BAB III

PENGATURAN *CYBER CRIME* (KEJAHATAN SIBER)

A. Perkembangan *Cyber Crime* (Kejahatan Siber)

Pada dasarnya setiap teknologi diciptakan untuk memenuhi suatu kebutuhan tertentu manusia. Setelah diciptakan teknologi dikembangkan agar dapat semakin efektif dan efisien untuk memenuhi kebutuhan yang dimaksud, teknologi yang lama pasti akan ditinggalkan. Akan tetapi setelah teknologi dikembangkan, penggunaan teknologi tersebut dapat sesuai dengan tujuan penciptaan dan pengembangannya maupun di luar tujuan awalnya. Teknologi informasi dan komunikasi yang ada pada saat ini merupakan hasil pengembangan dari teknologi sebelumnya, khususnya teknologi komputer, telekomunikasi, dan internet. Saat ini teknologi yang dimaksud sudah terjelma dalam laptop, komputer PC, handphone, tablet, atau *gadget* lainnya yang memudahkan masyarakat dunia untuk berinteraksi dan melakukan transaksi. Semudah itu juga pelaku kejahatan dunia maya melakukan aksi kejahatannya dengan menggunakan alat dan perangkat tersebut.[62]

Pada masa awalnya, *cyber crime* didefinisikan sebagai kejahatan komputer. Penggunaan istilah tindak pidana untuk kejahatan komputer masih belum seragam masih banyak yang mengunakan istilah "*computer misuse*", "*computer abuse*", "*computer fraud*", "*computer-related crime*", "*computer-assisted crime*", atau "*computer crime*". Tetapi pada umumnya lebih menerima

[62]Josua Sitompul, 2012, *Cyberspace, Cyber crime, Cyber Law Tinjauan Aspek Hukum Pidana*, Jakarta, PT. Tatanusa, hlm. 1.

pemakaian istilah *"computer crime"* oleh karena dianggap lebih luas dan biasa dipergunakan dalam hubungan Internasional.[63]

The British Law Commision misalnya, mengartikan *"computer fraud"* sebagai manipulasi komputer dengan cara apapun yang dilakukan dengan itikad buruk untuk memperoleh uang, barang atau keuntungan lainnya atau dimaksudkan untuk menimbulkan kerugian pada pihak lain. Mandell membagi *"computer crime"* atas dua kegiatan, yaitu:

1. Penggunaan komputer untuk melaksanakan perbuatan penipuan, pencurian atau penyembunyian yang dimaksud untuk memperoleh keuntungan keuangan, keuntungan bisnis, kekayaan atau pelayanan;
2. Ancaman terhadap komputer itu sendiri, seperti pencurian perangkat keras atau lunak, sabotase dan pemerasan.[64]

Karakteristik kejahatan siber yang syarat dengan penggunaan komputer dan internet serta lintas negara membutuhkan penanganan yang tidak selalu dapat dilakukan berdasarkan cara atau metode konvensional. Dalam berbagai kasus, penyelesaian tindak pidana siber memerlukan kerjasama dari berbagai pihak, termasuk aparat penegak hukum dari negara lain. Kerjasama tersebut dapat terlaksana secara efektif apabila didukung oleh instrumen hukum baik regional maupun internasional yang selaras dengan hukum nasional masing-masing pihak.[65] Selain manfaatnya yang sangat besar dalam kehidupan sehari-hari, potensi kejahatan dibidang internet dan telekomunikasi ini juga sangat besar.

---

[63]Budi Suhariyanto, 2012, *Tindak Pidana Teknologi Informasi (Cybercrime),* Jakarta, RajaGrafindo Persada, hlm. 9.

[64]*Ibid,* hlm. 10.

[65]Josua Sitompul, *Cyberspace, Cybercrimes, Cyberlaw*, *op.cit.* hlm. 2

Mulai dari kasus pencemaran nama baik, situs-situs pemerintah dan swasta yang di-*hack,* penipuan di internet dan sebagainya. Berbagai usaha pun telah dilakukan sebagai upaya penanggulangan dalam kejahatan siber ini.[66]

Istilah *cyber crime* (kejahatan siber) mungkin merupakan istilah yang sudah tidak asing lagi bagi kita, istilah yang tidak dapat dipisahkan dengan teknologi komputer dan internet. *Cyber crime* adalah tindak pidana yang terjadi dalam *cyber space* yang dilakukan oleh manusia atau mesin atas dasar perintah manusia. Pada awal pembentukannya, internet berada dalam satu kontrol administrator yang ketat. Sistem administrator mengontrol secara penuh sistem dan perangkat keras serta perangkat lunak jaringan. Pengguna awal internet adalah anggota yang dapat diidentifikasi sehingga dalam hal pengguna melakukan penyalahgunaan jaringan atau perangkat, sistem administrator dapat segera mengetahui dan dapat mencegah terjadinya pembobolan sistem oleh para pelaku kejahatan. Kebebasan untuk menggunakan identitas anonim atau alias membutuhkan kepercayaan yang kuat antara para pihak yang melakukan transaksi.[67]

Ketentuan *cyber crime* dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) mengacu pada *EU Convention Cyber crime* yang merupakan instrumen Internasioanal yang digunakan oleh banyak negara. *Convention on Cyber crime* adalah salah satu instrumen Internasional yang mengatur *cyber crimes* secara regional. CoC dibuka dan ditandatangani oleh negara-negara anggota sejak 23 November 2001, tetapi baru

---

[66] *Ibid*
[67] *Ibid*

mulai berlaku pada tahun 2004. CoC yang paling banyak dijadikan acuan utama dalam pembentukan peraturan perundang-undangan mengenai tindak pidana siber oleh negara-negara di dunia termasuk di Indonesia. Kenyataannya masih ada pro kontra mengenai diperlukannya Undang-Undang khusus mengenai *cyber crime.*[68]

Convention on Cyber crime diatur mengenai dua jenis *cyber crime,* yaitu *cyber crime* dalam arti *computer crime* dan dalam arti *computer related crime* yaitu Article 2 (Illegal Access), Article 3 (Illegal Interception), Article 4 (Data Interferece), Article 5 (System Interference), Article 6 (Misuse of Devices), Article 7 (Computer Related Forgery), Article 8 (Computer Related Fraud). Berbagai peraturan perundang-undangan yang mengatur perbuatan-perbuatan pidana yang juga dapat menjadi suatu perbuatan "*Cyber crime*", seperti Access Device Fraud Act (Title 18 USC Section 1029), Wire Fraud Statute (Title 18 USC Section 1343), The Copyright Act of 1976 (Title 18 USC Section 2319), The Trademarks Counterfeit Act of 1984 (Title 18 USC Section 2320), Mail Fraud (Title 18 USC Section 1341), Identity Theft and Assumption Deterrence Act of 1998 (Title 18 USC Section 1028), Unlawful Access to Stored Communications (Title 18 USC Section 2701), dan lain-lain.[69]

Menurut Walden, *cyber crime* adalah bagian dari *computer crime.* Walden melihat bahwa pengklasifikasian computer crime dapat didasarkan pada teknologi *(technology-based),* motivasi *(motivation-based),* hasil *(outcome-based),* dan komunikasi *(communication-based),* serta informasi *(information-based).* Walden

---

[68] *Ibid*

[69] http://www.academia.edu/5851009/CYBERCRIME_DI_INDONESIA, diakses tanggal 8 Februari 2015 (19.05).

mengkategorikan tindak pidana menjadi tiga, yaitu: *computer-related crime, content-related crime, dan computer integrity offences.*[70]

B. Jenis-Jenis *Cyber Crime* (Kejahatan Siber)

Sesungguhnya banyak perbedaan dalam mengklasifikasikan *cyber crime.* Ternyata dari klasifikasi tersebut terdapat kesamaan dalam beberapa hal. Untuk memudahkan klasifikasi *cyber crime* tersebut, maka dari beberapa klasifikasi dapat disimpulkan:

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 atau operasinya.
4. Tindakan-tindakan yang menganggu operasi komputer.
5. Tindakan merusak peralatan komputer atau peralatan yang berhubungan dengan komputer atau sarana penunjangnya.[71]

Secara umum terdapat beberapa jenis kejahatan yang berhubungan erat dengan penggunaan teknologi informasi yang berbasis utama komputer dan jaringan telekomunikasi ini, dikelompokkan dalam beberapa jenis, antara lain:

a. ***Unauthorized acces to computer system and service***

Kejahatan yang dilakukan dengan memasuki/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa

---

[70]Ian Walden, *Computer Crimes and Digital,* Oxford University Press, New York, 2007, hlm. 19 (Dalam buku Josua Sitompul, 2012, *Cyberspace, Cyber crime, Cyber Law Tinjauan Aspek Hukum Pidana,* Jakarta, PT. Tatanusa, hlm. 37).

[71]Budi Suhariyanto, 2012, *Tindak Pidana Teknologi Informasi (Cybercrime),* Jakarta, RajaGrafindo Persada, hlm. 14.

sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya.[72] 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. Kejahatan ini diatur dalam Pasal 406 KUHP dan Pasal 30, Pasal 35, Pasal 46 Undang-Undang Nomor 11 tahun 2008 tentang ITE.

b. *Illegal contens*

Merupakan 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.[73] Kejahatan ini diatur dalam Pasal 27, Pasal 28, dan Pasal 29 Undang-Undang Nomor 11 tahun 2008 tentang ITE.

c. *Data forgery*

Merupakan kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai *scriptless document* melalui internet.[74] Kejahatan ini biasanya ditujukan pada dokumen dengan membuat seolah "salah ketik" yang pada akhirnya menguntungkan pelaku. Diatur dalam Pasal 362, Pasal 378, dan Pasal 335 KUHP, Pasal 35 Undang-Undang Nomor 11 tahun 2008 tentang ITE, Undang-Undang Nomor 19 Tahun

---

[72]Drs. H. Abdul Wahid, Mohammad Labib, 2005, *Kejahatan Mayantara (cyber crime),* Bandung, Refika Aditama, hlm. 82.
[73]*Ibid*
[74]*Ibid*

2002 tentang Hak Cipta, Undang-Undang Nomor 8 Tahun 1997 tentang Dokumen Perusahaan.

d. ***Cyber espionage***

Merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer *(computer network system)* pihak sasaran.[75] Kejahatan ini diatur dalam Pasal 112, 113, 114, 115, dan 116 KUHP. Pasal 323 KUHP mengatur tentang pembukaan rahasia perusahaan yang dilakukan oleh orang dalam (insider). Sedangkan perbuatan membocorkan data rahasia perusahaan dan memata-matai yang dilakukan oleh orang luar perusahaan dapat dikenakan Pasal 50 jo Pasal 22, Pasal 51 jo Pasal 29 ayat (1), dan Pasal 57 jo Pasal 42 ayat (1) Undang-Undang Nomor 36 tahun 1999 tentang Telekomunikasi.

e. ***Cyber sabotage and extortion***

Kejahatan ini dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet.[76] Diatur dalam Pasal 33 dan Pasal 49 Undang-Undang Nomor 11 tahun 2008 tentang ITE.

f. ***Offense against intellectual property***

Kejahatan ini ditujukan terhadap hak atas kekayaan intelektual yang dimiliki pihak lain di internet. Sebagai contoh adalah peniruan tampilan pada *web page* suatu sistem milik orang lain secara illegal, penyiaran suatu

---

[75] *Ibid*
[76] *Ibid*

informasi di internet yang ternyata merupakan rahasia dagang orang lain dan sebagainya.[77] Diatur dalam Pasal 27 sampai Pasal 35 Undang-Undang Nomor 11 tahun 2008 tentang ITE.

g. ***Infringements of privacy***

Kejahatan ini ditujukan terhadap informasi seseorang yang merupakan hal sangat pribadi dan rahasia. Kejahatan ini biasanya ditujukan terhadap keterangan seseorang pada formulir data pribadi yang tersimpan secara *computerized.* Yang apabila diketahui oleh orang lain akan dapat merugikan korbannya secara materiil maupun immaterial seperti nomor kredit, nomor PIN ATM, cacat atau penyakit tersembunyi dan sebagainya.[78] Kejahatan ini diatur dalam Pasal 282 ayat (1) KUHP dan Pasal 27, Pasal 45 Undang-Undang Nomor 11 tahun 2008 tentang ITE.

Berdasarkan kriteria jenis-jenis kejahatan *cyber* di atas, maka dapat diklasifikasikan lebih sederhana, jenis-jenis aktivitas kejahatan komputer dapat dikelompokkan dalam dua golongan: penipuan data dan penipuan program. Dalam bentuk *pertama,* data yang tidak sah dimasukkan ke dalam sistem atau jaringan komputer atau data yang tidak sah dan seharusnya di *entry* diubah sehingga menjadi tidak valid atau tidak sah lagi. Fokus perhatian pada kasus pertama adalah adanya pemalsuan dan/atau perusakan data input dengan maksud untuk mengubah output. Bentuk kejahatan *kedua,* yang relatif lebih canggih dan lebih berbahaya adalah apabila seseorang mengubah program komputer baik dilakukan langsung di tempat komputer tersebut berada maupun dilakukan secara

---

[77] *Ibid*
[78] *Ibid*

remote melalui jaringan komunikasi data. Pada kasus ini penjahat melakukan penetrasi ke dalam sistem komputer dan selanjutnya mengubah susunan program dengan tujuan menghasilkan keluaran *(output)* yang berbeda dari seharusnya, meski program tersebut memperoleh masukan *(input)* yang benar.[79]

Kejahatan *cyber crime* yang paling banyak terjadi di Indonesia adalah berupa kejahatan internet. Kasus yang terjadi pada 2001 yaitu sebanyak 23 kasus dengan jumlah tersangka sebanyak 17 orang dan pada 2002 meningkat sebanyak 116 kasus dengan jumlah tersangka 124 orang. Kondisi ini tentunya akan merusak citra Indonesia di mata Internasional karena dianggap sebagai sarang (surga-*pen*) bagi para pemalsu kartu kredit *(carding)*. Salah satu contoh kasus *cyber crime* (kejahatan siber) yang kesulitan ditangani dengan KUHP adalah *carding* yang sempat populer dengan terungkapnya *carder* asal Bandung. Buyung alias Sam, mahasiswa berusia 25 tahun menggunakan kartu kredit orang lain untuk transaksi melalui internet.[80]

Kejahatan penipuan dengan menggunakan sarana komputer sebagai alat kejahatan utama yang terjadi sekarang ini seperti penipuan dengan menggunakan kartu kredit atau kartu ATM palsu masih sangat tinggi. Hal ini tentunya mengakibatkan kepentingan masyarakat luas menjadi terganggu. Selain itu, kepercayaan dunia internasional dalam melakukan transaksi secara elektronik di Indonesia dapat terancam. Penipuan yang terjadi di dunia siber dapat dilakukan dengan berbagai cara, mulai dari yang sederhana sampai kepada yang kompleks. Penipuan yang sederhana misalnya dengan mengirimkan *hoax* (pemberitaan

[79]Budi Suhariyanto, 2012, *Tindak Pidana Teknologi Informasi (Cybercrime),* Jakarta, RajaGrafindo Persada, hlm. 16-17

[80]*Ibid,* hlm. 56-57.

palsu) atau bertindak sebagai orang lain secara tidak sah dan melakukan penipuan lewat chatting. Penipuan yang lebih kompleks yaitu penipuan dapat dilakukan melalui gangguan terhadap data *(data interference)* dan gangguan terhadap sistem *(system interference).*[81]

Tindakan gangguan terhadap data maupun sistem komputer dapat dilakukan baik secara langsung (oleh pelaku) maupun secara tidak langsung (mislanya dengan menggunakan program komputer). Selain itu, sebelum gangguan dilakukan pelaku juga dapat melakukan tindakan lain yaitu memasuki suatu sistem komputer secara tidak sah *(illegal access),* dengan memasuki sistem komputer (dengan tidak sah), pelaku dapat mengontrol sistem dan melakukan gangguan terhadap data atau sistem komputer.[82] Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) telah mengatur tindak pidana akses illegal (Pasal 30), gangguan terhadap data (Pasal 32), dan gangguan terhadap sistem komputer (Pasal 33). Selain tindak pidana tersebut, Undang-Undang Nomor 11 tahun 2008 tentang ITE juga mengatur tindak pidana tambahan sebagaimana diatur dalam Pasal 36, yaitu "...dengan sengaja dan tanpa hak atau melawan hukum melakukan perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 34 yang mengakibatkan kerugian bagi orang lain".[83]

Penyidik harus tetap membuktikan tindak pidana tersebut terlebih dahulu, untuk menyimpulkan suatu *computer related fraud.* Dengan demikian, berdasarkan penelaahan terhadap ketentuan penipuan dalam KUHP serta ketentuan dalam Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan

---

[81] Josua Sitompul, *Cyberspace, Cybercrimes, Cyberlaw, op. cit.* hlm. 46-47.
[82] *Ibid*
[83] *Ibid*

Transaksi Elektronik (ITE), dapat disimpulkan bahwa pengaturan mengenai penipuan dengan menggunakan sarana komputer belum terakomodir. Pengaturan mengenai penipuan dengan menggunakan sarana komputer penting untuk dihadirkan dalam sistem hukum pidana di Indonesia untuk melindungi kepentingan atau nilai hukum yang sama. Secara umum, yang dimaksud dengan transaksi elektronik ialah segala bentuk transaksi terhadap data.[84] Berdasarkan Pasal 1 butir 2 Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), yang dimaksud dengan transaksi elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer, dan/atau media elektronik lainnya.

Konsep transaksi elektronik yang dianut dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) bersifat luas, karena mencakup segala transaksi baik dalam bidang perdagangan *(commerce)* maupun di luar perdagangan, termasuk perbuatan teknis dengan menggunakan media elektronik seperti mengirimkan email atau virus, membuat website, mengubah konfigurasi sistem, atau melakukan *hacking* yang memiliki akibat timbulnya tindak pidana.[85] Dalam dunia kita saat ini, komputer bukan hanya sekedar alat hitung, tetapi media yang juga dapat menyebarkan informasi dan memberikan layanan multiguna. Telepon genggam yang memiliki berbagai fitur layanan bukan hanya sekedar alat telekomunikasi, tetapi juga sarana untuk mengekspresikan diri dan mencari informasi. Teknologi informasi dan komunikasi juga memudahkan setiap orang untuk berkomunikasi dan berinteraksi

---

[84] *Ibid*
[85] *Ibid*

melalui internet. Layanan email seperti *yahoomail, gmail,* atau *hotmail* merupakan kebutuhan utama dalam berkomunikasi di dunia siber.[86]

Korban tindak pidana siber dapat tersebar di berbagai negara dan total kerugian yang dialami para korban pun tidak sedikit. Eksistensi *cyber crime* (kejahatan siber) di dunia virtual menimbulkan kesulitan tersendiri dalam proses penegakkan hukum. Kesulitan yang timbul misalnya dalam menentukan tempat kejadian perkara *(locus delicti).* Penyidik juga mengalami kesulitan dalam mencari saksi yang melihat atau mendengar kejadian. Kesulitan lain timbul dalam hal mengumpulkan alat bukti.[87] Dengan adanya internet informasi dapat disebar dan diteruskan ke berbagai penjuru dunia dengan seketika serta dapat diakses dari berbagai negara, konten-konten yang dilarang dapat tersebar luas tanpa diketahui identitas aslinya.[88] Dengan demikian, internet dapat menjadi sarana untuk menyebarkan informasi yang menimbulkan dampak yang luas dan tidak terbatas. Hal ini tentunya dapat menimbulkan kerugian bagi korban, baik secara materil maupun imateril.[89]

Tindakan mengakses komputer atau sistem elektronik dapat dilakukan dengan menggunakan *malicious software (malware)* yaitu piranti lunak yang diciptakan untuk memasuki sistem komputer tanpa persetujuan pemiliknya. Piranti ini dapat dikirim oleh pelaku dalam bentuk email, dan dalam email tersebut, calon korban diminta untuk mengunduh piranti lunak yang umum. Ketika sudah diunduh piranti itu maka kode-kode berbahaya juga masuk ke dalam

---

[86] *Ibid*
[87] *Ibid*
[88] *Ibid,* hlm. 149.
[89] *Ibid*

sistem.[90] Dengan *keylogger* seseorang dapat memonitor dan merekam tombol-tombol keyboard yang ditekan oleh pengguna komputer termasuk *password* email atau eBanking tanpa diketahui oleh pengguna. Kemudian pelaku dapat menggunakan password tersebut untuk masuk ke dalam sistem elektronik email atau e-Banking korban.[91] Pelaku juga dapat mengetahui kode akses korban dengan cara menebak. Pelaku mengumpulkan informasi mengenai tempat dan tanggal lahir, hewan kesukaan, nama ayah korban, semua itu mungkin dapat diperoleh dengan tebakan saja.

Suatu sistem pengamanan dalam sistem keamanan informasi umumnya dipasang atau diterapkan untuk mencegah seseorang yang tidak memiliki hak atau wewenang dapat masuk dalam suatu sistem elektronik. Selain itu, sistem pengaman diterapkan untuk menjaga sistem elektronik agar tetap berfungsi sebagaimana mestinya serta menjaga integritas dan ketersediaan informasi atau dokumen elektronik yang ada di dalamnya, apalagi informasi atau dokumen elektronik memiliki nilai ekonomis bagi pemiliknya. Penerapan sistem keamanan informasi sangat beragam mulai dari yang paling sederhana, seperti menggunakan kode akses sampai yang paling kompleks, seperti mengatur konfigurasi jaringan internet dan komputer. Sebagai contoh, Anjungan Tunai Mandiri (*Automated Teller Machine* - ATM) termasuk dalam sistem elektronik.[92]

Dalam sistem elektronik ATM ini secara sederhana terdiri dari perangkat keras serta perangkat lunak yang memungkinkan seorang nasabah untuk melakukan transaksi seperti pengiriman uang (transfer), pengambilan uang,

---

[90] *Ibid*, hlm. 202-203
[91] *Ibid*
[92] *Ibid*, hlm. 207.

pengecekan saldo tabungan, pembelian pulsa, pembayaran tagihan, atau transaksi elektronik lainnya. ATM merupakan sistem elektronik yang kompleks karena terhubung dengan berbagai sistem elektronik lainnya, baik ATM dari satu bank yang berada di seluruh Indonesia maupun dengan ATM bank lainnya serta terhubung dengan intenet sehingga membentuk jaringan yang sangat luas. ATM memiliki fungsi yang sangat vital dalam masyarakat di era modern ini. Karena fungsi yang signifikan tersebut ATM dilengkapi berbagai sistem pengaman baik secara fisik maupun secara logis, atau kombinasi keduanya. Sistem pengamanan ATM dapat berupa pengamanan fisik terhadap ATM itu sendiri maupun pengamanan terhadap transaksi yang dilakukan oleh nasabah melalui ATM.[93]

Pengamanan fisik terhadap ATM dapat dilakukan dengan misalnya memasang *closed circuit television (cctv)*, memasang kunci brankas ATM, dan menempatkan ATM dalam ruangan yang terlindungi dari panas maupun hujan. Sedangkan pengamanan logis terhadap transaksi ATM misalnya dengan menerapkan sistem akses berdasarkan kartu ATM dan kode akses (*password*).[94]

C. Dampak Terjadinya *Cyber crime* (Kejahatan Siber)

Perkembangan masyarakat dan IPTEK (Ilmu Pengetahuan dan Teknologi) dalam berbagai studi menunjukkan korelasi positif dengan perkembangan kriminalitas. Lebih dari dua dekade yang lalu telah muncul apa yang disebut sebagai *Cyber crime* (Kejahatan siber) sebagai dampak negatif dari perkembangan teknologi komputer. Kejahatan tersebut cukup menghebohkan dunia hukum (khususnya hukum pidana) bahkan di negara-negara maju. Sekalipun Indonesia

---

[93] *Ibid.*, hlm. 208.
[94] *Ibid*

masih tergolong negara berkembang yang belum sepenuhnya memanfaatkan teknologi informasi, namun trend kejahatan modern dengan memanfaatkan teknologi informasi telah bermunculan. Bahkan kejahatannya cenderung mengalami peningkatan yang luar biasa sehingga pernah menduduki urutan kedua setelah Ukrania.[95]

Merebaknya kejahatan dan kelemahan sistem hukum untuk menangkalnya akan berdampak buruk bagi citra sebuah negara. Jika hal ini dibiarkan terus menerus maka bukan tidak mungkin Indonesia menjadi negara yang dikucilkan dari lintas peradaban modern.[96] Sebagai akibat dari perkembangan yang seperti itu, maka secara lambat laun, teknologi informasi dengan sendirinya juga telah mengubah perilaku masyarakat dan peradaban manusia secara global. Perkembangan yang sangat pesat dalam teknologi internet menyebabkan kejahatan baru di bidang itu juga muncul, misalnya kejahatan manipulasi data, sabotase, provokasi, *money laundering*, *hacking*, pencurian software maupun perusakan hardware dan lainnya.[97]

Terkait dengan berbagai kejahatan siber yang menggunakan internet dimana pengguna awal intenet yang dapat diidentifikasi dalam hal pengguna melakukan penyalahgunaan jaringan atau perangkat, sistem administrator dapat segera mengetahuinya dan dapat memberikan sanksi. Akan tetapi, setelah internet "dilepas" untuk publik, maka bermunculan bermacam sistem administrator baik berupa organisasi maupun individu dari berbagai domain internet. Hal ini

---

[95]Al. Wisnusubroto, 1999, *Kebijakan Hukum Pidana Dalam Penanggulangan Penyalahgunaan Komputer,* Yogyakarta, Universitas Atmajaya Yogyakarta, hlm. 2.

[96]*Ibid*

[97]Agus Rahardjo, 2002, *Cybercrime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi,* Bandung, Citra Aditya Bakti, hlm. 1

mengakibatkan aparat penegak hukum tidak memiliki kontrol yang kuat yang berguna untuk melacak pelaku tindak pidana *cyber crime.*[98]

Setiap pengguna internet dapat menggunakan mesin pencari (*search engine*) untuk memperoleh informasi yang dibutuhkan yang dilengkapi dengan fitur-fitur untuk mencari informasi secara detail. Pertukaran data komputer dari satu komputer ke komputer lain dilakukan dengan memindahkan secara fisik data yang dimaksud dengan cara menyimpan data tersebut dalam media penyimpanan dan berjalan menuju komputer lain yang mungkin berbeda ruangan, gedung, jalan, atau bahkan mengirimkannya lewat pos apabila berada di luar kota atau di luar negara. Dengan adanya internet, seseorang dapat mengirimkan data secara instan kemanapun. Transaksi juga mudah dilakukan darimana saja dan kapan saja apabila menggunakan internet.[99]

Transaksi seperti membayar listrik, membeli pulsa, transfer dari bank satu ke bank yang lain, dan melakukan pembelian barang secara online tidak perlu pergi ke ATM karena sudah adanya layanan fasilitas ATM yang menggunakan internet banking sehingga dapat dengan mudah dilakukan. Kemudahan serta manfaat yang diberikan oleh pemanfaatan perkembangan teknologi intenet tersebut yang berdampak pada masyarakat dan juga menimbulkan berbagai permasalahan hukum. Transaksi online mudah dilakukan karena tidak perlu bertemu langsung atau tanpa mengenal satu sama lain antara penjual dan pembeli. Transfer uang yang dapat dilakukan secara instan pun dapat menimbulkan

---

[98]Josua Sitompul, 2012, *Cyberspace, Cyber crime, Cyber Law Tinjauan Aspek Hukum Pidana,* Jakarta, PT. Tatanusa, hlm. 27.
[99]*Ibid,* hlm. 28

keraguan dalam keamanannya apabila uang tersebut diambil orang lain tanpa diketahui para pihak.

Hubungan antara hukum dan teknologi internet tentu saja akan menjadi unik. Dunia *cyber* sebagai manifestasi sistem informasi dan telekomunikasi yang terpadu dalam suatu jaringan global adalah ruang tanpa batas yang dapat diisi dengan sebanyak mungkin kategori. Baik yang sudah ada, akan ada, dan mungkin akan terus berkembang. Dari perdagangan, perhubungan, kesehatan, sampai militer, dan sebagainya. Bahkan anda sendiri dapat membentuk komunitas dari tingkatan keluarga, arisan sampai pada tingkatan sebuah negara di dunia *cyber* yang tiada batas (*unlimited world*). Terus berkembangnya pemanfaatan teknologi internet untuk berbagai kegiatan sehari-hari telah membuka jalan bagi "kebebasan *cyber*".[100]

Kebebasan tersebut baik untuk kegiatan bisnis maupun dalam kegiatan awam sehari-hari, segala sesuatu yang terjadi dalam dunia *cyber* dapat dilakukan dengan mudah, bebas, canggih, cepat, efisien. Tak perlu lagi bertemu muka secara langsung. Semua ini tentu akan menimbulkan masalah apabila tidak atau belum secara utuh diatur oleh hukum.[101] Namun demikian hal tersebut belum diimbangi dengan kesiapan dunia hukum dan alat perlengkapannya. Kejahatan siber bukanlah suatu bentuk kejahatan sederhana, karena pembuktiannya yang sulit dan seringkali dihadapkan pada belum adanya peraturan yang jelas dan tegas. Tidak jarang pelakunya berhasil melakukan penipuan sampai ratusan ribu dolar dan kerugian-kerugian lain pada sistem jaringan data komputer, ternyata hanya

[100]Febri, http://febri-jd.blogspot.com/, diakses 21 Januari 2015 (18.30).
[101]*Ibid*

dihukum satu atau dua tahun penjara. Sementara itu, *cyber crime* yang terjadi dalam perbankan di Indonesia cenderung meningkat.[102]

Berikut data contoh kasus *cyber crime* (kejahatan siber) dalam Perbankan:

No.	Jenis Kasus	Pasal/Dasar Hukum	Keterangan
1.	Kasus "*Computer Crime Unauthorized Transfer*" Dana Bank di Bank Negara Indonesia 1946 New York Agency (Tahun 1986/1987)	Pasal 363 ayat (1) ke-4 KUHP (Pencurian yang dilakukan secara bersama-sama)	Dari sisi modus operandi termasuk dalam jenis *unauthorized transfer* yang dilakukan dari jarak berjauhan dengan menghubungkan komputer. Dan adanya "orang dalam" yang memegang kode rahasia BNI 1946. Motivasi terjadinya kejahatan ini adalah karena adanya faktor politik dalam menjalankan suatu bisnis besar yang memerlukan biaya yang tidak sedikit
2.	Kasus penyalahgunaan kartu kredit dalam *e-banking* dan *e-commerce* (transaksi elektronik) Tahun 2001	Pasal 378 KUHP (Tindak Pidana Penipuan)	Kasus penipuan yang dilakukan seperti ini dikenal dengan *carding* yang modus operandinya dengan menggunakan kartu kredit secara illegal dan termasuk dalam jenis *cyber crime* "*computer-related fraud* atau *data diddling*. Dilihat dari motivasinya karena adanya faktor ekonomi yang dipengaruhi oleh promosi barang-barang produksi, faktor sosial budaya yang dipengaruhi dengan kemajuan teknologi informasi dan sumber daya manusianya

Berdasarkan data tersebut di atas merupakan contoh kasus *cyber crime* dalam Perbankan karena sebab-sebab lain.

Kasus pertama, diputus di Pengadilan Negeri Jakarta Pusat tentang pentransferan (pendebetan) uang milik BNI 1946 ke beberapa rekening di Panama

[102] *Ibid*

City melalui Bank perantara di New York yang menggunakan cara *"Electronic Payment System"* (E.P.S) yaitu dalam jenis *Unauthorized Transfer* (transfer yang tidak sah) yang dilakukan dari jarak berjauhan dengan memanfaatkan teknologi komputer dan internet. Dalam kasus tersebut atas nama Terdakwa Seno Adjie dan Rudy Demsy. Terdakwa Seno Adjie dan Rudy Demsy dituntut dengan Pasal 363 ayat (1) ke-4 KUHP, karena Terdakwa telah melakukan kejahatan secara bersama-sama.[103] Kesesuaian antara unsur-unsur dari Pasal 363 ayat (1) ke-4 KUHP dalam perkara tersebut yaitu:

a. Unsur "barang siapa" yang dimaksud "barang siapa" dalam hukum pidana adalah subjek hukum (pelaku tindak pidana), yang pengertiannya adalah siapa saja sehingga yang dimaksud "barang siapa" tidak lain adalah Terdakwa Seno Adjie dan Rudy Demsy.
b. Unsur "mengambil suatu barang" bahwa Terdakwa Seno Adjie bersama dengan Rudy Demsy (mantan karyawan BNI 1946 New York Agency), telah mengoperasikan komputer dengan memakai kode rumus *password enter* dan *Testkey* yang berkode RUDEMS untuk memindahkan (mentransfer) uang milik BNI 1946 ke rekening Bank lain di Panama dan Bank penerima lain tersebut melalui *"transfer electronic payment system"*. Dengan selesainya transfer melalui komputer tersebut, maka beralih dana (uang) dari rekening BNI 1946 ke dalam rekening seseorang di Bank penerima.

---

[103]Sumber kasus:*"Men-'Digger' Dana BNI 1946, Rp 30 Milyar"*, Tempo, Nomor 24, Tahun XVII, 24 Oktober 1987, hlm. 34-40 (Dalam buku Al. Wisnubroto, 2011, *Konsep Hukum Pidana Telematika,* Yogyakarta, Universitas Atmajaya Yogyakarta, hlm. 240).

c. Unsur "barang tersebut seluruhnya atau sebagian kepunyaan/milik orang lain". Bahwa uang yang ditransfer oleh Terdakwa Seno Adjie bersama Rudy Demsy dari BNI 1946 ke Bank penerima tersebut bukan milik Terdakwa melainkan milik BNI 1946.

d. Unsur "dengan maksud untuk memiliki secara/dengan melawan hukum". Bahwa uang tersebut ditransfer dengan tanpa hak.

e. Unsur "dilakukan oleh dua orang atau lebih secara bersama-sama". Bahwa dalam kasus ini kerjasama antara Seno Adjie dengan Rudy Demsy. Dengan terpenuhinya unsur-unsur tersebut, maka diterapkan ketentuan tentang "pencurian yang dilakukan dua orang atau lebih secara bersama-sama".[104]

Pada era tahun 1980-an dan sebelumnya, seringkali terjadinya kejahatan yang berbasis teknologi telematika atau lebih dikenal kejahatan komputer lebih banyak melibatkan "orang dalam". Semenjak perkembangan pemanfaatan teknologi telematika memasuki era internet dimana jaringan koneksi komputer semakin terbuka dan bersifat global, maka peran "orang dalam" pun mulai digeser dengan siapa saja yang termasuk "orang luar".[105]

Kasus diatas termasuk dalam pencurian yang dilakukan dengan sarana komputer. Kasus tersebut juga terjadi di dalam dunia perbankan karena menggunakan cara *"Electronic Payment System"* (E.P.S), yang maksudnya lalu lintas pembayaran antar lintas bank secara otomatis dengan memanfaatkan teknologi yang berbasis komputer atau teknologi informasi. Dalam kasus ini juga

---

[104] *Ibid*, hlm. 252-253.
[105] *Ibid*, hlm. 102.

dapat dikategorikan *cyber crime* karena menggunakan teknik *"hacking"* untuk melakukan *illegal access* pada sistem EPS Bank BNI yang selanjutnya melakukan transfer uang secara melawan hukum ke bank-bank yang lain. Dari sisi modus operandi yang digunakan dengan adanya "orang dalam" (bekas karyawan Bank BNI 1946) yang memegang kode rahasia Bank BNI hingga saat dilakukannya kejahatan tersebut. Sehingga dapat dilakukan pentransferan dengan jarak jauh.[106]

Penerapan kebijakan hukumnya adalah mengarah pada Pasal 363 ayat (1) ke-4 KUHP yaitu "pencurian yang dilakukan oleh dua orang bersama-sama atau lebih" dengan unsur-unsur yaitu "mengambil barang" yang dilakukan secara non fisik, tanpa menyentuh barang yang diambil itu (*electronic payment system*). Unsur "dengan maksud memiliki" bahwa dengan selesainya transfer tersebut sehingga sejumlah nilai yang ditransfer telah berpindah dan masuk ke dalam rekening seseorang dalam suatu Bank.[107]

Pada kasus kedua, diputus di Pengadilan Negeri Sleman tentang kasus penyalahgunaan kartu kredit dalam *e-banking* dan *e-commerce* (transaksi elektronik) tahun 2001 yang secara ilegal mempergunakan kartu kredit orang lain untuk berbelanja di toko online. Dalam kasus ini atas nama Terdakwa Petrus Pangkur alias Bony Diobok-obok pada tanggal 3 Maret 2001. Kasus penipuan yang dilakukan seperti ini dikenal dengan *carding* yang modus operandinya dengan menggunakan kartu kredit secara illegal dan termasuk dalam jenis *cyber crime "computer-related fraud* atau *data diddling*". Dilihat dari motivasinya karena adanya faktor ekonomi yang dipengaruhi oleh promosi barang-barang

---

[106] *Ibid*
[107] *Ibid*

produksi, faktor sosial budaya yang dipengaruhi dengan kemajuan teknologi informasi dan sumber daya manusianya. Dalam dunia telematika kasus ini memanfaatkan teknologi yang berbasis internet.[108]

Proses transaksinya dengan kartu kredit ilegal milik orang lain dengan mencantumkan dan mengirimkan data/informasi yang tidak benar, ini juga merupakan kejahatan komputer pada layanan internet banking dalam bidang perbankan karena menggunakan kartu kredit yang menjadi salah satu cakupan akses intenet banking dalam transaksi non tunai yang bisa dilakukan dengan EDC MasterCard Electronic yaitu VISA yang diminta pada saat Terdakwa *chatting*. Tedakwa dituntut dengan Pasal 378 KUHP atas perbuatan kejahatan tersebut. Karena perbuatan Terdakwa telah memenuhi unsur-unsur Pasal 378 KUHP yakni:

1) Unsur "dengan maksud menguntungkan diri sendiri atau orang lain secara melawan hukum". Bahwa Tedakwa sengaja atau memiliki maksud/tujuan untuk menguntungkan dirinya sendiri (menggunakan kartu kredit milik orang lain untuk membeli helm dan sarung tangan), yang mana perbuatan itu dilakukan secara melawan hukum yaitu dengan menggunakan kartu kredit jenis VISA 4388 5750 4013 3003 *expiration date* 06/03.
2) Unsur "dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat, ataupun rangkaian kebohongan, membujuk/menggerakkan orang lain untuk menyerahkan barang sesuatu kepadanya atau supaya member hutang maupun menghapuskan hutang". Bahwa Terdakwa telah

[108]Sumber kasus: Salinan Dokumen Penyidikan Kepolisian DIY tanggal 18 September 2001; *Salinan Putusan Pengadilan Negeri Sleman* tanggal 23 Agustus 2002 (Dalam buku Al. Wisnubroto, 2011, *Konsep Hukum Pidana Telematika,* Yogyakarta, Universitas Atmajaya Yogyakarta, hlm. 286).

menggunakan kartu kredit jenis VISA 4388 5750 4013 3006 *expiration date* 06/03 dengan terlebih dahulu merubah identitas pemilik kartu tersebut menjadi "Bony Diobok-Obok, alamat Gg. Ujung Burjo No. 009 Yogyakarta". Dengan kartu kredit yang telah dimodifikasi tersebut Terdakwa menggunakannya untuk memesan barang (helm dan sarung tangan) melalui internet sehingga seolah-olah kartu kredit tersebut sah dan valid dipergunakan untuk bertransaksi.[109]

Dengan terpenuhinya unsur-unsur Pasal 378 KUHP maka Terdakwa terbukti melakukan tindak pidana penipuan dan dihukum dengan pidana penjara selama 1 (satu) tahun 3 (tiga) bulan.

Berdasarkan kedua kasus yang telah diuraikan di atas, keduanya terjadi sebelum lahirnya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) maka terdakwa yang melakukan tindak pidana tersebut dijerat dengan pasal-pasal yang ada dalam Kitab Undang-Undang Hukum Pidana (KUHP) meskipun dalam tindak pidana tersebut menggunakan sarana teknologi informasi dan elektronik. Tetapi di Indonesia pada saat ini telah memiliki perundang-undangan khusus tentang transaksi elektronik, yaitu Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), meskipun tidak ada satu pasal pun yang secara khusus mengatur masalah *carding*, namun melalui interprestasi yang bersifat kontekstual maka beberapa ketentuan dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) yang dapat diterapkan adalah:

---

[109] *Ibid*, hlm. 288-289.

1. Apabila cara "mengintip" nomor kartu kredit tersebut dilakukan dengan menyadap aktivitas transaksi antara pemilik kartu dengan toko *online* melalui sarana internet maka pelaku dapat dikenakan Pasal 31 ayat (1) atau (2) yang mengatur masalah "*illegal interception*" jo. Pasal 47 UU Nomor 11 tahun 2008 tentang ITE yang mengatur sanksinya.
2. Perbuatan menggunakan nomor kartu kredit milik orang lain tersebut untuk "mengakali" toko *online* sehingga pelaku dapat berbelanja sejumlah barang tanpa membayar, dapat dikenakan Pasal 35 UU Nomor 11 tahun 2008 tentang ITE yang mengatur masalah "*computer-realted forgery*" jo. Pasal 51 ayat (1) UU Nomor 11 tahun 2008 tentang ITE yang mengatur sanksinya.[110]

Adapun beberapa kasus yang ditangani oleh Polda DIY mengenai kasus dalam Perbankan seperti *carding*. Berdasarkan wawancara di Polda DIY dengan Penyidik AKP. Novita Ekasari dari Ditkrimsus bagian Kasubdit 1 yang khusus menangani masalah perbankan pernah menangani kasus *carding* tetapi dari sistem offline yaitu di lokasi daerah Depok yang Pelakunya seorang wiraswasta. Pelaku sengaja mengambil ATM dari teman si Pelapor karena ATM tersebut sengaja diambil oleh teman Pelapor untuk kemudian diberikan kepada Pelaku. Dari Ditkrimsus bagian Kasubdit 2 dengan Penyidik Kompol Hendri Multi juga pernah menangani kasus *carding* yang Terdakwanya WNA asal Nigeria melakukan penipuan uang kurang lebih 350 juta terhadap nasabah Bank BCA Yogyakarta.

---

[110] *Ibid*

Terdakwa atau pelaku utama belum berhasil ditemukan namun Terdakwa yang lain sudah tertangkap.[111]

Dalam konteks *cyber crime* media yang digunakan oleh pelaku (*hacker*) kebanyakan adalah komputer dan internet. Ketika komputer merupakan sasaran dari tindak kejahatan, tujuan si pelaku adalah untuk mencari informasi dari atau menyebabkan kerusakan pada komputer, suatu sistem komputer, atau jaringan komputer. Bentuk kejahatan semacam ini menjadikan sistem komputer sebagai sasarannya baik untuk mendapatkan informasi yang disimpan pada sistem komputer maupun untuk menguasai sistem itu. Bentuk kejahatan seperti ini pada umumnya melibatkan hacker yang melakukan kejahatan pada sistem komputer untuk mendapatkan akses secara tidak sah. Pencurian informasi dapat dilakukan dalam berbagai cara seperti pembobolan nomor-nomor kartu kredit atau pencurian informasi pribadi orang lain dengan tujuan untuk melakukan pemerasan uang atau untuk alasan-alaan bisnis.[112]

[111]Hasil wawancara dengan AKP. Novita Ekasari dan Kompol Hendri Multi, selaku Penyidik di POLDA DIY dari Ditkrimsus bagian Kasubdit 1 pada hari Jumat Tanggal 7 November 2014.
[112]Maskun, 2013, *Kejahatan Siber Cyber Crime,* Jakarta, Kencana, hlm. 55-56.