Cyber Crime dan Upaya Penanggulangannya

Agung Yoga
Program Studi Teknik Informatika, Fakultas Sains dan Teknologi, Universitas PGRI Yogyakarta, Kabupaten Bantul, Provinsi Daerah Istimewa Yogyakarta, Indonesia
Email: agungyoga@gmail.com

Abstrak
Di era yang serba cepat ini kita mendapat kan apa-apa dengan mudah bahkan data pribadi kita bisa di ketahui oleh orang yang tidak kita kenal. Tujuan tulisan ini adalah untuk membahas Cyber Crime Dan Upaya Penanggulangannya. Penelitian ini adalah penelitian hukum normatif yaitu penelitian dengan menggunakan metode atau cara yang di pergunakan di lakukan meneliti bahan pustaka yang ada penelitian ini menggunakan bahan hukum primer sekunder dan tersier. Hasil penelitian menunjukan bahwa kejahatan internet bisa menyerang siapa saja. Kita bisa melihat bahwa ada kemungkinan besar jika kejahatan cyber bisa terjadi jika ada peluangan, dam peluang itu adalah kesalahan yang kita perbuat atau keteledoran kita sebagai pengguna internet.
Kata Kunci: Cyber Crime, Penanggulangannya

PENDAHULUAN

Di era yang serba cepat ini kita mendapat kan apa-apa dengan mudah bahkan data pribadi kita bisa di ketahui oleh orang yang tidak kita kenal. Bahkan kita sering tidak sadar jika kita hampir setiap hari menghabis kan waktu kita di internet dan menambahkan internet dalam daftar kebutuhan pokok bulanan. Informasi sangat mudah kita dapat kadang kita tidak tahu itu benar atau salah, iklan di medsos yang mengikuti keinginan kita saat itu ,dan juga pesan siaran di aplikasi pesan yang mudah sering kita dapatkan menjadi kekhawatiran saya terhadap internet yang dapat mempengaruhi perilaku orang.Kasus-kasus di internet dari mulai penipuan hingga penyebaran infomasi personal yang sering kita dengar adalah sisi kelam internet yang kita wajib ketahui, yang saya khawatirkan adalah ketika kita sudah tenggelam kedalam internet tanpa tahu sisi kelam internet itu seperti apa. Tetapi kita juga tidak bisa menghindari kemajuan teknologi yang begitu cepat ini.

METODE PENELITIAN

Penelitian ini adalah penelitian hukum normatif yaitu penelitian dengan menggunakan metode atau cara yang di pergunakan di lakukan meneliti bahan pustaka yang ada penelitian ini menggunakan bahan hukum primer sekunder dan persier, dimana bahan hukum primer yang di gunakan adalah peraturan perundang undangan yang berkaitan dengang penelitiaan ini, bahan hukum sekunder literatul-literatul tertulis berkaitan dengan pokok permasalahan yaitu buku-buku, jurnal-jurnal artikel-artikel dan lain sebagainya serta bahan hukum tersier.

HASIL PENELITIAN DAN PEMBAHASAN

Menurut Parker (Hamzah 1993:18), cyber crime adalah suatu tindakan atau kejadian yang berkaitan dengan teknologi komputer. Dimana seseorang mendapatkan keuntungan dengan merugikan pihak lain. Jenis-jenis cyber crime:

1. Pencurian Data. Aktivitas cyber crime yang satu ini biasanya dilakukan untuk memenuhi kepentingan komersil karena ada pihak lain yang menginginkan data rahasia pihak lain. Tindakan ini tentu bersifat ilegal masuk ke dalam aktifitas kriminal karena bisa

menimbulkan kerugian materil yang berujung pada kebangkrutan suatu lembaga atau perusahaan.

2. Cyber Terorism. Cyber terorism merupakan tindakan cyber crime yang sedang banyak diperangi oleh negara-negara besar di dunia, termasuk Indonesia. Pasalnya, aktivitas cyber terorism kerap kali mengancam keselamatan warga negara atau bahkan stake holder yang mengatu jalannya pemerintahan.
3. Hacking. Jenis cyber crime berikutnya adalah Hacking. Tindakan berbahaya yang kerap kali dilakukan oleh para programer profesional ini biasanya secara khusus mengincar kelemahan atau celah dari sistem keamanan untuk mendapatkan keuntungan berupa materi atau kepuasan pribadi. Jika menilik dari kegiatan yang dilakukan, hacking sebenarnya tidak selalu memiliki konotasi buruk karena ada pula hacker positif yang menggunakan kemampuannya untuk kegiatan bermanfaat dan tidak merugikan. Misalnya, seorang hacker yang diberi tugas untuk melacak keberadaan seorang buronan atau hacker yang bekerjasama dengan pihak bewenang untuk memberantas aktivitas ilegal di ranah digital.
4. Carding. Carding adalah istilah yang digunakan untuk menyebut penyalahgunaan informasi kartu kredit milik orang lain. Para carder (pelaku carding) biasanya menggunakan akses cartu credit orang lain untuk membeli barang belanjaan secara online. Kemudian, barang igratisan tersebut dijual kembali dengan harga murah untuk mendapatkan uang. Tindak kejahatan digital dengan cara carding biasanya kerap terjadi di luar negeri, sementara untuk pengguna di Indonesia angka kasus yang tercatat belum terlalu besar seiring masih minimnya pengguna kartu kredit yang gemar bertransaksi di dunia maya.
5. Defacing. Di antara tindakan cyber crime sebelumnya, Defacing bisa dibilang menjadi aktivitas kejahatan online yang paling ringan. Hal tersebut salah satunya karena para pelaku deface biasanya menyasar website-website non-profit seperti situs pemerintahan, sekolah, atau universitas.
6. Cybersquatting. Istilah cybersquatting mungki belum begitu familiar di kalangan pengguna di Tanah Air. Wajar memang pasalnya tindakan penyerobotan nama domain sendiri memang memerlukan modal serta kejelian yang tidak dimiliki banyak orang. Hasil cyber crime ini biasanya berupa uang tebusan yang nilainya tidak wajar.
7. Cyber Typosquatting. Hampir mirip dengan cybersquatting, tindakan cyber typosquatting sama-sama mengincar nama domain milik perusahaan terkenal untuk dijadikan sasaran. Bedanya, aktivitas ini memanfaatkan kemiripan nama domain serta kelalaian pengguna yang jarang memeriksa ulang URL website perusahaan. Salah satu tujuan dari cyber typosquatting adalah untuk menjatuhkan citra baik dari brand bersangkutan dengan cara melakukan tindakan penipuan atau hal-hal ilegal lain yang melanggar undang-undang.
8. Menyebarkan Konten Ilegal. Menyebarkan konten ilegal yang melanggar undang-undang menjadi kasus cyber crime paling banyak diperhatikan. Pasalnya, aktivitas ini biasanya melibatkan tokoh terkenal atau konten yang mampu memancing kontroversi. Beberapa contoh konten llegal yang masuk dalam ranah cyber crime di antaranya adalah video porno, penjualan senjata api ilegal, jual beli narkotika, dan lain sebagainya.
9. Malware. Seperti yang sudah kami jelaskan di dalam artikel tentang bahaya malware, Anda harus lebih waspada jika tidak ingin komputer atau website mengalami kendala. Secara umum, malware terdiri dari beragam jenis, ada virus, trojan horse, adware, worm, browser hijacker, dan lain sebagainya.

Undang-Undang Tentang Cyber Crime

Undang-Undang Nomor 11 Tahun 2008 Tentang Internet & Transaksi Elektronik (ITE) Undang-undang ini, yang telah disahkan dan diundangkan pada tanggal 21 April 2008,

walaupun sampai dengan hari ini belum ada sebuah PP yang mengatur mengenai teknis pelaksanaannya, namun diharapkan dapat menjadi sebuah undang-undang cyber atau cyberlaw guna menjerat pelaku-pelaku cybercrime yang tidak bertanggungjawab dan menjadi sebuah payung hukum bagi masyarakat pengguna teknologi informasi guna mencapai sebuah kepastian hukum.

1. Pasal 27 UU ITE tahun 2008 : Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan yang melanggar kesusilaan. Ancaman pidana pasal 45(1) KUHP. Pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 1.000.000.000,00 (satu miliar rupiah). Diatur pula dalam KUHP pasal 282 mengenaikejahatan terhadap. kesusilaan.
2. Pasal 28 UU ITE tahun 2008 : Setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik.
3. Pasal 29 UU ITE tahun 2008 : Setiap orang dengan sengaja dan tanpa hak mengirimkan informasi elektronik dan/atau dokumen elektronik yang berisi ancaman kekerasaan atau menakut-nakuti yang dutujukkan secara pribadi (Cyber Stalking). Ancaman pidana pasal 45 (3) Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam pasal 29 dipidana denganpidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp. 2.000.000.000,00 (dua miliar rupiah).
4. Pasal 30 UU ITE tahun 2008 ayat 3 : Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses computer dan/atau system elektronik dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol system pengaman (cracking, hacking, illegal access). Ancaman pidana pasal 46 ayat 3 setiap orang yang memebuhi unsure sebagaimana dimaksud dalam pasal 30 ayat 3 dipidana dengan pidana penjara paling lama 8 (delapan) dan/atau denda paling banyak Rp 800.000.000,00 (delapan ratus juta rupiah).
5. Pasal 33 UU ITE tahun 2008 : Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya system elektronik dan/atau mengakibatkan system elektronik menjadi tidak bekerja sebagaiman mestinya.
6. Pasal 34 UU ITE tahun 2008 : Setiap orang dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan atau memiliki.
7. Pasal 35 UU ITE tahun 2008 : 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 seolah-olah data yang otentik (Phising = penipuan situs).

Undang-Undang No 19 Tahun 2002 tentang Hak Cipta Menurut Pasal 1 angka (8) Undang – Undang No 19 Tahun 2002 tentang Hak Cipta, program komputer adalah sekumpulan intruksi yang diwujudkan dalam bentuk bahasa, kode, skema ataupun bentuk lain yang apabila digabungkan dengan media yang dapat dibaca dengan komputer akan mampu membuat komputer bekerja untuk melakukan fungsi-fungsi khusus atau untuk mencapai hasil yang khusus, termasuk persiapan dalam merancang intruksi-intruksi tersebut. Undang-Undang No 36 Tahun 1999 Tentang Telekomunikasi Menurut Pasal 1 angka (1) Undang – Undang No 36 Tahun 1999, Telekomunikasi adalah setiap pemancaran, pengiriman, dan/atau penerimaan dan setiap informasi dalam bentuk tanda-tanda, isyarat, tulisan,

gambar, suara, dan bunyi melalui sistem kawat, optik, radio, atau sistem elektromagnetik lainnya. Undang-Undang No 8 Tahun 1997 Tentang Dokumen Perusahaan Undang-Undang No. 8 Tahun 1997 tanggal 24 Maret 1997 tentang Dokumen Perusahaan, pemerintah berusaha untuk mengatur pengakuan atas mikrofilm dan media lainnya (alat penyimpan informasi yang bukan kertas dan mempunyai tingkat pengamanan yang dapat menjamin keaslian dokumen yang dialihkan atau ditransformasikan. Misalnya Compact Disk – Read Only Memory (CD – ROM), danWrite – Once -Read – Many (WORM), yang diatur dalam Pasal 12 Undang-Undang tersebutsebagai alat bukti yang sah. Undang-Undang No 25 Tahun 2003 tentang Perubahan atas Undang-Undang No. 15 Tahun 2002 tentang Tindak Pidana Pencucian Uang Jenis tindak pidana yang termasuk dalam pencucian uang (Pasal 2 Ayat (1) Huruf q). Penyidik dapat meminta kepada bank yang menerima transfer untuk memberikan identitas dan data perbankan yang dimiliki oleh tersangka tanpa harus mengikuti peraturan sesuai dengan yang diatur dalam Undang-Undang Perbankan.

Undang-Undang No 15 Tahun 2003 tentang Pemberantasan Tindak Pidana TerorismeUndang-Undang ini mengatur mengenai alat bukti elektronik sesuai dengan Pasal 27 huruf b yaitu alat bukti lain berupa informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu. Digital evidence atau alat bukti elektronik sangatlah berperan dalam penyelidikan kasus terorisme. karena saat ini komunikasi antara para pelaku di lapangan dengan pimpinan atau aktor intelektualnya dilakukan dengan memanfaatkan fasilitas di Internet untuk menerima perintah atau menyampaikan kondisi di lapangan karena para pelaku mengetahui. pelacakan terhadap Internet lebih sulit dibandingkan pelacakan melalui handphone. Fasilitas yang sering digunakan adalah e-mail dan chat roomselain mencari informasi dengan menggunakan search engine serta melakukan propaganda melalui bulletin board atau mailing list.

Saya akan menjabarkan pembahasan mengenai cyber crime. Di era yang serba canggih ini internet sudah menjadi kebutuhan dan bukan lagi menjadi barang mewah. Semua orang telah menggunakan internet,bahkan menambahkan internet di daftar belanja bulanan. Kita bisa bertemu siapa pun dari berbagai belahan dunia manapun. Informasi yang dulu kita dapat dari media cetak seperti Koran atau semacam nya bisa kita peroleh dengan mudah dan cepat. Internet bisa di sebut salah satu bentuk kemajuan peradaban manusia sebagai tanda kita telah memasuki jaman yang berbeda dalam waktu yang terbilang cukup cepat. Saya kira factor inilah yang bisa dimanfaat kan para “penjahat internet” untuk melakukan kejahatan nya. Seperti contoh nya generasi yang terlahir dari jaman internet belum ada atau belum semaju sekarang ada kemungkinan bahwa mereka belum mengerti internet dan kagok dalam penggunaannya, nah hal ini lah yang bisa dimanfaat kan oleh mereka. Bahkan kita pun yang terlahir di jaman sekarang pun bisa menjadi mangsanya, artinya kejahatan internet itu bisa menyerang semua pengguna internet.

Di tahun 2020 ini kita telah menyaksikan perkembangan internet yang cukup pesat dari mulai mall yang bisa kita akses dari rumah, transportasi pribadi yang bisa kita pesan dengan dawai kita bahkan kita sudah menganggap satu mobil dengan orang yang tidak dikenal itu normal. Pekerjaan yang bisa kita lakunan dengan rebahan yang dulu kita anggap tidak mungkin kini semua itu mungkin dan lumrah. Sekarang kita dapat mengetahui tanggal lahir, alamat rumah bahkan hobi nya hanya dengan mengunjungi profil social media-nya. Dan juga kita dapat mengetahui posisi terkini seseorang hanya dengan melihat update-an nya. Mungkin kita menganggap itu sebagai hal lumrah tetapi perlu kita sadar bahwa tidak semua pengguna internet adalah orang yang benar-benar baik kita juga tidak tahu apa yang ada dipikiran para pengguna internet saat melihat tanggal lahir kita beserta foto-foto “manja” yang kita unggah. Berbagai kasus yang terjadi di internet kadang di pengaruhi oleh kelalaian kita sendiri dari

hal yang kita anggap itu trend dan dari hal yang kita anggap itu lumrah. Dari mulai memberikan informasi pribadi atau bahkan foto pribadi ke orang yang kita kenal di internet, orang yang tidak kita kenal secara langsung dan orang yang hanya kita lihat melalui layar. Seakan kita menganggap semua orang itu baik tetapi suatu kejahatan kadang terjadi karena ada kesempatan. Dari data yang bisa kita lihat diatas kejahatan internet meliki berbagai jenis dan modus hal itu menyimpulkan bahwa kejahatan internet memilki peluang untuk berkembang seiring kemajuan jaman. Oleh karena itu wawasan kita tentang internet pun harus berkembang guna mengimbangi para penjahat internet. Oleh karena itu saya akan mejabara kan beberapa jenis kejahantan internet guna untuk menjadi sedikit pengingat agar kita bisa berhati-hati dalam mejelajah di dunia internet ini.

KESIMPULAN

Dari kasus yang sudah ada kita bisa simpulkan bahwa kejahatan internet bisa menyerang siapa saja. Kita bisa melihat bahwa ada kemungkinan besar jika kejahatan cyber bisa terjadi jika ada peluangan, dam peluang itu adalah kesalahan yang kita perbuat atau keteledoran kita sebagai pengguna internet. Kita tidak sada bahwa kita sebenarnya memasuki dunia yang bisa menjadiakan manusia itu siapa saja bahakan apa saja. Kesadaran akan tumbuh bila kita sudah mengetahui dampak baik dan buruk nya. Kita sudah memasuki zaman yang serba cepat dan semua bisa kita dapat dengan mudah, ada kemungkinan yang cukup besar jika semakin majunya internet akan semakin maju juga kejahatan internet.

DAFTAR PUSTAKA

Amalia, Dista. 2011. Kasus Cybercrime Di Indonesia. Semarang: UNISSULA

Danuri, Muhamad. 2017. Trend Cyber Crime Dan Teknologi Informasi Di Indonesia. Semarang: Universitas Dian Nuswantoro