ANALISIS TINDAKAN HUKUM TERHADAP PELAKU PENYEBARAN VIRUS KOMPUTER MELALUI *E-MAIL* (*CYBER SPAMMING)* BERDASARKAN UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK

Elisabeth
Sistem Informasi, STMIK Profesional Makassar
email : lisastmikprof@gmail.com

Abstrak

Perkembangan teknologi informasi berdampak pada revolusi bentuk kejahatan yang konvensional menjadi lebih modern. Jenis kegiatannya mungkin sama, namun dengan media yang berbeda yaitu dalam hal ini internet, suatu kejahatan akan lebih sulit diusut, diproses, dan diadili. Kejahatan yang seringkali berhubungan dengan internet antara lain penyebaran virus komputer melalui pengiriman e-mail (cyber spamming) sebagai kejahatan yang dapat dilakukan melalui kecanggihan teknologi informasi dan komunikasi dalam hal ini melalui penyalahgunaan media internet.

Ada dua masalah yang diangkat dalam penelitian ini yaitu: Bagaimana Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik mengatur tindak pidana penyebaran virus komputer melalui pengiriman e-mail; dan tindakan hukum apa yang dapat dilakukan terhadap pelaku tindak pidana penyebaran virus komputer melalui pengiriman e-mail?

A. PENDAHULUAN

Teknologi informasi dalam perkembangannya saat ini telah mengantar manusia kepada globalisasi modern yang berdampak kepada kebebasan setiap orang di dunia untuk berinteraksi dengan siapapun dan dimanapun mereka berada. Internet adalah sarana utama yang digunakan, sebab melalui sarana internet seseorang dapat terhubung dengan relasi atau bahkan dengan orang asing yang mungkin tidak dikenal dan berdomisili di luar negeri.

Sebagai bangsa yang sedang tumbuh dan berkembang menuju masyarakat industri yang berbasis teknologi informasi, Indonesia dalam beberapa hal masih tertinggal. Keadaan ini di sebabkan masih relatif rendahnya sumber daya manusia di Negara kita ini dalam mengikuti perkembangan informasi dan komunikasi ini, selain itu juga kemampuan dalam menghadapi masalah hukum yang timbul. Dmpak negatif yang timbul diantaranya adalah tingkat kejahatan yang tinggi di berbagai bidang termasuk beragam modus operandinya.

Awalnya semua kejahatan yang terjadi harus dapat difasilitasi dengan peraturan perundang-undangan yang ada, baik itu Kitab Undang-Undang Hukum Pidana dan peraturan lainnya di bidang hukum pidana, walaupun kejahatan yang dilakukan melalui media internet tidak diatur dalam peraturan-peraturan di atas. Pada aplikasinya terhadap kejahatan melalui internet diberlakukan peraturan yang mengatur kejahatan konvensional dan hakim dituntut dapat melakukan penemuan hukum sendiri sebagaimana diamanatkan dalam Undang-Undang Nomor 4 Tahun 2004 Tentang Pokok-Pokok Kekuasaan Kehakiman, biasanya hakimpun mengusahakan pemecahannya melalui yurisprudensi, yang merupakan suatu keharusan. Tetapi pada kenyataan yang ada, lebih mengarah pada pembentukan hukum baru dengan asumsi KUHP tidak akan mampu mengatur kejahatan di atas, sehingga menimbulkan kesulitan bagi para penegak hukum (polisi, jaksa, hakim dan advokat) untuk mengatasi kondisi tersebut.

Tatkala harus berhadapan dengan tindak pidana penyebaran virus komputer melalui pengiriman *e-mail* menimbulkan masalah baru yang akan muncul, terutama menyangkut barang bukti. Hal ini disebabkan dalam hukum acara pidana yang berlaku tidak diatur mengenai alat bukti elektronik. Tetapi saat ini telah lahir Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (selanjunya disebut Undang-Undang ITE) yang di dalamnya mengatur berbagai aktivitas yang dilakukan dan terjadi di dunia maya (*cyberspace)*, termasuk pelanggaran hukum yang terjadi. Salah satu pelanggaran hukum tersebut adalah penyebaran virus komputer melalui pengiriman *e-mail* (*cyber spamming*). Undang-Undang ITE telah mengatur tentang pembuktian yang menyangkut teknologi informasi temasuk internet, tetapi masih banyak kendala-kendala dalam kenyataannya, sehingga seringkali pelaku penyebaran virus komputer melalui pengiriman *e-mail* ini tidak lolos dari hukuman.

B. ASPEK HUKUM TINDAK PIDANA PENYEBARAN VIRUS KOMPUTER

Pada dasarnya semua hukum bertujuan untuk menciptakan suatu keadaan dalam pergaulan hidup bermasyarakat, baik dalam lingkungan yang kecil maupun dalam lingkungan yang lebih besar, agar di dalamnya terdapat suatu keserasian, suatu ketertiban, suatu kepastian hukum dan lain sebagainya. Kemajuan teknologi

informasi menjadi awal dari keberadaan *cyber crime*, secara yuridis dapat membawa dampak pada hukum yang mengatur tentang hal tersebut. Perhatian terhadap *cyber crime* tersebut disebabkan dampak *cyber crime* yang bersifat negatif dan dapat merusak seluruh bidang kehidupan modern saat ini, oleh karena kemajuan teknologi komputer menjadi salah satu pendukung kehidupan masyarakat.

Cyber Crime adalah suatu upaya memasuki/ menggunakan fasilitas Komputer/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 alam maya) atau kejahatan dibidang komputer dengan secara illegal, dan terdapat difinisi yang lain yaitu sebagai kejahatan komputer yang ditujukan kepada sistem atau jaringan komputer, yang mencakup segala bentuk baru kejahatan yang menggunakan bantuan sarana media elektronik internet. Dengan demikian Cyber Crime merupakan suatu tindak kejahatan didunia alam maya, yang dianggap betentangan atau melawan undang-undang yang berlaku, oleh karenanya 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). Teknologi informasi 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 komputer melalui *e mail (cyber spamming).*

Virus komputer adalah 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. Efek dari virus komputer ini sangat beragam mulai dari munculnya pesan-pesan aneh, sampai pada tahap merusak dokumen atau *file* dan bahkan dapat merusak jaringan komputer itu sendiri. Virus komputer ini berasal dari penciptaan pengguna komputer yang dengan sengaja menyebarkan virus tersebut ke seluruh dunia. Virus komputer yang dimaksud sangan beragam dengan nama tersendiri dan

daya pengrusak tersendiri pula. Penyebaran virus komputer ini dapat terjadi dengan berbagai cara termasuk penyebaran virus komputer melalui pengiriman *e-mail (cyber spamming*).

Tindakan untuk menyebarkan virus komputer melalui pengiriman *e-mail (cyber spamming*) ini dapat dianggap sebagai suatu perbuatan yang layak dipidana, karena sepintas terlihat bahwa pelaku penyebaran virus komputer melalui pengiriman *e-mail (cyber spamming*) ini memiliki niat untuk merusak dokumen bahkan komputernya, sehingga dapat merugikan pihak lain, dengan demikian terdapat unsur pertanggungjawaban pidana di dalamnya. Perbuatan menyebarkan virus komputer melalui pengiriman *e-mail (cyber spamming*) ini tidak diatur dalam Kitang Undang-Undang Hukum Pidana. Saat ini, walaupun di Indonesia telah ada Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (selanjutnya disebut Undang-Undang ITE), tetapi tindakan penyebaran virus komputer melalui pengiriman *e-mail* tidak diatur secara khusus. Namun demikian Pasal 30 ayat (2) Undang-Undang ITE yang menegaskan beberapa perbuatan yang dilarang dan diancam sanksi pidana, termasuk larangan mengakses komputer dan atau sistem elektronik pihak lain secara melawan hukum, sehingga perbuatan menyebarkan virus komputer melalui pengiriman *e-mail (cyber spamming*) dapat dianggap sebagai sebuah tindak pidana.

Pasal 30 ayat (2) Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik mengandung unsur-unsur, baik unsur subjektif maupun objektif, yaitu :

Unsur subjektif:

1.Dengan sengaja

2.Secara melawan hukum

Unsur Objektif:

1. Mengakses komputer dan/atau sistem elektronik dengan cara apa pun

2. Untuk tujuan memperoleh informasi elektronik dan/atau dokumen elektronik

Berdasarkan Pasal 1 angka 1 UU ITE, yang dimaksud dengan 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. Sementara itu, Pasal 1

angka 4 UU ITE menyebutkan, bahwa yang dimaksud dengan dokumen elektronik adalah setiap informasi elektronik yang dibuat, diteruskan, dikirimkan, diterima atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal atau sejenisnya, yang dapat dilihat, ditampilkan dan/atau didengan melalui komputer atau sistem elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, kode akses, simbol atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya. Selain itu, yang dimaksud dengan sistem elektronik menurut pasal 1 angka 5 adalah serangkaian perangkat atau prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkanda/atau menyebarkan informasi elektronik. Sementara itu, Pasal 1 ayat 14 Undang-Undang ITE menyatakan bahwa komputer adalah alat untuk memproses data elektronik, magnetik, optik, atau sistem yang melaksanakan fungsi logika, aritmatika, dan penyimpanan.

Pada kasus penyebaran virus komputer melalui pengiriman *e-mail (cyber spamming*) ini sulit untuk membuktikannya, karena 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"

dan 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 dari 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.

Ketentuan mengenai alat bukti di atas merupakan ketentuan hukum acara pidana yang bersifat memaksa (*dwingen recht*), artinya semua jenis alat bukti yang telah diatur 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 dapat diperoleh melalui alat-alat bukti yang diajukan 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.

3. Teori Pembuktian Menurut Undang-Undang Secara Positif, merupakan pembuktian yang berlatar belakang sistem pembuktian berdasarkan keyakinan atau *Conviction in time theory*. Pembuktian pada sistem ini didasari dengan alat-alat bukti yang sah yang telah ditetapkan 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 menurut 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.

Berbicara mengenai alat bukti petunjuk, tidak terlepas dari ketentuan Pasal 188 (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 di atas, 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 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 dapat dianggap sebagai petunjuk, yang merupakan perluasan dari alat bukti surat sebagai bahan untuk dijadikan petunjuk bagi hakim dalam membuktikan suatu perkara termasuk kasus penyebaran virus komputer melalui pengiriman *e*-mail yang telah diuraikan pada bagian sebelumnya.

Tindak pidana penyebaran virus komputer melalui pengiriman *e*-mail *(cyber spamming)* dimungkinkan melibatkan lebih dari satu sistem hukum 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 melalui pengiriman *e*-mail 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 (*The Juridiction to Prescribe)*, yurisdiksi untuk menghukum (*The Juridicate to Enforce*) dan yurisdiksi untuk menuntut (*The Jurisdiction to Adjudicate*). Pada *The Jurisdiction to Adjudicate* terdapat beberapa asas yaitu:

1. Asas *Subjective Territorial* yaitu berlaku hukum berdasarkan tempat pembuatan dan penyelesaian tindak pidana dilakukan di Negara lain,

2. Asas *Objective Territorial* yaitu hukum yang berlaku adalah akibat utama perbuatan itu terjadi dan memberikan dampak kerugian bagi Negara yang bersangkutan,
3. Asas *Natonality* adalah hukum berlaku berdasarkan kewarganegaraan pelaku,
4. Asas *Passive Natonality* adalah hukum berlaku berdasarkan kewarganegaraan korban,
5. Asas *Protective Principle* adalah berlakunya berdasarkan atas keinginan Negara untuk melindungi kepentingan Negara dari kejahatan yang dilakukan diluar wilayahnya dan
6. Asas *Universality* adalah yang berlaku untuk lintas negara terhadap kejahatan yang dianggap sangat serius seperti pembajakan dan terorisme (*crime against humanity*).

C. KASUS-KASUS TERKAIT DENGAN PENYEBARAN VIRUS KOMPUTER MELALUI INTERNET

Beberapa saat lalu dunia dihebohkan dengan virus Chernobyl (CIH), yang dapat merusak data di hard disk dan juga mengahapus BIOS (untuk motherboard yang memakai flash bios yang tidak diproteksi). sehingga mengakibatkan kerugian cukup besar. Saat ini ada ancaman serupa dengan virus CIH (Chernobyl), yang telah dapat dideteksi kehadirannya. Virus ini akan menyerang pada tanggal 25 Desember tiap tahunnya.

1. Virus tanggal 25 Desember yaitu Win32.Kriz, Win32Kriz.3270, Win32Kriz.3862, dan masih akan bertambah variannya (jenisnya). Type: Polymorphic virus (dapat menyembunyikan identitasnya setiap kali menulari), Saat aktif tanggal 25 Desember tiap tahun. Aksinya mirip virus Chernobyl tetapi lebih ganas (merusak data di harddisk, merusak CMOS dan BIOS), dan juga memberikan message / pesan anti agama.
2. Virus Prilissa, merupakan varian virus Melissa variant (Prilisia), yang pada hari natal dapat memformat hard disk. Prilissa menginfeksi dokumen Word 97 dan menyebar lewat attachment e-mail. Saat dokumen yang terinfeksi dibuka, virus mematikan setting sekuriti proteksi virus, konfirmasi konversi dan membuka file list. Prilissa diekskusi di system, kemudian menduplikat dirinya dengan mengirim e-mail menggunakan MS Outlook ke 50, email address pertama yang terdapat di address

lists. Messagenya berisi Message From (username) yang mana user name nya adalah user name system. Body messagenya berisikan kalimat This document is very Important and you've GOT to read this.

Virus Melissa LoveLetter muncul di Amerika Serikat, variannya VeryFunnyJoke langsung muncul dalam beberapa saat, diikuti dengan lebih dari 30 jenis lainnya dalam dua bulan kemudian. Dan tidak semua varian berasal dari penulis program yang misterius. Beberapa perusahaan pernah terinfeksi oleh varian virus yang disebarkan oleh pegawainya sendiri yang penuh rasa ingin tahu terhadap virus yang mereka yang terima, menciptakan variannya, dan melepaskannya dalam sistem komputer perusahaan mereka terkadang secara tidak sengaja, dan terkadang memang ingin melakukannya.

Ada beberapa kasus penyebaran virus komputer lainnya di tahun 2003, yaitu:

1. Randon menyebarkan dirinya melalui IRC chat channels dan komputer yang disharing terhubung di dalam sebuah jaringan. Yang paling adalah mempunyai ciri-ciri yang khusus yaitu mempunyai malicious code yang merupakan sebuah dropper jenis worm yang menyusup pada beberapa file di komputer yang terinfeksi, beberapa diantaranya adalah virus yang mempunyai efek yang dapat berubah-rubah. actions they carry out include opening ports, running applications, propagating dan memasukkan Denial of Service (DoS) serta membanjiri dengan penyerangan, dan lain-lainnya. Randon dapat menghubungi ke web page dan mendownload sebuah backdoor jenis Trojan. Sebuah petunjuk kehadiran dari worm ini di dalam sebuah komputer adalah adanya peningkatan network traffic melalui ports 445 dan 6667.
2. Worm Lentin.P menyebar melalui e-mail dalam sebuah message dengan ciri khas yang berubah-rubah. Virus ini juga memanfaatkan kelemahan pada Internet Explorer versi 5.01 dan 5.5 yang akan bekerja secara automatis ketika message yang membawa worm ditampilkan melalui Outlook Preview Pane. Ia juga menyebar melalui network, dan setiap hari Rabu ia akan mengcopykan dirinya sendiri pada komputer yang disharing di dalam system jaringan. Lentin.P mematikan

program antivirus dan firewall, melancarkan dapat menyerang dengan menggunakan DoS, dan menutup Windows Task Manager.

Pada Maret 2003, empat buah virus yang cukup berbahaya telah ditemukan. Virus tersebut antara lain NiceHello, CodeRed.F, Deloder.A dan Prom- serta sebuah Virus Trojan yang dikenal sebagai SysComm. **NiceHello** tidak dapat menembus rangking pertama Top Rangking virus, karena pada minggu itu masih dipegang oleh Klez.I pada posisi teratas Top 10 rangking virus. Dan dapat diketahui Virus Worm Klez tetap menempati posisi teratas dalam waktu lebih dari 1½ tahun. NiceHello menyerang melalui e-mail pada sebuah message yang sangat mudah untuk dikenali, karena pada setiap message ada tertera ungkapan dalam bahasa Spanyol: ***es solo para vos*** (hanya untuk kamu). Setelah menginfeksi sebuah komputer, worm ini mengirimkan sebuah copy dirinya ke semua alamat yang didapat dari Contact List program instant messaging MSN Messenger. Dengan cara yang sama, NiceHello mengirimkan sebuah e-mail ke virus author, dimana berisi MSN Messenger user name dan password dari pemilik komputer yang terinfeksi.

Worm yang kedua adalah **CodeRed.F**, ini adalah varian dari virus worm yang dikenal sebagai CodeRed.IIS.2, dimana perbedaannya hanya 2 byte saja dari virus CodeRed yang aslinya. Modifikasi ini memungkinkan CodeRed.F terus menerus menyebar sampai tahun 34952, mengingat virus worm CodeRed.IIS.2 hanya berfungsi sampai akhir tahun 2002. CodeRed.F memanfaatkan kelemahan pada Index Server 2.0, Indexing Service dan Internet Information Server (versions 4.0 dan 5.0). Ketika virus ini menginfeksi sebuah komputer, ia membuat sebuah file dengan kateristik Trojan yang dalam sebuah file yang dikenal sebagai "EXPLORER.EXE", virus ini membuat 2 virtual drives, dimana digunakan untuk mengakses komputer yang terinfeksi. Kemudian, menyebabkan komputer diblokir untuk alasan yang tidak jelas, setiap 48 jam CodeRed.F akan merestart komputer anda sebagai operating system dalam bahasa Chinese, dan merestart semuanya itu dengan sebuah system operasi dalam bahasa yang berbeda setiap 24 jam sekali.

Virus worm yang ketiga adalah **Deloder.A**, yang menyebar melalui networking dan internet, serta dapat mematikan sharing resource : C$, D$, E$,

ADMIN$ dan IPC$. Pada komputer-komputer itulah kode-kode jahat menginfeksi, ia membuat dan menjalankan sebuah virus backdoor trojan. Untuk memperoleh remote access ke komputer lainnya, Deloder.A mencoba untuk menghubungkan ke IP addresses tertentu dengan menggunakan TCP port 445.

Worm Prom, hanya menginfeksi komputer yang dijalankan dengan menggunakan system operasi Windows XP/2000/NT. Virus ini menyebar melalui e-mail dalam sebuah message yang sulit dikenal, karena ia mempunyai karakter yang berubah-rubah. Virus worm lainnya adalah **Ganda.A** yang penyebarannya juga menggunakan e-mail, dan sekali waktu aktif ketika sebuah message yang membawa worm dibuka melalui Outlook Preview Pane, dan juga menyerang dengan memanfaatkan kelemahan dari Internet Explorer versi 5.01 dan 5.5. Sekali worm ini menginfeksi sebuah komputer, ia akan mengirimkan ke semua alamat yang didapatnya dari Windows address book, pada file-file *.EML, *.HTM" dan *.DBX serta Internet cache. Ganda.A dalah sebuah worm yang menginfeksi file-file PE, dengan mengcopykan dirinya dengan menyisipkan code-code tertentu.

Akhirnya, analisa virus kali ini ditutup dengan varian dari virus worm **Lovgate 'F' dan 'G'**, yang mana virus-virus tersebut menyebar melalui e-mail dan networking. Untuk menyebar ke setiap komputer yang ada di dalam sebuah jaringan, virus ini melakukan penggandaan dirinya secara besar-besaran pada direktori dan subdirektori yang disharing dan dapat diakses. Virus ini juga mengirimkan dalam jumlah besar email yang didalamnya termasuk juga file yang terinfeksi ke alamat email yang ditemukan dari Inbox dan beberapa direktori. Lovgate.F dan Lovgate.G dibuat dengan menggunakan bahasa pemrograman Microsoft Visual C^{++} dan dikompres dengan ASpack.

Pada tanggal 10 April 2003, VAKSINCOM bekerja sama dengan Tabloid PCPlus dan Polaris Center mengadakan WorkShop System Recovery VaksinGuard ProMagic. ProMagic hanya membutuhkan kurang dari 1 menit, hard disk akan kembali seperti sedia kala, tanpa harus menginstall ulang.

Insiden virus di Indonesia bulan Maret 2003:

1. W32/FunLove.4099 (14.749)
2. W32/Klez.H@mm (2.362)
3. W32/Sircam.A@mm (524)

4. Bugbear.A@mm (224)
5. W97M/Marker.EF (169)
6. VBS/Redlof.A@mm (150)
7. JS/Exploit_based (86)
8. W97M/Bablas.A (78)
9. Serb.3322 (72)
10. Die_Hard.K (68)

D. PENUTUP

KESIMPULAN

Berdasarkan analisis yang telah diuraikan pada bagian sebelumnya, maka dapat disimpulkan hal-hal sebagai berikut:

1. Perbuatan penyebaran virus komputer melalui pengiriman *e mail* merupakan salah satu perbuatan yang dilarang sebagaimana diatur dalam Pasal 30 ayat (2) Undang-Undang ITE, karena dalam hal ini *e mail* dianggap sebagai informasi dan/atau dokumen elektronik yang dapat dijadikan salah satu alat bukti sebagaimana diatur dalam pasal 5 ayat (1) dan (2) Undang-Undang ITE. Selain itu, *e mail* dapat pula dianggap sebagai alat bukti surat yang selanjutnya dijadikan alat bukti petunjuk sesuai ketentuan Pasal 184 KUHAP. Dengan demikian, tindakan penyebaran virus komputer melalui pengiriman *e mail* dapat dijerat dengan Pasal 46 ayat (2) juncto Pasal 30 ayat (2) Undang-Undang ITE.
2. Tindakan hukum yang dapat dilakukan terhadap pelaku penyebaran virus komputer melalui pengiriman *e mail* antara lain dengan tuntutan secara hukum dengan memperhatikan yurisdiksi dan hukum yang berlaku, karena dalam 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 *Natonality* adalah hukum berlaku berdasarkan kewarganegaraan pelaku, Asas *Passive Natonality* adalah hukum berlaku berdasarkan kewarganegaraan korban, Asas *Protective Principle*

adalah berlakunya berdasarkan atas keinginan Negara untuk melindungi kepentingan Negara dari kejahatan yang dilakukan diluar 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 komputer melalui pengiriman *e mail* tersebut dapat dikenakan Pasal 46 ayat (2) juncto Pasal 30 ayat (2) Undang-Undang ITE.

REKOMENDASI

Adapun saran-saran Penulis adalah sebagai berikut:

1. Demi terwujudnya kepastian hukum yang mengatur mengenai kasus penyebaran virus melalui *e-mail (cyber spamming)* sebagaimana diatur dalam Pasal 30 (2) Undang-Undang ITE, hendaknya pemerintah harus segera menerbitkan Peraturan Pemerintah sebagai peraturan pelaksana bagi Undang-Undang tersebut. Hal ini dimaksudkan agar para aparat penegak hukum dapat mempunyai dasar untuk melaksanakan aturan yang telah diatur didalam Undang-Undang tersebut.
2. Berdasarkan teori Pembinaan Hukum Nasional dari Mochtar Koesuma atmadja yaitu Mempertahankan, Memperbaiki, dan Memperbaharui peraturan Perundang-undangan yang ada, maka Undang-Undang ITE perlu diperbaiki, karena tidak didukung oleh peraturan Perundang-undangan yang secara khusus mengatur mengenai hukum acara dalam wilayah hukum yang terjadi dalam dunia maya sehingga tindakan hukum terhadap pelaku penyebaran virus melalui *e-mail (cyber spamming)* berdasarkan Pasal 46 ayat (2) juncto Pasal 30 ayat (2) Undang-Undang ITE, menjadi tidak maksimal.

DAFTAR PUSTAKA

[1] Agus raharjo **Cyber Crime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi**, Bandung : Citra Aditya Bakti, 2002

[2] Ahmad M Ramli, **Cyberlaw dan HAKI dalam Sistem Hukum Indonesia**, Bandung : Refika Aditama, 2004

[3] Al Wisnubroto, **Kebijakan Hukum Pidana dalam Penanggulangan Penyalahgunaan Komputer**, Yogyakarta : Universitas Widyatama, 1999

[4] Andi Hamzah, **Hukum Acara Pidana Indonesia,** Jakarta : CV Sapta Arta Jaya, 1996

[5] Andri Kristanto, **Jaringan Komputer**, Yogyakarta : Graha Ilmu, 2003

[6] Muladi. **Kapita Selekta Sistem Peradilan Pidana**. Badan Penerbit Universitas Diponegoro. Semarang. 1995.

[7] Munir Fuady. **Teori Hukum Pembuktian (Pidana dan Perdata).** Citra Aditya Bhakti. Jakarta. 2006.

[8] _____ **Pembahasan Permasalahan dan Penerapan KUHAP: Pemeriksaan Sidang Pengadilan, Banding, Kasasi dan Peninjauan Kembali.** Sinar Grafika. Jakarta.2003.

[9] Otje Salman S.*dan* Anthon F. Susanto. **Teori Hukum: engingat, Mengumpulkan, dan membuka Kembali.** Refika Aditama. Bandung. 2004.

[10] Romli Atmasasmita. **Sistem Peradilan Pidana Perspektif Eksistensialisme dan Abolisionisme.** Putra Abardin bandung. 2000.

[11] Soejono Soekanto. **Pengantar Penelitian Hukum.**UI-Press. Jakarta. 1996.

[12] Undang-Undang *Nomor* 8 Tahun 1981 Tentang Hukum Acara Pidana

[13] Undang-*Undang* Nomor 11 tahun 2008 Tentang Informasi dan Transaksi Elektronik

[14] Undang-*Undang* Nomor 4 Tahun 2004 Tentang Pokok-Pokok Kekuasaan Kehakiman