BAB III

CYBER CRIME DAN PERMASALAHANNYA

A. Pengertian Kejahatan Dunia Maya (*Cyber Crime*)

Cyber crime merupakan bentuk-bentuk kejahatan yang timbul karena memanfaatkan teknologi internet. Beberapa pendapat mengidentikan *cybercrime* dengan *computer crime*.[1] Sejalan dengan kemajuan teknologi infomasi, telah muncul beberapa kejahatan yang mempunyai karakteristik yang sama sekali baru. Kejahata tersebut adalah kejahatan yang timbul sebagai akibat penyalahgunaan jaringan internet, yang membentuk *cyber space* (ruang siber). Kejahatan ini *(cyber crime*) sering dipersesikan sebagai kejahatan yang dilakukan dalam ruag atau wilayah siber. Rusbagio Ishak, Kadit Serse Polda Jateng megatakan, *cyber crime* ini potensial meimbulkan kerugiann pada beberapa bidang: politik, ekonomi, social budaya

[1] Aep S. Hamidin, *Tips & Trik Kartu Kredit Memaksimalkan dan Mengelola Resiko Kartu Kredit*, Yogyakarta: MedPress, 2010, h. 81

yang signifikan dan lebih memperhatika dibandigkan degan kejahatan yag berintensitas tinggi lainnya.[2]

Cyber crime adalah sebuah perbuatan yang tecela dan melanggar kepatutan di dalam kehidupan mayarakat serta melanggar hukum, sekalipun sampai sekarang sukar untuk menemukan norma hukum yang secara khusus mengatur *cyber crime*. Oleh karena itu peran masyarakat dalam upaya menegakan hukum terhadap *cyber crime* adalah penting untuk menentukan sifat dapat dicela dan melanggar kepatutan masyarakat dari suatu perbuatan *cyber crime*.[3]

Menurut kepolisian Inggris, *Cyber Crime* adalah segala macam penggunaan jaringan komputer untuk tujuan kriminal dan/atau kriminal berteknologi tinggi dengan menyalahgunakan kemudahan teknologi digital. Kejahatan dunia maya merupakan istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer menjadi alat, sasaran, atau tempat terjadinya kejahatan. Termasuk ke dalam kejahatan dunia

---

[2] Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantra (Cyber Crime)*, Bandung: PT Refika Aditama, 2005), h. 65

[3] Dikdik M. Arief Mansur, dan Elisatris Gultom, *Cyber Law Aspek Hukum Teknologi Informasi, (*Bandung Pt. Grafika Aditama 2005), h. 89

maya, antara lain adalah penipuan lelang secara *online*, pemalsuan cek, penipuan kartu kredit/*carding*,*confidence fraud*, penipuan identitas, pornografi anak, dan sebagainya. Namun istilah ini juga digunakan untuk kegiatan kejahatan tradisional di mana komputer digunakan untuk mempermudah atau memungkinkan kejahatan itu terjadi. [4]

Perkembangan teknologi jaringan komputer global atau internet telah menciptakan dunia baru yang dinamakan *Cyberspace*. *Cyberspace* adalah sebuah dunia komunikasi berbasis komputer (*computer mediated communication)* ini menawarkan realitas yang baru, yaitu realitas virtual (*virtual reality*). Perkembangan ini membawa perubahan yang mendasar pada tatanan sosial dan budaya dalam skala budaya. Perkembangan *Cyberspace* merubah pengertian tentang masyarakat, komunitas, komunikasi, interaksi sosial dan budaya. Dengan menggunakan internet, penggunaan dimanjakan untuk berkelana menelusuri dunia *Cyberspace* dengan menebus batas

[4] Nurul Irfan dan Masyrofah, *Fiqih Jinayah*, Jakarta: Amzah 2013, h. 185.

kedaulatan suatu negara, batas budaya, batas agama, politik, ras, hirarki, birokrasi dan sebagainya.[5]

Berbicara masalah *cyber crime* tidak lepas dari permasalahan keamanan jaringan komputer atau keamanan informasi berbasis internet dalam era global ini, apalagi jika dikaitkan dengan persoalan informasi sebagai komoditi. Informasi sebagai komoditi memerlukan kehandalan pelayanan agar apa yang disajikan tidak mengecewakan pelanggan. Untuk mencapai tingkat kehandalan tentang informasi itu sendiri 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 di bawah ini tentang apa yang dimaksud dengan *cyber crime*? Di antaranya adalah Menurut Kepolisian Ingris, *Cyber crime* adalah segala macam penggunaan jaringan komputer untuk tujuan criminal dan/atau criminal berteknologi tinggi dengan

[5] Ricky Adjie Purnama, "Cyber Crime Dalam Perspektif Hukum Positif dan Hukum Islam"(Skripsi Fakultas Syari"ah IAIN SMH Bante, 2007), h. 12

menyalahgunakan kemudahan teknologi digital.[6] Dari berbagai macam definisi tentang *cyber crime* dapat disimpulkan bahwa *cyber crime* merupakan tindak pidana yang memanfaatkan kecanggihan teknologi dengan berbagai macam jaringan yang dapat merugikan banyak pihak ataupun Negara.

B. Bentuk-bentuk *Cyber Crime*

Cyber crime merupakan suatu bentuk kejahatan yang relatife baru apabila dibandingkan dengan bentuk-bentuk kejahatan lainnya yang bersifat konvensional (*street crime*). Kejahatan dalam dunia maya (*Cyber Crime*) secara sederhana dapat diartikan sebagai jenis kejahatan yang dilakukan dengan mempengaruhi media internet sebagai alat bentuknya. Semakin berkembangnya teknologi dapat dilakukan berbagai macam tindak kejahatan, karena disebabkan oleh berbagai faktor sebagaimana dijelaskan di atas. Adapun macam-macam kejahatan berteknologi dari laporan pihak korban maupun hasil dari

---

[6] Zainul Irfan, *Pencegahan dan Penanganan Cybercrime di Indonesia*, Jurnal Regulasi dan Hukum ICT, Magister Teknik Elektro Universitas Mercu Buana, h. 3

identifikasi pakar hukum disesuaikan dan diklasifikasikan dengan undang-undang yang berlaku.[7]

Berdasarkan bentuk aktivitas yang dilakukannya, *cyber crime* dapat digolongkan menjadi beberapa bentuk sebagai berikut:

1. *Unauthorized Acces*

   Merupakan kejahatan yang terjadi ketika seseorang memasuki atau menyusup kedalam suatu sistem jaringan komputer secara tidak sah, tanpa izin, atau tanpa sepengatahuan dari pemilik sistem jaringan komputer yang dimasukinya. *Probing* dan *port* merupakan contoh kejahatan ini.

2. *Illegal Contens*

   Merupakan kejahatan yang dilakukan dengan memasukan data atau informasi ke internet tentang suatu hal yang tidak benar, tidak etis, dan dapat dianggap dapat melanggar hukum atau mengganggu ketertiban umum, contoh nya adalah: a) penyebar pornografi. Contohnya pemuatan suatu berita bohong atau fitnah yang akan menghancurkan martabat atau harga

[7] Dikdik M. Arief Mansur, dan Elisatris Gultom, *Cyber Law Aspek Hukum Teknologi Informasi*,.. h. 26

diripihak lain. b) pemuatan hal-hal yang berhubungan dengan pornografi. c) pemuatan suatu informasi yang merupakan rahasia Negara, agitasi, dan propaganda untuk melawan pemerintah yang sah, dan sebagainya.

3. Penyebar virus secara sengaja

Penyeber virus pada umumnya dilakukan dengan menggunakan email. Sering kali orang yang emailnya terkena virus tidak menyadari hal ini. Virus ini kemudian dikirim ketempat lain memalui emailnya.

4. Data *forgery*

Kejahatan jenis ini dilakukan dengan tujuan memalsukan data ke dokumen-dokumen penting yang ada di internet. Dokumen-dokumen ini biasanya dimiliki oleh institusi atau lembaga yang memiliki situs berbasis web data base.

5. *Cyberterorism*

Suatu tindakan *cyber crime* termasuk *cyber terrorism,* jika mengancam pemerintah atau warga Negara, termasuk *cracking* ke situs pemerintah atau militer.[8]

[8] Aep S. Hamidin, *Tips dan Trik Kartu Kredit; Memaksimalkan Manfaat dan Mengelola Resiko Kartu Kredit…* h. 83-86

6. *Political hacker*

Aktivitas politik yang kadang-kadang dengan hacktivis merupakan situs web dalam usaha menempelkan pesan atau mendiskreditkan lawannya. Tahun 1998 hacker ini dapat mengubah ratusan situs web untuk menyampaikan pesan dan kampanye tentang anti nuklir.

7. Perjudian *(gambling)*

Bentuk judi kasino virtual saat ini telah banyak beroperasi di internet. Kegiatan ini biasanya akan terhindar dari hukum positif yang berlaku dikebanyakan Negara. Selain itu, hal ini dapat memberikan peluang bagi penjahat terorganisasi untuk melakukan praktik pencurian uang (*money laundry*) dimana-mana).[9]

8. *Cyber espionage*

Cyber espionage yaitu kejahatan yang memanfaatkan kejahatan interne untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan

[9] Soemarno Partodihadjo, *Tanya Jawab Seputar Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronoik.* (Jakarta: Gramedia Pustaka Utama Kompas, 2008), h. 150-152

computer *(computer network system)* pihak sasaran. Kejahatan ini biasanya ditujukkan terhadap saingan bisnis yang dokumen ataupun data-data pentingnya tersimpan didalam suatu sistem komputerisasi.

9. *Infringements of Privacy*

   Infringements of Privacy yaitu kejahtan yang ditujukkan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia. Kejahtan ini biasanya ditujukkan terhadap keterangan pribadi seseorang yang tersimpan pada formulir data pribadi yang tersimpan secara komputerisasi, yang apabila diketahui oleh orang lain, maka dapat merugikan orang secara material maupun immaterial, seperti nomor kartu kredit, nomor pin ATM, keterangan tentang catatan atau penyakit tersembunyi dan sebagainya.

10. *Offence against intellectual property*

    Offence against intellectual property yaitu kekayaan yang ditujukkan terhadap hak kekayaan intelektual yang dimiliki seseorang di internet. Sebagai contoh adalah peniruan tampilan web page suatu situs milik orang lain secara illegal, penyiaran

suatu informasi di internet yang ternyata merupakan rahasia dagang orang lain, dan sebagainya. [10]

Cyber crime merupakan sebuah tindak pidana dengan cara mengakses berbagai jaringan internet dan bentuk dari kejahatan di dunia maya, *cyber crime* juga memilki berbagai bentuk-bentuk sebagai ciri klarifikasi kejahatan didunia maya. Dari bentuk-betuk criber crime ada 10 bentuk kejatan dunia maya salah satunya: *Unauthorized Acces, Illegal Contens,* dan lain sebagaiannya seperti yang tertera di atas.

C. Faktor Penyebab Terjadinya Cyber Crime

Kejahatan dunia maya (*cyber crime*) adalah istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer menjadi perantara, sasaran atau tempat terjadinya kejahatan. Seperti kejahatan dunia maya antara lain adalah penipuan lelang secara online, pemalsuan cek, penipuan kartu kredit/carding, confidence fraud, penipuan identitas,

[10] Maskun, *Kejahatan Siber Cyber Crime*, Jakarta: Kencana 2013, h. 53-54.

pornografi anak, dan lain-lain. Adapun yang menjadi penyebab terjadinya *cyber crime* antara lain :

1. Akses internet yang tidak terbatas.
2. Kelalaian pengguna komputer. Hal ini merupakan salah satu penyebab utama kejahatan komputer.
3. Mudah dilakukan dengan alasan keamanan yang kecil dan tidak diperlukan peralatan yang super modern. Walaupun kejahatan komputer mudah untuk dilakukan tetapi akan sulit untuk melacaknya, sehingga ini mendorong para pelaku kejahatanuntuk terus melakukan halm ini.
4. Para pelaku merupakan orang yang pada umumnya cerdas,mempunyai rasa ingin tahu yang besar dan fanatik akan teknologi komputer. Pengetahuan pelaku kejahatan komputer tentang cara kerja sebuah komputer jauh diatas operator computer.
5. Sistem keamanan jaringan yang lemah. f. Kurangnya perhatian masyarakat. Masyarakat dan penegak hukum saat ini masih memberi perhatian sangat besar terhadap kejahatan konvensional. Pada kenyataanya pelaku kejahatankomputer masih terus melakukan aksi kejahatannya. [11]

Bahwasaya aktivitas internrt walaupun dianggap sebagai suatu aktivitas maya, dalam pengaturannya tidak dapat dilepaskan dari manusia dalam mengoprasikannya. Manusia dalam alam nyatalah yang bertanggung jawab atas akibat dari perbuatannya. Dengan demikian aktivitas dalam *Cyber Space* tidak dapat dipisahkan dari alam nyata. Regulasi yang berkaitan dengan internet tidak lepas

[11] "Etika Profesi Teknologi Informasi Dan Komunikasi (*Cyber Crime* dan *Cyber Law*)" http://eptikcyberprojek.blogspot.com diakses pada tanggal 3 September 2019, Pukul 17:48 Wib.

dari aktivitas manusia pada dunia maya.[12] *Cyber Crime* merupakan kegiatan kriminal yang memang sudah direncanakan sebelumnya namun, ada beberapa faktor pendorong terjadinya tindak kejatan tersebut salah satunya ialah akses internet yang tidak terbatas. Akses internet yang tidak terbatas ini menimbukan tidak terbatas dalam mengakses berbagai macam situs, dari sinilah kejatan didunia ini mulai terjadi karena tidak ada batasan dalam mengases berbagai jaringan.

D. Faktor Pendorong Laju Petumbuhan Cyber Crime

Beberapa faktor pendorong laju pertumbuhan *cyber crime* yaitu:

1. Kesadaran hukum masyarakat

Proses penggunaan hukum pada dasarnya adalah upaya mewujudkan keadilan dan ketertiban di dalam kehidupan bermasyarakat. Melalui sistem peradilan pidana dan sistem pemidanaan. Pada dasarnya hak-hak warga Negara yang terganggu akibat perbuatan melawan hukum seseorang akan

[12] Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantra (Cyber Crime),*… h.113

diseimbangkan kembali. Mengenai kendala proses penataan terhadap hukum, jika masayarakat di Indonesia memiliki pemahaman yang benar akan tindak pidana *cyber crime* baik secara langsung mapun tidak langsung masayarakatakan membentuk suatu pola penataan. Pola penataan ini dapat berdasarkan karena akan ketentuan akan ancaman pidana yang dikenakan bila melakukan perbuatan *cyber crime* atau pola penataan itu tumbuh atas kesadaran mereka sediri sebagai masyarakat hukum. Faktor keamanan

Rasa aman tentunya akan dirasakan oleh pelaku kejahtan *(cyber crime)* pada saat sedang menjalakan "aksinya". Hal ini tidak lain karena Internet lazim dipergunakan di tempat-tempat yang relative tutup, seperti di rumah, kamar, tempat kerja, perpustakan bahkan di warung internet (warnet). Begitu pula, ketika perlu sedang beraksi di tempat terbuka, tidak mudah orang lain mengetahui "aksinya". Karena di warnet tidak mempunyai penyekat ruangan, sangat suli bagi orang awam untuk menegtahui bahwa seseorang sedang melakukan tindak pidana. Disamping itu, apabila pelaku telah melakukan tindak pidana, maka dengan

mudah pelaku dapat menghapus semua jejak kejahatan yang telah di lakukan mengingat internet menyediakan fasilitas untuk meghapus data/fail yang ada. Akibatnya saat pelaku tertangkap sukar bagi aparat penegak hukum untuk menemukan bukti-bukti kejahatan.

1. Faktor penegakan hukum

Faktor penegak hukum sering menjadi penyebab maraknya kejahatan siber (*cyber crime).* Karena masih sedikit aparat penegak hukum yang memahami sebeluk beluk teknologi (internet), sehingga pada saat pelaku tindak kejahatan pidana ditangkap, aparat penegak hukum mengalami kesulitan alat bukti yang dapat dipakai untuk menjerat pelaku, terlebih dahulu apabila kejahatan yang dilakukan memiliki sistem pengoprasian yang sangat rumit.

2. Faktor ketiadaan Undang-undang

Perubahan-perubahan sosial dan perubahan-perubahan hukum tidak selalu langsung bersama-sama pada artinya pada keadaan-keadaan tertentu perkembangan hukum mungkin tetinggal oleh perkembangan unsur-unsur lainnya dari

masyarakat. Begitu juga dengan perkembangan hukum di tengah-tengah teknologi informasi sangat jauh tertinggal. Dalam konteks upaya hukum terhadap pelaku *cyber crime*, tentunya saat ini cenderung sangat membatasi penegak hukum di Indonesia untuk melakukan penyelidikan atau penyidikan guna mengungkap perbuatan tersebut karena suatu aturan undang-undan yang mengatur *cyber crime* beleum tersedia apalagi atas legalitas ini tidak memperbolehkan adanya suatu analogi untuk menentukan perbuatan pidana. [13] Kejahatan didunia maya dapat terjadi dimana saja dan oleh siapa saja. Kejahata ini tidak akan terjadi jika tingginya akan kesadaran masyarakat untuk bertanggung jawab dalam mengakases berbagai macam jaringan internet. Hal ini dapat meminimalisir pertumbahan kejahatn didunia maya.

E. Ruang Lingkup Kejahatan Cyber Crime

Membahas ruang lingkup kejahatan telematik adalah hal yang penting dalam rangka memberi batasan cakupan kejahatan telematik. Didasari bahawa perkembangan telemati (internet)

[13] Dikdik M. Arief Mansur, dan Elisatris Gultom, *Cyber Law Aspek Hukum Teknologi Informasi*,.. h. 89-94

yang begitu cepat berbading lurus dengan modus kejahatan yang muncul. Beberapa tahun yang lalu, puluhan ribu pemakai internet terkena virus e-mail "*Melissa" dan "explore-zip.worm"* yang menyebar dengan cepat, menghapus arsip-arsip, haruskan sistem-sistem, yang menyebabkan perusahan-perusahaan harus mengeluarkan jutaan dollar untuk mendapatkan bantuan dan batas waktu. Pada bulan februari 2000, misalnya, beberapa jaringan konsumen dan komersial yang paling popular seperti Yahoo!, Amazon, eBay, CNN.com, dan E-trade ditutup oleh para pecantol (*craker)* yang mengirimkan begitu banyak pesan-pesan sehingga jaringan-jaringan tersebut kelebihan beban. Disamping itu, jaringan-jaringan lain telah menjadi sasaran pembajakan halaman (*pagecking)* yang menghubungkan para pemakai kejarngan-jaringan yang tidak diingikan.[14] Perkembangan teknologi yang semakin pesat harus dibatasi penggunaannya hal ini guna membatasi rungan lingkup terjadinya kejahatan didunia maya.

[14] Maskun, *Kejahatan Siber Cyber Crime,…* h. 50-51

F. Pencegahan Tindakan Cyber Crime

Di era globalisasi informasi ini sudah bisa atau sedang kita rasakan akibat buruknya bagi kehidupan dan peradaban manusia, disamping ada manfaat yang bisa diperoleh manusia. Manusia memang sudah banyak mendapatkan keuntungan dengan globalisasi informasi, karena manusia diberi kemudahan mendapatkan atau mengakses informasi sebanyak-banyaknya, sehingga manusia dapat menguasai dinamika sains dan teknologi. Akan tetapi sisi buruk telah benar-benar hadir secara real dalam kehidupan manusia. Kehidupan manusia semakin akrab dengan berbagai bentuk kejahatan alam maya *(cyber crime)*, yang tidak bisa dipungkiri sevagai akibat dan bahkan sasaran dari globalisasi informasi. Berbagai produk teknologi seperti computer misalnya telah di jadikan sebagai media untuk kepentingan informasi global, dan produk teknologi inilah yang sekaligus memperlancar maraknya *cybercrime.*[15]

Tindak pidana *cyber crime* memakan korban yang tidak sedikit jumlahnya, terutama dari sisi finansial. Sebagian besar

[15] Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantra (Cyber Crime),...,* h. 125

korban hanya bisa menyesali apa yang sudah terjadi. Mereka berharap bisa belajar banyak dari pengalaman yang ada, yang perlu dilakukan sekarang adalah melakukan pencegahan terhadap kemungkinan-kemungkinan yang dapat merugikan kita sebagai pelaku IT. Pencegahan itu dapat berupa:

1. *Educate User* (memberikan pengetahuan baru terhadap *Cyber Crime* dan dunia internet)
2. *Use hacker's perspective* (menggunakan pemikiran dari sisi *hacker* untuk melindungi sistem Anda)
3. *Patch System* (menutup lubang-lubang kelemahan pada sistem)
4. *Policy* (menentukan kebijakan-kebijakan dan aturan-aturan yang melindungi sistem anda dari orang-orang yang tidak berwenang)
5. IDS *(Intrusion Detection System) bundled with IPS (Intrusion Prevention System)*
6. *Firewall* AntiVirus.[16]

G. Penanggulangan Tindakan Cyber Crime

Pada perkembangannya internet ternyata membawa sisi negatif, dengan membuka peluang munculnya tindakan-tindakan anti social yang selama ini di anggap tidak mungkin terjadi atau tidak terpikirkan akan terjadi. Sebuah teori menyatakan sebuah teori menyatakan, *crime is product of society its self,* yang secara

[16] Zainul Irfan, *Pencegahan Dan Penanganan Cybercrime Di Indonesia,*…. h.9

sederhana dapat diartikan bahwa masyarakat itu sendirilah yang menghasilkan kejahatan.[17] Fenomena *cyber crime* memang harus di waspadai karena keajahatan ini agak berbeda dengan kejahatan lain pada umumnya. *Cyber crime* dapat dilakukan tanpa mengenal batas territorial dan tidak memerlukan interaksi langsung antara pelaku dengan korban kejahatan. Berikut ini cara penanggulangannya:

1. Melakukan modernisasi hukum pidana nasional beserta hukum acaranya.
2. Meningkatkan sistem pengamanan jaringan computer nasional sesuai standar internasional.
3. Meningkatkan pemahaman serta keahlian aparatur penengak hukum mengenai upaya pencegahan, investigasi dan penuntut perkara-perkara yang berhubungan dengan *cyber crime*.
4. Meningkatkan kesadaran warga Negara mengenai masalah *cyber crime* serta pentingnya mencegah kejahatan tersebut terjadi.
5. Meningkatkan kerja sama antar Negara, baik bilateral, regional maupun multilateral, dalam upaya penanganan *cyber crime*.[18]

Pertama patut dikemukakan bahwa kebijakan penanggulangan *cyber crime* dengan hukum pidana termasuk bidang *penal policy*, yang merupakan bagian dari *criminal policy* (kebijakan penanggulangan kejahatan). Dilihat dari sudut

[17] Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantra (Cyber Crime)*,…, h. 39

[18] Aep S. Hamidin, *Tips dan Trik Kartu Kredit; Memaksimalkan Manfaat dan Mengelola Resiko Kartu Kredit…..,* h. 88-89

criminal policy, upaya penanggulangan kejahatan (termasuk penanggulangan *cyber crime)* tidak dapat dilakukan semata-mata secara persial dengan hukum pidana (sarana penal), tetapi harus ditempuh pula dengan pendekatan integral/sistemik. Sebagai salah satu betuk *high tech crime* yang data dilampaui batas-batas negara (bersifat *transnatioal transborder*,merupakan hal yang wajar jika upaya peaggulaga CC juga harus ditempuh dengan pendekatan teknologi (*techo reventio).* Disamping itu, diperluka juga pendekatan budaya/kultur, pedekata moral/edukatif, dan bahkan pendekatan global (kerja sama internasional).[19]

[19] Barda Nawawi Arief, *Tindak Pidaa Mayantara Perkembagan Kejahatan Cyber Crime Di Indonesia*, Jakarta: Raja Grafido Persada, 2007, h. 89-90