Rechtsidee
Vol. 2 (2), December 2015, Page 79-178
P. ISSN. 2338-8595, E. ISSN. 2443-3497

Available online at:
http://ojs.umsida.ac.id/index.php/rechtsidee

Law Enforcement of Cyber Terorism in Indonesia

Penegakan Hukum terhadap Terorisme Dunia Maya di Indonesia

Sri Ayu Astuti
Fakultas Hukum Universitas Muhammadiyah Sidoarjo
Jl. Majapahit Nomor 666 B, Sidoarjo, Jawa Timur, Indonesia, Kode Pos 61215
Telp.: +62 31 8928097
Email: saar_1126@yahoo.co.id

Diterima: 15 Agustus 2015; Disetujui: 10 November 2015.

Abstract

Cyber terrorism is one of the category of crimes that cross border organized and has been established as an extraordinary crime. This crime is becoming a serious threat to countries in the world. In this regard, the Government's attitude of firmness needed to enforce cyber laws against the freedom development in social media. The development of the immeasurable it in the country of Indonesia required the limitations by doing legal liability over the behavior of law which deviates towards the use of technology tools. Strict law enforcement efforts as a clear attitude to stop actively moving massive terrorism, by enacting the provisions of the law on information and electronic transactions as well as the law of terrorism effectively.
Keywords: information technology; criminal acts of cyber terrorism; cyber law enforcement;

Abstrak

Perbuatan pidana terorisme dunia maya masuk dalam kategori kejahatan lintas batas negara yang terorganisir dan telah ditetapkan sebagai kejahatan luar biasa. Kejahatan ini menjadi ancaman serius bagi negara-negara di dunia. Di dalam hal ini diperlukan ketegasan sikap Pemerintah untuk menegakkan hukum dunia maya terhadap kebebasan yang berkembang di dalam media sosial. Perkembangan yang tak terukur itu di negara Indonesia diperlukan batasan dengan melakukan pertanggungjawaban hukum atas perilaku hukum yang menyimpang terhadap penggunaan alat teknologi. Upaya penegakan hukum yang tegas sebagai sikap yang jelas untuk menghentikan giat terorisme yang bergerak masif, dengan memberlakukan ketentuan Undang-Undang Informasi dan Transaksi Elektronik serta Undang-Undang Terorisme secara efektif.
Kata kunci: teknologi informas; tindak pidana terorisme dunia maya; penegakan hukum dunia maya*;*

1. Pendahuluan

Terorisme kini berkembang lebih cepat seiring dengan cepatnya perkembangan teknologi, hingga sistem perkembangan gerakan masif dalam kejahatan pidana terorisme bukan lagi pada bentuk konsep konvensional dalam sebaran kebencian pada pemerintahan yang berdaulat saja, tapi banyak mencederai dan merusak kehidupan kemanusiaan dalam konsep pemikiran radikalisme dan berkembang menjadi radikalisasi.

Perkembangan teknologi terjadi dengan pesat dan tanpa batas (borderless) membawa dampak pada setiap orang dalam proses interaksi kehidupannya. Perkembangan teknologi tersebut terkait dengan penggunaan teknologi informasi yang bergerak menggunakan sistem *internet conection network*.

Aspek perkembangan terhadap kemanfaatan internet itu memasuki ruang lini kehidupan masyarakat tanpa mengenal strata yang hidup dalam tatanan bentuk kehidupan masyarakat yang telah lama berjalan dengan keteraturan norma dan nilanya. Konsekuensi

terjadinya perkembangan teknologi dengan dunia internet itu menuai dampak negatif dan positif dalam proses pergaulan internasional dengan menggunakan desaign teknologi internet di dalam penggunaan ruang maya.

Dampak positif yang ada terjadi dalam ruang kehidupan nyata adalah mempermudah percepatan komunikasi dan informasi yang ada dalam kelanjutan capaian pada sasaran yang dituju. Kehidupan sosial begitu dinamis dalam pemerataan informasi dengan berbagai peristiwa yang terjadi diberbagai belahan dunia dapat diketahui dalam hitungan detik. Namun sebaliknya berbagai peristiwa tadi yang terjadi diantaranya adalah peristiwa akibat dari perilaku dan perbuatan hukum yang menyimpang dari kelaziman manusia, dengan menggunakan media sosial sebagai alat untuk menggerakan maksud dan mencapai tujuan negatifnya, misal gerakan masif menyebarkan ideologi dari kelompok radikalisasi yang menginginkan orang percaya bahwa gerakan yang dilakukannya adalah benar, setelah itu melakukan tindak lanjut dengan memberikan pandangan bahwa pemerintahan yang sah dan berdaulat perlu dihancurkan dengan suatu gerakan tindakan nyata di luar ruang *cyber* dengan memberikan ancaman tekanan yang menimbulkan ketakutan pada semua orang atau yang dikenal dengan teror.

Kondisi tersebut yang terjadi dalam era globalisasi yang mulai hadir di Abad ke-20 tepatnya saat terjadi revolusi elektronika yang memudahkan seluruh transaksi dan interaksi kehidupan manusia. Akhirnya dunia dapat menyatu dan saling tahu dan terbuka serta saling bergantung satu sama lain. Di dalam situasi itu pergerakan kemajuan teknologi itu melahirkan penggabungan komputer dengan telekomunikasi yang menghadirkan fenomena teknologi yang sangat mengagumkan yaitu mengubah konfigurasi desain komunikasi dari konvensional ke sistem digital. Dalam hal ini terjadi 3 (tiga) proses hingga mencapai dunia virtual yang menjadi nyata. dimensi pertama adalah kenyataan keras pada kehidupan empiris (biasa disebut *hard reality*), dimensi kedua merupakan kenyataan dalam keadaan simbolik dan nilai-nilai yang dibentuk (dipadankan dengan sebutan *soft reality*), maka dengan dimensi ketiga dikenal kenyataan maya *(virtual reality*) yang melahirkan suatu format masyarakat lainnya[1].

Terkait dengan hal tersebut di atas dengan kemajuan teknologi yang tertuju pada kemajuan telekomunikasi, multimedia dan teknologi informasi (telematika) yang akhirnya memberikan dampak perubahan pada tatanan organisasi dan hubungan masyarakat, karena

[1] Josua Sitompul, *Cyberspace, Cybercrimes, Cyberlaw Tinjauan Aspek Hukum Pidana* (Jakarta: Tatanusa, 2012).

tidak dapat dihindari fleksibilitas dan kemampuan telematika dengan cepat memasuki berbagai aspek kehidupan manusia.

Kemajuan teknologi dengan penemuan internet merupakan satu penyebab terjadinya perubahan sosial dan penyebab terjadinya pertentangan dalam masyarakat diantaranya adalah revolusi dalam ruang masyarakat, sebagaimana juga dikatakan Satjipto Raharjo[2]:

> *Dalam kehidupan manusia banyak alasan yang dapat dikemukakan sebagai penyebab timbulnya suatu perubahan di dalam masyarakat, tetapi perubahan dalam penerapan hasil-hasil teknologi modern dewasa ini banyak disebut-sebut sebagai salah satu sebab bagi terjadinya perubahan sosial.*

Sejalan dengan hal di atas Soerjono Soekanto[3] mengatakan bahwa kemajuan di bidang teknologi akan berjalan dengan munculnya perubahan-perubahan di bidang kemasyarakatan. Perubahan-perubahan itu dapat mengenai nilai sosial, kaidah-kaidah sosial, pola-pola perikelakuan, organisasi dan susunan lembagai kemasyarakatan.

Kemajuan teknologi membawa tuntutan tersendiri dalam kehidupan masyarakat dalam ketentuan kebutuhan masyarakat, pemerintah dan regulasi yang mengatur kehidupan dalam ruang terbuka atas penggunaan teknologi informasi yang berkembang dan membawa dampak perubahan perilaku budaya hukum dengan sebuah pertanggungjawaban dalam pola hukum baru.

Kenyataan itu adalah dengan penegakan hukum terhadap banyaknya tindak kejahatan yang kini mulai bergerak dan dilakukan dari ruang *cyber*. Pengaruh dari penggunaan media internet dan dengan pola komunikasi yang semakin aktif di berbagai bentuk media sosial semakin membuka kreatifitas pola perilaku budaya hukum yang menyimpang dari bentuk pola kejahatan konvensional. Beberapa jenis tindak pidana semakin mudah dilakukan, bahkan yang terjadi semakin banyak tindak pidana dilakukan atas nama kebebasan tanpa batas di ruang maya tersebut. Sebut saja semakin tinggi angka kejahatan pencemaran nama baik, pornografi, prostitusi, pembobolan rekening, perusakan jaringan *cyber* (*hacking*), sampai dengan penanaman ideologi melalui tindakan komunikasi dengan *hate speech* terhadap pemerintahan berdaulat, bahkan kejahatan terorisme dari ruang maya itu terus berkembang dengan pola yang beragam[4].

Kejahatan *cyber* belakangan sangat dikenal dalam bentuk kejahatan model baru dewasa ini. Kejahatan cyber terkait dengan perubahan perilaku budaya hukum yang

[2] AI Wisnubroto, *Strategi Penanggulangan Kejahatan Telematika* (Yogyakarta: Atma Jaya, 2010).
[3] Sitompul, *Cyberspace, Cybercrimes, Cyberlaw Tinjauan Aspek Hukum Pidana*.
[4] *Ibid.*

menyentuh setiap orang dalam interaksi sosial akibat dari pesatnya penggunaan teknologi informasi.

Secara umum kejahatan yang dilakukan di dunia *cyber* dimengerti sebagai[5]:

> *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.*

Pada dasarnya *cyber crime* meliputi semua tindak pidana yang berkenaan dengan informasi, sistem informasi (*information system*) itu sendiri, serta sistem komunikasi yang merupakan sarana untuk penyampaian/pertukaran informasi itu kepada pihak lainnya (*transmitter/originator to recipient*).

Tindak pidana di ruang maya itu yang populer disebut sebagai *cyber crime* di dalam literatur juga dikenal istilah computer crime. Pendapat lain seperti Organization for Economic Cooperation Development (OECD)[6] juga mengemukakan istilah computer related crime yang berarti: "*Any illegal, unethical or unauthorized behavior involving automatic data processing and/or transmission data*".

Ada beberapa kategori tindak pidana yang masuk dalam *cyber crime* yang dipandang merupakan *extra ordinary crime* oleh karena bentuk kejahatannya yang masuk pada unsur kejahatan yang terorganisir dan melewati batas negara yaitu *cyber terrorism*.

Aksi terorisme yang marak belakangan ini ditenggarai merupakan hasil giat masif dari ruang *cyber*. Kejahatan berkaitan dengan ideologi dan pencucian otak (*brain wash*) mengenai paham negara dan perekrutannya dengan melakukan komunikasi aktif menggunakan alat teknologi, menjadi kegiatan utama yang digerakan kepentingan kelompok radikalisasi untuk melakukan aksinya. Contoh nyata yang dapat kita lihat saat ini adalah organisasi Radikal IS atau yang lebih dikenal dengan ISIS (*Islamic State of Iraq and Syam/Syria*) menggunakan jejaring media sosial untuk merekrut anggota baru dan terus secara kuat mempublikasikan keberadaan kelompoknya sebagai kekuatan negara baru yang akan memimpin kekhalifahan di muka bumi dan dengan berbagai cara melakukan aksi teror melalui dunia maya.

Indonesia sebagai negara hukum berupaya membuat regulasi dalam penanganan kejahatan teknologi informasi khususnya dalam pengelolaan informasi dan transaksi elektronik beserta infrastruktur dan pengaturannya. Undang-Undang Informasi dan Transaksi

[5] Maskun, *Kejahatan Siber (Cyber Crime) Suatu Pengantar* (Jakarta: Kencana Prenada Media, 2013).
[6] *Ibid.*

Elektronik[7] diharapkan dapat mengatasi berbagai kejahatan *cyber*, dan dikuatkan dengan ketentuan Undang-Undang Nomor 15 Tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme[8]. Kebijakan pemerintah akan diperkuat lagi dengan beberapa Pasal yang termuat dalam RUU KUHP yang baru ,semua dilakukan pemerintah untuk menjaga keamanan Negara dan melindungi warga negaranya dari tindakan kejahatan terorisme yang diwujudkan di ruang nyata.

3. Pembahasan

3.1 Penggunaan Teknologi Informasi dan Perubahan Perilaku Budaya Hukum

Masyarakat Indonesia memasuki pergaulan Internasional melalui media internet dengan berbagai pola komunikasi dalam kemajuan teknologi. Kemajuan teknologi informasi itu ditandai dengan kehadiran perangkat keras bernama komputer dan perangkat lunak program internet. Definisi komputer dari Institut Komputer Indonesia[9] adalah suatu rangkaian peralatan dan fasilitas yang bekerja secara elektronik, dibawah kontrol suatu sistem pengoperasian (*operating system*) untuk melaksanakan pekerjaan berdasarkan rangkaian instruksi yang disebut program, serta mempunyai media penyimpanan di dalam mesin (*internal storage*) yang digunakan untuk menyimpan operating system, program dan data yang diperoleh. Sementara itu internet merupakan program atau perangkat lunak (software) yang membentuk sistem pengoperasian (oeprating system) dan peralatan itu digunakan sebagai alat proses data elektronik, magnetik, optikal, untuk melaksanakan fungsi logika, aritmetika, penyimpanan, dan penemuan data kembali[10].

Akibat dari penggunaan teknologi informasi dengan perangkat bernama komputer itu melahirkan gaya hidup yang berbeda dalam kenyataan yang sebenarnya. Perilaku budaya hukum dalam setiap orang di dunia maya berbeda hingga melahirkan istilah-istilah baru dalam pola kehidupan di dunia dunia maya.

Dampak secara umum keberadaan teknologi informasi memberikan pengaruh terhadap terjadinya perubahan dari akibat kemajuan teknologi informasi yang berkembang yaitu terjadinya masalah-masalah sosial. Kondisi itu dikarenakan masyarakat yang belum

---

[7] *Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik* (Jakarta, Indonesia: Lembaran Negara Republik Indonesia Tahun 2008 No. 58, Tambahan Lembaran Negara Republik Indonesia No. 4843, 2008).

[8] *Undang-Undang Republik Indonesia Nomor 15 Tahun 2003 Tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2002 Tentang Pemberantasan Tindak Pidana Terorisme, Menjadi Undang-Undang* (Jakarta: Lembaran Negara Republik Indonesia Tahun 2003 No. 45, Tambahan Lembaran Negara Republik Indonesia No. 4284, 2003).

[9] Institut Komputer Indonesia, *Pengenalan Komputer (Introducing to Computer)* (Jakarta: Institut Komputer Indonesia, 1981). *p*. 2.

[10] Widodo, *Sistem Pemidanaan Dalam Cyber Crime* (Yogyakarta: Laksbang Mediatama, 2010). *p*. 27.

siap menerima perubahan secara cepat akan dampak dari kehadiran komputer atas asas kemanfaatan yang begitu besar baik positif maupun negatif. Perubahan yang terjadi bukan saja dalam bentuk pola berpikir tetapi juga telah mengurai nilai-nilai masyarakat lebih luas lagi dari nilai-nilai baku dalam tatanan masayarakat konvensional, dan perubahan itu melahirkan masyarakat dunia maya secara virtual menjadi nyata. perubahan yang terjadi juga memberikan dampak buruk pada pola kejahatan gaya baru yang lebih dikenal di dalam tindak pidana sebagai kejahatan di ruang maya.

Perilaku budaya hukum masyarakat kini telah bergeser, dari mampu menghargai orang lain, dan mentaati nilai, norma dan kaidah hukum yang berlaku pada kelaziman di dalam masyarakat, kini atas nama kebebasan hak asasi manusia, seseorang dapat berlaku sekehendak hati dan atas kepentingan yang melekat dalam dirinya.

Perilaku hukum bukan hanya berarti taat hukum, tetapi semua perilaku yang merupakan reaksi terhadap sesuatu yang sedang terjadi dalam sistem hukum (*reacting to something going on the legal system*) sehingga tidak mentaati hukum yang diberlakukan dalam sistem kehidupan masyarakat sosial. Kaitannya perilaku hukum dalam kehidupan masyarakat bukan hanya reaksi taat,(*obey*) dan tidak taat (*disobery*) melainkan juga reaksi menggunakian *(use*) atau tidak menggunakan (*not use*) terhadap suatu aturan hukum.

Kemanfaatan media (*the covergance media*) membawa perubahan pada perilaku dalam penggunaan teknologi informasi, ketika setiap orang tidak mampu memahami hakikat perubahan dalam bidang teknologi informasi itu. Akibat pengaruh penggunaan media internet dalam kehidupan masyarakat dewasa ini yang paling nyata tidak hanya memperoleh kemudahan dalam segala urusan secara legal, tetapi terjadi juga munculnya jenis tindak pidana yang semakin banyak dilakukan dengan beragam modus operandi. Hal itu berkaitan dengan kemanfaatan teknologi yang digunakan oleh para pelaku kejahatan di ruang dunia maya (*cyberspace*) dengan istilah *cybercrime*.

Terminologi *cybercrime* menunjukan bahwa kejahatan yang dilakukan itu ada dalam ranah *cyberspace.* Kejahatan yang berbasis pada teknologi informasi dengan menggunakan media komputer sebagaimana terjadi saat ini, dapat disebut dengan beberapa istilah yaitu *computer misuse, computer abuse, computer fraud, computer – related crime, computer-assisted crime*, atau *computer crime*[11].

[11] Wisnubroto, *Strategi Penanggulangan Kejahatan Telematika. p.* 1.

Kejahatan yang menggunakan teknologi informasi dengan alat yang dikenal sebutannya komputer itu menurut penulis adalah segala bentuk kejahatan yang dilakukan dengan pola komputerisasi melalui jaringan dan para penggunanya.

Kejahatan dunia maya atau *cybercrime* dengan menggunakan teknologi informasi kecanggihan komputer itu, dari pandangan keilmuan secara umum dibagi dalam 2 (dua) kategori yaitu :

1. *Cybercrime* dalam pengertian sempit adalah kejahatan terhadap penggunaan sistem komputer;
2. *Cybercrime* dalam pengertian luas mencakup kejahatan terhadap sistem atau jaringan komputer dan kejahatan yang menggunakan sarana komputer.

Perubahan di dalam masyarakat telah terjadi, batasan wilayah hukum masyarakat satu negara dengan negara lain telah terlampaui oleh kegiatan di ruang dunia maya yang membawa berbagai dampak hukum akibat perilaku budaya hukum yang juga telah berubah.

Di dalam hal ini perlu disikapi dengan tegas oleh pemerintah atas dampak dari perubahan perilaku budaya hukum yang ada dengan membatasi penggunaan teknologi dalam hal pengawasan secara ketat terhadap provider yang ada dan beroperasi di Indonesia. kondisi ini sudah banyak dilakukan oleh negara tetangga seperti malaysia, singapura dan negara tetangga lainnya yang lebih tegas dalam hal mengawal dan megawasi beroperasinya para owner dari provide yang ada. Situasi tesebut dilakukan guna mengurangi tingkat kejahatan yang terjadi di ruang dunia maya akibat dari perilaku pengguna dengan perilaku yang tidak pada kepantasan dan menyimpang dalam menggunakan sarana perangkat lunak dan keras komputer. Ketegasan sikap itu diperlukan ketentuan peraturan perundang-undangan hukum media yang memiliki subtansi tegas dalam melindungi kepentingan kemanan Negara Kesatuan Republik Indonesia, sekaligus melindungi warga negara dalam kemanan diri sebagai pengguna dari ruang *cyber,* meski Indonesia telah memiliki satu Undang-Undang berkaitan dengan Telekomunikasi yaitu Undang-Undang Informasi dan Transaksi Elektronik yang telah mengakomodir mengatasi kejahatan *cyber* atau *cyber crime*.

3.2 Tindak Pidana *Cyber Terrorism* di Dunia Maya (*Cyberspace*) sebagai *Cybercrime*

Hukum pada dasarnya merupakan batasan bagi masyarakat dalam bertingkah laku terhadap pelanggaran dan untuk itu diperlukan sanksi dengan daya paksa otoritas tertinggi dalam kedaulatan suatu negara. Hukum diperlukan untuk menciptakan ketertiban dalam masyarakat dan memberikan keadilan. Ketertiban dan keadilan itu diperuntukan bagi individu maupun kolektif.

Kemajuan teknologi yang berkembang dalam dunia modern saat ini adalah suatu kemajuan yang ditandai setiap orang menggengamdunia dengan sentuhan jari dalam perangkat teknologi, dan setiap orang melakukaninteraksi sosialnya dengan seluruh giat dari jarak jauh dimulai dari ruang maya dikenal dengan istilah *cyberspace*.

Mengapa gerak di ruang dunia maya itu harus dibatasi dengan perangkat hukum oleh karena kehidupan nyata itu berpindah ke ruang maya dengan segala aspek negatif yang terjadi dan menjadi persoalan hukum.

Cyberspace merupakan dunia virtual yang dibentuk dari hasil penyatuan antara manusia dan teknologi, yaitu dari perkembangan teknologi informasi dan komunikasi (*Information and communication technology*–ICT). Teknologi Informasi dan komunikasi merupakan gabungan dari teknologi komputer, telekomunikasi serta jaringan komputer dan telekomunikasi, seperti yang digambarkan oleh Koops[12], sebagai berikut :

> *technologies that store, transmit, and/or process information and communication...the term is generally used to indicate "modern" or "high" technology, in particular electronic data – processing technologies. Thus, ICT focuses on computers, telecommunication, and computer and telecommunication networks. The term is sometimes used as a virtual synonym for the internet*.

Di dalam dunia *cyberspace* bersifat *bordeless* itu setiap orang datang dari mana saja dan kapan saja serta dapat memasuki ruang yang teramat luas untuk saling berkomunikasi tanpa perlu berada secara fisik di dalam ruang tempat mereka berkomunikasi.

Di ruang maya *cyberspace* itu sebagai dunia baru dalam kehidupan manusia modern terdapat makna hak asasi manusia. Dunia *cyber* tiap manusia memiliki eksistensi diri yaitu memiliki kebebasan mendasar sebagai salah satu hak bagi setiap orang untuk tidak menggunakan identitas asli, meski di Indonesia kulturnya berbeda dengan jelas menggunakan identitas diri asli. Semakin berkembang dunia maya maka semakin berkembang juga ideologi kebebasan dalam dunia *cyber*. Hal ini dinyatakan dan disebut oleh Langdon Winner sebagai *cyberlibertarianism* yaitu[13]:

> *a collection of ideas that links ecstatic enthusiasm for electronically mediated forms of living with radical, right wing libertarian ideas about the proper definition of freedom, social life, economic, and politics in the years to come*.

Bila penggagas ideologi ini mengatakan bahwa internet milik bersama oleh karena itu setiap orang memiliki hak penuh untuk berada dan melakukan interaksi di dalamnya. Maka

[12] Jaap Koops et al., eds., *Starting Points for ICT Regulation, Deconstructing Prevalent Policy One-Liners*, *IT & Law Series*, vol. 9 (The Haque, 2006).
[13] Sitompul, *Cyberspace, Cybercrimes, Cyberlaw Tinjauan Aspek Hukum Pidana*. *p*..35.

penulis melihat dunia maya itu dalam sistem internet merupakan ruang tak bertuan, dan itu berarti setiap orang berhak ada di dalamnya untuk melakukan interaksi di dunia tersebut.

Akan tetapi regulasi dalam dunia nyata untuk menarik permasalahan hukum dari ruang maya yang terjadi tetap diperlukan, hingga dibutuhkan perangkat hukum untuk menyelesaikan perkara hukum yang terjadi di ruang maya (*cyberspace*) itu. Menurut penulis kebebasan itu siapapun memilikinya, namun kebebasan itu juga harus memiliki batasan oleh karena setiap orang yang memiliki kebebasan dapat memberikan penghargaan atas kebebasan yang dimilikinya sendiri sebagai sebuah ketertiban bersama dalam menjaga ketertiban dan keadilan secara umum, dan sebagai hak melekat bagi setiap manusia.

Kebebasan menggunakan identitas dimanfaatkan untuk menipu, kebebasan untuk berekspresi digunakan untuk menyebarkan informasi yang berisi fitnah, kebebasan untuk mengembangkan teknologi dan kreativitas digunakan untuk merusak dan menyebarkan virus.

Atas kebebasan berekspresi di ruang maya (*cyberspace)* itu menimbulkan bentuk kejahatan baru yang dikenal dengan *cyber crime* yang tentunya tidak diatur di dalam Undang-undang konvensional, dan juga dapat pula berupa kejahatan konvensional yang menggunakan sarana komputer atau sistem komputer, seperti halnya kejahatan teror, atau dikenal dengan istilah *cyber terrorism*, karena kegiatannya menggunakan perangkat komputer untuk menyebarkan ideologi yang bersifat teror dalam upaya menjalankan aksi kejahatannya di dunia maya.

Pengertian pada definisi terorisme banyak bermunculan, satu yang dapat kita lihat adalah pendapat dari Golose[14] yang menyatakan

> *terorisme merupakan tindakan yang melawan hukum dengan cara menebarkan teror secara meluas kepada masyarakat dengan ancaman atau kekerasan, baik yang diorganisir maupun tidak, serta menimbulkan akibat berupa penderitaan fisik dan atau psykologis dalam waktu yang berkepanjangan sehingga dikategorikan sebagai tindak kejahatan yang luar dan kejahatan terhadap manusia.*

Di samping itu dapat kita lihat juga pengertian Tindak Pidana Terorisme dalam ketentuan peraturan Undang-Undang Nomor 15 Tahun 2003 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang (Perppu) Nomor 1 Tahun 2002 tentang Pemberantasan Tindak Pidana Terorisme. Pada Pasal 1 angka 1 Perppu tersebut enyatakan bahwa tindak pidana terorisme adalah "*segala perbuatan yang memenuhi unsur–unsur tindak pidana sesuai dengan ketentuan dalam Peraturan Pemerintah Pengganti Undang-Undang ini*".

[14] Romli Atmasasmita, "Aspek Nasional Dan Global Pemberantasan Terorisme," *Jurnal Hukum Internasional* 2, no. 3 (2003). *p*. 228.

Aksi kejahatan terorisme kini banyak melakukan pergerakannya dengan memanfaatkan teknologi informasi dan komunikasi yang dikenal dengan istilah *cyber terrorism.* Bentuk kejahatan terorisme memiliki karakteristik melewati lintas batas negara dalam dunia maya dikenal dengan *cyber terrorism*. Perhatian dunia tertuju pada cyber terrorism ini memiliki alasan kuat, karena menjadi ancaman bagi semua negara-negara di dunia yang memiliki tujuan hidup damai tanpa ada tekanan teror pada setiap warganegaranya.

Berkemangnya infrastruktur vital berbasis komputerisasi seperti sistem perbankan, *e-commerce*, *e-goverment* dan lain-lain maka potensi kejahatan terorisme dengan kemanfaatan teknologi informasi sangat rentan terjadi dalam ruang maya (*cyberspace*). Contoh nyata ditemukannya laptop yang digunakan salah satu tokoh peledakan bom bali imam samudera yang disita penyidik, dan diketahui adanya hubungan yang kuat antara aksi terorisme dengan tindak pidana berbasis teknologi informasi, bahwa internet dijadikan sarana komunikasi, propaganda, serta cardign untuk memperoleh dana bagi pembiayaan aksi teror[15].

Kemajuan teknologi informasi dan telekomunikasi memicu semakin berkembangnya bentuk-bentuk kejahatan terorisme di ruang maya. Fakta ini menunjukan pada argumen Jean-Jacques Rousseau[16] yang mengatakan bahwa :

> *Kemajuan seni dan ilmu pengetahun tidak menunjukkan moralitas manusia.sebagaimana sebuah teori mengatakan, crime is a product of society it self yang dapat diartikan bahwa masyarakat itu sendirilah yang melahirkan suatu kejahatan. Semakin tinggi tingkat intelektualitas suatu masyarakat, maka semakin canggih pula kejahatan yang mungkin terjadi dalam masyarakat tersebut.*

Aksi kejahatan teroris yang berpindah dari dunia nyata ke dalam bentuk terorisme dunia maya (*cyberspace*), merupakan aksi kejahatan yang bisa diperhitungkan kecepatannya menguasai daerah strategis yang menjadi objek uantuk dilakukan aksi teror pada sasarannya.

Aksi teroris yang menggunakan sarana kemajuan teknologi informasi dan telekomunikasi memang dirasakan tidak mengenal prinsip-prinsip diskriminasi target yang menjadi sasarannya. Aksi terorisme sebagai kejahatan luar biasa (*extra ordinary crime*), dikarenakan memiliki karakteristik kejahatan dalam tingkat pola internasional, dengan bentuk kejahatan yang terorganisir secara internasional.

[15] *Ibid*. *p*. 48.

[16] Mochtar Kusamaatmadja, *Pengantar Hukum Internasional,* 9th ed. (Bandung: Putra Abardin, 1999). *p.* 15. Mochtar Kusumaatmadja menyatakan bahwa kemajuan teknologi memberi pengaruh yang sangat besar terhadap perkembangan masyarakat Internasional dan hukum Internasional yang mengaturnya.

Aksi teroris yang menggunakan kemanfaatan teknologi (*convergance technology*) adalah menunjuk pada kemanfaatan penggunaan *cyberspace* untuk menjalankan rangkaian proses aksi kejahatannya.

Di dalam ketentuan Perppu No. 1 Tahun 2002 dan Undang-Undang Nomor 15 Tahun 2003 tidak disebutkan secara eksplisit apa yang dimaksud dengan cyber terrorism. Di dalam Pasal 27 Undang-Undang Nomor 15 Tahun 2003 hanya disebutkan alat bukti elektronik (*electronik evidence*) sebagai alat bukti yang sah. Informasi yang dikirmkan, diterima atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu, dan data yang merekam secara elektronik merupakan alat bukti.

Tidak mudah untuk mendefinisikan *cyber terrorism* karena banyak definisi yang berkembang. Andi Hamzah[17] menyatakan bahwa "*kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara ilegal*". Sejalan dengan pendapat Andi Hamzah, yang didukung oleh pemikiran dan pendapat Cahyana[18] yang menyatakan bahwa:

> *terorisme pada dasarnya sudah terjadi jika seseorang atau kelompok orang melakukan kegiatan ilegal melalui teknologi informasi. Menurutnya penyusupan ke dalam sistem komputer yang diproteksi milik orang lain dan mencuri data atau merusak data maupun informasi digolongkan sebagai terorisme informasi.*

Dari uraian tersebut menegaskan bahwa pada pemahaman *cyber terrorism* harus memiliki karakteristik bukan saja hanya menggunakan unsur media telekomunikasi dan informasi atau kecanggihan teknologi saja telekomunikasi yang digunakan sebagai sarana dan objek sasaran untuk melaksanakan aksi terorisme yang lebih penting dan yang dikedepankan adalah bentuk provokasi pada sifat kalimat yang dikomunikasikan yang mengandung kebencian (*hate speech*) dan secara terus menerus dilakukan sebarannya melalui alat teknologi telekomunikasi. Sebagai contoh pada Tahun 2015 ada banyak situs yang diblokir oleh pihak Kementerian Komunikasi dan Informasi RI yang bekerjasama dengan BNPT (Badan Nasional Penanggulangan Terorisme RI, yang banyak menuai kritikan tajam dari berbagai kalangan atas tindakan tersebut.

Bagi penulis itu adalah salah satu upaya untuk mengurangi sinisme dalam hal kebencian yang ditebarkan kepada Pemerintah dan mempengaruhi masyarakat awam dalam

[17] Andi Hamzah, *Aspek-Aspek Pidana Di Bidang Komputer* (Jakarta: Ghalia, 1989).
[18] Cahyana Ahmadjayadi, "Dampak Teknologi Komunikasi Dan Informasi Terhadap Kegiatan Terorisme" (Bandung: Badan Pembinaan Hukum Nasional, 2003). *p.* 10.

memahami aqidah yang seharusnya. Tentunya dengan tujuan untuk menjaga keamanan dan pertahanan bagi Negara Kesatuan Republik Indonesia.

Di dalam pemikiran Michael Vatism[19] ada 3 (tiga) cara bagaimana kaum teroris memanfaatkan komputer sebagai alat (*tool*) untuk melakukan kejahatan di ruang *cyber* (*cyber crime*) dalam menjalankan aksinya, dapat dibuktikan sebagai berikut :

1. Komputer sebagai alat dengan membuat home page yang digunakan sebagai sarana propaganda, rekruitmen, mengumpulkan data/informasi dari sektor privat atau data rahasia dan mengadakan hubungan dengan kelompok teroris lainnya, dan seluruh aktivitas menggunakan *encrypt*;
2. Sebagai penerima atau alat bukti; dengan ditemukannya data – data pada komputer yang dijadikan alat bukti adanya tindak pidana terorisme yang telah atau sedang direncanakan, ini dilakukan dengan men-*decrypt* dokumen (*file-file*) *encrypt* pada komputer pelaku;
3. Target, dalam hal ini pelaku kejahatan mengadakan konsolidasi dan koordinasi dalam melakukanan sasaran aksi terornya, misalnya pada kasus laptop milik pelaku kejahatan bom bali setelah dilakukan *decrypt* terbukti internet dipakai untuk mengadakan koordinasi pada aksi teror dan targetnya.

Cyber Terrorism merupakan salah satu jenis kejahatan yang masuk dalam kategori *Cyber Crime* karena kejahatan dalam dunia maya (*cyber crime*) secara sederhana dapat diartikan sebagai jenis kejahatan yang dilakukan dengan mempergunakan media internet sebagai alat bantu melakukan aksi terornya. *Cyber terrorism* dalam ruang maya (*cyber space*) berkembang begitu pesat dengan berbagai pola interaksi kejahatan yang dilakukan setiap orang yang berniat untuk melakukan tindak pidana di ruang maya.

Fakta hukum menunjukan terjadinya penyalahgunaan terhadap kemanfaatan internet oleh para teroris, sebagaimana halnya yang pernah terjadi di Indonesia yang dilakukan oleh Imam Samudera, terpidana mati atas kasus bom Bali, dengan perannya mengontrol jaringan teroris dari bilik penjara dengan berkomunikasi melalui internet. Imam Samudera berhasil menyelundupkan laptop ke dalam sel nya atas bantuan seorang sipir Lembaga Pemasyarakatan (LAPAS) Kerobokan yaitu Benny Irawan yang berhasil direkrut sebagai anggota teroris di dalam Lapas[20].

[19] Michael Vatis, "Cyber-Terrorism and Information Warfare Threats and Responses," in *The Terrorism Studies Program at The George Washington University* (Washington: The Potomac Institute for Policy Studies, 1998). *p.* 68.

[20] Petrus Reinhard Golose, *Invasi Terrorisme Ke Cyberspace* (Jakarta: YPKIK, 2015). *p.* 18.

Bukti lain adanya penyalahgunaan pada situs internet dalam penyebaran propaganda terorisme. Media Online yang populer menyebarkan paham terorisme adalah arrahmah.com dan diketahui adanya keterlibatan Muhammad Jibril yang juga bergelar *Princes of Jihad* sebagai pendiri dan *Chief Executif Officer* (CEO)[21].

Tindak pidana *Cyber terrorism* merupakan kejahatan yang dilakukan dengan menggunakan alat teknologi berupa komputer di ruang maya (*cyberspace*) dengan unsur utamanya melakukan kegiatan teror, propaganda, koordinasi dari jarak jauh dan dengan menebarkan kebencian (*hate teror*), menghimpun dana, perekrutan, pelatihan dan perencanaan secara terorganisir yang melewati batas negara, hingga menjadi kejahatan di dunia maya (*cyber crime*). Tindakan melawan hukum yang dilakukan setiap orang dan atas nama kelompok tertentu ini di *cyberspace* mengakibatkan timbulnya korban jiwa dan materiil yang besar terhadap keamanan orang lain, atas upaya penyerangan pada sistem komputer yang merusak data, sistem komputer serta infrastruktur vital.

Dengan demikian jelas sudah *cyber terrorism* sebagai kejahatan di ruang maya (*cybercrime*) perlu ditegaskan pengaturan hukumnya dalam Hukum Nasional Indonesia, agar dapat dipidanakan atas pertanggungjawaban hukum bagi setiap orang dan atau kelompok tertentu dengan sengaja melakukan aksi kejahatan di ruang maya yang menyebabkan terganggunya keamanan terhadap orang lain dengan pembuktian unsur elektronika yang ada.

3.3 Penegakan Hukum atas Tindak Pidana *Cyber Terrorism* dalam Hukum Nasional

Aksi teorisme merupakan tindakan seorang atau kelompok orang yang ingin mempertahankan hidup individu dan kolektif kelompoknya, dengan upaya yang dilakukan secara keliru yaitu mengancam dan membahayakan kelangsungan hidup orang lain. Itu berarti tindak pidana kejahatan teroris harus dilarang dan pelakunya dihukum dalam ketentuan hukum yang berlaku dalam setiap negara yang berdaulat dan memiliki ketentuan hukum.

Indonesia sebagai negara hukum yang ditegaskan dalam Pasal 1 Ayat (3) UUD 1945 dalam konteks Konstitusi Negara, telah merespon terjadinya percepatan kebutuhan akan antisipasi permasalahan hukum akibat perilaku hukum menyimpang dalam menggunakan komputer dan berinteraksi untuk melakukan kejahatan.

Tidak dipungkiri pengaturan khusus *cyber terrorism* memang belum ada, meski Indonesia telah memiliki beberapa ketentuan Undang-undang yang terkait dengan *cyber terrorism*. Sejauh mana sebenarnya kebutuhan akan *cyber law* sebagai *lex specialis* pada

[21] *Ibid.*

pengaturan *cyber terrorism.* Perlu dimasukan secara khusus pengaturan tindak pidana *cyber terrorism* pada ketentuan Hukum Dunia maya (*cyber law*) yang sejatinya kebutuhannya telah mendesak untuk digunakan. Ini disebabkan semakin tinggi frekuensi penggunaan teknologi dengan sistem yang berkembang, dengan konvergensi media (*convergance of media*) yang ada.

Pengaturan mengenai *cyber terrorism* dalam *cyber law* diharapkan bisa memberikan kepastian tegas dalam penjelasan hukum mengenai pengaturan kejahatan *cyber terrorism* secara khusus. Tentunya memiliki alasan utama yaitu adanya aspek yang terkait dengan kejahatan tindak pidana *cyber terrorism* yang dipertegas secara komprehensif dalam sebuah ketentuan undang-undang *cyber law* yang mengatur pergerakan dan penggunaan serta penyimpangan dalam tindakan kejahatan *cyber* yang menggunakan komputer sebagai alat utama dan kemanfaatan dari media teknologi yang berkembang.

Artinya tidak hanya bergantung pada satu Undang-Undang (*umbrella act*) saja, meski kita tahu telah ada Undang-Undang Nomor 15 Tahun 2003, ataupun Undang-Undang Nomor 36 Tahun 1999 Tentang Telekomunikasi, atau Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Memang secara yuridis dalam penyelesaian masalah hukum tindak pidana *cyber terrorism* ini hakim yang menangani harus melakukan penemuan hukum melalui penafsiran dan konstruksi hukum. Namun demikian bila pemangunan hukum nasional mengapresiasi hadirnya *cyber law* secara terintgrasi akan menjadi sebuah penguatan kepastian hukum yang lebih baik, mengingat banyak sekali gerakan terkait tindak pidana terorisme semakin berkemang dengan berbagai pola komunikasi dalam kemanfaatan media yang ada, sebagai alat komunikasi untuk melakukan aksi kejahatannya.

Di dalam ketentuan Undang-Undang Nomor 15 Tahun 2003 tentang Terorisme dapat digunakan untuk menjerat pelaku *Cyber Terrorism* karena terdapat Pasal yang mengatur tindak pidana terrorism pada ketentuan Pasal 6, Pasal 7, Pasal 9, Pasal 11 dan Pasal 12. Pada ketentuan Undang-Undang ini dinyatakan bahwa seseorang dianggap melakukan aksi terorisme dan dapat dijatuhi hukuman walaupan tindak pidana terorisme belum terjadi atau baru hanya sampai pada tahap dengan maksud atau dengan tujuan atau merencanakan tindak pidana terorisme.

Untuk mengetahui seseorang atau sekelompok orang memiliki maksud dan rencana melakukan tindak pidana terorisme tentunya pihak penyidik harus mendapatkan barang bukti guna mendukung dugaan tersebut bila ternyata telah ada niat dalam upaya tindak pidana

terorisme. Ketentuan Pasal 27 Undang-Undang Nomor 15 Tahun 2003, telah menyatakan berbagai macam alat bukti, dan satu diantaranya menyebutkan adanya alat bukti elektronik sebagai alat bukti yang sejajar dan sah sebagaimana dimaksud dalam hukum Acara Pidana.

Sejajar dengan pembuktian itu disebutkan juga dalam ketentuan Pasal 184 KUHAP bahwa alat bukti itu adalah berupa Informasi yang diucapkan, dikirimkan, disimpan secara elektronik dengan menggunakan alat optik seupa dengan hal itu yaitu data, rekaman, atau informasi yang dapat dilihat, dibaca, dan atau didengar, yang dapat dikeluarkan dengan atau tanpa batuan suatu sarana, baik yang tertuang di atas kertas, benda fisik apapun selain kertas, atau yang terekam secara elektronik, termasuk tetapi tidak terbatas pada tulisan, suara atau gambar, peta, rancangan, foto, atau sejenisnya, huruf, tanda, angka, simbol, atau perforasi yang memiliki makna atau dapat difahami oleh orang yang mampu membaca atau memahaminya.

Akan tetapi persoalannya tidak semudah yang kita fahami. Itu dikarenakan ada permasalahan dalam kesulitan keterukuran untuk mengetahui niat seseorang merencanakan, bermaksud dan bertujuan melakukan aksi terorisme. Analisa yang tajam dalam hal penyalahgunaan alat komputer dalam bentuk komunikasi dan informasi yang berkembang tidak boleh meleset hingga terjadi salah tangkap. Aparat hukum dalam hal ini penegak hukum yang berwenang harus benar-benar dapat menganalisa secara validitas terkait penggunaan alat-alat bukti elektronik yang digunakan untuk komunikasi secara elektronik apakah itu telah digunakan penyalahgunaan atau tidak dengan alat komputer dengan program internet.

Terkait upaya pembuktian bahwa seseorang atau kelompok tertentu melakukan tindak pidana *cyber terrorism* dalam investigasi terorisme, maka penting kiranya kita melihat beberapa ketentuan yang terdapat pada Undang-Undang Patriot Amerika Serikat, yang bisa menjadi perbandingan dalam penciptaan Undang-Undang terkait dengan *cyber terrorism* atau kejahatan terorisme di ruang maya.Undang-Undang Patriot amerika Serikat itu diantaranya mengatur mengenai[22]:

a. *Ketentuan "roving wiretap" agar departemen kehakiman memiliki kekuasaan untuk menyadap guna menelusuri jejak para tersangka tanpa mengindahkan telepon yang mereka gunakan.*
b. *Memperkenalkan sharing informasi yang semula dilindungi oleh grand jury di antara aparat intelejen dan aparat penegak hukum.*

[22] Abdul Hakim G. Nusantara, *Undang-Undang Pemberantasan Tindak Pidana Terorisme Dalam Perspektif Negara Hukum* (Bandung: Badan Pembinaan Hukum Nasional, 2003). *p.* 1.

c. *Memperkenankan penyitaan pesan-pesan voicemail sesuai dengan surat perintah (warrant)*
d. *Meningkatkan kekuasaan untuk menelusuri jejak para tersangka melalui internet.*
e. *Mensyaratkan pembukaan (disclosure) komunikasi para pelanggan atau catatan oleh para provider pelayanan komputer di daerah yang jauh (remote) dan pelayanan jasa komunikasi elektronik seperti ISPs kepada publik tanpa ditunda jika penyedia jasa (provider) mempunyai alasan yang dapat dipercaya adanya suatu yang membahayakan secara langsung atau mematikan atau melukai secara fisik.*
f. *Memberikan kekebalan (immunity) kepada provider jasa komunikasi elektronik atau wire atau orang yang menyediakan informasi, fasilitas atau bantuan teknis sesuai perintah atau permintaan pengadilan guna memberi bantuan darurat.*
g. *Melegalisasi tindakan aparat penegak hukum untuk menangkap (intercept) komunikasi elektronik atau wire dari penyalahgunaan komputer dan memiliki alasan untuk meyakini isi komunikasi tersebut relevan bagi penyelidikan.*
h. *Memuat ketentuan matahari terbenam (sunset principle) di mana beberapa ketentuan yang berkenaan dengan pengawasan akan berakhir.*

Ketentuan Undang-Undang Patriot Amerika Serikat di atas hanyalah sebagai pembanding. Negara Indonesia telah memiliki Undang-Undang Nomor 15 Tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme yang pada saat kelahiran undang-undang tersebut dijiwai dengan semangat proteksi kedaulatan negara, proteksi HAM bagi tersangka/terdakwa, dan juga proteksi terhadap korban-korban terorisme serta fasilitas publik[23].

Saat ini telah dilakukan upaya oleh kementerian POLHUKAM, Hukum dan HAM, dan lembaga terkait lainnya seperti Badan Nasional Penanggulangan Teroris (NCTA *National Counter Terrorism Act*) untuk melakukan revisi terhadap Undang-Undang Nomor 15 Tahun 2003 yang dalam kebutuhan terhadap penanganan tindak pidana terorisme telah berkembang dengan penggunaan alat teknologi bernama komputer, dan perilaku kejahatannya telah berubah pola dengan penyalahgunaan alat teknologi komunikasi dan informasi tersebut, hingga lahir istilah *cyber crime* dalam tindak pidana *cyber terrorism.*

Termasuk juga Basrief Arief[24] yang menyatakan "*Terorisme merupakan kejahatan luar biasa (extra ordinary crime) yang membutuhkan pola penanganan yang luar biasa pula (extra ordinary measure) yang berbeda dengan penanganan tindak pidana pada umumnya*".

Maka kondisi itu melahirkan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1Tahun 2002 yang kemudian menjadi Undang-Undang Nomor 15 Tahun 2003

[23] Atmasasmita, "Aspek Nasional Dan Global Pemberantasan Terorisme." *p*. 11
[24] Kejaksaan Agung Republik Indonesia, *Panduan Penanganan Perkara Tindak Pidana Terorisme Kejaksaan Agung Republik Indonesia*, cet ke I, 2013. *p.* v.

tentang Pemberantasan Tindak Pidana Terorisme, yang saat ini mengalami upaya revisi dalam Program Legislasi Nasional 2016.

Kendati demikian dengan adanya rencana melakukan amandemen itu sebaiknya dipikirkan juga adanya upaya penyusunan perundang-undangan terkait dengan *cyber terrorism* dalam pembangunan hukum nasional yaitu hadirnya *cyber law* Indonesia.

Terkait dengan pembangunan hukum nasional secara khusus mengenai *cyber law* perlu perhatian serius yang diharapkan menjadi undang-undang specialis, maka jiwa undang-undang yang akan mengatur *cyber law* mengandung *philosophy* kehidupan manusia yang adil. Untuk itu dalam pandangan pakar hukum media[25]. menyatakan sebagai berikut :

1. Ketentuan mengenai terorisme dan undang-undang lain terkait cyber terrorism harus sesuai dengan budaya, kondisi masyarakat, stabilitas politik pemerintahan, struktur geografis dan asas keseimbangan antara proteksi HAM serta pembatasan HAM dalam kerangka pandangan legastik-moralistik yang menegaskan pendekatan politik.
2. Penyusunan rumusan delik harus memperhatikan kepentingan keamanan negara (*Nasional Defence*), kepentingan peradilan yang baik (*due process of law*) dan kepentingan perlindungan korban (*victim protection*).
3. Kebijakan kontra terorisme harus tetap memperhatikan mekanisme demokratis dan titik keseimbangan prinsip kebebasan dan prinsip keamanan. Ditegakannya *civil liberties* seperti tetap memperhatikan *non derogable rights*, diantaranya dengan menghormati hak untuk diperlakukan sama di depan hukum. Penghormatan terhadap hak asasi manusia merupakan salah satu syarat berdirinya negara hukum.
4. Terkait dengan kewenangan luar biasa para penegak hukum dalam menangani aksi terorisme pada umumnya dan *cyber terrorism* pada khususnya, maka perlu dipertimbangkannya penerapan *sunset principle*, yaitu pemberlakuan hukum yang bersifat *time limited*, khususnya bagi pasal-pasal yang dimaksudkan untuk memberi kewenangan luar biasa kepada para penegak hukum dalam menangani aksi terorisme; perlu diperhatikannya sistem peradilan pidana yang terpadu sebab proses investigasi melibatkan aparat *non-judicial* seperti Badan Intelejen Nasional (BIN) dan TNI. Selain itu, keterlibatan BIN dan TNI dalam mekanisme *pre-trial* yang diadopsi sistem Anglo Saxon tanpa mengadopsi sistem peradilan akan mengindahkan hak-hak untuk mengajukan keberatan (*harbeas corpus*) sehingga mekanisme praperadilan tidak dapat dilakukan; perlu adanya regulasi yang rinci mengenai *code of conduct, rule of*

[25] Atmasasmita, "Aspek Nasional Dan Global Pemberantasan Terorisme." *p*. 80.

engagement dan ketentuan pidana bagi aparat yang melakukan pelanggaran; diaturnya secara khusus mengenai hak-hak tersangka ataupun terdakwa dan dalam proses penyelidikan dan penyidikan, investigasi dan hearing harus dilakukan sesuai ketentuan Undang-Undang Nomor 5 Tahun 1998 yang melarang penyiksaan dalam proses penyidikan dan penyelidikan.

5. Pengertian terorisme termasuk diantaranya cyber terrorism harus lebih tegas dan jelas bukan berupa ketentuan pasal karet (*un-predictable*).
6. Terorisme hanya dapat dicegah melalui kebijakan negara yang komprehensip untuk membentuk pemerintahan yang demokratis, sejahtera dan tegaknya keadilan. Bersamaan dengan itu perlu diadakannya kerjasama internasional mengingat sifat internet yang beroperasi secara virtual dan lintas batas negara.
7. Sanksi pidana dalam suatu undang-undang *lex specialist* harus ditetapkan dengan memperhatikan syarat-syarat : ketetapan sanksi dalam *lex specialist* tidak boleh lebih rendah dari ketetapan yang tercantum dalam undang-undang lainnya; mempertimbangkan harmonisasi dengan undang-undang lain yang sudah ada terlebih dahulu agar tidak terjadi tumpang tindih produk hukum atau inkonsistensi hukuman; dan sanksi dapat berupa hukuman penjara atau denda.

Permasalahan hukum yang ditimbulkan akibat kejahatan dunia maya (*cyber crime*) seperti *cyber terrorism*, dipandang serius untuk disikapi dengan menghadirkan undang-undang khusus di luar KUHP, seperti halnya ketentuan hukum *cyber law* yang diharapkan dapat menjamin adanya kepastian hukum dalam kejelasan tindak pidana *cyber terrorism*, prediktabilitas dan kepastian hukum dalam mengatasi persoalan *cyber terrorism*.

3.4 *Cyber Terrorism* dalam Aspek Penegakan Hukum Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Hukum pada prinsipnya merupakan pengaturan terhadap sikap tindak perilaku seseorang dan masyarakat yang terhadap pelanggarannya dikenakan sanksi oleh negara. Kendati dunia siber ialah dunia virtual, tapi hukum tetap diperlukan untuk mengatur sikap tindak masyarakat setidaknya disebabkan tiga hal yaitu[26]:

1. Masyarakat yang berada di dunia virtual itu adalah masyarakat yang berasal dari dunia nyata ;
2. masyarakat tersebut memiliki nilai dan kepentingan baik secara sendiri-sendiri maupun bersama-sama yang harus dilindungi;

[26]Sitompul, *Cyberspace, Cybercrimes, Cyberlaw Tinjauan Aspek Hukum Pidana. p.* 38.

3. Meski terjadi di dalam dunia virtual, transaksi yang dilakukan oleh masyarakat memiliki pengaruh dalam dunia nyata, baik secara ekonomis maupun non ekonomis.

Dari alasan di atas itu maka keharusan untuk mengadakan pembangunan hukum nasional atas kebutuhan dan perubahan masyarakat sosial melahirkan *cyber law*, menjadi penting. Ini menunjuk pada hukum yang harus benar-benar difungsikan sebagai "*a tool social of engineering*". Tentunya dimaksudkan agar pembangunan hukum yang ada dan berdampak pada kesejahteraan umat menjadi nyata dan persoalan kepastian hukum menjadi tujuan dalam kehidupan masyarakat yang adil dan damai serta tercapainya negara sejahtera (*welfare state*).

Untuk itu lahirnya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, menjadi hal yang nyata guna mengatasi permasalahan hukum di dalam penyimpangan terhadap penggunaan dunia virtual yang menimbulkan tindak pidana sebagaimana halnya timbulnya berbagai tindak pidana kejahatan dalam dunia *cyber*, yang menjadi sorotan dunia saat ini adalah *cyber terrorism*.

UU ITE merupakan cyberlaw pertama di Indonesia yang mengatur secara khusus tentang informasi dan transaksi elektronik, setelah kehadiran UU telekomunikasi sebelumnya. Materi UU ITE dapat dikelompokan menjadi 2 (dua) bagian besar: (1) Pengaturan informasi dan transaksi elektronik; (2) Pengaturan mengenai perbuatan yang dilarang (*cybercrime*).

Ketentuan *cybercrime* dalam UU ITE mengacu pada EU *Convention Cybercrime* (CoC) yang merupakan instrumen internasional yang digunakan oleh banyak negara.[27] Di dalam CoC diatur mengenai dua jenis *cybercrime* yaitu :

1. *Cybercrime* dalam arti computer *crime* yang diatur ialah kejahatan yang ditujukan terhadap kerahasiaan, integritas, dan ketersediaan data dan sistem komputer dan yang termasuk kategori ini adalah *illegal access*, *illegal interception*, data *interference*, *system interference*, dan *misuse of device*.
2. *Cybercrime* dalam arti *computer-related crime*, ruang lingkup ini adalah computer *related forgery* dan computer-*related fraud*.

CoC juga mengatur kejahatan yang terkait dengan pemroduksian, penyebaran dan penyimpanan konten tertentu, *cyber terrorism* adalah yang dimaksudkan.

Bila dibandingkan pada ketentuan substantif (*substantive law*) dalam CoC dengan perbuatan yang dilarang dalam UU ITE mengenai *cyber crime*, memang terdapat beberapa hal yang harus dilakukan dengan pendekatan secara hukum teknologi (*law is technology*)

[27] *Ibid.*

yaitu yang ditujukan pada kerahasiaan, integritas, ketersediaan informasi elektronik dan system elektronik itu sendiri. Dalam KUHP belum terdapat tindak pidana yang diatur secara cukup hingga diperlukan aturan secara khusus. Sedangkan ketentuan attempt and aiding or abetting dalam CoC tidak diatur secara khusus dalam UU ITE, karena ketentuan dalam KUHP telah cukup. Ini berarti dapat dikatakan bahwa *teori technology is law* juga diterapkan.

Perkembangan bentuk-bentuk *cyber crime* sangat cepat seiring dengan perkembangan teknologi informasi yang berbasis pada komputer, dan UU ITE serta RUU KUHP telah merespon dengan upaya penegakan hukum *cyber*. Dalam penegakan hukum terhadap tindak pidana *cyber terrorism*, hendaknya aparat hukum dan hakim sebagai pemberi keadilan dapat menggunakan ketentuan UU ITE dan KUHP sesuai dengan tindak kejahatan yang dilakukan, agar keadilan yang diinginkan untuk melindungi negara dan warga negara dapat tercapai.

4. Kesimpulan

Kejahatan dunia maya (*cyber crime*) merupakan fenomena sosial yang terjadi di ruang maya, sejatinya adalah kejahatan secara konvensional yang berpindah ruang di dalam dunia maya, namun esensinya sama yaitu melakukan tindak pidana kejahatan dengan penggunaan kemajuan teknologi adalah komputer dengan program internet sebagai alat (*tool*) dalam melakukan tindak pidana kejahatan.

Konsekuensi logis atass kemajuan teknologi menimbulkan kejahatan yang berbasis teknologi dalam penyalahgunaan komputer (*computer misuse*), yang banyak dikenal dengan istilah kejahatan dunia maya (*cyber crime*).

Kejahatan dunia maya ini termasuk di dalamnya adalah kejahatan terorisme (*cyber terrorism*). Tindak pidana terorisme menjadi perhatian dunia, karena sifatnya yang melakukan teror dengan menggunakan perangkat komputer (*computer related crime*) dalam melakukan aksi tindak pidana terorismenya tentunya dengan *convergance* teknologi memudahkan kejahatan terorisme dalam ruang maya bergerak leluasa disebabkan jangkauan sasaran dan objek yang dituju bersifat tanpa batas (*borderless*).

Cyber terrorism dinyatakan sebagai kejahatan yang luar biasa (*extra ordinary crime*) dan semua negara menyoroti tindak kejahatan ini yang berdampak pada gangguan keamanan negara dan setiap orang yang menjadi warga negara tidak merasa aman dan tenang oleh aksi kejahatan teroris yang mulai berinvasi ke dalam ruang maya (*cyber space*). Kejahatan terorisme dikatakan *extra ordinary crime* itu karena sifat kejahatan teroris kini bergerak melakukan aksinya melampaui batas negara dan terorganisir (*transnational organice crime*).

Cyber crime adalah satu diantara perkembangan kejahatan berbasis teknologi yang membawa permasalahan di bidang hukum. Kejahatan di ruang dunia maya (*cyber crime*) dalam dunia virtual ini merupakan kejahatan modern yang bersifat kompleks, rumit dan tidak mengenal batas waktu/ruang (*borderless*), memerlukan penanganan hukum secara khusus *lex specialis* dalam menghadirkan perangkat hukum yang berkaitan dengan penegakan hukum dunia maya (*cyber law*).

Untuk memenuhi kebutuhan masyarakat pencari keadilan maka lahir Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang saat ini menjadi hukum cyber law pertama di Indonesia yang dapat dijadikan upaya penegakan hukum dalam menyelesaikan permasalahan kejahatan dunia maya (*cyber crime*) meski diakui masih jauh dari harapan dalam melakukan penegakan hukum.

Undang-Undang ITE setelah berjalan ternyata tidak efektif dan belum mampu menjawab persoalan hukum dalam mengatasi perkembangan kejahatan di ruang dunia maya yang semakin berkembang khususnya kejahatan terorisme (*cyber terrorism*), yang secara intensif menyebarkan kebencian (*hate speech*) dalam melakukan aksi terorisme-nya.

Cyber Terrorism perlu diatur secara khusus dalam ketentuan Undang-Undang khusus tentang penyalahgunaan komputer/*cyber crime* atau diatur dalam bab regulasi *cyber crime law* Indonesia yang harus disegerakan. Itu berarti perlunya dilakukan revisi terhadap Undang-Undang ITE agar dapat menyempurnakan penyelesaian permasalahan hukum dalam hal tindak pidana terhadap Informatika dan telematika, terkait penegakan hukum atas tindak pidana terorisme (*cyber terrorism*) dan kejahatan *cyber* (*cyber crime*) lainnya, yang banyak merugikan orang lain dan mengancam keamanan setiap orang dan keamanan negara secara luas.

Bibliography

A. Book

Golose, Petrus Reinhard. *Invasi Terrorisme Ke Cyberspace*. Jakarta: YPKIK, 2015.

Hamzah, Andi. *Aspek-Aspek Pidana Di Bidang Komputer*. Jakarta: Ghalia, 1989.

Indonesia, Institut Komputer. *Pengenalan Komputer (Introducing to Computer)*. Jakarta: Institut Komputer Indonesia, 1981.

Indonesia, Kejaksaan Agung Republik. *Panduan Penanganan Perkara Tindak Pidana Terorisme Kejaksaan Agung Republik Indonesia*. Cet ke I., 2013.

Kusamaatmadja, Mochtar. *Pengantar Hukum Internasional,*. 9th ed. Bandung: Putra Abardin, 1999.

Maskun. *Kejahatan Siber (Cyber Crime) Suatu Pengantar*. Jakarta: Kencana Prenada Media, 2013.

Nusantara, Abdul Hakim G. *Undang-Undang Pemberantasan Tindak Pidana Terorisme Dalam Perspektif Negara Hukum*. Bandung: Badan Pembinaan Hukum Nasional, 2003.

Sitompul, Josua. *Cyberspace, Cybercrimes, Cyberlaw Tinjauan Aspek Hukum Pidana*. Jakarta: Tatanusa, 2012.

Widodo. *Sistem Pemidanaan Dalam Cyber Crime*. Yogyakarta: Laksbang Mediatama, 2010.

Wisnubroto, AI. *Strategi Penanggulangan Kejahatan Telematika*. Yogyakarta: Atma Jaya, 2010.

B. Journal

Atmasasmita, Romli. "Aspek Nasional Dan Global Pemberantasan Terorisme." *Jurnal Hukum Internasional* 2, no. 3 (2003).

Koops, Jaap, Miriam Lips, Corien Prins, and Maurice Scellekens, eds. *Starting Points for ICT Regulation, Deconstructing Prevalent Policy One-Liners*. *IT & Law Series*. Vol. 9. The Haque, 2006.

C. Proceeding

Ahmadjayadi, Cahyana. "Dampak Teknologi Komunikasi Dan Informasi Terhadap Kegiatan Terorisme." Bandung: Badan Pembinaan Hukum Nasional, 2003.

Vatis, Michael. "Cyber-Terrorism and Information Warfare Threats and Responses." In *The Terrorism Studies Program at The George Washington University*. Washington: The Potomac Institute for Policy Studies, 1998.

D. Regulation

Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. Jakarta, Indonesia: Lembaran Negara Republik Indonesia Tahun 2008 No. 58, Tambahan Lembaran Negara Republik Indonesia No. 4843, 2008.

Undang-Undang Republik Indonesia Nomor 15 Tahun 2003 Tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2002 Tentang Pemberantasan Tindak Pidana Terorisme, Menjadi Undang-Undang. Jakarta: Lembaran Negara Republik Indonesia Tahun 2003 No. 45, Tambahan Lembaran Negara Republik Indonesia No. 4284, 2003.