CYBER CRIME DAN PENERAPAN CYBER LAW DALAM PEMBERANTASAN CYBER LAW DI INDONESIA

Lita Sari Marita
Dosen Tetap AMIK BSI Jakarta
Jl. Kramat Raya No 18Jakarta Pusat
Email : lita.lsm@bsi.ac.id

Abstract

Using of internet connection is not a new things nowday, every one can acces internet whereever, whenever, anytime anywhere they need or want. Is not dificult to find hotspot area, so nothing more can's stop people to knowing and connecting with other people in all country.

Considering of using internet causing negatif affcet, such as cyber cryme, when there is a cybercrime then we know we need cyber law.to knowing what is cyber crime and what is cybercrime this is a explaination to be known.

This paper made for us to know deeply about cyber crime and cyber law, consist of definition, sample and conclution, hoply with reading this people may understanding what is cyber crime and cyber law.

Keyword : internet, cybercrime, cyber law

I. PENDAHULUAN

Perkembangan Teknologi Informasi dan Komunikasi terus berkembang dengan pesatnya, sekarang ini menggunakan Teknologi Informasi dan Komunikasi bisa dilakukan secara *mobile*, kegiatan-kegiatan yang biasanya dilakukan di dunia nyata sekarang ini berpindah dengan penggunaan gadget transaksi seperti perbankan dan berkirim surat beralih menjadi kegiatan dunia maya. Transaksi berpindah dengan menggunakan i-Pad, *Smartphone, handphone, laptop*. Kita tidak lagi mengalami kesulitan untuk mengakses informasi dari seluruh penjuru dunia selain karena banyak perangkat mobile yang memang sudah didukung oleh Teknologi Informasi dan Komunikasi juga karena banyak tersedianya hotspot gratis dibanyak tempat.

Perkembangan Teknologi Informasi dan Komunikasi yang cukup pesat ini juga diikuti dengan maraknya penyalahgunaan Teknologi Informasi dan Komunikasi, sehingga telah menjadi isu yang sangat meresahkan yaitu terjadinya kejahatan yang dilakukan di dunia maya atau sekarang ini dikenal dengan istilah *cybercrime*. Telah banyak kasus kejahatan yang terjadi didunia maya ini yang tentu saja merugikan dan memberikan dampak yang negatif, *cybercrime*

ini tidak hanya meliputi Indonesia tetapi juga global.

Beberapa kasus kejahatan yang terjadi dipicu oleh maraknya pengunaan email, ebanking, ecommerce di Indonesia. Semakin maraknya kasus *cybercrime* yang terjadi terutama di Indonesia telah menarik perhatian pemerintah untuk segera memiliki undang-undang yang bisa digunakan untuk bisa menjerat para pelaku kejahatan di dunia maya. Pemerintah Indonesia Sendiri telah mengesahkan undang-undang *cybercrime* yaitu cyber law kedalam undang-undang ITE no 11 tahun 2008, diharapkan dengan adanya undang-undang ITE no 11 tahun 2008 ini bisa mengatasi, meminimalisir, membuat jera pelaku kejahatan di dunia maya.

II. Kajian Literatur

Setiap kali membahas suatu hal adalah penting untuk mengetahui dan memahami apa yang dibicarakan, hal ini dimaksudkan agar bisa lebih memahami hal yang sedang dibicarakan sehingga tidak terlihat bodoh.

Berbicara tentang *cybercrime* berarti harus tahu dulu apa pengertian dari *cybercrime.*

Pengertian *cybercrime*

Cybercrime menurut Menurut The U.S. Dept.of Justice, computer crime adalah indakan ilegal apapun yg memerlukan pengetahuan tentang teknologi komputer untuk perbuatan jahat, penyidikan, atau penuntutan.

Menurut Andi Hamzah (1989) *cybercrime* adalah kejahatan dibidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara ilegal.

Cybercrime adalah tindak kriminal yang dilakukan dengan menggunakan teknologi komputer sebagai alat kejahatan utama. Merupakan kejahatan yang memanfaatkan perkembangan teknologi komputer khususnya internet.

Menurut Freddy haris, *cybercrime* merupakan suatu tindak pidana dengan karakteristik-karakteristik sebagai berikut :

1. *Unauthorized access*(dengan maksud untuk memfasilitasi kejahatan).
2. *Unauthorized alteration or destruction of data.*
3. Mengganggu atau merusak operasi komputer
4. Mencegah atau menghambat akses pada komputer.

Dalam undang-undang ITE no 11 tahun 2008 sendiri mendefinisakan *cybercrimes* atau kejahatan elektronik sebagai :

Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, electronic data interchange (EDI), surat elektronik (electronic mail), telegram, teleks, telecopy atau sejenisnya, huruf,

tanda, angka, Kode Akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.

2. Transaksi Elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan Komputer, jaringan Komputer, dan/atau media elektronik lainnya.

3. Teknologi Informasi adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan/atau menyebarkan informasi.

4. Dokumen Elektronik adalah setiap Informasi Elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui Komputer atau Sistem Elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.

5. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik.

Meskipun belum ada kesepahaman mengenai definisi kejahatan komputer atau kejahatan dunia maya(*cybercrime)* namun ada kesamaan dalam mendefinisikannya yaitu upaya memasuki dan atau menggunakan fasilitas komputer atau jaringan komputer tanpa ijin dan dengan melawan hukum dengan atau tanpa menyebabkan perubahan dan atau kerusakan pada fasilitas komputer yang dimasuki atau digunakan tersebut.

Cybercrime memiliki karakteristik sebagai berikut :

1. Ruang lingkup kejahatan
2. Sifat kejahatan
3. Pelaku kejahatan
4. Modus kejahatan
5. Jenis kerugian yang ditimbulkan.

Berdasarkan karakteristik diatas , untuk mempermudah penanganannya maka *Cybercrime* diklasifikasikan menjadi :

1. Cyberpiracy, yaitu penggunaan teknologi komputer untuk mencetak ulang software atau informasi, lalu mendistribusikan informasi atau software tersebut lewat teknologi komputer.
2. Cybertresspass, yaitu penggunaan teknologi komputer untuk meningkatkan akses pada sistem komputer suatu organisasi atau indifidu.
3. Cybervandalism, yaitu penggunaan teknologi komputer

untuk membuat program yang mengganggu proses transmisi elektronik dan menghancurkan data dikomputer.

Pada dasarnya *Cybercrime* meliputi semua tindak pidana yang berkenaan dengan informasi, sistem informasi itu sendiri, serta sistem komunikasi yang merupakan sarana untuk penyampaian atau pertukaran informasi itu kepada pihak lainnya.

Jenis-jenis kejahatan yang termasuk kedalam *cybecrime* adalah :

1. *Cyber terorism*
   National Police Agency of Japan(NPA) mendefinisikan *Cyber terorism* sebagai electronic attacks through computer networkings againstcritical infrastruckctures that have potential critical effects and economic activities of that nation.
2. *Cyber-pornography*
   Penyebar luasan *obscene* materials termasuk pornography, indecent *exposure* dan *child pornography*.
3. *Cyber-harrassment*
   Pelecehan seksual melalui email, websites atau chat program
4. *Cyber-stalking crimes of stalking* melalui penggunaan komputer dan internet.
5. *Hacking*
   Penggunaan programming abilities dengan maksud yang bertentangan dengan hukum.
6. Carding(credit card fraud)
   Melibatkan berbagai macam aktifitas yang melibatkan kartu kredit. Terjadi ketika seseorang yang bukan pemilik kartu kredit menggunakan kartu kredit tersebut melawan hukum.

Cyber law

Dimana ada kejahatan maka disitulah hukum berpijak, setiap kejahatan harus ada hukuman yang diberikan. Kejahatan selalu dikaitkan dengan hukuman yang akan dijatuhkan terhadap kejahatan yang dilakukan, jika dari awal membahas tentang hukum maka pembahasan selanjutnya adalah tentang hukum yang diberlakukan terhadap kejahatan dunia maya.

Kejahatan dunia maya bukan hanya kejahatan yang telah terjadi di indonesia, *cyber crime* adalah kejahatan yang telah mendunia, bahkan sudah melintas negara, melintas negara karena dampak kejahatan dilakukan oleh seseorang disebuah negara ternyata berdampak dinegara lain, hal ini disebabkan *cyber crime* adalah melintas waktu dan ruang.

Di Indonesia sendiri tampaknya belum ada satu istilah yang disepakati atau paling tidak hanya sekedar terjemahan atas terminologi ”cyber law”. Sampai saat ini ada beberapa istilah yang dimaksudkan sebagai terjemahan dari ”cyber law”, misalnya, Hukum Sistem Informasi, Hukum Informasi, dan Hukum

Telematika (Telekomunikasi dan Informatika).

Pembahasan mengenai ruang lingkup ”cyber law” dimaksudkan sebagai inventarisasi atas persoalan-persoalan atau aspek-aspek hukum yang diperkirakan berkaitan dengan pemanfaatan Internet. Secara garis besar ruang lingkup ”cyber law” ini berkaitan dengan persoalan-persoalan atau ’ aspek hukum dari *E-Commerce, Trademark/Domain Names, Privacy and Security on the Internet, Copyright, Defamation, Content Regulation, Disptle Settlement*, dan sebagainya.

Electronic Commerce dan *Domain Name* adalah ruang lingkup atau area yang harus dicover oleh *cyberlaw*. Ruang lingkup cyberlaw ini akan terus berkembang seiring dengan perkembangan yang terjadi pada pemanfaatan Internet dikemudian hari**.**

Hampir seluruh Negara di dunia sudah memikirkan dan mengantisipasi bagaimana cara mengatasi kejahatan ini, karena kejahatan dunia maya tidak baru terjadi sekarang ini, tetapi sudah terjadi tepatnya setelah adanya internet

Sebelum adanya undang-undang ITE tahun 2008 yang merupakan satu-satunya udang-undang yang ada di Indonesia untuk menanggulangin masalah cyber crime maka selama ini Indonesia menggunakan KUHP (Kitab Undang-undang Hukum Pidana)didalam mengatasi masalah cyber crime yang terjadi. Tetapi saat ini, sejak dari tahun 2008 setelah disyahkannya undang-undang ITE tahun 2008 maka hukum di Indonesia mulai memberlakukan penggunaan undang-undang tersebut disetiap terjadi kejahatan dunia maya.

Sebenarnya Indonesia sudah tertingal jauh menangani masalah yang berkaitan dengan cyber crime, tertinggal jauh dalam menyiapkan perangkat hukum dalam mengatasi masalah cyber crime. Negara-negara tetangga seperti Malaysia, singapura, brunai dan Thailand sudah lama memiliki kebijakan dan udang-undang untuk mengatasi masalah kejahatan yang terjadi di dunia maya.

Beberapa hukum yang digunakan dinegara-negara yang berkaitan dengan penanggulangan masalah cyber crime bisa dilihat sebagai berikut :

Amerika merupakan Negara yang paling dahulu memiliki perangkat hukum yang digunakan untuk mengatasi masalah cyber crime.

1. USA
   Di USA cyber law yang mengatur transaksi elektronik dikenal dengan Uniform electronic Transaction(UETA), adalah salah satu dari beberapa peraturan perundang-undangan Amerika Serikat yang diusulkan oleh National Conference of commissioners on Uniform State Laws
2. Singapore

Memiliki cayberlaw yaitu The electronic Act(akta Elektronik)1998, electronic Communication Privacy Act(Akta Privasi Komunikasi Elektronik)1996. The electronic Transactions Act telah ada sejak juli 1998 untuk menciptakan kerangka yang sah tentang undang-undang untuk transaksi perdagangan elektronik Singapore yang memungkinkan bagi mentri komunikasi informasi dan kesenian untuk membuat peraturan mengenai perijinan dan peraturan otoritas sertifikasi di singapora.

III. KAJIAN LITERATUR

Metode penelitian yang digunakan dalam penulisan ini adalah studi pustaka, yaitu studi dokumen yang kegiatannya mengumpulkan data tentang penelitian yang dibahas dari sejumlah sumber seperti buku, surat kabar, jurnal penelitian, literatur dan penelitian. Buku, jurnal dan literatur dimaksudkan untuk memperoleh teori dan pengetahuan yang dapat menunjang penelitian.

IV. PEMBAHASAN

Sekalipun teknologi informasi memberikan banyak kemudahan manusia, tetapi kemajuan ini pun secara bersamaan menimbulkan berbagai permasalahan yang tidak mudah ditemukan jalan keluarnya. Salah satu masalah yang muncul akibat akibat perkembangan teknologi informasi adalah lahirnya kejahatan-kejahatan yang sifatnya baru, khususnya mempergunakan internet sebagai alat bantunya. Lazim dikenal dengan sebutan kejahatan dalam dunia maya.

Kejahatan dunia maya sudah selayaknya menjadi perhatian khusus diseluruh dunia, terutama bagi Negara-negara yang sudah menjadikan teknologi informasi sebagai bagian besar dikehidupan mereka. Kenapa seperti ini, karena kejahatan ini bisa menjadi ancaman yang sangat serius.

Motif Cyber crime ada dua jenis yaitu :

1. Menyerang individu, yaitu kejahatan yang menyerang individu seseorang dengan motif dendam atau iseng yang bertujuan untuk merusak nama baik, mencoba ataupun mempermainkan seseorang utnuk mendapatkan kepuasan pribadi, contohnya : pornografi dan cyberstalking
2. Cyber crime yang menyerang hak cipta atau hak milik, yaitu kejahatan yang dilakukan terhadap hasil karya orang lain dengan motif menggandakan, memasarkan, mengubah yang bertujuan untuk kepentingan pribadi atau umum ataupun demi materi maupun nonmateri.
3. Cyber crime yang menyerang pemerintah, yaitu kejahatan yang dilakukan dengan pemerintah sebagai objek dengan motif melakukan terror, membajak ataupun merusak keamanan suatu pemerintahan yang bertujuan

untuk mengacaukan system pemerintaha, atau menghancurkan suatu Negara.

Sedangkan berdasarkan motifnya maka cyber crime terbagi menjadi dua,

1. Cyber crime sebagai tindak kejahatan murni, dimana orang yang melakukan kejahatan dilakukan secara disengaja, dimana orang tersebut seara sengaja dan terencana utnuk melakukan pengerusakkan, pencuria, tindakan anarkis terhadap suatu system informasi ataupun system computer.
2. Cyber crime sebagai tindak kejahatan abu-abu, dimana kejahatan ini tidak jelas antara kejahatan criminal atau bukan, karena dia melakukan pembobolan tetapi tidak merusak, mencuri ataupun melakukan perbuatan anarkis terhadap system informasi ataupun system computer. Ini yang biasa dilakukan oleh para hacker, dimana seorang hacker biasanya memasuki system jaringan ataupun system computer dengan tujuan untuk mengetahui apakah system tersebut aman tau tidak, tidak ada yang dirusak oleh para hacker, mereka murni menguji system yang nantinya akan bisa membuat perbaikan bagi system yang di hack.

Berdasarkan klasifikasi dan jenisnya maka beberapa klasifikasi beserta jenisnya adalah sebagai berikut :

1. Cyberpiracy, yaitu penggunaan teknologi komputer untuk mencetak ulang software atau informasi, lalu mendistribusikan informasi atau software tersebut lewat teknologi komputer. Jenisnya ada :piracy Piracy sekarang ini marak terjadi di Indonesia, yang sangat terlihat adalah pembajakan software, film lagu, bisa kita lihat betapa banyak dan mudahnya kita bisa membeli cd software dan cd lagu maupun film bajakan, di tempat-tempat pembelanjaan, semua bebas seolah tidak ada yang melarang, walaupun pemerintah Indonesia sendiri telah dengan jelas melarangnya melalui undang-undang hak cipta.
2. Cybertresspass, yaitu penggunaan teknologi komputer untuk meningkatkan akses pada sistem komputer suatu organisasi atau indifidu. Yang termasuk kedalam klasifikasi ini adalah : unauthorized access to computer system and service, illegal contents, cyber espionage, carding
3. Cybervandalism, yaitu penggunaan teknologi komputer untuk membuat program yang mengganggu proses transmisi elektronik dan menghancurkan. Yang termasuk kedalam klasifikasi

ini adalah : cyber sabotage and extortion, cracking

Kasus cybercrime yang paling banyak terjadi di Indonesia adalah berupa kejahatan menggunakan internet untuk memesan barang dari perusahaan asing diluar negri dengan menggunakan karrtu kredit yang dipalsukan. Kasus yang terjadi pada tahun 2001 yaitu sebanyak 23 kasus dengan jumlah tersangka sebanyak 17 orang dan pada tahun 2002(sampai dengan agustus 2002)sebanyak 116 kasus dengan jumlah tersangka sebanyak 124 orang. Kondisi ini tentunya akan merusak citra Indonesia dimata dunia internasional karena Indonesia dianggap sebagai sarang pemalsu kartu kredit.

Di Indonesia sendiri cyber crime sudah begitu maraknya, walau memang tidak ter *blow up* dimedia, bahkan patut diacungi jempol. Kenyataan di dunia nyata yang sering mengatakan dunia kita adalah dunia terbelakang, namun pengecualian untuk hal yang satu ini, karena prestasi gemilang diraih oleh para hacker, cracker dan carder local.

Beberapa kasus yang terjadi baik di Indonesia atau pelakunya adalah orang Indonesia maupun dibeberapa Negara lainnya.

1. Pada tahun 2000 seorang hacker asal indoensia diadili dinegri asing yaitu singapura. Adalah wenas yang menggunakan nama maya hc didakwa melakukan aktifitas illegal mterhadap server dua perusahaan di Singapura baik yang dilakukannya sewaktu masih di Australia maupun setelah mendarat di Singapura. Sampai akhir persidangan belum dapat diambil keputusan mengenai kasus tersebut, baik hakim, penuntu umum maupun pengacara terdakwa sama-sama membutuhkan waktu tambahan untuk mempelajari kasus unik tersebut, karena pengadilan rendah singapaura ini baru pertama kali menghadapi kasus cybercrime yang melibatkan warga Negara asing.
2. Adalah Petrus Sangkar pemuda berusia 22 tahun bersama tiga rekannya sesama cracker berhasil membobol lewat internet, Mereka dituduh membeli barang melalui internet secara tidak sah. Pada bulan maret dan April 2001 berhasil membobol kartu kredit orang lain senilai Rp. 5 Milyar, pada akhirnya ditangkap kepolisian Yogyakarta. Kasus pembobolan ini terungkap setelah ada surat dari Departemen Luar negri dan kepolisian internasional. Menurut surat itu ada nama-nama pembeli barang dikirim, kartu kredit tidak diakui oleh pemiliknya, kemudian polisi melakukan pelacakan kebeberapa perusahaan jasa angkutan barang di

Yogyakarta, dan akhirnya pelaku ditangkap.

3. Monica Gate, adalah salah satu kasus yang menghebohkan dunia karena melibatkan priseden Amerika menjabat saat itu Bill Clinton, terungkapnya affair sang presiden dengan seorang wanita muda bernama monica, terungkap melalui rekaman

No	Perkara	Salinan Putusan	Pasal yang dikenakan
1	Putusan Pengadilan Jakarta Pusat taun 1998 telah menerapkan pasal pencurian dalam kasus unauthorized Transfer dana BNI 46 Ney York Agency	Salinan Putusan Pengadilan Negri Jakarta Pusat No. 135/X/Pid.B/PN.jkt.Pst tanggal 11 Maret 1988 a.n Seno Adjie	Pasal 363 KUHP : ayat 4 berbunyi Pencurian dilakukan oleh dua orang atau lebih dengan bersekutu
2	Putusan Pengadilan Jakarta Barat tahun 1989 telh menerapkan pasal pencurian dalam kasus"data diddling"bank Bali Cabang	Salinan Putusan Pengadilan Negri Jakarta Barat No. 1050/Pid.S/1989/PN.jkt.Brt tanggal 20 November 1989 a.n	Pasal 362 KUHP : Barang Siapa yang mengambil suatu barang, yang selutuhnya atau sebagian kepunyaan orang lain, dengan maksud untuk memilikinya secara melawan hukum diancam karena pencurian dengan pidana penjara maksimum lima tahun
3	Putusan Pengadilan Negri Sleman tahun 2002 telah menerapkan pasal tentang penipuan dalam kasus carding	Salinan Putusan Pengadilan Negri Sleman No. 94/Pid.B/2002/PN.slmn a.n Petrus Pangkur alias Boni Dioboko bok	Pasal 378 KUHP : Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain dengan melawan hukum, dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat ataupun dengan rangkaian kebohon

			gan mengger akkan orang lain untuk menyera hkan sesuatu benda kepadan ya, atau supaya memberi hutang maupun menghap uskan piutang, diancam karena penipuan dengan pidana penjara paling lama 4 tahun
4	Putusan Pengadila n Negri Semarang tahun 2003 telah menerapka n pasal tentang pencurian dalam kasus carding	Salinan Putusan Pengadil an Negri Semaran g No. 504/Pid. B/2003/P N. Smg	Pasal 362 KUHP: Barang siapa yang mengam bil suatu barang, yang seluruhn ya atau sebagian kepunya an orang lain, dengan maksud untuk memiliki nya secara melawan hukum diancam karena pencuria n dengan pidana penjara maksimu m lima tahun

Sumber : Analisis Penanganan Carding dan Perlindungan Nasabah dalam Kaitannya dengan Undang-Undang Informasi dan Transaksi Elektronik no.11 Tahun 2008 Leo T. Panjaitan *Teknik Elektro, Universitas Mercu Buana, Jakarta*

Melihat beberapa kasus diatas maka dapat disimpulkanm kasus yang banyak terjadi di Indonesia adalah cyber crime berupa carding, atau penipuan kartu kredit. Kasus-kasus diatas merupakan kasus lama yang terjadi, sehingga masih menggunakan KUHP didalam penanganannya, tetapi banyak kalangan menilai KUHP tidaklah tepat jika dugunakan untuk menjerat para pelaku kejahatan cyber crime. Maka sejak tahun 2008 mulai diberlakukan Undang Undang ITE tahun 2008 untuk menjerat para pelaku kejahatan di dunia maya. Walaupun belum juga semua kejahatan dunia maya bisa dijerat dengan Undang undang ITE tahun 2008, tapi untuk sementara ini undang-undang tersebut dianggap cukup mewakili.

Kasus terbaru yang sedang terjadi saat ini adalah kasus farhat abas yang dituduhkan oleh beberapa orang telah melakukan pencemaran nama baik seseorang melalui akun twitter nya, farhat dituduhkan telah menghina ras tertentu dan kepada orang tertentu dalam akun twitternya, karena pencemaran dilakukan di

media social yang merupakan media terjadinya cyber crime maka kasus ini dianggap sebagai kasus cyber crime dan akan dijerat undang-undang ITE 2008

Jika jenis-jenis cybercrime dikelompokkan kedalam pasal-pasal undang-udang ITE tahun 2008 maka akan terlihat seperti dibawah ini

Pasal 27

(1) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan.

(2) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian.

(3) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik.

(4) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman.

Cyber crime yang dimaksud dalam pasal 27 diatas adalah pencemaran nama baik di media social seperti kasus farhat abas baru-baru ini, perjudian online

Pasal 28

(1) Setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik.
(2) Setiap Orang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan (SARA).

Cyber crime yang dimaksud dalam pasal 28 diatas adalah pencurian kartu kredit.

Pasal 29

(1) Setiap Orang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi.

Pasal 30

(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun.
(2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.
(3) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

Pasal 31

(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain.
(2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan. Kecuali intersepsi sebagaimana dimaksud pada ayat (1) dan ayat (2), intersepsi yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi penegak hukum lainnya yang ditetapkan berdasarkan undang-undang.
(4) Ketentuan lebih lanjut mengenai tata cara intersepsi sebagaimana dimaksud pada ayat (3) diatur dengan Peraturan Pemerintah.

Pasal 32

(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi

Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik.

(2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak.

(3) Terhadap perbuatan sebagaimana dimaksud pada ayat (1) yang mengakibatkan terbukanya suatu Informasi Elektronik dan/atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya.

Pasal 33

(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya.

Pasal 34

(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki:

a. perangkat keras atau perangkat lunak Komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33;

b. sandi lewat Komputer, Kode Akses, atau hal yang sejenis dengan itu yang ditujukan agar Sistem Elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33.

(2) Tindakan sebagaimana dimaksud pada ayat (1) bukan tindak pidana jika ditujukan untuk melakukan kegiatan penelitian, pengujian Sistem Elektronik, untuk perlindungan Sistem Elektronik itu sendiri secara sah dan tidak melawan hukum.

Pasal 35

(1)Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik.

Pasal 36

(2) Setiap Orang 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.

Pasal 37

(1)Setiap Orang dengan sengaja melakukan perbuatan yang dilarang sebagaimana dimaksud

(2)dalam Pasal 27 sampai dengan Pasal 36 di luar wilayah Indonesia terhadap Sistem Elektronik

(3)yang berada di wilayah yurisdiksi Indonesia.

V. PENUTUP

Internet membuka wawasan bagi siapa saja penggunanya, karena dengan penggunaan internet maka informasi akan sangat mudah didapatkan. Pengetahuan tidak lagi didapatkan dari buku dan bahan ajar lainnya, tapi cukup dengan mencari diinternet makan ilmu barupun akan datang. Tetapi dengan mudahnya mendapatkan pengetahuan di internet, perlu juga disadari bahwa pengetahuan yang didapatkan diinternet haruslah disikapi dengan kebijakan akan isi dari pengetahuan tersebut digunakan untuk kepentingan apa, seharusnya pengetahuan yang didapatkan tersebut memiliki kegunaan yang ditujukan untuk pengembangan kebaikan bukan untuk keburukan.

Ternyata internet akan menjadi sumber kejahatan jika digunakan oleh orang-orang yang tidak bertanggung jawab, dan lahirlah istilah *cyber crime*, yaitu kejahatan yang dilakukan oleh orang-orang yang tidak bertanggung jawab, didalam penggunaan informasi diinternet, atau biasanya dapat didefinisikan sebagai kejahatan yang dilakukan dengan menggunakan computer dan jaringan computer didalam melakukan kejahatannya. Berbagai macam kejahatan muncul seiring dengan lajunya penggunaan internet.

Dimana ada kejahatan tentu saja harus ada ganjaran terhadap kejahatan yang dilakukan tersebut, karenany muncullah cyber law, yaitu hukum yang diberlakukan

kepada siapa saja yang telah melakukan kejahatan cyber crime.

Hampir seluruh Negara sudah memiliki undang-undang yang diberlakukan untuk mengatasi cyber crime, amerika menggunakan Uniform electronic Transaction(UETA), singapura menggunakan singapura menggunakan The electronic Act(akta Elektronik)1998, electronic Communication Privacy Act(Akta Privasi Komunikasi Elektronik)1996. Indonesia sendiri menggunakan undang-undang ITE tahun 2008. Begitu maraknya cyber crime didunia sehingga penangannyannya perlu mendapatkan perhatian khusus dari pemerintah, apalagi Negara Indonesia yang secara tidak disangka-sangka memiliki tingkat kejahatan tinggi dalam cyber crime. Kasus yang marak belakangan ini adalah, kasus farhat abas yang dianggap melakukan cyber crime yaitu melakukan pencemaran nama baik terhadap salah satu pejabat dki.

DAFTAR PUSTAKA

DRS. Abdul Wahid, S.H, MA, Mohammad Labib, SH, Kejahatan Mayantara (Cyber Crime), PT. Refika Aditama, Bandung, 2005

Drs. Dikdik M. Arief Mansur, SH, MH, Elisatris Gultom, SH. MH , Cyber Law (Aspek Hukum Teknologi Informasi), PT. Refika Aditama, Bandung, 2005

RIWAYAT HIDUP PENULIS

Nama Lengkap : Lita Sari Marita

Tempat Tanggal Lahir: Jakarta, 09 Mei 1979

Pekerjaan : Dosen

Pendidikan : S2

Email : lita.lsm@bsi.ac.id

Telp/HP: 80888569/08161992302

Tulisan ilmiah yang pernah diterbitkan:

1. Komunikasi dua arah dalam kegiatan belajar mengajar, di terbitkan di cakrawala BSI VOL VIII No.1 januari 2008
2. Peluang Kerja Lulusan Teknologi informasi, di terbitkan di cakrawala BSI VOL X No.1 Maret 2010
3. Metode Pembayaran dengan e-commerce, diterbitkan di cakrawala BSI Vol XII No. 2 September 2012