Analisis Cyber Law dalam Pemberantasan Cyber Terorism di Indonesia

Eka Lusyanti Marpaung
Sistem Informasi
Fakultas Ilmu Komputer
Universitas Sriwijaya
echamarpaung@gmail.com

Mila Astuti
Sistem Informasi
Fakultas Ilmu Komputer
Universitas Sriwijaya
milaastuti44@gmail.com

Ali Ibrahim
Sistem Informasi
Fakultas Ilmu Komputer
Universitas Sriwijaya
aliibrahim@ilkom.unsri.ac.id

Abstrak - Kejahatan komputer perlu di waspadai juga tindakan terorisme yang dilakukan melalui cyberspace ini. Hal ini memungkinkan terjadi di dunia maya hanya saja caranya berbeda dengan tindakan terorisme konvensional yang ada di dunia nyata tetapi efeknya dapat dirasakan juga pada dunia nyata. analisis ini merupakan suatu penelitian yang bersifat yuridis-normatif. Untuk menghimpun bahan yang diperlukan, maka telah menggunakan metode penelitian kepustakaan, yaitu dengan cara mempelajari buku-buku hukum, artikel artikel yang membahas masalah hukum, himpunan peraturan perundang-undangan yang berlaku di Indonesia, serta berbagai sumber tertulis lainnya. Hasil analisis menunjukkan tentang bagaimana merumuskan delik terhadap tindak pidana cyber terrorism sesuai dengan hukum positif yang berlaku di Indonesia serta bagaimana penerapan hukum positif Indonesia terhadap tindak pidana cyber terorism. Pertama, delik pada Undang- Undang No. 15 Tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme dan Undang-Undang Nomor 11 Tahun 2008

Kata kunci :internet, cyber crime, cyber law,terorism

I. PENDAHULUAN

Perkembangan teknologi informasi pada khususnya internet yang semakin berkembang pesat tentunya membawa dampak bagi *user* yang dalam hal ini pengguna internet baik dampak positif maupun negatif yang ditimbulkan. Mulai dari dampak positif kita dapat banyak sekali merasakan manfaat terutama dibidang komunikasi yang tidak lagi mengenal batasan-batasan baik jarak maupun waktu. Tersedianya komunikasi melalui internet merupakan sebuah keuntungan yang besar bagi perkembangan arus informasi yang sangat diperlukan di dalam kehidupan sehari-hari.Namun, dampak negatifnya pun sangat dapat dirasakan dan dilihat, dimana kita telah mengenal suatu kejahatan atau yang biasa disebut dengan *Crime* berintegrasi dengan dunia internet sehingga disebut *Cyber Crime* yang dalam implementasinya merupakan sebuah kejahatan yang dilakukan dengan memanfaatkan perkembangan teknologi internet.di Indonesia mulai dengan isu fanatisme agama, tidak hanya di Indonesia yang rentan terhadap *Cyber Terrorism* di negara-negara lain juga, dan ini bersifat laten. Kelompok-kelompok radikal menggunakan media internet untuk mengrekrut, mengajarkan, menghasut,dan memprovokasi masyarakat untuk membenarkan kekerasan atas nama agama.Berdasarkan latar belakang diatas penulis menganggap perlu diadakan kajian mengenai *crime* berintegrasi khususnya mengenai *cyber terrorism*.

II. KAJIAN PUSTAKA

Menurut Andi Hamzah (1989) cyber crime adalah kejahatan dibidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara ilegal. Cyber crime 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, cyber crime merupakan suatu tindak pidana dengan 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 cyber crime atau kejahatan elektronik sebagai :

1. 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, 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, atausejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui Komputer atauSistem Elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol atau perforasiyang memiliki makna atau arti atau dapat dipahami oleh orang yang mampumemahaminya.

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 (cyber crime) namun ada kesamaandalam 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.

Cyber crime 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 Cyber crime diklasifikasikan menjadi ;

1. Cyber piracy, yaitu penggunaan teknologi komputer untuk mencetak ulang software atau informasi, lalu mendistribusikan informasi atau software tersebut lewat teknologi komputer.
2. Cyber tresspass, yaitu penggunaan teknologi komputer untuk meningkatkan akses pada sistem komputer suatu organisasi atau indifidu. 3. Cyber vandalism, yaitu penggunaan teknologi komputer untuk membuat program yang mengganggu proses transmisi elektronik dan menghancurkan data dikomputer. Pada dasarnya Cyber crime 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 cyber crime 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.

III. METODE PENELITIAN

A. Pengumpulan Dan Pengolahan Data

Data yang digunakan pada penelitian ini adalah data primer yang diambil langsung dari hasil pengamatan terhadap objek yang diteliti. Pengambilan data dilakukan dengan berbagai metode di antaranya dengan metode pengamatan.Langkah berikutnya dilakukan metode menganalisis dan mengklasifikasi data yang dijalani dengan memperoleh data historis. Adapun teknik pengumpulan data yang dilakukan dalam penelitian ini terdiri dari 4 macam, yaitu:

1. Studi literatur

   Tahap pertama yang dilakukan adalah mempelajari tentang teori dan topik yang akan dibahas. Dalam proses ini, semua teori yang berhubungan dengan topik “Keamanan Sistem Informasi” dikumpulkan dari berbagai sumber; buku, jurnal, internet, dan sebagainya.

2. Pengamatan secara langsung

   Pengamatan secara langsung terhadap sistem bertujuan untuk mempelajari bagaimana proses aliran data menjadi informasi dalam cyber terorism. Selanjutnya adalah ketidaksesuaian yang terjadi beserta jenis-jenis dan penyebabnya.

3. Pengumpulan data historis

   Tahap pengumpulan data historis merupakan tahap yang paling penting dalam penelitian ini, karena dari data historis itulah diketahui jenis-jenis ketidaksesuaian, sumber prosesnya, jumlah serta spesifikasinya, hingga akibat ketidaksesuaian pada kegagalan tersebut yang merupakan salah satu data yang penting untuk dianalisis.

No	Perkara	Salinan Putusan	Pasal yang dikenakan
1	Putusan Pengadilan Jakarta Pusat taun 1998 telah menerapkan	Salinan Putusan Pengadilan Negri Jakarta Pusat No.	Pasal 363 KUHP : ayat 4 berbunyi Pencurian dilakukan

	pasal pencurian dalam kasus unauthorized Transfer dana BNI 46 Ney York Agency	135/X/Pid. B/PN.jkt.Pst tanggal 11 Maret 1988 a.n Seno Adjie	oleh dua orang atau lebih dengan bersekutu
2	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 Diobokobok	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 kebohongan menggerakkan orang lain untuk menyerahkan sesuatu benda kepadanya, atau supaya memberi hutang maupun menghapuskan piutang, diancam karena penipuan dengan pidana penjara paling lama 4 tahun
3	Putusan Pengadilan Negri Semarang tahun 2003 telah menerapkan pasal tentang pencurian dalam kasus carding	Salinan Putusan Pengadilan Negri Semarang No. 504/Pid.B/2003/PN. Smg	Pasal 362 KUHP: Barang siapa yang mengambil suatu barang, yang seluruhnya atau sebagian kepunyaan orang lain, dengan maksud untuk memilikinya secara melawan hukum diancam karena pencurian dengan pidana penjara maksimum 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

IV. HASIL DISKUSI

Hasil diskusi menunjukkan tentang bagaimana merumuskan delik terhadap tindak pidana *cyber terrorism* dalam transaksi elektronik sesuai dengan hukum positif yang berlaku di Indonesia serta bagaimana penerapan hukum positif indonesia terhadap tindak pidana *cyber terrorism* dalam transaksi elektronik. delik pada Undang- Undang No. 15 Tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme dan Undang-Undang Nomor 11 Tahun 2008 tentang ITE untuk menjerat pelaku tindak pidana *cyber terrorism* yang mana *cyber terrorism* dapat dijerat menggunakan Undang-Undang Nomor 23 tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme dan Undang-Undang Nomor 11 Tahun 2008 tentang ITE.Dalam kaitannya dengan penentuan hukum yang berlaku dikenal beberapa asas yang biasa digunakan, yaitu :

1. Subjective Territoriality

   yang menekankan bahwa keberlakuan hukum ditentukan berdasarkan tempat perbuatan

dilakukan dan penyelesaian tindak pidananya dilakukan di negara lain.

2. Objective Territoriality

   yang menyatakan bahwa hukum yang berlaku adalah hukum dimana akibat utama perbuatan itu terjadi dan memberikan dampak yang sangat merugikan bagi negara yang bersangkutan.

3. Nationality

   yang menentukan bahwa negara mempunyai jurisdiksi untuk menentukan hukum berdasarkan kewarganegaraan pelaku.

4. Passive Nationality

   yang menekankan yurisdiksi berdasarkan kewarganegaraan korban.

5. Protective Principle

   yang menyatakan berlakunya hukum didasarkan atas keinginan negara untuk melindungi kepentingan negara dari kejahatan yang dilakukan di luar wilayahnya, yang umumnya digunakan apabila korban adalah negara atau pemerintah.

6. Universality

   Asas ini selayaknya memperoleh perhatian khusus terkait dengan penanganan hukum kasus-kasus cyber. Asas ini disebut juga sebagai "universal interest jurisdiction". Pada mulanya asas ini menentukan bahwa setiap negara berhak untuk menangkap dan menghukum para pelaku pembajakan. Asas ini kemudian diperluas sehingga mencakup pula kejahatan terhadap kemanusiaan (crimes against humanity), misalnya penyiksaan, genosida, pembajakan udara dan lain-lain. Meskipun di masa mendatang asas jurisdiksi universal ini mungkin dikembangkan untuk internet piracy, seperti computer, cracking, carding, hacking and viruses, namun perlu dipertimbangkan bahwa penggunaan asas ini hanya diberlakukan untuk kejahatan sangat serius berdasarkan perkembangan dalam hukum internasional.

Oleh karena itu, untuk ruang cyber dibutuhkan suatu hukum baru yang menggunakan pendekatan yang berbeda dengan hukum yang dibuat berdasarkan batas-batas wilayah. Ruang cyber dapat diibaratkan sebagai suatu tempat yang hanya dibatasi oleh screens and passwords. Secara radikal, ruang cyber telah mengubah hubungan antara legally significant (online) phenomena and physical location.

V. KESIMPULAN

Cyber terrorism menyebabkan banyak kerugian bagi berbagai pihak, tidak hanya kerugian materil tetapi juga non-materil, karena menyebarkan isu yang berisi ancaman, memprovokasi dan mengajak untuk bergabung dalam aksi terrorisme. Sehingga diperlukan *cyberlaw* untuk mengatur etika dalam aktivitas di dunia maya. Undang-undang yang digunakan sebagai landasan untuk menjerat pelaku *cyber terrorism* adalah UU Nomor 15 tahun 2003 tentang terrorisme dan UU Nomor 11 tahun 2008 tentang ITE.

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 orangorang 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.

VI. REFERENSI

Drs. Abdul Wahid. SH. MA. Mohammad Labib SH. (2005). Kejahatan Mayantar (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

Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Didik M. Mansur Arief dan Elisatris Gultom,. Cyber law: Aspek Hukum Teknologi Informasi: Bandung: Refika Aditama. 2005

Andi, Hamzah, Aspek-aspek Pidana di Bidang Komputer: Jakarta: Sinar Grafika. 1990

Barda Nawawi Arif, 2001, Masalah Penegakkan Hukum & Kebijakan Penanggulangan Kejahatan, Ctra Aditya Bakti, Bandung,.

Rahardjo, Agus. Cyber Crime: Pemahaman dan Upaya Penangulangan Kejahatan Berteknologi. Citra Aditya Bhakti, Bandung,2002.

Widodo. Sistem Pemidanaan Dalam Cyber Crime Alternatif Ancaman Pidana Kerja Sosial Dan Pidana Pengawasan Bagi Pelaku Cyber Crime, Laksbang Mediatama, Yogyakarta. 2009.