Os vírus de computador e a legislação penal brasileira

Não há quem não tenha sentido os efeitos [1] do famigerado vírus de computador *MyDoom* [2], a primeira grande praga de 2004, já no topo dos "rankings" de janeiro das empresas antivírus e sites de segurança. Esta categoria de "malware" (abreviatura para "malicious software") ou "worm" contém um executável (.zip, ou ainda, .bat, .cmd, .exe, .pif ou .scr) que, uma vez aberto, espalha-se para centenas de outras caixas de entrada e, segundo consta, também nas redes P2P, de troca de arquivos.

No dia 26, primeiro dia da epidemia, o *MyDoom* infectou uma em cada dez mensagens enviadas, e os antivírus e filtros bloquearam cerca de 1,2 milhão de e-mails contaminados. A praga virtual afetou pelo menos meio milhão de computadores em 168 países, e já é considerada a mais agressiva da história. Destronou o Sobig.f, que em agosto do ano passado contaminou 250 mil máquinas nas primeiras 24 horas [3].

Mas no caso do *MyDoom-A* e *MyDoom-B* (sua variante) [4], há um "plus": têm a capacidade de gerar ataques DDoS [5] contra os sites da SCO e da Microsoft, respectivamente, o que inspirou algumas pessoas a pensar que se trata de represálias vindas de concorrentes. Teorias conspiratórias à parte, tanto a SCO (que se diz proprietária dos códigos do Unix, base do Linux) como a Microsoft já se adiantaram em oferecer vultosas recompensas para quem apontasse os culpados.

Não há dúvida de que os vírus de computador, quer sejam epidêmicos ou não, causam danos a empresas, repartições públicas e individuais. Paralisam sistemas e redes, ocasionando atrasos na entrega de mensagens e a perda de muitas delas, além da perda de negócios e de produtividade.

Ações cíveis e penais podem ser intentadas contra o responsável pela criação de um vírus informático [6]. No âmbito cível, irão buscar a responsabilização pelas perdas e danos sofridos, na forma de indenizações. Como maior dificuldade, a constituição da prova. Mas é na esfera penal que surgem as maiores dúvidas.

O projeto de lei 84/99, a "coisa" e o dano eletrônico

O atual Código Penal, Decreto-lei nº 2.848/40, prevê o crime de dano como sendo:

Art. 163. Destruir, inutilizar ou deteriorar coisa alheia.

Pena – detenção, de 1 (um) a 6 (seis) meses, ou multa.

Note-se, no entretanto, que a escola tradicional não equiparou programa de computador ("software") a uma "coisa", talvez por ser anterior à Internet e exigir a figura do dolo específico (vontade de prejudicar).

Com vistas a atualizar a legislação no que tange aos crimes informáticos [7], foi proposto (entre outros) o projeto de lei nº 84 de 1999, de autoria do deputado Luiz Piauhylino, já aprovado na Câmara e com substitutivo seguindo tramitação no Senado sob o nº 89/03 [8].

Esse projeto prevê a “difusão de vírus eletrônico” como categoria do crime de dano eletrônico. Para efeitos do § 2º do artigo 163 proposto, passa a equiparar-se à “coisa”:

I – o dado, a informação ou a base de dados presente em meio eletrônico ou sistema informatizado;

II – a senha ou qualquer meio de identificação que permita o acesso a meio eletrônico ou sistema informatizado.

Assim, o projeto propõe acréscimo de § 3º, a “difusão de vírus eletrônico”, dispondo que:

§ 3º – Nas mesmas penas do § 1º incorre quem cria, insere ou difunde dado ou informação em meio eletrônico ou sistema informatizado, indevidamente ou sem autorização, com a finalidade de destruí-lo, inutilizá-lo, modifica-lo ou dificultar-lhe o funcionamento.

Observamos que § 1º do art. 163 apresentado (atualmente há apenas o parágrafo único, contra o qual não foi proposta modificação de redação) trata do dano qualificado:

§ 1º – Se o crime é cometido:

I – com violência à pessoa ou grave ameaça;

II – com emprego de substância inflamável ou explosiva, se o fato não constitui crime mais grave;

III – contra o patrimônio da União, Estado, Município, empresa concessionária de serviços públicos ou sociedade de economia mista;

IV – por motivo egoístico ou com prejuízo considerável para a vítima:

Pena – detenção, de 6 (seis) meses a 3 (três) anos, e multa, além da pena correspondente à violência. (que não se aplica).

Deste modo, caso seja aprovado o projeto, os vírus de computador serão uma categoria de dano eletrônico, e equiparados ao dano real. E os dados, bases de dados, informações, senhas e métodos de identificação que permitam acesso serão considerados uma “coisa” passível de proteção do Direito Penal [9].

Cavalos de Tróia e a sentença de Campo Grande

Diante das diversas categorias do que se chama comumente de “vírus de computador” ou “malwares”, os cavalos de Tróia (*Trojan horses*), arquivos travestidos de verdadeiros que contêm em seu interior um programa “espião” (como um “keylogger”), são também disseminados na forma de mensagens não solicitadas (“spam”), ou em páginas clonadas na Internet.

Não são obrigatoriamente epidêmicos. Uma vez executados, esses “scams” [10] capturam senhas e

dados pessoais sem que o usuário perceba, e de posse desses dados, o agente poderá efetuar transferências bancárias ilícitas, por exemplo.

Recentemente um "cracker" de 19 anos e um policial militar foram condenados em Campo Grande/MS [11]. Para a juíza da 3ª Vara da Justiça Federal [12], Janete Lima Miguel Cabral, os arquivos troianos encontrados foram entendidos como "vírus de computador", e utilizados para viabilizar a prática de estelionato (art. 171, "caput", combinado com o § 3º do artigo 288 – quadrilha ou bando), ambos do Código Penal, e quebra de sigilo (artigo 10 da Lei Complementar nº 105/01):

Art. 171. Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento:

Pena – reclusão, de 1 (um) a 5 (cinco) anos, e multa.

Por tal ótica, e em consonância com a exposição de motivos da Parte Especial, o arquivo troiano é o artifício, ardil ou meio fraudulento utilizado para que o agente atinja o resultado, e exige que a vantagem obtida, para si ou para terceiro, seja mais ou menos expressiva.

Art. 10 da LC 105/01. A quebra de sigilo, fora das hipóteses autorizadas nesta Lei Complementar, constitui crime e sujeita os responsáveis à pena de reclusão, de um a quatro anos, e multa, aplicando-se, no que couber, o Código Penal, sem prejuízo de outras sanções cabíveis.

O entendimento jurisprudencial

Ainda são pouquíssimos os julgados de 2º grau que abordaram o tema "vírus de computador". Trazemos dois exemplos cíveis não muito recentes:

AÇÃO DE INDENIZAÇÃO – Alegada utilização de disquete contaminado por vírus, no computador da pessoa jurídica, causando dano ao sistema – Não apresentação do disquete – Contestação específica das rés – Inexistência de prova da contaminação, porque não exibido o disquete – Perícia unilateralmente produzida – Inutilidade – Ação improcedente – Apelação provida em parte, apenas para redução da honorária. (TJ/SP – 4ª C.D.Priv. – AC 108.150-4/6-00, Rel. Des. Narciso Orlandi, j. 15.02.2001, v.u.)

PROCESSO CIVIL E CIVIL – APELO ADESIVO – AMPLITUDE – INDENIZAÇÃO POR DANOS MORAIS – CADASTRO NEGATIVO DO SPC – VÍRUS DE COMPUTADOR – CASO FORTUITO – INEXISTÊNCIA – CONDUTA PREVISÍVEL E EVITÁVEL – MAJORAÇÃO DA CONDENAÇÃO ANTE AS PECULIARIDADES DA CASO EM APREÇO. (…) A infeção de computador por vírus, ante o rápido desenvolvimento tecnológico da informática, inclusive com o aparecimento da rede de computadores "internet", é hipótese bastante previsível e também evitável, com os modernos mecanismos de defesa, os quais devem ser empregados por todos aqueles que trabalham com referidas máquinas e com grandes bases de dados, sendo a inexistência de tal proteção, derivando de tal infeção o irregular cadastro negativo do SPC, conduta negligente, afastada, assim, a hipótese de caso fortuito. Deve-se majorar a verba de ressarcimento, tendo em vista a hipótese em análise, observando o binômio punição/compensação, quando se nota que a atitude ilícita da instituição perdurou por mais de dois anos, com a imputação indevida ao cadastro do autor de mais de 500 protestos.

(TJ/MG – 3ª C.Cív., AC 281.733-6, Rel. Juiz Dorival Guimarães Pereira, j. 16.06.1999, v.u.)

E ainda, a notícia da recente decisão do TRF da 1ª Região, em 14/01/2004 (DJ de 03/02/2004), no pedido de reconsideração de decisão que indeferiu liminar em habeas corpus (HC 2003.01.00.042372-9/PA). Nele, o Ministério Público Federal assim se manifestou, e o pedido não foi acolhido:

"A situação de (nome suprimido), *contudo, é completamente diversa dos demais posto que (sic) seu papel na organização criminosa é bastante superior aos outros requerentes, não apenas no faturamento, mas sobretudo na importância decisória e na prática dos atos que lhe competiam. Era ele quem confeccionava e aperfeiçoava programas TROJAN, além de prestar assistência técnica mediante pagamento de valores variados. Confessou que utilizava e-mails para prática de delitos por meios eletrônicos. Sua libertação, nessa fase inicial da ação penal, significará o retorno de operação da quadrilha porque um de seus 'cérebros' voltará a agir por estar (sic) em liberdade, até mesmo para ajudar no ganho a ser repassado àqueles que não possam trabalhar momentaneamente.'*

Outras possibilidades

Em tese, pode ser também aplicável a interceptação de comunicações de informática ou telemática, crime previsto no artigo 10 da Lei nº 9.296/96, que regulamenta o inciso XII do artigo 5º da Carta Magna. Dispõe que:

Art. 10. Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei.

Pena: reclusão, de 2 (dois) a 4 (quatro) anos, e multa.

Quanto à conduta prevista no § 3º do artigo 163 proposto pelo PL 84/99, entendemos que o troiano contendo arquivo espião não destrói, não inutiliza e nem dificulta (necessariamente) o funcionamento de uma máquina ou rede. Mas sem dúvida modifica, podendo causar danos, mas nem sempre uma vantagem ilícita.

E ainda poderão ser cabíveis em concurso, conforme o caso, os crimes de falsa identidade, violação de direitos autorais, violação do direito de marca, (e prática de "spam", quando enfim considerada um crime) etc., além de qualificadoras, atenuantes e outras possibilidades a serem desvendadas pela doutrina e jurisprudência.

Crime contra a segurança dos meios de comunicação

Já nos casos de vírus como o *MyDoom*, altamente danosos a milhares de pessoas de uma só vez, ou seja, de rápida disseminação, haveria ainda mais duas possibilidades trazidas pelo PL 84/99 – que fez um "upgrade" nos artigos 265 e 266 do Código Penal, estendendo-os à "telecomunicação":

Art. 265. Atentar contra a segurança ou o funcionamento de serviço de água, luz, força, calor ou telecomunicação, ou qualquer outro de utilidade pública:

Pena – reclusão, de 1 (um) a 5 (cinco) anos, e multa.

Art. 266. Interromper ou perturbar serviço telegráfico, radiotelegráfico, telefônico ou de telecomunicação, impedir ou dificultar-lhe o restabelecimento:

Pena – detenção, de 1 (um) a 3 (três) anos e multa.

A pena do artigo 266 se revela muito branda para casos de vírus de computador epidêmicos, que ocasionam danos consideráveis à Rede. Preferimos defender a aplicabilidade do art. 265 atualizado, se for o caso.

Serviço de valor adicionado?

Porém, antes que possamos qualificar a atuação de vírus e cavalos de Tróia como perturbação de serviço de telecomunicações ou atentado a serviço de utilidade pública, restará uma discussão conceitual. A Lei nº 9.472/97 (Lei de Telecomunicações) diz que:

Art. 60, § 1° – Telecomunicação é a transmissão, emissão ou recepção, por fio, radioeletricidade, meios ópticos ou qualquer outro processo eletromagnético, de símbolos, caracteres, sinais, escritos, imagens, sons ou informações de qualquer natureza.

Para fins tributários, a corrente majoritária entende que provimento de acesso à Internet é um serviço de valor adicionado:

Art. 61. Serviço de valor adicionado é a atividade que acrescenta, a um serviço de telecomunicações que lhe dá suporte e com o qual não se confunde, novas utilidades relacionadas ao acesso, armazenamento, apresentação, movimentação ou recuperação de informações.

§ 1º – Serviço de valor adicionado não constitui serviço de telecomunicações, classificando-se seu provedor como usuário do serviço de telecomunicações que lhe dá suporte, com os direitos e deveres inerentes a essa condição.”

Assim, estão presentes as seguintes definições legais, e pode haver algumas dificuldades frente à interpretação analógica versus interpretação extensiva:

a-) serviços de telecomunicação e serviços de valor adicionado (da Lei nº 9.472/97);

b-) sistemas de informática e telemática (da Lei nº 9.296/96); e

c-) meios eletrônicos e sistemas informatizados (do PL 84/99).

Crime de perigo comum

Além de outras discussões doutrinárias — se alguns tipos de vírus de computador poderiam ser considerados, no futuro, integrantes da categoria dos crimes contra a incolumidade pública, mais propriamente um crime de perigo comum (artigo 250 e seguintes do CP), e da necessidade de melhor tipificação — os vírus ganharam um aliado "de peso": o "spam", e estão sendo disseminados para todo o globo [13].

Isso não é novidade, como também não é novidade que algumas pessoas estão até "se acostumando" com tantos vírus e "spams". Se detectados, são filtrados, apagados sumariamente ou acabam sendo executados de forma culposa (ou em virtude de "bug" de sistema), dando vazão à epidemia da vez.

Versões ainda mais danosas não tardarão e a guerra cibernética está instaurada. O fato é que os vírus de computador — e em breve, pode-se prever, nos celulares e dispositivos portáteis — estão gerando uma grande desconfiança, e afetando o correio eletrônico como um mecanismo seguro para as comunicações.

Notas de rodapé

[1] "Como evitar o vírus MyDoom", no site do Jornal da Globo, em 27/01/2004.

[2] "O que você precisa saber sobre o vírus MyDoom", na página da Microsoft Brasil, em 30/01/2004.

[3] Conforme "Vírus irado", na coluna Século 21 da revista Istoé nº 1791, de 04/02/2004.

[4] "MyDoom.B: conheça mais sobre essa praga", *in* Infoguerra, em 20/01/2004.

[5] Vide artigo de Reginaldo César Pinheiro intitulado "Os Ataques DDoS e os Reflexos Penais Informáticos", *in* Consultor Jurídico, em 11/08/2002.

[6] Em termos de jurisdição e visando facilitar, admitamos que o autor resida no Brasil e que o vírus tenha sido concebido aqui.

[7] A única lei específica para crimes informáticos em vigor no Brasil é a de nº 9.983 de 14/07/2000, que modificou a Parte Especial do Código Penal. É aplicável apenas a funcionários públicos. A íntegra pode ser obtida na página da Presidência da República.

[8] A íntegra pode ser obtida no site do Senado Federal.

[9] Há, ainda, os problemas inerentes à identificação da autoria, e da correta interpretação dos cabeçalhos recebidos (propriedades), mas são temas para futuros artigos.

[10] "O que é scam", no site da Terra Informática.

[11] “Fraudes on-line causam condenação de duas pessoas no Mato Grosso do Sul”, no site da Módulo Security, em 12/01/2004.

[12] Da fundamentação decisória da r. sentença:

“*Outra prova significativa é o laudo de exame em ambiente computacional distribuído (f. 844-926), onde foram analisados os equipamentos apreendidos na residência do acusado Guilherme. Nos computadores desse acusado foram encontradas dezenas de arquivos contendo dados bancários de correntistas diversos, inclusive senhas, e também inúmeros registros de conversas mantidas entre Guilherme e outros, onde há referência a invasões de servidores, colocação de “trojan” (vírus de computador), etc.*“.

[13] Há alguns anos, a atuação dos vírus era mais localizada. Normalmente eram disseminados por meio de disquetes ou junto a programas baixados da Internet, e eram mais destrutivos. Segundo consta, conseguiam infectar até a BIOS da máquina, inutilizando-a.

Date Created
03/02/2004