Volume 5 Nomor 2 (2023) Pages 15 – 26
EduLaw : Journal of Islamic Law and Yurisprudance
Email Journal : edulaw.bbc@gmail.com
Web Journal : http://journal.bungabangsacirebon.ac.id/index.php/edulaw

KARAKTERISTIK CYBERCRIME DI INDONESIA

Amin Suhaemin[1], Muslih[2]

Mahasiswa Prodi Hukum Pidana Islam UI Bunga Bangsa Cirebon
Dosen Prodi Hukum Pidana Islam UI Bunga Bangsa Cirebon

Email : asuha0376@gmail.com, moesabdee84@gmail.com,

Received: 2023-07-30; Accepted: 2023-08-25; Published: 2023-08-30

Abstrak

Cybercrime muncul akibat dampak negatif dari perkembangan aplikasi internet. Motif melakukan kejahatan ini di samping untuk mendapat keuntungan juga iseng. Kejahatan ini juga muncul karena ketidakmampuan hukum termasuk aparat dalam menjangkaunya. Kejahatan ini bersifat maya dimana pelaku tidak tampak secara fisik. Begitu hebatnya kejahatan ini bahkan dapat meresahkan dunia internasional. Tujuan penelitian ini untuk mengetahui apa sebenarnya tindak pidana Cybercrime, bagaimana karakteristiknya, jenis-jenis dan faktor pendorong terjadinya cybercrime. Metode dari penelitian ini adalah metode kepustakaan (Library Research), Sumber data yang penulis ambil berupa buku dan artikel-artikel ilmiah. Analisis data yang penulis gunakan adalah analisis deskriptif, yaitu menganalisis semua sumber yang diperoleh terkait artikel ini, kemudin menemukan karakeristik dan faktor pendorong terjadinya kejahatan cybercrime. Hasil yang didapat dari penulisan ini adalah Cybercrime sebagai kejahatan yang muncul sebagai akibat adanya komunitas dunia maya di internet, memiliki karakteristik yang khas dibandingkan kejahatan konvensional, karakteristik unik dari kejahatan di dunia maya tersebut anatara lain menyangkut lima hal berikut: 1) ruang lingkup, 2) sifat kejahatan, 3) pelaku kejahatan, 4) modus kejahatan, dan 5) jenis kerugian yang ditimbulkan. Sedangkan jenis-jenis kejahatan cybercrime bisa dibedakan berdasarkan; 1) modus atau jenis aktifitasnya, 2) berdasarkan motif, dan 3) berdasarkan sasaran kejahatan. Adapun faktor pendorong terjadinya cybercrime adalah: 1) Akses internet yang tidak terbatas, 2) Kelalaian penggunaan komputer, 3) Mudah dilakukan dengan resiko keamanan yang kecil dan tidak diperlukan peralatan yang super modern, 4) Para pelaku merupakan orang yang pada umumya cerdas, mempuyai rasa ingin tahu besar, dan fanatik akan teknologi komputer, 5) Kurangnya perhatian masyarakat dan penegak hukum, 6) Sistem keamanan jaringan yang lemah, 7) Cybercrime dipandang sebagai produk ekonomi.

Kata Kunci: *Cybercrime, Karakteristik,*

Abstract

Cybercrime arises due to the negative impact of the development of internet applications. The motive for committing this crime is not only to gain profit, but also for fun. This crime also

arises because of the inability of the law, including the apparatus, to reach it. This crime is virtual where the perpetrator is not physically visible. So great is this crime that it can even disturb the international community. The purpose of this study is to find out what cybercrime actually is, what are its characteristics, types and driving factors for cybercrime. The method of this research is the library method (Library Research), The data sources that the authors take are in the form of books and scientific articles. The data analysis that the writer uses is descriptive analysis, namely analyzing all sources obtained related to this article, then finding the characteristics and driving factors of cybercrime. The results obtained from this writing are Cybercrime as a crime that arises as a result of the virtual world community on the internet, has distinctive characteristics compared to conventional crime, The unique characteristics of crime in cyberspace include the following five things: 1) scope, 2) nature of the crime, 3) perpetrator of the crime, 4) mode of crime, and 5) type of loss incurred. Meanwhile, the types of cybercrime crimes can be distinguished based on; 1) mode or type of activity, 2) based on motive, and 3) based on the target of the crime. The driving factors for cybercrime are: 1) Unlimited internet access, 2) Negligence in using a computer, 3) Easy to do with little security risk and no need for super modern equipment, 4) The perpetrators are generally intelligent people, have great curiosity, and fanatical about computer technology, 5) Lack of public and law enforcement attention, 6) Weak network security system, 7) Cybercrime is seen as an economic product.

Keywords: *Cybercrime, Characteristics*

A. LATAR BELAKANG MASALAH

Seiring dengan berkembangnya pemanfaatan internet, maka mereka yang memiliki kemampuan di bidang komputer dan memiliki maksud-maksud tertentu dapat memanfaatkan komputer dan internet untuk melakukan kejahatan yang merugikan pihak lain. Perkembangan Internet yang semakin hari semakin meningkat baik teknologi dan penggunaannya, membawa banyak dampak baik positif maupun negatif. Tentunya untuk yang bersifat positif kita semua harus mensyukurinya karena banyak manfaat dan kemudahan yang didapat dari teknologi ini. Tidak dapat dipungkiri bahwa teknologi Internet juga membawa dampak negatif yang tidak kalah banyaknya dengan manfaat yang ada. Internet membuat kejahatan yang semula bersifat konvensional berkembang menjadi sebuah kejahatan modern dengan tingkat kerugian yang lebih besar dengan dampak yang luas.

Hilangnya batas ruang dan waktu di Internet mengubah banyak hal. Perkembangan yang pesat dalam pemanfaatan jasa internet pada akhirnya mengundang terjadinya kejahatan, yang lebih dikenal dengan nama Cybercrime. Cybercrime merupakan perkembangan dari computer crime. Indonesia sebagai salah satu negara dengan penduduk terpadat di dunia juga tidak lepas dari persoalan tersebut. Indonesia menyumbang 2,4% kejahatan cyber di dunia. Angka ini naik 1,7% dibanding tahun 2010 lalu di mana Indonesia menempati peringkat 28. Hal ini tak lain disebabkan oleh terus meningkatnya jumlah pengguna internet di Indonesia (Kompas, 16 Mei 2012).

Menurut data, Indonesia masuk lima besar pengguna jejaring sosial terbanyak di dunia, disinyalir penjahat cyber lebih mudah lagi dalam menjalankan aksinya. Para penjahat cyber memanfaatkan jaringan pertemanan melalui jejaring sosial, karena sebagian besar pengguna jejaring sosial percaya begitu saja atas link atau konten yang mereka terima dari sesama teman. Tanpa melakukan konfirmasi atau pengecekan lebih lanjut pengguna jejaring sosial tersebut melakukan akses langsung ke web atau situs yang mereka terima, yang tanpa disadari berisi program jahat. (Kompas, 16 Mei 2012).

TB. Ronny R. Nitibaskara menyebutkan cyber crime sebagai kejahatan yang terjadi melalui atau pada jaringan computer di dalam internet. (Widodo, 2009). Tapi pada dasarnya, istilah cybercrime merujuk pada suatu tindakan kejahatan yang berhubungan dengan dunia maya (cyberspace) dan tindakan yang menggunakan komputer. (Dikdik M Arief Mansur dan Elisatris Gultom, 2009). Secara sederhana cybercrime adalah istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer menjadi alat, sasaran atau tempat terjadinya kejahatan. (Nunuk Sulisrudatin, 2018).

Cyber Law atau atau ada yang menyebutnya Cyberspace Law di Indonesia sudah dimulai sejak pertengahan tahun 1990-an bersamaan dengan semakin berkembang pesatnya pemanfaatan internet. Dilihat dari ruang lingkupnya cyber law meliputi setiap aspek yang berhubungan dengan subyek hukum yang memanfaatkan teknologi internet yang dimulai pada saat mulai "on-line" dan seterusnya pada saat memasuki dunia maya. Oleh karena itu, dalam pembahasan cyber law, tidak dapat lepas dari isu yang menyangkut prosedural, seperti yuridikdsi, pembuktian, penyidikan, kontrak/transaksi elekrtonik, pornografi, pencurian melalui internet, perlindungan konsumen, pemanfaatan internet dalam aktifitas keseharian manusia, seperti e-commerce, e-government, e-tax, e-learning, e-health dan sebagainya. Dengan demikian maka ruang lingkup cyber crime sangat luas, tidak hanya semata-mata mencakup aturan-aturan yang mengatur kegiatan bisnis yang melibatkan konsumen (consumers), manufaktur (manufactures), service providers dan pedagang perantara (intermediares) dengan menggunakan internet (e-commerce). Dalam konteks demikian pelu dipikirkan tentang rezim hukum baru terhadap kegiatan di dunia maya. (Nazarudin, 2011).

Hukum yang salah satu fungsinya menjamin kelancaran proses pembangunan nasional sekaligus mengamankan hasil-hasil yang telah dicapai harus dapat melindungi hak para pemakai jasa internet sekaligus menindak tegas para pelaku Cybercrime. Melihat dari sifatnya Cybercrime termasuk dalam kategori borderless cryme (kejahatan tanpa batasan ruang dan waktu), sehingga dalam memberantas tindak kejahatan Cybercrime, diperlukan langkah-langkah yang kompleks, terintegrasi serta berkesinambungan dari banyak pihak, tidak hanya tugas penegak hukum semata.

Tujuan dari penulisan ini adalah untuk mengetahui apa sebenarnya Cybercrime itu, bagaiamana karakteristik kejahatan melalui Cybercrime, apa saja jeni-jenis kejahatan yang termasuk cybercrime serta apa sajakah yang menjadi faktor pendorong terjadinya Cybercrime, melalaui tulisan singkat ini penulis akan menjelaskan lebih lanjut dalam makalah yang berjudul "Cybercrime (Pengertian, Karakteristik, Jenis-Jenis Dan Faktor Pendorong Terjadinya Cybercrime)".

B. METODOLOGI PENELITIAN

Metode dari penelitian ini adalah metode kepustakaan (*Library Research*), penulis mengambil data yaitu tulisan-tulisan yang terkait dengan kejahatan cybercrime. Sumber data yang penulis ambil berupa buku dan artikel-artikel ilmiah. Analisis data yang penulis gunakan adalah analisis deskriptif, yaitu menganalisis semua sumber yang diperoleh terkait artikel ini, kemudin menemukan karakeristik dan faktor pendorong terjadinya kejahatan *cybercrime.*

C. HASIL DAN PEMBAHASAN

1. Pengertian Cybercrime

Cybercrime merupakan salah satu bentuk atau dimensi baru dari kejahatan masa kini yang mendapat perhatian luas dunia internasional. (Nawawi Arief, 2007). Masih menurut Nawawi Arief (2007: 1). Dalam arti sempit cybercrime adalah computer crime yang ditujukan terhadap sistem atau jaringan komputer, sedangkan dalam arti luas, cybercrime mencakup seluruh bentuk baru kejahatan yang ditujukan pada komputer, jaringan komputer dan penggunaanya serta bentuk-bentuk kejahatan tradisional yang sekarang dilakukan dengan menggunakan atau dengan bantuan peralatan komputer (computer related crime). Dengan demikian cybercrime meliputi kejahatan, yaitu yang dilakukan:

a. Dengan menggunakan sarana-sarana dari sistem atau jaringan komputer (by means of a computer system or network);
b. Di dalam sistem atau jaringan komputer (in a computer system or network); dan
c. Terhadap sistem atau jaringan komputer (against a computer system or network).

Dari definisi tersebut, maka dalam arti sempit cybercrime adalah computer crime yang ditujukan terhadap sistem atau jaringan komputer, sedangkan dalam arti luas, cybercrime mencakup seluruh bentuk baru kejahatan yang ditujukan pada komputer, jaringan komputer dan penggunanya serta bentuk-bentuk kejahatan tradisional yang sekarang dilakukan dengan menggunakan atau dengan bantuan peralatan komputer (computer related crime). (Nunuk Sulisrudatin, 2018:31).

Untuk memudahkan pemahaman, berikut beberapa pendapat tentang apa yang dimaksud dengan Cybercrime. Menurut Gregory (2005) Cybercrime adalah suatu bentuk kejahatan virtual dengan memanfaatkan media komputer yang terhubung ke internet, dan mengekploitasi komputer lain yang terhubung dengan internet juga. Adanya lubang-lubang keamanan pada sistem operasi menyebabkan kelemahan dan terbukanya lubang yang dapat digunakan para hacker, cracker dan script kiddies untuk menyusup ke dalam komputer tersebut.

Sedangkan menurut Kepolisian Inggris Tahir (2009) ”Cybercrime adalah segala macam penggunaan jaringan komputer untuk tujuan kriminal dan atau kriminal berteknologi tinggi dengan menyalahgunakan kemudahan teknologi digital”. Menurut Tavani dalam Fajri (2008:31) definisi Cybercrime, yaitu ”kejahatan dimana tindakan kriminal hanya bisa dilakukan dengan menggunakan teknologi cyber dan terjadi di dunia cyber”. Andi Hamzah mengartikan Cybercrime sebagai kejahatan di bidang komputer secara umum sebagai penggunaan komputer secara illegal.

Dari beberapa pengertian di atas, cybercrime dapat dirumuskan sebagai perbuatan melawan hukum yang dilakukan dengan memakai jaringan komputer sebagai sarana/alat atau komputer sebagai objek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain. (Arifah, 2011:3).

2. Karakteristik dan Jenis-Jenis Cybercrime

Cybercrime merupakan kejahatan yang muncul sebagai akibat adanya komunitas dunia maya di internet, memiliki karakteristik yang khas dibandingkan kejahatan konvensional, yaitu antara lain:

a. Ruang lingkup kejahatan

Perbuatan yang dilakukan secara illegal, tanpa hak atau tidak etis tersebut terjadi di ruang/wilayah maya (cyberspace), sehingga tidak dapat dipastikan yurisdiksi hukum negara mana yang berlaku terhadapnya

b. Modus kejahatan

Perbuatan tersebut dilakukan dengan menggunakan peralatan apapun yang bisa terhubung dengan internet.

c. Jenis kerugian yang ditimbulkan

Perbuatan tersebut mengakibatkan merugikan materil maupun imateril (waktu, nilai, jasa, uang, barang, harga diri, martabat, kerahasiaan informasi) yang cenderng lebih besar dibandingkan kejahatan konvensional.

d. Pelaku kejahatan

Pelakunya adalah orang yang menguasai penggunaan internet beserta aplikasinya.

e. Sifat kejahatan

Perbuatan tersebut seringkali dilakukan secara transnasional/melintasi batas negara. (Fuady, 2005:4).

Dari beberapa karakteristik di atas, untuk mempermudah penanganannya maka cybercrime dapat diklasifikasikan menjadi:

a. Cyberpiracy

Pengunaan teknlogi komputer untuk mencetak ulang software atau informasi, lalu mendistribusikan informasi atau software tersebut lewat teknologi komputer.

b. Cybertrespass

Penggunaan teknologi kumputer untuk meningkatkan akses pada sistem komputer suatu organisasi atau individu.

c. Cybervandalism

Penggunaan teknologi komputer untuk membuat program yang mengganggu proses transmisi elektronik, dan menghancurkan data komputer. (Eliasta, 2016:37).

3. Jenis-jenis Cybercrime

Berdasarkan modus atau jenis aktifitasnya cybercrime (Abidin, 2015:2-4) dapat digolongkan menjadi beberapa jenis sebagai berikut:

a. Anauthorized Acces

Merupakan kejahatan yang terjadi ketika seseorang memasuki atau menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa ijin atau tanpa sepengetahuan dari pemilik sistem jaringan computer yang dimasukinya.

b. Illegal Contens

Merupakan kejahatan yang dilakukan dengan memasukan data atau informasi ke internet tentang suatu hal yang tidak benar, tidak etis dan dapat dianggap melanggar hokum atau mengganggu ketertiban umum, contohnya adalah penyebaran pornografi.

c. Penyebaran virus secara sengaja

Penyebaran virus pada umumnya dilakukan dengan menggunakan email. Seringkali orang yang sistem emailnya terkena virus tidak menyadari hal ini. Virus ini kemudian dikirimkan ke tempat lain melalui emailnya.

d. Data Forgery

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

e. Cyber Espionage, Sabotage and Extortion

Cyber Espionage merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki system jaringan komputer pihak sasaran. Sabotage and Extortion merupakan jenis kejahatan yang dilakukan dengan membuat gangguan, perusakan atau pengahancuran terhadap suatu data, program computer atau sistem jaringan komputer yang terhubung dengan internet.

f. Cyberstalking

Kejahatan jenis ini dilakukan untuk mengganggu atau melecehkan seseorang dengan memanfaatkan komputer, misalnya dengan menggunakan email, dan dilakukan berulang-ulang. Kejahatan tersebut menyerupai teror yang ditujukan kepada seseorang dengan memanfaatkan media internet. Hal itu bias terjadi karena kemudahan dalam membuat email dengan alamat tertentu tanpa harus menyertakan identitas diri yang sebenarnya.

g. Carding

Carding merupakan kejahatan yang dilakukan untuk mencuri nomor kartu kredit milik orang lain dan digunakan dalam transaksi perdagangan di internet.

h. Hacking dan Cracker

Istilah hacker biasanya mengacu pada seseorang yang punya minat besar untuk mempelajari sistem secara detail dan bagaimana meningkatkan kapabilitasnya. Adapun mereka yang sering melakukan aksi-aksi perusakan di internet lazimnya disebut cracker. Boleh dibilang cracker ini sebenarnya adalah hecker yang memanfaatkan kemampuannya untuk hal-hal yang negatif. Aktifitas cracking di internet memiliki lingkup yang sangat luas, mulai dari pembajakan account milik orang lain, pembajakan situs web, menyebarkan virus, hingga pelumpuhan targer sasaran. Tindakan yang terakhir disebut sebagai DoS (Denial of Service). DoS attack merupakan serangan yang bertujuan melumpuhkan target (hang, crash) sehingga tidak dapat memberikan layanan.

i. Cybersquatting and Typosquatting

Cybersquatting merupakan kejahatan yang dilakukan denga mendaftarkan domain nama perusahaan orang lain dan kemudian berusaha menjualnya kepada perusahaan tersebut dengan harga yang lebih mahal. Adapun Typosquatting adalah kejahatan dengan membuat domain plesetan yaitu domain yang merip dengan nama domain orang lain. Nama tersebut merupakan nama domain saingan perusahaan.

j. Hijacking

Hijacking merupakan kejahatan melakukan pembajakan hasil karya orang lain. Yang paling sering terjadi adalah software piracy (pembajakan perangkat lunak).

k. Cyber Terosrism

Suatu tindakan cybercrime termasuk cyber terorism jika mengancam pemerintah atau warga negara, termasuk crecking ke situs pemerintah atau militer. Beberapa contoh kasus cyber terrorism diantaranya adalah:

1) Ramzi Yousef, dalang penyerangan pertama ke gedung WTC, diketahui menyimpan detail serangan dalam file yang dienkripsi di laptopnya.
2) Osama bin Laden diketahui menggunakan steganography untuk komunikasi jaringannya.
3) Suatu website yang dinamai Club Hecker Muslim diketahui menuliskan daftar tip untuk melakukan hacking ke Pentagon.
4) Seorang hecker yang menyebut dirinya sebagai Dokter Nuker diketahui telah kurang lebih lima tahun telah melakukan defacing atau mengubah isi halaman web dengan propaganda anti-American, anti-Israel dan Pro bin Laden.

Berdasarkan motif kegiatannya, cybercrime dapat digolongkan menjadi beberapa jenis diantaranya sebagai berikut:

a. Cybercrime sebagai tindak kejahatan murni

Kejahatan yang murni merupakan tindak kriminal merupakan kejahatan yang dilakukan karena motif kriminalitas. Kejahatan jenis ini biasanya menggunakan internet hanya sebagai sarana kejahatan. Contoh kejahatan semacam ini adalah Carding, yaitu pencurian nomor kartu kredit milik orang lain dan digunakan dalam transaksi perdagangan di internet. Juga pemanfaatan media internet (webserver, mailing, list) untuk menyebarkan material bajakan. Pengirim email anonym yang berisi promosi (spamming) juga dapat dimasukan dalam contoh kejahatan yang menggunakan internet sebagai sarana. Di beberapa negara maju, spamming dapat dituntut dengan tuduhan pelanggaran privasi.

b. Cybercrime sebagai tindak kejahatan abu-abu

Pada jenis kejahatan di internet yang termasuk dalam wilayah "abu-abu" cukup sulit menentukan apakah itu merupakan tindak kriminal atau bukan mengingat motif kegiatannya terkadang bukan untuk kejahatan. Salah satu contohnya adalah probing atau portscanning. Ini adalah sebutan untuk semacam tindakan pengintaian terhadap sistem milik orang lain dengan mengumpulkan informasi sebanyak-banyaknya dari system yang diintai, termasuk sistem operasi yang digunakan, port-port yang ada, baik yang terbuka maupun yang tertutup, dan sebagainya. (Eliasta Ketaren, 2016:3).

Sedangkan berdasarkan sasaran kejahatan, cybercrime dapat dikelompokan menjadi beberapa kategori seperti berikut ini:

c. Cybercrime yang menyerang individu (Againts Person)

Jenis kejahatan ini, sasaran serangannya ditujukan kepada perorangan atau individu yang memiliki sifat atau kriteria tertentu sesuai tujuan penyerangan tersebut. Beberapa contoh kejahatan ini antara lain:

1) Pornografi

Kegiatan yang dilakukan dengan membuat, memasang, mendistrubusikan, dan menyebarkan material yang berbau pornografi, cabul serta mengekspos hal-hal yang tidak pantas.

2) Cyberstalking

Kegiatan yang dilakukan untuk mengganggu atau melecehkan seseorang dengan memanfaatkan computer, misalnya dengan menggunakan email yang dilakukan secara

berulang-ulang seperti halnya terror di dunia cyber, gangguan tersebut bisa saja berbau seksual, religius dan lain sebagainya.

3) Cyber-Tresspass

Kegiatan yang dilakukan melanggar area privasi orang lain, misalnya web hecking, breaking ke PC, probing, port scanning dan lain sebagaiya.

4) Cybercrime menyerang hak milik (Againts Property)

Cybercrime yang dilakukan untuk mengganggu atau menyerang hak milik orang lain. Beberapa contoh kejahatan jenis ini misalnya pengaksesan computer secara tidak sah melalui dunia cyber, pemilikan iformasi elektronik secara tidak sah/pencurian informasi, carding, cybersquatting, hijacking, data forgery dan segala kegiatan yang bersifat merugikan hak milik orang lain.

5) Cybercrime menyerang pemerintah (Againts Government)

Dilakukan dengan tujuan khusus penyerangan terhadap pemerintah. Kegiatan tersebut misalnya cyber terrorism sebagai tindakan yang mengancam pemerintah termasuk juga cracking ke situs resmi pemerintah atau situs militer. (Abidin, 2015:4-5).

4. Faktor Pendorong Terjadinya Cybercrime

Setiap tindakan kriminal atau kejahatan pastinya ada factor penyebabnya. Beberapa faktor yang menyebabkan kejahatan komputer (cybercrime) adalah:

a. Akses internet yang tidak terbatas. Saling terhubungnya antara jaringan yang satu dengan jaringan yang lain memudahkan pelaku kejahatan untuk melakukan aksinya.
b. Kelalaian penggunaan computer.
c. Mudah dilakukan dengan resiko keamanan yang kecil dan tidak diperlukan peralatan yang super modern. Walaupun kejahatan komputer mudah untuk dilakukan tetapi akan sangat sulit untuk melacaknya, sehingga ini mendorong para pelaku kejahatan untuk melakukan hal ini.
d. Para pelaku merupakan orang yang pada umumya cerdas, mempuyai rasa ingin tahu besar, dan fanatik akan teknologi computer. Pengetahuan pelaku kejahatan komputer tentang cara kerja sebuah komputer jauh di atas operator komputer.
e. Kurangnya perhatian masyarakat dan penegak hukum.
f. Sistem keamanan jaringan yang lemah.
g. Cybercrime dipandang sebagai produk ekonomi. (Eliasta, 2016:5).

5. Contoh Kasus Cybercrime di Indonesia

a. Pencurian dan penggunaan account internet milik orang lain.

Pencurian account ini berbeda dengan pencurian secara fisik karena pencurian dilakukan cukup dengan menangkap “user_id” dan “password” saja. Tujuan dari pencurian itu hanya untuk mencuri informasi saja. Pihak yang kecurian tidak akan merasakan kehilangan. Namun, efeknya akan terasa jika informasi tersebut digunakan oleh pihak yang tidak bertanggung jawab. Hal tersebut akan membuat semua beban biaya penggunaan account oleh si pencuri dibebankan kepada si pemilik account yang sebenarnya. Kasus ini banyak terjadi di ISP (Internet Service Provider). Kasus yang pernah diangkat adalah penggunaan account curian yang dilakukan oleh dua Warnet di Bandung.

Kasus lainnya: Dunia perbankan dalam negeri juga digegerkan dengan ulah Steven Haryanto, yang membuat situs asli tetapi palsu layanan perbankan lewat Internet BCA. Lewat

situs-situs "Aspal", jika nasabah salah mengetik situs asli dan masuk ke situs-situs tersebut, identitas pengguna (user ID) dan nomor identifikasi personal (PIN) dapat ditangkap. Tercatat 130 nasabah tercuri data-datanya, namun menurut pengakuan Steven pada situs Master Web Indonesia, tujuannya membuat situs plesetan adalah agar publik memberi perhatian pada kesalahan pengetikan alamat situs, bukan mengeruk keuntungan.

Persoalan tidak berhenti di situ. Pasalnya, banyak nasabah BCA yang merasa kehilangan uangnya untuk transaksi yang tidak dilakukan. Ditengarai, para nasabah itu kebobolan karena menggunakan fasilitas Internet banking lewat situs atau alamat lain yang membuka link ke Klik BCA, sehingga memungkinkan user ID dan PIN pengguna diketahui. Namun ada juga modus lainnya, seperti tipuan nasabah telah memenangkan undian dan harus mentransfer sejumlah dana lewat Internet dengan cara yang telah ditentukan penipu ataupun saat kartu ATM masih di dalam mesin tiba-tiba ada orang lain menekan tombol yang ternyata mendaftarkan nasabah ikut fasilitas Internet banking, sehingga user ID dan password diketahui orang tersebut.

Modus kejahatan ini adalah penyalahgunaan user_ID dan password oleh seorang yang tidak punya hak. Motif kegiatan dari kasus ini termasuk ke dalam cybercrime sebagai kejahatan "abu-abu". Kasus cybercrime ini merupakan jenis cybercrime uncauthorized access dan hacking-cracking. Sasaran dari kasus ini termasuk ke dalam jenis cybercrime menyerang hak milik (against property). Sasaran dari kasus kejahatan ini adalah cybercrime menyerang pribadi (against person).

Beberapa solusi untuk mencegah kasus di atas adalah:

1) Penggunaan enkripsi untuk meningkatkan keamanan.

Penggunaan enkripsi yaitu dengan mengubah data-data yang dikirimkan sehingga tidak mudah disadap (plaintext diubah menjadi chipertext). Untuk meningkatkan keamanan authentication (pengunaan user_id dan password), penggunaan enkripsi dilakukan pada tingkat socket. Hal ini akan membuat orang tidak bias menyadap data atau transaksi yang dikirimkan dari/ke server WWW. Salah satu mekanisme yang popular adalah dengan menggunakan Secure Socket Layer (SSL) yang mulanya dikembangkan oleh Nerscape. Selain server WWW dari netscape, server WWW dari Apache juga dapat dipakai karena dapat dikonfigurasikan agar memiliki fasilitas SSL dengan menambahkan software tambahan, sperti open SSL.

2) Penggunaan Firewall

Tujuan utama dari firewall adalah untuk menjaga agar akses dari orang tidak berwenang tidak dapat dilakukan. Program ini merupakan perangkat yang diletakkan antara internet dengan jaringan internal. Informasi yang keluar dan masuk harus melalui atau melewati firewall. Firewall bekerja dengan mengamati paker Intenet Protocol (IP) yang melewatinya.

3) Perlunya CyberLaw

Cyberlaw merupakan istilah hukum yang terkait dengan pemanfaatan TI. Istilah lain adalah hukum TI (Low of IT), Hukum Dunia Maya (Virtual World Law) dan hukum Mayantara.

• Melakukan pengamanan sistem melalui jaringan dengan melakukan pengaman FTP, SMTP, Telnet dan pengaman Web Server

b. Kejahatan kartu kredit yang dilakukan lewat transaksi online di Yogyakarta

Polda DI Yogyakarta menangkap lima carder dan mengamankan barang bukti bernilai puluhan juta, yang didapat dari merchant luar negeri. Begitu juga dengan yang dilakukan mahasiswa sebuah perguruan tinggi di Bandung, Buy alias Sam. Akibat perbuatannya selama setahun, beberapa pihak di Jerman dirugikan sebesar 15.000 DM (sekitar Rp 70 juta).
Para carder beberapa waktu lalu juga menyadap data kartu kredit dari dua outlet pusat perbelanjaan yang cukup terkenal. Caranya, saat kasir menggesek kartu pada waktu pembayaran, pada saat data berjalan ke bank-bank tertentu itulah data dicuri. Akibatnya, banyak laporan pemegang kartu kredit yang mendapatkan tagihan terhadap transaksi yang tidak pernah dilakukannya.
Modus kejahatan ini adalah penyalahgunaan kartu kredit oleh orang yang tidak berhak. Motif kegiatan dari kasus ini termasuk ke dalam cybercrime sebagai tindakan murni kejahatan. Hal ini dikarenakan si penyerang dengan sengaja menggunakan kartu kredit milik orang lain. Kasus cybercrime ini merupakan jenis carding. Sasaran dari kasus ini termasuk ke dalam jenis cybercrime menyerang hak milik (against property). Sasaran dari kasus kejahatan ini adalah cybercrime menyerang pribadi (against person).

Beberapa solusi untuk mencegah kasus di atas adalah:

1) Perlu adanya cyberlaw: Cybercrime belum sepenuhnya terakomodasi dalam peraturan / Undang-undang yang ada, penting adanya perangkat hukum khusus mengingat karakter dari cybercrime ini berbeda dari kejahatan konvensional.
2) Perlunya Dukungan Lembaga Khusus: Lembaga ini diperlukan untuk memberikan informasi tentang cybercrime, melakukan sosialisasi secara intensif kepada masyarakat, serta melakukan riset-riset khusus dalam penanggulangan cybercrime.
3) Penggunaan enkripsi untuk meningkatkan keamanan. Penggunaan enkripsi yaitu dengan mengubah data-data yang dikirimkan sehingga tidak mudah disadap (plaintext diubah menjadi chipertext). Untuk meningkatkan keamanan authentication (pengunaan user_id dan password), penggunaan enkripsi dilakukan pada tingkat socket. (Nawayatamara, 2018).

c. Kasus Pornografi Ariel

Pada tahun 2008 telah terjadi kasus video porno Ariel “Peter Pan” dengan Luna Maya dan Cut Tari. Video tersebut diunggah di internet oleh seorang yang berinisial ‘RJ’. Pada kasus tersebut modus sasaran serangannya ditujukan kepada preorangan atau individu yang memiliki sifat atau kriteria tertentu sesuai tujuan penyerangan tersebut. Pengunggah dan orang terkait dalam video tersebut pun ikut diseret pasal-pasal sebagai berikut; Pasal 29 UURI No. 44 tahun 2008 tentang pronografi, Pasal 56 dengan hukuman minimal 6 bulan sampai 12 tahun. Atau denda dengan minimal Rp. 250 juta hingga Rp. 6 miliar. Dan atau Pasal 282 ayat 1 KUHP.

d. Kasus Prita Mulyasari

Prita Mulyasari digugat dan dilaporkan ke polisi oleh Rumah Sakit Omni Internasional atas tudahan pencemaran nama baik lewat millis. Kasus ini bermula dari surat elektronik yang dibuat Prita Mulyasari yang berisi pengalamannya saat dirawat di unit gawat darurat Omni Internasional. Prita Mulyasari dikenakan pasal 27 UU ITE ancaman hukuman 6 tahun penjara dan denda Rp. 1 miliar.

D. KESIMPULAN

Berdasarkan apa yang telah dibahas dalam makalah di atas, maka dapat disimpulkan cybercrime adalah perbuatan melawan hukum yang dilakukan dengan memakai jaringan komputer sebagai sarana/alat atau komputer sebagai objek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain. Kejahatan ini muncul akibat dampak negatif dari perkembangan aplikasi internet. Motif melakukan kejahatan ini di samping karena uang juga iseng. Kejahatan ini juga muncul karena ketidakmampuan hukum termasuk aparat dalam menjangkaunya. Kejahatan ini bersifat maya dimana pelaku tidak tampak secara fisik. Begitu hebatnya kejahatan ini bahkan dapat meresahkan dunia internasional.

Cybercrime sendiri sebagai kejahatan yang muncul sebagai akibat adanya komunitas dunia maya di internet, memiliki karakteristik yang khas dibandingkan kejahatan konvensional, karakteristik unik dari kejahatan di dunia maya tersebut anatara lain menyangkut lima berikut: 1) ruang lingkup, 2) sifat kejahatan, 3) pelaku kejahatan, 4) modus kejahatan, dan 5) jenis kerugian yang ditimbulkan. Sedangkan jenis-jenis kejahatan cybercrime bisa dibedakan berdasarkan; 1) modus atau jenis aktifitasnya, contohnya: Anauthorized Acces, Illegal Contens, Penyebaran virus secara sengaja, Data Forgery, Cyber Espionage, Sabotage and Extortion, Cyberstalking, Carding, Hacking dan Cracker, Cybersquatting and Typosquatting, Hijacking dan Cyber Terosrism; 2) berdasarkan motif kegiatannya yaitu: Cybercrime sebagai tindak kejahatan murni dan Cybercrime sebagai tindak kejahatan abu-abu, 3) berdasarkan sasaran kejahatan diantaranya: Cybercrime yang menyerang individu (Againts Person), Cybercrime menyerang hak milik (Againts Property), Cybercrime menyerang pemerintah (Againts Government).

Beberapa faktor yang menyebabkan kejahatan komputer (cybercrime) adalah: 1) Akses internet yang tidak terbatas. Saling terhubungnya antara jaringan yang satu dengan jaringan yang lain memudahkan pelaku kejahatan untuk melakukan aksinya, 2) Kelalaian penggunaan computer, 3) Mudah dilakukan dengan resiko keamanan yang kecil dan tidak diperlukan peralatan yang super modern, 4) Para pelaku merupakan orang yang pada umumya cerdas, mempuyai rasa ingin tahu besar, dan fanatik akan teknologi komputer, 5) Kurangnya perhatian masyarakat dan penegak hokum, 6) Sistem keamanan jaringan yang lemah, 7) Cybercrime dipandang sebagai produk ekonomi..

E. DAFTAR PUSTAKA

Andysah Putera Utama Siahaan, Pelanggaran Cybercrime Dan Kekuatan Yurisdiksi Di Indonesia, *Jurnal Teknik Dan Informatika*, Vol.5 No.1 Januari 2018, https://jurnal.pancabudi.ac.id/index.php/Juti/article/view/82

Dikdik M Arief Mansur dan Elisatris Gultom, *Cyber Law Aspek Hukum Teknologi Informasi*, (Bandung: Refika Aditama, 2009)

Dista Amalia Arifah, Kasus *Cybercrime* Di Indonesia, *Jurnal Bisnis dan Ekonomi* (JBE), 2 Vol. 18, No. 2, 2011, https://www.unisbank.ac.id/ojs/index.php/fe3/article/view/2099.

Dodo Zaenal Abidin, Kejahatan Dalam Teknologi Informasi dan Komunikasi, J*urnal Ilmiah Media Procesor,* Vol.10, No.2. 2015, https://ejournal.unama.ac.id/index.php/

Eliasta Ketaren, Cybercrime, Cyber Space dan Cyber Law, *Jurnal Times*, Vol. v No.2, 2016, http://download.garuda.kemdikbud.go.id/

Lita Sari Marita, Cyber Crime Dan Penerapan Cyber Law Dalam Pemberantasan Cyber Law Di Indonesia, *Cakralawa*: Jurnal Humaniora Bina Sarana Informatika, Vol.15. No.2, 2015, https://scholar.google.co.id/citations?user=R-kzzIkAAAAJ&hl=id

M.E. Fuady, *Cybercrime* Fenomena Kejahatan Melalui Internet di Indonesia, *Jurnal Mediator*, Vol.6, No.2, 2005, https://ejournal.unisba.ac.idindex.

Nawayatamara, *Pengertian Cybercrime, Contoh Kasus Cyber Crime Dan Penyelesaiannya*, https://eptik9.wordpress.com/2018/05/22/contoh-kasus-cyber-crime-dan penyelesaiannya/

Nazarudin Tianotak, Urgensi Cyberlaw Di Indonesia Dalam Rangka Penangan Cybercrime Disektor Perbankan, *Jurnal Sasi*, Vol. 17 No. 4 , 2011, https://ejournal.unpatti.ac.id/

Nunuk Sulisrudatin, Analisa Kasus Cybercrime Bidang Perbankan Berupa Modus Pencurian Data Kartu Kredit, *Jurnal Ilmiah Hukum Dirgantara*, 2 Volume 9 No. 1, September 2018, https://journal.universitassuryadarma.ac.id/index.php/jihd/article/

Widodo, *Sistem Pemidanaan Dalam Cyber Crime Alternatif Ancaman Pidana Kerja Sosial dan Pidana Pengawasan Bagi Pelaku Cyber crime*, (Yogyakarta: Laksbang Mediatama, 2009)