BAB II

TINJAUAN UMUM MENGENAI TINDAK PIDANA CYBER CRIME (MAYANTARA)

A. Pengertian Cyber Crime

Membahas masalah *cyber crime* tidak lepas dari permasalahan keamanan jaringan komputer atau keamanan informasi berbasis internet dalam era global ini, apabila jika dikaitkan dengan persoalan informasi sebagai komoditi. Informasi sebagai komoditi memerlukan kehandalan pelayanan agar apa yang disajikan tidak mengecewakan pelanggannya. Untuk mencapai tingkat kehandalan tentunya informasi tersebut harus selalu dimutaakhirkan sehingga informasi yang disajikan tidak ketinggalan zaman. Kejahatan dunia maya *(cyber crime)* ini muncul seiring dengan perkembangan teknologi informasi yang begitu cepat. Untuk lebih mendalam ada beberapa pendapat tentang apa yang dimaksud dengan *cyber crime*?

Menurut Indra Safitri mengemukakan, kejahatan dunia maya 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.[1]

Penulis berpendapat bahwa *cyber crime* merupakan fenomena sosial yang merupakan sisi gelap dari kemajuan teknologi informasi yang menimbulkan kejahatan yang dilakukan hanya dengan duduk manis di depan komputer.

Menurut Kepolisian Inggris, *cyber crime* adalah segala macam penggunaan jaringan komputer untuk tujuan kriminal dan/atau kriminal berteknologi tinggi dengan menyalahgunakan kemudahan teknologi digital.[2]

Perkembangan teknologi informasi telah menggeser pradigma para ahli hukum dalam memberikan definisi dari kejahatan komputer, diawalnya para ahli hanya terfokus pada alat dan perangkat keras, yaitu komputer. Namun berkembangnya teknologi seperti internet, maka fokus dari definisi *cyber crime* adalah aktivitas yang dapat dilakukan di dunia siber melalui sistem informasi yang digunakan, sebagaimana yang diutarakan oleh Barda Nawawi Arief dengan kejahatan mayantara.Pada perkembangannya internet ternyata membawa sisi negatif, dengan membuka peluang munculnya tindakan-tindakan anti sosial yang selama ini dianggap tidak mungkin terjadi atau tidak terpikirkan akan terjadi. Sebuah teori menyatakan, *crime*

---

[1]Indra Safitri, 1999, *Tindak Pidana Di Dunia Cyber"* dalam *Insider, Legal Journal From Indonesian Capital & Investmen Market.*

[2]Abdul Wahid dan Mohammad Labib, 2005, *Kejahatan Mayantara (Cyber Crime)*, Jakarta: PT. Refika Aditama, hlm. 40.

is product of society its self, yang secara sederhana dapat diartikan bahwa masyarakat itu sendirilah yang menghasilkan kejahatan.

Pada dasarnya *cyber crime* merupakan kegiatan yang memanfaatkan komputer sebagai sarana atau media yang didukung oleh sistem telekomunikasi, baik menggunakan telepon atau *wireles system* yang menggunakan antena khusus yang nirkabel. Hal inilah yang disebut "telematika" yaitu konvergensi antar teknologi telekomunikasi, media dan informatika yang semula masing-masing berkembang secara terpisah.

Kejahatan yang lahir sebagai dampak negatif dari perkembangan aplikasi internet ini sering disebut dengan *cyber crime.* Dari pengertian ini tampak bahwa *cyber crime* mencakup semua jenis kejahatan beserta modus operandinya yang dilakukan sebagai dampak negatif aplikasi internet.

Widodo menjelaskan *cyber crime* dapat dibedakan menjadi 2 (dua) kategori, yaitu *cyber crime* dalam arti sempit dan *cyber crime* dalam arti luas. *Cyber crime* dalam arti sempit adalah kejahatan terhadap sistem komputer, sedangkan dalam arti luas mencakup kejahatan terhadap sistem atau jaringan komputer dan kejahatan yang menggunakan komputer.[3]

Secara umum, dapat kita simpulkan bahwa *cyber crime* merupakan keseluruhan bentuk kejahatan yang ditujukan terhadap komputer, jaringan

[3]Widodo, 2009, *Sistem Pemidanaan dalam Cyber Crime,* Yogyakarta: Laksbang Meditama, hlm. 24.

komputer, dan para penggunanya serta bentuk-bentuk kejahatan tradisional berupa tindak pidana dengan bantuan komputer.

B. Karakteristik dan Bentuk-Bentuk Cyber Crime

Menurut Abdul Wahid dan M. Labib, *cyber crime* memiliki beberapa karakteristik, yaitu :[4]

1) perbuatan yang dilakukan secara illegal, tanpa hak atau tindakan etis terjadi diruang/wilayah siber, sehingga tidak dapat dipastikan yuridiksi negara mana yang berlaku terhadapnya;
2) perbuatan tersebut dilakukan dengan menggunakan peralatan apapun yang berhubungan dengan internet;
3) perbuatan tersebut mengakibatkan kerugian materiil maupun immateriil yang cenderung lebih besar dibandingkan dengan kejahatan konvensional;
4) pelakunya adalah orang yang menguasai penggunaan internet dan aplikasinya;
5) perbuatan tersebut sering dilakukan secara transnasional.

Cyber crime muncul akibat kemajuan teknologi informasi dan digital, yang memudahkan orang-orang untuk melakukan komunikasi, mendapatkan informasi serta memudahkan bisnis. Disisi lain, kemudahan yang diberikan oleh teknologi, menjadikan teknologi sebagai target untuk memperoleh dan menyebarkan gangguan. Dengan demikian, karakteristik

[4]Abdul Wahid dan M. Labib, *Kejahatan Mayantara (Cybercrime), op.cit*. hlm. 76.

dari *cyber crime* adalah penggunaan atau pemanfaatan teknologi informasi yang berbasis komputer untuk melakukan kejahatan yang didukung oleh teknologi informasi dan digital.

Kejahatan yang berhubungan erat dengan penggunaan teknologi yang berbasis komputer dan jaringan telekomunikasi dalam beberapa literatur dan praktiknya dikelompokkan dalam bentuk, antara lain[5] :

1. *Unauthorized access to computer system and service*, yaitu kejahatan yang dilakukan dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin, atau tanpa pengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. Biasanya pelaku kejahatan (hacker) melakukannya dengan maksud sabotase ataupun pencurian informasi penting dan rahasia. Namun, ada juga yang melakukannya hanya karena merasa tertantang untuk mencoba keahliannya menembus suatu sistem yang memiliki tingkat proteksi tinggi. Kejahatan ini semakin marak dengan berkembangnya teknologi internet.
2. *Illegal contents*, yaitu kejahatan dengan memasukkan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis, dan dianggap melanggar hukum atau menganggu ketertiban umum.
3. *Data forgery*, yaitu kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai *scrptless document* melalui internet. Kejahatan ini biasanya ditujukan pada dokumen-dokumen e-

[5]Maskun, 2013, *Kejahatan Siber (Cyber Crime) Suatu Pengantar*, Jakarta: Kharisma Putra Utama, hlm. 51-54.

commerce dengan membuat seolah-olah terjadi “salah ketik” yang pada akhirnya akan menguntungkan pelaku.

4. *Cyber espionage,* yaitu kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer *(computer network system)*pihak sasaran. Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen atau data-data pentingnya tersimpan dalam suatu sistem komputerisasi.
5. *Cyber sabotage and extortion,* yaitu kejahatan yang dilakukan dengan membuat gangguan, perusakan, atau pengahancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang tersambung dengan internet.
6. *Offence against intellectual property,* yaitu kekayaan yang ditujukan terhadap hak kekayaan intelektual yang dimiliki seseorang di internet. Contohnya peniruan tampilan *web page* suatu situs milik orang lain secara ilegal.
7. *Infringements of privacy,* yaitu kejahatan yang ditujukan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia.

Adapun jenis-jenis *cyber crime* berdasarkan motifnya, yaitu :

a. *Cyber crime* sebagai tindak kejahatan murni

Dimana orang yang melakukan kejahatan yang dilakukan secara di sengaja. Contohnya pencurian, tindakan anarkis terhadap suatu sistem informasi atau sistem komputer.

b. *Cyber crime* sebagai tindakan kejahatan abu-abu

   Dimana kejadian ini tidak jelas antara kejahatan kriminal atau bukan, karena pelaku melakukan pembobolan tetapi tidak merusak, mencuri, atau melakukan perbuatan anarkis terhadap sistem informasi atau sistem komputer.

c. *Cyber crime* yang menyerang individu

   Kejahatan yang dilakukan terhadap orang lain dengan motif dendam atau iseng yang bertujuan untuk merusak nama baik, contohnya pornografi, *cyber stalking*, dan lain-lain.

d. *Cyber crime* yang hak cipta (hak milik)

   Kejahatan yang dilakukan terhadap hasil karya seseorang dengan motif menggandakan, memasarkan, mengubah yang bertujuan untuk kepentingan pribadi/umum ataupun demi materi/nonmateri.

e. *Cyber crime* yang menyerang pemerintah

   Kejahatan yang dilakukan dengan pemerintah sebagai objek dengan motif melakukan teror, membajak ataupun merusak keamanan.

C. Aturan Hukum Cyber Crime

Muhammad Kusnardi dan Bintan Saragih berpendapat bahwa negara hukum menentukan alat-alat perlengkapan yang bertindak menurut dan terikat kepada peraturan-peraturan yang ditentukan terlebih dahulu oleh

alat-alat perlengkapan yang dikuasakan untuk mengadakan peraturan-peraturan tersebut.[6]

Alat negara itu yang bertanggung jawab untuk menggunakan hukum sebagai senjata guna melawan berbagai bentuk kejahatan yang akan, sedang atau telah mengancam bangsa. Alat negara (penegak hukum) dituntut bekerja keras seiring dengan perkembangan dunia kejahatan, khususnya perkembangan *cyber crime* yang semakin mengkhawatirkan. Alat negara ini menjadi subjek utama yang berperang melawan *cyber crime.*

Misalnya Resolusi PBB Nomor 55 Tahun 1963 tentang upaya untuk memerangi kejahatan penyalahgunaan TI (Teknologi Informasi) pada tanggal 4 Desember 2001, memberikan indikasi bahwa ada masalah internasional yang sangat serius, gawat dan harus segera ditangani.

Penyalahgunaan TI telah menjadi salah satu agenda dari kejahatan di tingkat global. Kejahatan di tingkat global ini menjadi ujian berat bagi masing-masing negara untuk memeranginya. Alat yang digunakan oleh negara untuk memerangi *cyber crime* ini adalah hukum. Hukum difungsikan salah satunya mencegah terjadinya dan menyebarnya *cyber crime*, serta menindak jika *cyber crime* terbukti telah menyerang atau merugikan masyarakat dan negara.

---

[6]Muhammad Kusnardi dan Bintan Saragih dalam kutipan Abdulla Wahid, dkk, 2005, *Kejahatan Mayantara (Cyber Crime),* Bandung: Refika Aditama, hlm. 136.

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

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang diundangkan di Jakarta pada tanggal 21 April 2008 dan dicatat dalam Lembaran Negara Republik Indonesia tahun 2008 Nomor 58 boleh dibilang sebagai jawaban pemerintah Indonesia untuk menghalangi *cyber crime.* Namun bukan Undang-Undang yang pertama kali di Indonesia yang dapat menjangkau *cybercrime*, karena jauh sebelum Undang-Undang ini disahkan, penegak hukum menggunakan KUHP untuk menjerat pelaku-pelaku *cyber crime* yang tidak bertanggung jawab dan menjadi sebuah payung hukum bagi masyarakat pengguna teknologi informasi guna mencapai sebuah kepastian hukum.

a) Pasal 27 Undang-Undang ITE Tahun 2008 :

"Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan yang melanggar kesusilaan. Ancaman pidana Pasal 45 ayat (1) KUHP. Pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp. 1.000.000.000,00 (satu miliar rupiah)".

Diatur pula dalam KUHP Pasal 282 mengenai kejahatan terhadap kesusilaan.

b) Pasal 28 Undang-Undang ITE Tahun 2008 :

"Setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi Elektronik".

c) Pasal 29 Undang-Undang ITE Tahun 2008 :

"Setiap orang dengan sengaja dan tanpa hak mengirimkan informasi elektronik dan/atau dokumen elektronik yang berisi ancaman, kekerasan atau menakut-nakuti yang ditujukan secara pribadi *(Cyber Stalking)*. Ancaman pidana Pasal 45 ayat (3), setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 29 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp. 2.000.000.000,00 (dua miliar rupiah)".

d) Pasal 30 ayat (3) Undang-Undang ITE Tahun 2008 :

"Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan *(cracking, hacking, illegal access).* Ancaman pidana Pasal 46 ayat (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 Rp. 800.000.000,00 (delapan ratus juta rupiah)".

e) Pasal 33 Undang-Undang ITE Tahun 2008 :

Setiap orang dengan sengaja dan tanpa hak melakukan atau melawan hukum melakukan tindakan apapun yang berakibat terganggunya

sistem elektronik dan/atau mengakibatkan sistem elektronik menjadi tidak bekerja sebagaimana mestinya.

f) Pasal 34 Undang-Undang ITE Tahun 2008 :

   Setiap orang dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan atau memiliki.

g) Pasal 35 Undang-Undang ITE Tahun 2008 :

   Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengerusakan informasi elektronik dan/atau dokumen elektronik dengan tujuan agar informasi elektronik dan/atau dokumen elektronik tersebut seolah-olah data yang otentik (*phising*, penipuan situs).

Aturan hukum mengenai cyber crime juga diatur didalam Kitab Undang-Undang Hukum Pidana, yaitu :

a) Pasal 362 KUHP, yang dikenakan untuk kasus carding.
b) Pasal 378 KUHP, dapat dikenakan untuk penipuan.
c) Pasal 335 KUHP, dapat dikenakan untuk kasus pengancaman dan pemerasan yang dilakukan melalui e-mail yang dikirimkan oleh pelaku untuk memaksa korban melakukan sesuatu sesuai dengan apa yang diinginkannya.
d) Pasal 311 KUHP, dapat dikenakan untuk kasus pencemaran nama baik dengan menggunakan media internet.

e) Pasal 303 KUHP, dapat dikenakan untuk menjerat permainan judi yang dilakukan secara online di internet dengan penyelenggaraan dari Indonesia.
f) Pasal 282 KUHP, dapat dikenakan untuk penyebaran pornografi.
g) Pasal 282 dan 311 KUHP, dapat dikenakan untuk kasus penyebaran foto atau film pribadi seseorang.
h) Pasal 406 KUHP, dapat dikenakan pada kasus deface atau hacking yang membuat sistem milik orang lain.

b. Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi

Sebelum ada Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, undang-undang ini yang digunakan untuk mengancam pidana bagi perbuatan yang dikategorikan sebagai tindak pidana *cyber crime.*

Bentuk-bentuk tindak pidana *cyber crime* dalam Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi adalah tanpa hak, tidak sah, atau manipulasi akses ke jaringan telekomunikasi. Hal ini merujuk kepada pengertian *cyber crime* menurut Konferensi PBB yaitu *cyber crime* merupakan perbuatan yang tidak sah yang menjadikan komputer atau jaringan komputer, baik pada sistem keamanannya. Telekomunikasi merupakan bentuk jaringan dan sistem komputer sehingga perbuatan yang dilarang dalam pasal tersebut dapat dikategorikan sebagai tindak pidana *cyber crime.*