TINDAK PIDANA DUNIA MAYA BERUPA VIRUS DAN TROJAN HORSE MENURUT UU NO. 11 TAHUN 2008 TENTANG ITE

Marco Orias
Universitas 45 Surabaya
Indonesia
Email : Marcoori2703@gmail.com

Abstract

Cybercrime or crime at cyberspace has many forms or shapes, hacking is The first crime, also seen from The technical aspects, hacking have excess. First, The man who hacking must be can do other forms of cybercrime with ability to enter into computer system and then broke that system. Second, technically the quality of the hacking result from hacking that more seriously if compared with other forms of cybercrime, such as viruses and The Trojan Horse. As that becomes problem in this research is how an arrangement crime of Virus and The Trojan Horse, and how the law enforcements tackling crime of Virus and The Trojan Horse. Research approach used normative juridical. This approach leads to laws and regulations as a major study of law and behavior of the perpetrator that wrongly use technology and information as concrete support to strengthening that juridical analysis. Result of research indicated that the role of law enforcement in handling crimes of Viruses and Trojan Horse that exercised so far was still very minimal.This cause many obstacles found by law enforcements, the existing statuary barriers, constraints of investigation, and the resistance of the people themselves.The most important thing is the system verification in order to cope with the crime of Viruses and Trojan Horse through repair or revision of existing statuary barriers, whether Law No.11 Year 2008 and The other regulation that related with The crimes of Viruses and The Trojan Horse.

Keyword**: **Criminal Act; Cyberspace; Viruses; and The Trojan Horse.

Abstrak

Kejahatan dunia maya atau kejahatan di dunia maya memiliki banyak bentuk,peretasan adalah kejahatan pertama, juga dilihat dari aspek teknis, peretasan memiliki kelebihan , pertama orang yang melakukan peretasan harus bisa melakukan bentuk lain cybercrime dengan kemampuan masuk ke sistem computer dan kemudian merusak sistem itu. Kedua, secara teknis kualitas hasil peretasan dari peretasan itu lebih serius jika dibandingkan dengan bentuk-bentuk cybercrime lainnya, seperti Virus dan *Trojan Horse*.Adapun yang menjadi masalah dalam penelitian ini adalah bagaimana suatu pengaturan kejahatan Virus dan *Trojan Horse* dan bagaimana penegakan hukum yang menangani kejahatan Virus dan *Trojan Horse*.Pendekatan penelitian menggunakan yuridis normatif. Pendekatan ini mengarah pada hukum dan perilaku pelaku yang salah menggunakan teknologi dan informasi sebagai dukungan kongkrit untuk memperkuat analisis yuridis tersebut. Hasil penelitian menunjukkan bahwa peran penegak hukum dalam menangani kejahatan Virus dan *Trojan Horse* yang dilakukan selama ini masih sangat minim. Hal ini menyebabkan banyak hambatan yang ditemukan oleh penegak hukum, hambatan hukum yang ada, kendala penyelidikan ,dan perlawanan masyarakat itu sendiri.Yang paling penting adalah verifikasi sistem untuk mengatasi kejahatan Virus dan *Trojan Horse* melalui perbaikan atau revisi baru hukum yang ada, apakah UU No.11 Tahun 2008 dan Peraturan lain yang terkait dengan Kejahatan Virus dan *Trojan Horse*.

Kata Kunci : Dunia Maya; Tindakan kriminal; Virus; dan *Trojan Horse*.

A. PENDAHULUAN

Cyber Crime dapat diartikan sebagai perbuatan melawan hukum dan/atau tanpa hak berbasis TI atau dengan memakai komputer dan/atau jaringan komputer sebagai sarana atau alat sehingga menjadikan komputer dan/atau jaringannya sebagai obyek maupun subyek tindak pidana yang dilakukan dengan sengaja.Selanjutnya dalam catatan ini saya memakai cyber crime sebagai tindak pidana TI dalam kaitannya dengan tindak pidana yang tidak diatur secara khusus dalam Kitab Undang-Undang Hukum Pidana (selanjutnya disebut KUHP). Kejahatan yang seringkali berhubungan dengan internet antara lain penyebaran Virus dan *Trojan Horse* sebagai kejahatan yang dapat dilakukan melalui kecanggihan TI dan komunikasi dalam hal ini melalui penyalahgunaan media internet. *The Trojan Horse*, diartikan sebagai suatu prosedur untuk menambah, mengurangi atau mengubah instruksi pada sebuah program, sehingga program tersebut selain menjalankan tugas yang sebenarnya juga akan melaksanakan tugas lain yang tidak sah. Tindakan ini dapat dikategorikan sebagai tindak pidana penggelapan (Pasal 372 dan 374 KUHP). Ketika berhadapan dengan tindak pidana penyebaran Virus dan *Trojan Horse* menimbulkan masalah baru yang akan muncul, karena dalam hukum acara pidana yang berlaku tidak diatur mengenai alat bukti elektronik. Namun demikian, saat ini telah berlaku Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik (selanjutnya disebut UU ITE) yang didalamnya mengatur berbagai aktifitas yang dilakukan dan terjadi di dunia maya, termasuk pelanggaran hukum yang terjadi. Salah satu pelanggaran hukum tersebut adalah penyebaran Virus dan *Trojan Horse*. UU ITE telah mengatur tentang pembuktian yang menyangkut TI termasuk internet, tetapi masih banyak kendala-kendala dalam kenyataannya sehingga seringkali pelaku penyebaran Virus dan *Trojan Horse* melalui internet lolos dari jeratan hukum. UU ITE ini mempunyai 13 (tiga belas) Bab dan 54 (lima puluh empat) Pasal di dalamnya yang mengatur berbagai kegiatan di dunia siber serta menerapkan azas-azas Ekstra Teritorial. Azas Kepastian Hukum, Azas Manfaat, Azas Kehati-hatian, Azas Itikad Baik dan Azas Netral Teknologi.

Berdasarkan uraian latar belakang diatas, dirumuskan permasalahan sebagai berikut :

1. Bagaimana pengaturan tindak pidana penyebaran Virus dan *Trojan Horse* dengan UU ITE?
2. Bagaimana tanggung jawab pidana terhadap pelaku tindak pidana penyebaran Virus dan *Trojan Horse*?

2. METODE PENELITIAN

1. Metode Pendekatan

   Metode pendekatan yang digunakan adalah pendekatan yuridis normatif, yaitu berdasarkan ketentuan/peraturan perundang-undangan yang berlaku dihubungkan dengan permasalahan yang telah dikemukakan.
2. Sumber Bahan Hukum

   Sumber bahan hukum meliputi : Bahan hukum Primer yaitu bahan hukum yang mempunyai kekuatan mengikat. yaitu : KUHP, UU ITE, Kitab Undang-Undang Hukum Acara Pidana (selanjutnya disebut KUHAP). Bahan hukum Sekunder yaitu bahan hukum yang memberikan penjelasan dari bahan hukum primer. Bahan hukum Tertier yaitu bahan hukum yang memberikan petunjuk dan penjelasan terhadap bahan hukum primer dan bahan hukum sekunder.
3. Teknik Pengumpulan Bahan Hukum

   Teknik pengumpulan bahan hukum dilakukan dengan cara : Inventarisasi peraturan perundang-undangan baik secara vertikal dan horizontal.
4. Teknik Pengolahan Bahan Hukum

   Teknik pengolahan bahan hukum dilakukan dengan cara : Bahan kepustakaan dikumpulkan lalu melakukan penelusuran yang berkaitan dengan tindakan pidana dunia maya berupa Virus dan *Trojan Horse*.

5. Analisis Bahan Hukum

Analisis Bahan Hukum menggunakan metode deduktif yaitu bahan hukum yang dikualifikasikan kemudian di analisa sehingga dapat memberikan gambaran permasalahan yang ada.

C. PEMBAHASAN

1. Pengaturan Tindak Pidana Virus dan *Trojan Horse* dengan UU ITE

Pasal 1 ayat (1) UU ITE memberikan pengertian 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. Selain itu, yang dimaksud dengan sistem elektronik menurut Pasal 1 ayat (5) adalah serangkaian perangkat atau prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan dan/atau menyebarkan informasi elektronik.

Penafsiran dengan metode yang sama terhadap KUHP sebelum ada UU ITE perlu dilakukan tentang pengertian dalam UU ITE sehingga terdapat batasan dan kejelasan makna agar tidak menimbulkan celah hukum (*loopholes*),yaitu :

'Melakukan tindakan apapun yang berakibat terganggunya sistem elektronik'

Pasal 33 UU ITE menyebutkan bahwa:

"Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apapun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya".

Sehubungan dengan hal itu, setiap orang yang melakukan tindakan apapun yang berakibat terganggunya sistem elektronik karena banyak kegiatan-kegiatan di dunia nyata yang secara nyata tidak ada hubungannya dengan *cybercrime* sehingga kalimat dari pasal ini kegiatan penyebaran Virus dapat dikategorikan sebagi suatu tindak kejahatan.

Pada kasus penyebaran Virus dan*Trojan Horse* ini untuk membuktikannya, dapat dipakai semua alat bukti berbentuk informasi dan/atau dokumen elektronik, namun hal tersebut dapat dijadikan alat bukti sebagaimana ditentukan dalam Pasal 5 ayat (1) UU ITE yang berbunyi :

"Informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah".

Pasal 5 ayat (2) UU ITE juga menegaskan bahwa :

"Informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya sebagaimana dimaksud pada ayat 1 merupakan perluasan dari alat bukti yang sah sesuai dengan hukum acara yang berlaku di Indonesia".

Dengan demikian, alat bukti yang digunakan hakim untuk menjatuhkan putusan pada perkara pidana, dapat diperluas menjadi 6 (enam) dari 5 (lima) ketentuan alat bukti sebagaimana telah diatur dalam Pasal 184 KUHAP, yaitu bahwa alat bukti yang sah adalah :

1. Keterangan saksi;
2. Keterangan ahli;
3. Surat;
4. Petunjuk;
5. Keterangan terdakwa;
6. Alat bukti menurut Pasal 5 ayat (1) dan ayat (2) UU ITE.

Meskipun ketentuan mengenai alat bukti di atas merupakan ketentuan hukum acara pidana yang bersifat memaksa (*dwingen recht*), artinya semua jenis alat bukti yang telah di atur dalam pasal tersebut tidak dapat ditambah atau dikurangi.

Secara umum terdapat beberapa teori mengenai sistem pembuktian yakni :

1. *Conviction in time Theory*, yaitu sistem pembuktian yang menyatakan bahwa salah tidaknya seorang terdakwa semata-mata ditentukan oleh penilaian keyakinan hakim. Keyakinan hakim ini didapat diperoleh melalui alat-alat bukti yang diajukan Keterangan Ahli dalam persidangan.
2. *Conviction Raisonee Theory*, merupakan sistem pembuktian berdasarkan keyakinan hakim untuk menentukan salah tidaknya terdakwa, namun dalam sistem ini keyakinan hakim dibatasi dan harus didasari dengan alasan-alasan yang jelas dan dapat diterima yang wajib diuraikan dalam putusannya, sesuai yang diuraikan juga oleh Keterangan Ahli dalam persidangan.
3. Teori Pembuktian Menurut Undang-Undang secara Positif, merupakan pembuktian yang berlatar belakang sistem pembuktian berdasarkan keyakinan atau *Conviction in timeTheory*. Pembuktian pada sistem ini didasari dengan alat-alat bukti yang sah yang telah di tetapkan oleh undang-undang disertai keyakinan hakim dalam menentukan salah tidaknya terdakwa.
4. Teori Pembuktian menurut Undang-Undang Secara Negatif (*Negatief Wettelijke stelsel*), merupakan sistem pembuktian yang menggunakan teori perpaduan antara sistem pembuktian undang-undang secara positif dengan sistem pembuktian menurut keyakinan atau *Conviction in time Theory*. Rumusan teori ini adalah bahwa salah tidaknya seorang terdakwa ditentukan oleh keyakinan hakim yang didasarkan pada cara dan dengan alat-alat bukti yang sah menurut undang-undang.

Sementara itu, sistem pembuktian yang dianut oleh KUHAP adalah sistem pembuktian menurut undang-undang secara negatif, karena merupakan perpaduan antara sistem pembuktian menurut undang-undang secara positif dengan sistem pembuktian menurut keyakinan atau *Conviction in time Theory*. Hal ini terlihat dari ketentuan Pasal 183 KUHAP yang menegaskan bahwa :

"Hakim tidak boleh menjatuhkan pidana kepada seseorang kecuali apabila dengan sekurang-kurangnya dua alat bukti yang sah ia memperoleh keyakinan bahwa suatu tindak pidana benar-benar terjadi dan bahwa terdakwalah yang bersalah melakukannya."

Berkaitan dengan alat bukti petunjuk, tidak terlepas dari ketentuan Pasal 188 Ayat (2) KUHAP yang membatasi kewenangan hakim dalam memperoleh alat bukti petunjuk, yang secara limitatif hanya dapat diperoleh dari :

1. Keterangan saksi;
2. Surat;
3. Keterangan Terdakwa.

Berdasarkan hal tersebut diatas, alat bukti petunjuk hanya dapat diambil dari ketiga alat bukti di atas. Pada umumnya, alat bukti petunjuk baru diperlukan apabila alat bukti lainnya belum mencukupi batas minimum pembuktian yang diatur dalam Pasal 183 KUHAP di atas.

Dengan demikian, alat bukti petunjuk merupakan alat bukti yang bergantung pada alat bukti lainnya yakni alat bukti saksi, surat dan keterangan terdakwa. Alat bukti petunjuk memiliki kekuatan pembuktian yang sama dengan alat bukti yang lain, namun hakim tidak terikat atas kebenaran persesuaian yang diwujudkan oleh petunjuk, sehingga hakim bebas untuk menilai dan mempergunakannya dalam upaya pembuktian. Selain itu, petunjuk sebagai alat bukti tidak dapat berdiri sendiri membuktikan kesalahan terdakwa, karena hakim tetap terikat pada batas minimum pembuktian sesuai ketentuan Pasal 183 KUHAP.

Informasi elektronik atau dokumen elektronik sebagai alat bukti, yang merupakan perluasan dari alat bukti surat sebagai bahan untuk dijadikan petunjuk bagi hakim dalam membuktikan suatu perkara termasuk kasus penyebaran Virus dan *Trojan Horse* yang telah diuraikan pada bagian sebelumnya.

Cyber Crime yang merupakan suatu upaya memasuki atau menggunakan fasilitas komputer atau jaringan komputer tanpa ijin dan melawan hukum atau tanpa menyebabkan perubahan atau kerusakan pada fasilitas komputer yang dimasuki atau digunakan

tersebut atau kejahatan yang dengan menggunakan sarana media elektronik internet (merupakan kejahatan dunia maya) atau kejahatan dibidang komputer dengan secara illegal, dan terdapat definisi yang lain yaitu sebagai kejahatan komputer ditujukan kepada sistem atau jaringan komputer, yang mencakup segala bentuk baru kejahatan yang menggunakan bantuan sarana media elektronik internet.

Cyber Crime merupakan suatu tindak kejahatan didunia alam maya, yang dianggap bertentangan atau melawan undang-undang yang berlaku, oleh karena untuk menegakkan hukum serta menjamin kepastian hukum di Indonesia perlu adanya *Cyber Law* yaitu hukum yang mengatasi kejahatan siber (kejahatan dunia maya melalui jaringan internet). TI menyentuh setiap aspek kehidupan modern dan tidak menutup kemungkinan dapat menimbulkan kejahatan dalam dunia maya. Salah satu kejahatan di dunia maya (*cyber crime*) ini adalah penyebaran Virus dan*Trojan Horse*.

Virus yang merupakan suatu program komputer yang menduplikasi atau menggandakan diri dengan menyisipkan salinannya ke dalam media penyimpanan dokumen serta ke dalam jaringan komputer secara diam-diam tanpa sepengetahuan pengguna komputer tersebut, mempunyai efek sangat beragam mulai dari munculnya pesan-pesan aneh, sampai pada tahap merusak dokumen atau *file* dan bahkan dapat merusak jaringan computer itu sendiri. Virus komputer ini berasal dari penciptaan pengguna computer yang dengan sengaja menyebarkan virus tersebut ke seluruh dunia. Virus computer yang dimaksud sangat beragam dengan nama tersendiri dan daya rusak tersendiri pula.

Trojan Horse atau Kuda Troya atau yang lebih dikenal sebagai *Trojan* dalam keamanan computer merujuk kepada sebuah bentuk perangkat lunak yang mencurigakan (*malicioussoftware/malware*) yang dapat merusak sebuah sistem atau jaringan. Tujuan dari *Trojan Horse* adalah memperoleh informasi dari target (password, kebiasaan user yang tercatat dalam sistem log, dan data), serta mengendalikan target (memperoleh hak akses pada target). *Trojan Horse* berbeda dengan perangkat lunak mencurigakan lainnya seperti virus komputer atau *worm* karena : *Trojan Horse* bersifat "*stealth*" (siluman dan tidak terlihat) dalam operasinya dan seringkali berbentuk seolah-olah program tersebut merupakan program baik-baik, sementara virus komputer atau worm bertindak lebih agresif dengan merusak sistem atau membuat sistem menjadi crash dan *Trojan Horse* dikendalikan dari komputer lain (komputer *attacker*). Penggunaan istilah *Trojan Horse* dimaksudkan untuk menyusupkan kode-kode mencurigakan dan merusak di dalam sebuah program baik-baik dan berguna ; seperti halnya dalam Perang Troya, para prajurit Sparta bersembunyi di dalam Kuda Troya yang ditujukan sebagai pengabdian kepada Raja Poseidon. Kuda Troya tersebut menurut para petinggi Troya dianggap tidak berbahaya, dan diijinkan masuk ke dalam benteng Troya yang tidak dapat ditembus oleh para prajurit Yunani selama kurang lebih 10 perang Troya bergejolak.

Kebanyakan *Trojan Horse* saat ini berupa sebuah berkas yang dapat dieksekusi (*.EXE atau *.COM dalam sistem operasi Windows dan DOS atau program dengan nama yang sering dieksekusi dalam sistem operasi UNIX, seperti ls, cat, dan lain-lain) yang dimasukkan ke dalam sistem yang ditembus oleh seorang *cracker* untuk mencuri data yang penting bagi pengguna (*password*, data kartu kredit, dan lain-lain). *Trojan Horse* juga dapat menginfeksi sistem ketika pengguna mengunduh aplikasi (seringnya berupa game computer) dari sumber yang tidak dapat dipercayai dalam jaringan internet. Aplikasi-aplikasi tersebut dapat memiliki kode *Trojan Horse* yang diintegrasikan di dalam dirinya dan mengijinkan seorang *cracker* untuk mengacak-acak sistem yang bersangkutan.

a. Pembobolan Komputer dan/atau Sistem Elektronik

Larangan melakukan perbuatan membobol sistem komputer yang diatur dalam UU ITE terdiri atas :

(a) Membobol komputer dan/atau sistem elektronik yang bertujuan untuk mengakses saja tanpa tujuan lain. Larangan perbuatan ini diatur dalam pasal 30 ayat (1) yang berbunyi :

"Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau sistem Elektronik milik orang lain dengan cara apa pun".

(b) Membobol komputer dan/atau sistem elektronik yang selain bertujuan untuk mengakses adalah juga memperoleh informasi elektronik dan/atau dokumen elektronik. Larangan perbuatan ini diatur dalam pasal 30 ayat (2) yang berbunyi :

"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".

(c) Membobol komputer dan/atau sistem elekronik yang bertujuan selain untuk mengakses juga untuk menaklukkan sistem pengamanan dari sistem komputer yang diakses itu. Larangan perbuatan ini diatur dalam pasal 30 ayat (3) yang berbunyi :

"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 pengaman".

b. Tindak Pidana Komputer terhadap Sistem Elektronik

Larangan terhadap perbuatan ini di atur dalam pasal 33 yang berbunyi :

"Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apapun yang berkaitan terganggunya sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya'.

Tindakan untuk menyebarkan virus dan *Trojan Horse* ini dapat diangap sebagai suatu perbuatan yang layak dipidana, karena sepintas terlihat bahwa pelaku penyebaran virus dan *Trojan Horse* melalui pengiriman email ini memiliki niat untuk merusak dokumen bahkan komputernya, sehingga dapat merugikan pihak lain, dengan demikian terdapat unsur pertanggungjawaban pidana di dalamnya. Perbuatan menyebarkan virus dan *Trojan Horse* melalui pengiriman *email* ini tidak diatur secara spesifik dalam KUHP. Saat ini, walaupun di Indonesia telah ada UU ITE, tetapi tindakan penyebaran virus dan *Trojan Horse* melalui pengiriman *email* juga tidak diatur khusus. Namun demikian Pasal 33 dan Pasal 30 ayat (2) UU ITE yang menegaskan beberapa perbuatan yang dilarang dan diancam sanksi pidana, termasuk larangan mengakses komputer dan atau sistem elektronik pihak lain searah melawan hukum, sehingga perbuatan menyebarkan virus dan *Trojan Horse* dapat dianggap sebagai sebuah tindak pidana.

2. Tanggung jawab Pidana Terhadap Pelaku Penyebaran Virus dan *Trojan Horse* Berdasarkan UU ITE.

Ada beberapa hal yang dapat dilakukan terhadap pelaku penyebaran virus dan *Trojan Horse* ini, yakni : pendekatan teknologi, pendekatan budaya-etika dan pendekatan hukum. Untuk mengatasi gangguan keamanan, pendekatan teknologi mutlak untuk dilakukan, karena tanpa suatu pengamanan melalui teknologi tertentu, maka jaringan akan mudah disusupi, diintersepsi atau diakses secara illegal dan tanpa hak. Pada ruang *cyber* pelaku pelanggaran seringkali menjadi sulit untuk dijerat hukum, karena tidak terpenuhinya unsur-unsur suatu ketentuan hukum, dalam hal ini berhubungan dengan masalah pembuktian.Selain itu, seringkali pengadilan di Indonesia tidak memiliki yurisdiksi terhadap pelaku dan perbuatan hukum yang terjadi, mengingat pelanggaran

hukum ini bersifat transnasional yang akibat hukumnya memiliki implikasi hukum di Indonesia. Berdasarkan hukum internasional, terdapat tiga macam yurisdiksi yakni: yurisdiksi untuk menetapkan undang-undang (*The Jurisdiction to prescribe*), yurisdiksi untuk penegakan hukum (*TheJurisdiction to enforce*), dan yurisdiksi untuk menuntut (*The Jurisdiction to adjudicate*).

Berbicara mengenai *cyber spamming* sebagai kejahatan transnasional erat kaitannya dengan beberapa yurisdiksi yaitu yurisdiksi untuk menetapkan undang-undang (*TheJurisdiction to Prescribe*), yurisdiksi untuk menghukum (*The Juridicate to Enforce*) dan yurisdiksi untuk menuntut (*The Jurisdiction Adjudicate*). Pada *The Jurisdiction toAdjudicate* terdapat beberapa asas yang dikenal dalam menentukan hukum yang berlaku yaitu:

a. *Asas Subjective Territorial* yaitu berlaku hukum yang menekankan berdasarkan bahwa keberlakuan hukum ditentukan berdasarkan tempat pembuatan dan penyelesaian tindak pidana di lakukan di Negara lain;
b. *Asas Objective Territorial* yang menyatakan bahwa hukum yang berlaku adalah hukum dimana akibat utama perbuatan itu terjadi dan memberikan dampak yang sangat merugikan bagi Negara yang bersangkutan;
c. *Asas Aktif Nationality* yang menentukan bahwa Negara memiliki yurisdiksi untuk menentukan hukum berdasarkan kewarganegaraan pelaku;
d. *Asas Passive Nationality* adalah hukum berlaku berdasarkan kewarganegaraan korban;
e. *Asas Protective Principle* adalah berlakunya berdasarkan atas keinginan Negara untuk melindungi kepentingan Negara dari kejahatan yang dilakukan di luar wilayahya, dalam hal ini digunakan apabila korban adalah Negara atau pemerintahan;
f. *Asas Protective Principle* adalah berlakunya berdasarkan atas keinginan Negara untuk melindungi kepentingan Negara dari kejahatanyangdilakukandiluarwilayahnya, dalam hal ini digunakan apabila korban adalah Negara atau pemerintahan;
g. *Asas Universality* yang pada mulanya menentukan bahwa setiap Negara berhak untuk menangkap dan menghukum para pelaku (*cybercrime*) kemudian diperluas sampai pada kejahatan terhadap kemanusiaan, dan berlaku untuk lintas Negara terhadap kejahatan yang diangggap sangat serius seperti pembajakan dan terorisme (*crime againsthumanity*).

Tindak pidana penyebaran Virus dan *Trojan Horse* dimungkinkan melibatkan lebih dari satu sistem atau menyangkut sistem hukum beberapa negara, sehingga dapat dikategorikan sebagai kejahatan transnasional. Pada praktiknya terdapat banyak faktor yang menyebabkan adanya kepentingan lebih dari satu negara dalam suatu kejahatan, baik pelakunya, korbannya, tempat terjadinya kejahatan atau perpaduan unsur-unsur tersebut.

Tindak pidana penyebaran Virus dan *Trojan Horse* dapat melibatkan orang-orang dari berbagai negara, menjadikan sebagai kejahatan transnasional, sehingga dalam proses penegakan hukumnya, harus pula memperhatikan jalinan kerjasama antara kepolisian Indonesia dengan negara-negara lain. Berbicara mengenai *cyber spamming* sebagai kejahatan transnasional erat kaitannya dengan beberapa yurisdiksi yaitu, yurisdiksi untuk menetapkan undang-undang (*TheJuridiction to Prescribe*), yurisdiksi untuk menghukum (*The Juridicate to Enforce*) dan yurisdiksi untuk menuntut (*The Jurisdiction to Adjudicate*). Dengan demikian, tindakan hukum yang dapat dilakukan terhadap pelaku penyebaran Virus dan *Trojan Horse* harus dilakukan sesuai yurisdiksinya dengan memperhatikan hukum yang berlaku.

Apabila telah terbukti bahwa penyebaran Virus melalui pengiriman *email* termasuk perbuatan yang dilarang sebagaimana diatur dalam Pasal 33 UU ITE, maka pelaku dapat dijerat dengan ketentuan ancaman pidana pada Pasal 49 UU ITE yang berbunyi :

"Setiap Orang yang memenuhi unsur se-

bagaimana dimaksud dalam Pasal 33, dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp. 10.000.000.000,00 (sepuluh miliar rupiah).”

Apabila telah terbukti bahwa penyebaran *Trojan Horse* melalui pengiriman *email* termasuk perbuatan yang dilarang sebagaimana diatur dalam Pasal 30 ayat (2) UU ITE, maka pelaku dapat dijerat dengan ketentuan ancaman pidana pada Pasal 46 ayat (2) UU ITE yang berbunyi:

“Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp.700.000.000,00 (tujuh ratus juta rupiah).”

Ketentuan tersebut sudah sesuai dengan tindak pidana penyebaran Virus dan *TrojanHorse*, mengingat cakupan wilayah penyebarannya yang transnasional serta dampak kerugian yang ditimbulkan Virus secara umum yakni dapat menyebabkan antara lain: loading start sistem operasi Windows (*98, XP, Vista, Seven*, dll) menjadi lambat, terdapat file yang tidak dapat dibuka (muncul pesan error), bahkan ada file yang hilang meski telah disimpan di *Hard disk* dan media penyimpanan lain seperti Disket, *Flashdisk, Hard Disk External*, dll. Sedangkan dampak kerugian yang ditimbulkan *Trojan Horse* secara umum yakni dapat menyebabkan antara lain: penyusupan pada data *log history* user computer dan pengintaian terhadap data/ dokumen dengan *extension**.doc, *.xlx, *.txt; dimana pada umumnya user menyimpan data *user name* maupun *password* untuk akses *e-banking*, dan akses sebagai member dari sebuah toko online atau website jual beli (www.jual beli.com, www.berniaga.com, www.kaskus.co.id, dll), computer beroperasi dengan lambat, terkadang ada file yang tidak dapat dibuka bahkan hilang dari computer dan media penyimpanan data lainnya. Di Indonesia sendiri saya memperkirakan setidaknya ada 1 (satu) dari 3 (tiga) komputer/laptop pasti telah terinfeksi virus / *Trojan Horse* (terutama computer / laptop yang program anti virusnya tidak rutin *update virusdefinition* secara otomatis dan periodik), sehingga saya menilai bahwa ancaman pidana tersebut diatas cukup berat bagi pelakunya. Sehingga menurut saya tidak perlu ada hukuman minimal dari ancaman pidana penjara dan/atau denda pada Pasal 49 dan Pasal 46 ayat (2) UU ITE, karena dapat dinilai bahwa ancaman pidana tersebut diatas cukup setimpal bagi pelakunya.

D. KESIMPULAN

Perbuatan penyebaran Virus dan Trojan Horse melalui email merupakan salah satu perbuatan yang dilarang sebagaimana diatur dalam UU ITE, karena dalam hal ini email dianggap sebagai informasi dan/atau dokumen elektronik yang dapat dijadikan salah satu alat bukti sebagaimana diatur dalam pasal 5 ayat (1) dan (2) UU ITE. Selain itu, email dapat pula dianggap sebagai alat bukti surat yang selanjutnya dijadikan alat bukti petunjuk sesuai ketentuan Pasal 184 KUHAP. Dengan demikian, tindakan penyebaran Virus dapat dijerat dengan Pasal 33 juncto Pasal 49 UU ITE, sedangkan tindakan penyebaran *Trojan Horse* dijerat dengan Pasal 30 ayat (2) juncto Pasal 46 ayat (2) UU ITE.

Tindakan hukum yang dapat dilakukan terhadap pelaku penyebaran Virus dan *Trojan Horse* antara lain dengan tuntutan secara hukum dengan memperhatikan yurisdiksi dan hukum yang berlaku, karena hal ini dimungkinkan pelaku berada di negara yang berbeda dengan negara tempat korban kejahatan ini berada, selain itu, sulit pula menentukan tempat kejadian (*locus delicti*) karena kejahatan ini terjadi di dunia maya. Namun demikian yurisdiksi dan hukum yang berlaku dapat ditentukan berdasarkan beberapa asas yang berlaku antara lain Asas *Subjective Territorial* yaitu berlaku hukum berdasarkan tempat pembuatan dan penyelesaian tindak pidana dilakukan di Negara lain, Asas *Objective Territorial* yaitu

hukum yang berlaku adalah akibat utama perbuatan itu terjadi dan memberikan dampak kerugian bagi negara yang bersangkutan. Asas *Nationality* adalah hukum berlaku berdasarkan kewarganegaraan pelaku, Asas *PassiveNationality* adalah hukum berlaku berdasarkan kewarganegaraan korban, Asas *ProtectivePrinciple* adalah berlakunya berdasarkan atas keinginan negara untuk melindungi kepentingan negara dari kejahatan yang dilakukan di luar wilayahnya dan Asas *Universality* adalah yang berlaku untuk lintas negara terhadap kejahatan yang dianggap sangat serius seperti pembajakan dan terorisme (*crime against humanity*). Apabila hukum pidana Indonesia yang berlaku, maka terhadap pelaku penyebaran Virus dan Trojan Horse tersebut dapat dikenakan Pasal 33 dan Pasal 30 ayat (2) UU ITE.

DAFTAR PUSTAKA

Buku

Abdul Wahid, dan Mohammad Labib. (2005). *Kejahatan Mayantara (Cyber Crime)*. Bandung: Refika Aditama.

Aloysius Wisnubroto. (1999). *Kebijakan Hukum Pidana dalam Penanggulangan Penyalahgunaan Komputer*. Yogyakarta : Universitas Widyatama.

Andi Hamzah. (1996). *Hukum Acara PidanaIndonesia*. Jakarta : CV Sapta Arta Jaya.

Asril Sitompul. (2001). *Hukum Internet, PengenalanMengenai Masalah Hukum di Cyberspace*. Bandung: PT Citra Aditya Bakti.

Barda Nawawi Arief. (2001). *Masalah Penegakan Hukum dan Kebijakan Penanggulangan Kejahatan*. Jakarta: PT.Raja Grafindo Persada, Jakarta.

Undang-Undang

Kitab Undang-Undang Hukum Pidana

Undang-Undang Nomor 8 Tahun 1981 Tentang Hukum Acara Pidana.

Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 48 Tahun 2009 Tentang Pokok-Pokok Kekuasaan Kehakiman.

Makalah, Jurnal

AR Budi, *Aspek Perlindungan Hukum Nasabah dalam Sistem Pembayaran Internet.*Artikel dalam Jurnal Hukum. No 16.

Didi Widayadi. (2000). *Kebijakan dan Strategi Operasional Polri dalam kaitan hakikatancaman Cybercrime*, makalah pada seminar Cyber Law, diselenggarakan oleh Yayasan Cipta Bangsa, Bandung, 29 Juli 2000.

Arief Muliawan, *Penegakan Hukum Tindak Pidana Informasi dan Transaksi Elektronika (cybercrime)*, disampaikan dalam seminar sehari dalam ranngka sosialisasi Undang-Undang Nomor 11 Tahun 2008 di Medan.

Koran

Suara Merdeka, dengan judul *Reserse Polda Jateng Ungkap Kejahatan InternasionalInternet*, 17 Nopember 2000.

Kompas, Berita Kompas Cyber Media (19/3/2002) 12 April 2002.

Website

http://id.wikipedia.org/wiki/Sejarah_Internet

http://id.wikipedia.org/wiki

http://idfl.org/showthread.php?t=81197/Sejarah Internet di Indonesia

http://www.kejahatan dunia maya asal ketik. com.mht/dunia maya

http://www. Man 3 Malang.com/jenis-jenis kejahatan internet.mht

http://www.Ebisnionline.com/kejahatan
internet;spamming