegal. kasus penyebaran foto atau film pribadi seseorang yang vulgar di Internet , misalnya kasus terdahulu antara Sukma Ayu-B'jah dan kasus Ariel.

## **7. Hacking**

*Pasal 406*

*Barang siapa dengan sengaja dan melawan hukum menghancurkan, merusakkan, membikin tak dapat dipakai atau menghilangkan barang sesuatu yang seluruhnya atau sebagian milik orang lain, diancam dengan pidana penjara paling lama dua tahun delapan bulan atau pidana denda paling banyak empat ribu lima ratus rupiah.*

Pasal di atas dapat digunakan pada kasus *deface* atau *hacking* yang membuat sistem milik orang lain, seperti *website* atau program menjadi tidak berfungsi atau dapat digunakan sebagaimana mestinya.

Dari beberapa contoh kasus yang dikaitkan dengan tindak pidana *cyber crime* maka sebenarnya masih terdapat beberapa kekurangan dalam upaya penegakan hukumnya, pada kenyataannya sanksi yang dikenakan apabila menggunakan KUHP memang ringan. Padahal beberapa kasus yang terjadi mengakibatkan kerugian yang besar sehingga tidak sepadan dengan akibat yang ditimbulkan. Disamping itu, delik yang berkaitan dengan *cyber crime* dalam KUHP membutuhkan penafsiran yang luas, padahal hukum pidana menganut asas legalitas yang nantinya berpengaruh dalam upaya menjerat pelaku, apakah perlu dengan penafsiran secara luas mengingat hukum pidana hanya menerima penafsiran secara otentik saja.

### **c. Kesimpulan**

1. Secara yuridis, *cyber crime* hingga saat ini belum memiliki definisi yang baku. Sebagian berpendapat *cyber crime* identik dengan *computer crime* namun ada pula yang berpendapat berbeda. Alasannya adalah tidak semua *cyber crime* tersebut menggunakan komputer sebagai alat, namun bisa menggunakan juga alat yang lain. Permasalahan yurisdiksi juga mempengaruhi kinerja aparat penegak hukum untuk melakukan proses peradilan karena *cyber crime* melintasi batas teritorial bahkan di luar teritorial negara.
2. Hukum pidana belum mampu memberikan keefektifan dalam penegakan hukumnya, karena pasal yang terdapat dalam KUHP yang berkaitan dengan *cyber crime* sanksi yang dikenakan cukup ringan. Padahal beberapa kasus yang terjadi mengakibatkan kerugian yang besar sehingga tidak sepadan dengan akibat yang ditimbulkan. *Cyber crime* dalam KUHP memerlukan penafsiran yang luas sebagai jalan menuju kepastian hukum.

## DAFTAR PUSTAKA

### **Buku :**

Abdul wahid dan Mohammad Labib, 2005, *Kejahatan Mayantara (cyber crime)*, Refika Aditama, Bandung.

Andi Hamzah, 2004, *KUHP dan KUHAP*, Rineka Cipta, Jakarta.

Barda Nawawi Arief, 2003, *Kapita Selekta Hukum Pidana*, Citra Aditya Bakti, Bandung.

Moeljatno, 2000, *Asas-asas Hukum Pidana*, Rineka Cipta, Jakarta.

Muladi dan Barda Nawawi Arief, 1992, *Bunga Rampai Hukum Pidana*, Alumni, Bandung.

P.A.F Lamintang, 1997, *Dasar-dasar Hukum Pidana Indonesia* (cetakan ketiga), Citra Aditya Bakti, Bandung.

### **Internet :**

“Landasan Hukum Penanganan *Cyber Crime* di Indonesia” –  
[www.hukumonline.com/htm](http://www.hukumonline.com/htm)