“SPAM”: uma análise das mensagens não solicitadas ou indesejadas[1]

Dilson Bastos Fernandes[2]

RESUMO
Este artigo analisa o fenômeno do spam sob uma perspectiva jurídica, abordando sua definição, impactos na sociedade e na segurança da informação, bem como a regulação existente no Brasil e no cenário internacional. O spam, caracterizado pelo envio de mensagens eletrônicas não solicitadas, apresenta desafios para o ordenamento jurídico brasileiro devido à ausência de uma legislação específica, tornando necessária a aplicação de princípios constitucionais e normas infraconstitucionais para coibir essa prática. Inicialmente, são discutidos os conceitos fundamentais relacionados ao spam, suas origens e os diferentes tipos, incluindo correntes, boatos, fraudes, propagandas e ameaças. Além disso, analisam-se os prejuízos causados tanto para os usuários quanto para os provedores de serviços de internet, considerando aspectos como sobrecarga de sistemas, invasão de privacidade e riscos à segurança da informação. O artigo também examina as estratégias de combate ao spam, com enfoque nas técnicas tecnológicas e regulatórias adotadas no Brasil, nos Estados Unidos e na Europa. No âmbito jurídico, discute-se a dificuldade na regulamentação da prática e as tentativas de implementação de legislações específicas para seu controle. Por fim, são apresentadas perspectivas futuras para o combate ao spam, considerando a evolução das tecnologias e a necessidade de maior conscientização e adoção de medidas de segurança.

PALAVRAS-CHAVE: Spam. Segurança da informação. Direito digital. Regulamentação. Privacidade.

ABSTRACT
This article analyzes the phenomenon of spam from a legal perspective, addressing its definition, impacts on society and information security, as well as the existing regulation in Brazil and in the international context. Spam, characterized by the sending of unsolicited electronic messages, presents challenges for the Brazilian legal system due to the absence of specific legislation, making it necessary to apply constitutional principles and infra-constitutional norms to curb this practice. Initially, the fundamental concepts related to spam, its origins, and different types, including chain letters, hoaxes, frauds, advertisements, and threats are discussed. In addition, the damages caused to both users and internet service providers are analyzed, considering aspects such as system overload, privacy invasion, and information security risks. The article also examines strategies for combating spam, focusing on technological and regulatory techniques adopted in Brazil, the United States, and

[1] Este trabalho é parte da dissertação de mestrado “O Estatuto Jurídico do Spamming no Brasil” depositada e defendida na *Universidad Politécnica y Artistica del Paraguay (Maestria em Derecho)*, em Assunção, Paraguai, com a classificação 5 (cinco) *suma cum laude.*

[2] Graduado em Direito pela Faculdade de Direito do Vale do Rio Doce (Fadivale) e em Engenharia Elétrica pela Universidade Vale do Rio Doce. Pós-graduação em Direito Civil, em Processo Civil pela Fadivale e em Direito Público pela ANAMAGIS - Newton de Paiva. Mestre em Direito Internacional Público pela Universidad Politécnica y Artística del Paraguay. Professor da disciplina de Direito Civil no curso de graduação da Fadivale. Foi por muitos anos Presidente da comissão Direito de Informática da Ordem dos Advogados do Brasil, 43ª Subseção de Minas Gerais. Advogado militante.

Europe. From a legal standpoint, the difficulties in regulating this practice and the attempts to implement specific legislation for its control are discussed. Finally, future perspectives on combating spam are presented, considering technological advancements and the need for greater awareness and the adoption of security measures.

KEYWORDS: Spam, information security, digital law, regulation, privacy.

SUMÁRIO

1 INTRODUÇÃO

O e-mail (*eletronic mail*), a mensagem eletrônica da internet, criado em 1971 pelo engenheiro de computação Ray Tomlinson, rapidamente tomou-se um dos meios de comunicação mais rápido, eficiente e barato.

Milhares e milhares de pessoas passaram a utilizar os serviços de correio eletrônico oferecidos pelos provedores de internet espalhados pelo mundo. Este serviço, permite o envio e recebimento de mensagens eletrônicas organizados em contas individuais, largamente utilizadas por pessoas naturais e pessoas jurídicas, tornando-se imediatamente parte do cotidiano destas pessoas.

Com utilização em escala mundial da internet, imediatamente houve um acúmulo de e-mails, sobrecarregando as caixas postais eletrônicas dos seus usuários.

O uso indiscriminado do e-mail criou uma conduta abusiva que foi denominada de "spam". Spam é o envio de mensagem não solicitada, indesejável, recebida pelo destinatário sem que este a autorize. O que caracteriza o spam não é o mero recebimento da mensagem eletrônica, mas o fato da mensagem não ter sido solicitada pelo internauta.

A problemática em torno dos e-mails ou mensagens eletrônicas não solicitadas é abordada por Lorenzetti (2004, p. 392) em sua obra Comércio Eletrônico, da seguinte forma:

> O envio de e-mails não solicitados pelo usuário constitui um modo de publicidade que diminui sensivelmente os custos de transação com relação ao correio tradicional, já que, uma vez que se consiga uma lista de usuários, podem-se enviar quantidades enormes de mensagens com baixíssimos custos. Os problemas são enfrentados pelo usuário do computador, que poderá receber vírus ou ficar diante da saturação de sua caixa postal de correio eletrônico, além da invasão de privacidade.

A associação do termo spam com os e-mails não solicitados, surgiu em uma cena de do programa de TV do grupo inglês *Monty Python*, onde um grupo de vikings inconvenientes estavam em uma lanchonete, onde a garçonete lia o cardápio, e a maioria dos itens era a base de SPAM. Enquanto a garçonete repetia a palavra várias vezes, o grupo de *vikings* ensaiava uma música: "SPAM, SPAM, SPAM, SPAM, SPAM, SPAM, SPAM, SPAM, adorável SPAM! Maravilhoso SPAM![3].

A partir desse quadro da TV inglesa, os usuários de um antigo ambiente utilizado para bate-papo virtual começaram a estabelecer um paralelo entre a irritante e repetitiva "música do spam" e as mensagens, da mesma forma, irritantes e repetitivas, que anunciavam produtos ou ideias. Em pouco tempo, o termo spam foi adotado por toda a comunidade da grande rede, designando tais mensagens.

Assim o termo para designar os e-mails não solicitados remonta à ideia de algo que se repete várias vezes, gerando muita chateação e perturbação, impossibilitando qualquer comunicação das outras pessoas presentes com a gritaria repetitiva.

Sendo assim, o objetivo do trabalho é trazer uma visão geral do spam no contexto da tecnologia e da legislação aplicável, valendo-se da abordagem dedutiva, por meio da pesquisa bibliográfica e documental. O texto está dividido em doze capítulos: o primeiro apresenta a introdução; o segundo aborda a nomenclatura apropriada para o termo; o terceiro trata da diferenciação da terminologia utilizada para o termo, o praticante e a pratica em si; o quarto discute sobre as versões da origem da prática do spam; o quinto examina os tipos de spam; o sexto verifica a atuação dos spammers; o sétimo analisa os problemas causados pelo spam; o oitavo demonstra os prejuízos causados pelo spam, o nono descreve o spam *zombie*, o décimo elenca algumas técnicas de combate ao spam, o décimo primeiro aborda o spam e o direito e o décimo segundo apresenta a conclusão.

[3] O texto original da cena do grupo Monty Phyton encontra-se no site: http://www.cs.berkeley.edu/~ddgarcia/spam.html#MontyPython. Acesso em: 14 dez. 2007.

2 SPAM e spam.

Na verdade, o termo SPAM (com letras maiúsculas) é a marca de um produto alimentício enlatado americano, um presunto condimentado, o *SPiced hAM* que é fabricado pela *Hormel Foods* desde 1930, sendo um produto tradicional e com uma legião de fãs no mundo inteiro.

Como a *Hormel Foods* não aprova a associação do seu produto SPAM ao envio de mensagens não solicitadas, o fabricante do presunto condimentado mantém uma nota de esclarecimento em seu site oficial[4], denominada "SPAM and the internet" esclarecendo que spam, grafado com letras minúsculas, diz respeito ao envio de mensagens não solicitadas pela Internet e não deve ser confundido com "SPAM®", grafado com letras maiúsculas, marca registrada pela *Hormel Foods*. O texto também reitera a objeção da Hormel à associação da imagem do produto SPAM® ao envio de mensagens não solicitadas pela Internet.

Portanto, ao fazer referência ao uso do termo em relação à internet, como mensagens não solicitadas ou indesejadas, recomenda-se o uso de letras minúsculas "spam" e para referir-se ao produto alimentício enlatado americano deve-se fazer uso de letras maiúsculas "SPAM".

3 TERMINOLOGIA UTILIZADA: SPAM, SPAMMER E SPAMMING.

O spam é considerado um abuso e se refere ao envio de mensagens não solicitadas, ou seja, o envio de mensagens indiscriminadamente a um ou vários usuários, sem que estes tenham requisitado tal informação. Não importa o número de mensagens enviadas e de destinatários, mas sim a característica principal do spam: as mensagens enviadas sem consentimento prévio do usuário destinatário.

O spamming é a ação de enviar spams e o mero recebimento da mensagem eletrônica não caracteriza o spamming, tampouco como vimos acima o seu volume. O que caracteriza sua ilicitude (penal, contravencional, consumerista ou civil) é o fato da mensagem não ter sido solicitada pelo internauta.

Caso o internauta tenha visitado algum site e se inscrito em alguma lista ou serviço para receber informações sobre determinados produtos, como também em

[4] Disponível em: http://www.spam.comilegal/spam. Acesso em: 15 dez. 2007.

alguma lista de discussão "*mailing list*" ou "*newsgroup*"[5], não há de se falar em spamming.

O spam caracteriza-se também quando os dados foram espontaneamente fornecidos, mas o volume de mensagens eletrônicas for excessivo ou divorciado de seus propósitos originais.

Quando os dados pessoais são cedidos a fornecedores de bens e serviços, é lícito pressupor que esses dados serão utilizados apenas nas situações em que forma contratados, ressaltando que se o responsável por tais informações cedê-las a terceiros, responderá solidariamente com aqueles que praticarem o spam.

Quem envia o spam é chamado de spammer.

O conteúdo do spam pode ser: propaganda de produtos e serviços, pedido de doações para obras assistenciais, correntes da sorte, propostas de ganho de dinheiro fácil, boatos desacreditando o serviço prestado por determinada empresa, dentre outros.

O spam é conhecido de forma genérica como mensagem eletrônica não solicitada, mas também recebe outras denominações como "lixo eletrônico" e "*junk e-mails*". Também é formalmente conhecido como: a) *Unsolicited Bulk E-mail* (UBE), termo usado para se referir aos e-mails não solicitados enviados em grande quantidade; e b) *Unsolicited Commercial E-mail* (UCE), termo usado para se referir aos e-mails comerciais não solicitados.

4 O PRIMEIRO SPAM

Existem duas versões para o registro do "primeiro spam", sendo a mais aceita e considerada "o aniversário do spam", o dia 5 de março de 1994, quando dois advogados Cantel e Siegel enviaram uma mensagem para um grupo de discussão da USENET[6], sobre uma loteria de green carás para imigrantes dos Estados Unidos.

O pior aconteceu no dia 12 de abril de 1994, quando os mesmos advogados enviaram a mesma mensagem da loteria dos *green cards* para todos os grupos de

[5] Grupos de discussão criados com o objetivo de trocar informações sobre um assunto especifico.
[6] Rede de grupos de discussão amplamente disseminada na Internet. A rede é formada por grupos de discussão, chamados *newsgroups*. Cada servidor que participa da Usenet troca as mensagens colocadas por seus usuários com os demais servidores. Assim, todo o conjunto de mensagens colocadas nos grupos de discussão está sempre atualizado.

discussão da USENET, utilizando um programa capaz de automatizar o envio em massa da mensagem de propaganda, técnica comumente utilizada pelos spammers dos nossos dias.

As reações foram imediatas e negativas, gerando apelos sobre a violação da Netiqueta - um conjunto de regras de boas maneiras para os usuários da rede. O grande número de mensagens trocadas sobre o assunto comprometeu o desempenho da rede, causando um dos conhecidos efeitos colaterais do spam.

A mensagem histórica da loteria dos *Green cards* pode ser encontrada em:
https://web.archive.org/web/20011214024742/math-www.uni-paderborn.de/~axel/BL/CS941211.txt

A outra versão sobre o registro do primeiro spam data de 3 de maio de 1978 quando um funcionário da DEC, profissional de marketing, enviou uma propaganda do novo sistema DEC 20, considerando que todos os usuários da Arpanet estariam interessados em receber as informações sobre o referido sistema.

A mensagem de divulgação do DEC 20 foi enviada para 320 endereços da Arpanet, já que esse era o limite aceito pelo sistema da época. A propaganda enviada pode ser encontrada no site: http://www.templetons.com/brad/spamreact.html

5 TIPOS DE SPAM

A internet surgiu com interesses voltados basicamente para o ensino e pesquisa, mas com a entrada do novo milênio verificamos a existência de uma rede que conecta computadores no mundo todo, usada para os mais diversos fins e por urna comunidade de usuários cada vez mais heterogênea. O mundo presencia a chamada democratização da Internet, onde todos os seguimentos da sociedade têm participação efetiva. Vários serviços e possibilidades são oferecidos, como o comércio eletrônico que hoje é uma realidade e com certeza, este panorama tem inúmeras vantagens, mas algumas regras básicas têm se perdido. Pode-se dizer que algumas "normas de bom comportamento" ou "normas básicas de convivência em sociedade" têm sido relegadas a segundo plano por parte da comunidade virtual.

Entretanto, o mau uso da rede pode tornar a vida dos milhões dc usuários e profissionais da Internet um verdadeiro pesadelo. O uso indiscriminado do correio eletrônico desvirtua o fim para que o e-mail foi criado: um meio de comunicação rápido, de baixo custo e eficiente.

Desde que o primeiro spam foi enviado em 1994, a prática de enviar mensagens não solicitadas tem sido aplicada com vários objetivos distintos e também utilizando diferentes aplicativos e meios de propagação na internet. Os tipos de spam mais frequentes são correntes, boatos, lendas urbanas, propagandas, ameaças, pornografia, códigos maliciosos, fraudes e golpes, spIM (*spam via Instant Messenger*), spam via redes sociais e spit (*spam over internet telephony*) (NIC.BR, 2007).

O spam não poupa nem mesmo os novos softwares e serviços disponíveis da rede tais como os blogs, redes sociais, instant messengers, etc.

I) Correntes

As correntes, conhecidas como *chain letters*, são textos que estimulam o leitor a enviar várias cópias a outras pessoas, gerando um processo contínuo de propagação.

Um texto característico de uma corrente geralmente quase obriga o usuário (destinatário) a repassar a mensagem um determinado número de vezes ou, ainda, "para todos os amigos" ou "para todos que ama". O texto pode contar uma história antiga, descrever uma simpatia (superstição) ou, simplesmente, desejar sorte. Atualmente, o envio em massa de correntes diminuiu bastante, continuando frequente em grupos e listas de discussão de amigos.

Algumas correntes utilizam métodos de engenharia social para convencer o usuário a repassar a mensagem, ou seja, a "não quebrar a corrente", sob pena de cair em desgraça ou anos de má sorte para aqueles que recusam a enviar n cópias do e-mail para *x* pessoas nos próximos *y* dias.

Exemplos de correntes podem ser encontrados na rede como a ajuda para uma criança com câncer, que Bill Gates vai distribuir sua fortuna para todos que receberem a mensagem, empresas de telefonia que estão distribuídos aparelhos celulares de graça, etc. (Quatrocantos.com, 2007).

Em todas elas a "recompensa" só vem depois que o usuário enviar cópias da mensagem para um determinado número de pessoas.

II) Boatos

Os boatos são os conhecidos *hoaxes* que circulam na rede que contam histórias alarmantes, falsas naturalmente que chegam a causar pânico em algumas pessoas, instigando o leitor a imediatamente continuar a divulgação do texto

recebido. Frases apelativas são utilizadas tais como: "envie este e-mail para todos os seus amigos", "envie este e-mail para todas as pessoas que você ama".

Alguns dos boatos que circularam recentemente na rede: a) a Rede Globo de Televisão utiliza o dinheiro arrecadado do Criança Esperança para deduzir seu imposto; b) o Orkut será pago; c) o guaraná Kuat causa câncer e impotência; d) a combinação entre Coca-cola light e a pastilha Mentos provoca uma explosão no estômago; e) a Disney está dando a você férias grátis; f) a seleção brasileira vendeu a copa do mundo de 1988, num esquema; g) bilionário que envolveu a Nike, a Adidas, a CBF, a FIFA e os jogadores; h) o Windows possui um arquivo chamado Jdbgmgr.exe, com o ícone de um urso. que na verdade seria um vírus. Observação: esse arquivo realmente existe no Windows, mas faz parte do sistema, ou seja: não é um vírus; e i) as fotos supostas fotos de dentro do avião da Gol que caiu na floresta Amazônica, e circularam por e-mail, na verdade são *screenshots* de cenas do seriado *Lost* (Quatrocantos.com, 2007).

III) Lendas urbanas

As lendas urbanas também são histórias que trafegam na rede. Suas características diferem dos *hoaxes* pelo tom de verdade que é passado pela pessoa, trazem consigo alguma fonte de referência "o pai do meu amigo me contou", "aconteceu com um amigo do meu amigo", etc. e geralmente são histórias populares tristes ou assustadoras. Trata-se da versão tecnológica do folclore, o *netlore* (folclore na rede).

Um exemplo de lenda urbana que circulou na rede no início da década foi uma estória assustadora, o caso do roubo de rins. Falava de pessoas que foram seduzidas em boates ou ambientes noturnos, depois drogadas com soníferos fortíssimos e ao acordarem em uma banheira cheia de gelo, descobriam que tiveram um dos seus rins cirurgicamente extraído por uma quadrilha especializada na venda de órgãos humanos para transplante[7].

A história é tão comovente que imediatamente passa a ser divulgada pelo recebedor da mensagem.

IV) Propagandas

Os spams ou mensagens não solicitadas com conteúdo de propaganda são conhecidos como UCE (*unsolicited comercial e-mail*). A publicidade pode envolver

[7] Correntes, hoaxes e spams. Disponível em: http://www.e-farsas.corn/corrente_roubo_rim.htm. Acesso: 20 dez. 2007.

produtos, serviços, pessoas, novos sites, candidatos a cargos políticos, enfim, propaganda em geral, conquistando cada vez mais espaço nas caixas postais eletrônicas dos usuários.

Esse tipo de spam é motivo de discussão e polêmica, afinal, é possível fazer marketing na Internet sem fazer spam. No entanto, aqueles que insistem em divulgar sua imagem ou negócio por meio de mensagens não solicitadas, acabam comprometendo sua credibilidade. A solução é o marketing responsável na rede.

Por outro lado, alguns spams oferecem produtos que não existem e serviços que nunca serão entregues. Os casos mais comuns são os e-mails vendendo pílulas milagrosas para melhorar o desempenho sexual de homens e mulheres ou, ainda, para perder peso dormindo (NIC.BR, 2007).

A questão-chave relacionada á propaganda e ao spam é que a internet se apresenta como um meio fértil para divulgação de produtos, atinge um grande número de pessoas a baixo custo, mas na verdade quem paga a conta é quem recebe a propaganda.

A própria definição de spam é clara, ao recebermos uma mensagem não solicitada, estamos, sim, sendo vítimas de spam, mesmo que seja um e-mail de uma promoção que muito nos interessa ou um determinado produto que estamos procurando. Não existe o "spam útil".

Outro problema são os formulários e cadastros *on line*, quando o próprio internauta informa seus dados pessoais e muitas vezes passa desapercebido um campo já ativado, permitindo o envio de informações sobre produtos, separados por áreas específicas ou não. Isso ocorre, principalmente em sites que oferecem promoções, brindes, assinaturas grátis de revistas por alguns meses, etc.

Assim, a rede mundial de computadores tornou-se um território atrativo para o envio de propagandas comerciais não solicitadas.

V - Ameaças, brincadeiras e difamação

Muitas mensagens eletrônicas são enviadas com o intuito de fazer brincadeiras inconvenientes, algumas com ameaças e outras difamar amigos e amigas, namorados e namoradas, maridos e esposas, trazendo sérias consequências para estas pessoas. Sabemos que o ato de enviar uma grande quantidade de mensagens, por si, já caracteriza o spam.

Neste caso, se a pessoa natural ou jurídica, atingida por essa prática se sentir lesada pode registrar um boletim de ocorrência na polícia que após a abertura de inquérito será aberto um procedimento criminal por calúnia ou difamação.

VI - Pornografia

O envio de material pornográfico na rede é uma prática antiga e muito comum. O usuário fica constrangido ao receber uma mensagem não solicitada com fotos e cenas de sexo, inclusive de pedofilia. A publicação de fotos de nudez e práticas sexuais envolvendo crianças é crime previsto nos arts. 241 e 241-A do ECA, *in verbis*:

> Art. 241. Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
> Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa.
> Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
> Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa.
> § 1º Nas mesmas penas incorre quem:
> I – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o caput deste artigo;
> II – assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo.
> § 2º As condutas tipificadas nos incisos I e II do § 1º deste artigo são puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o caput deste artigo (Brasil, 1990).

Outro problema grave é o recebimento deste tipo de mensagem por crianças e adolescentes, que muitas vezes dominam mais a tecnologia da informática que os seus pais_ Assim, os adultos devem vigiar o que os menores estão acessando e utilizar os recursos técnicos anti-spa.m. bem corno instalar programas que permitam o monitoramento das atividades das crianças e adolescentes na rede mundial de computadores. Os casos devem ser denunciados imediatamente aos órgãos competentes.

VII - Spams via *instant messengers* e rede de relacionamentos

Com o surgimento de novos serviços e aplicativos na Internet, uma nova geração de spams tomou conta dessas tecnologias, sendo os mais populares o Orkut (rede de relacionamentos) e o MSN[8] (serviço de mensagens instantâneas).

[8] Disponível em: http://www.msn.corn.br. Acesso em: 20 dez. 2007.

O spim é o termo empregado para os "spams via Instant Messenger", ou seja, o envio de mensagens eletrônicas não solicitadas por meio dos aplicativos de troca de mensagens instantâneas como, por exemplo, o MSN e o ICQ[9].

A rede de relacionamentos mais popular atualmente é o Orkut[10], com milhões de usuários espalhados pelo globo. Em pouco tempo, as redes de relacionamento ou redes sociais multiplicaram o seu número de usuários comprovando a teoria dos seis graus de separação que diz que uma pessoa pode conhecer outra no mundo, por meio de não mais do que seis pessoas intermediárias.

Esses tipos de sites propiciam um terreno fértil para a propagação de spam, principalmente, de boatos e propagandas. Por outro lado, a maioria deles possui opções de configuração que permitem aos usuários protegerem-se das mensagens não solicitadas enviadas por pessoas que não estejam em suas listas de contatos.

VIII - Spam com vírus indexados

O vírus é um programa que entre clandestinamente no sistema e modifica o seu funcionamento. É capaz de se multiplicar infectando outros programas e fica oculto, latente no sistema, aguardando o momento e entrar em ação, quando podem causar desde pequenos transtornos até danos irreparáveis ao sistema.

Um vírus propagado por e-mail normalmente é recebido como um arquivo anexado à uma mensagem de correio eletrônico. O conteúdo dessa mensagem procura induzir o usuário a clicar sobre o arquivo anexado, fazendo com que o vírus seja executado. Quando este tipo de vírus entra em ação, ele infecta arquivos e programas e envia cópias de si mesmo para os contatos encontrados nas listas de endereços de e-mail armazenadas no computador do usuário.

É importante ressaltar que este tipo específico de vírus não é capaz de se propagar automaticamente. O usuário precisa executar o arquivo anexado que contém o vírus, ou o programa leitor de e-mails precisa estar configurado para autoexecutar arquivos anexados[11].

IX - Spam com códigos maliciosos

[9] Disponível em: http://www.icq.com. Acesso em: 20 dez. 2007.
[10] Rede social ou rede de relacionamentos. Disponível em: http://www.orkut.com. Acesso em: 20 dez. 2007.
[11] Tutorial sobre segurança e proteção. Disponível em: http://www.hostmaior.com.br/oque-virus.php. Acesso: 22 dez. 2007.

São programas que executam ações maliciosas em um computador. Diversos tipos de códigos maliciosos são inseridos em e-mails, contendo textos que se valem de métodos de engenharia social para convencer o usuário a executar o código malicioso em anexo. Em geral, estes códigos também são utilizados em spams enviados por fraudadores.

Há uma frequente confusão entre vírus, worms, trojans (cavalos-de-tróia), códigos maliciosos, etc. Vários vírus já foram classificados como worms e vice-versa.

Os worms são semelhantes aos vírus, mas possuem capacidade de replicação, geram cópias de si mesmos ou de algumas de suas partes. Para se propagar, usam recursos da rede, como o e-mail ou páginas eletrônicas da rede.

Dentre os códigos maliciosos mais comuns enviados via spam, pode-se citar as seguintes categorias, segundo NIC.BR (2007):

i) Backdoor: programa que permite a um invasor retornar a um computador comprometido. Normalmente este programa é colocado de forma a não ser notado.

ii) Spyware: termo utilizado para se referir a uma grande categoria de software que tem o objetivo de monitorar atividades de um sistema e enviar as informações coletadas para terceiros. Podem ser utilizados de forma legítima, mas, na maioria das vezes, são utilizados de forma dissimulada, não autorizada e maliciosa.

iii) Keylogger: programa capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado de um computador. Normalmente, a ativação do keylogger é condicionada a uma ação prévia do usuário, como por exemplo, após o acesso a um site de comércio eletrônico ou Internet Banking, para a captura de senhas bancárias ou números de cartões de crédito.

iv) Screenlogger: forma avançada de keylogger, capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o mouse é clicado, ou armazenar a região que circunda a posição onde o mouse é clicado.

v) Cavalo de tróia: programa, normalmente recebido como um "presente" (por exemplo, cartão virtual, álbum de fotos, protetor de tela, jogo, etc), que além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário.

Os primeiros vírus se propagavam através de disquetes infectados. Com o advento da Internet e do serviço de correio eletrônico, o uso massivo do e-mail

potencializou o uso do spam, quando os desenvolvedores de vírus perceberam que este serviço seria uma poderosa arma para propagação das chamadas "pragas virtuais", surgindo os vírus que infectam o sistema no momento que o usuário inocentemente executa aquele chamativo arquivo anexado. Para piorar aquele chamativo ou interessante arquivo anexado ao e-mail pode seu um worm, que envia cópias de si mesmo para todos os endereços da agenda de correio eletrônico do usuário e assim por diante.

X - Fraudes, golpes e engenharia social

Não é uma tarefa simples atacar e fraudar dados em um servidor de uma instituição bancária ou comercial. Então, os golpistas têm concentrado seus esforços na exploração de fragilidades dos usuários, para realizar fraudes comerciais e bancárias através da Internet.

As nuances semânticas da distinção entre fraudes e golpes, não são significativas na explanação sobre o spam. A fraude é abuso de confiança, ação praticada de má-fé, falsificação e o golpe pode ser definido como manobra desonesta com o fim de enganar, prejudicar, roubar outrem.

Para obter vantagens, os golpistas ou fraudadores têm utilizado amplamente e-mails com discursos que, na maioria dos casos, envolvem engenharia social e que tentam persuadir o usuário a fornecer seus dados pessoais e financeiros. Em muitos casos, o usuário é induzido a instalar algum código malicioso ou acessar uma página fraudulenta, para que dados pessoais e sensíveis, como senhas bancárias e números de cartões de crédito, possam ser furtados. Desta forma, é muito importante que usuários de Internet tenham certos cuidados com os e-mails que recebem e ao utilizarem serviços de comércio eletrônico ou *Internet Banking*.

Engenharia social é o termo utilizado para descrever um método de ataque, onde alguém faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações. Geralmente utilizado em e-mails ou por telefone.

Um bom exemplo de engenharia social é quando o usuário recebe uma mensagem e-mail, onde o remetente é o gerente ou alguém em nome do departamento de suporte do seu banco. Na mensagem ele diz que o serviço de Internet Banking está apresentando algum problema e que tal problema pode ser corrigido se você executar o aplicativo que está anexado à mensagem. A execução

deste aplicativo apresenta uma tela análoga àquela que você utiliza para ter acesso a conta bancária, aguardando que você digite sua senha. Na verdade, este aplicativo está preparado para furtar sua senha de acesso a conta bancária e enviá-la para o golpista.

A Internet tornou-se um terreno fértil para a disseminação de golpes, novos e antigos. Os antigos, já praticados por meio de cartas ou ligações telefônicas, migraram para a Internet, propagados via spam. Um exemplo é o Golpe da Nigéria, também conhecido como golpe do 419 ou do 171, os famosos "contos do vigário".

Os golpes nigerianos são classificados como *advance fee fraud* (AFF), ou seja, fraude da antecipação de pagamentos. Utilizando engenharia social, são elaboradas mensagens longas, contando histórias mirabolantes e pedindo que o usuário envie determinada quantidade de dinheiro, prometendo altas recompensas no futuro, quando o objetivo colocado na história for concretizado. Esses objetivos são tão diversos quanto a quantidade de golpes nigerianos. Entre eles, o financiamento para a construção de aeroportos na Nigéria, o resgate da fortuna de um parente ex-ditador da Nigéria ou outro país africano, e o resgate de um astronauta perdido numa base espacial.

Ao responder a este tipo de mensagem e efetivar o pagamento antecipado, você não só perderá o dinheiro investido, mas também nunca verá os milhares ou milhões de dólares prometidos como recompensa.

Normalmente, estas mensagens apresentam quantias astronômicas e abusam da utilização de palavras capitalizadas (todas as letras maiúsculas) para chamar a atenção do usuário. Palavras como "URGENT" (urgente) e "CONFIDENTIAL" (confidencial) também são comumente usadas no assunto da mensagem para chamar a atenção do usuário.

O usuário deve se perguntar por que foi escolhido para receber estes "milhares ou milhões" de dólares, entre os inúmeros usuários que utilizam a Internet.

Os golpes na intemet também são conhecidos como scam. Em 1998 a FTC (*Federal Trade Comission*)[12] produziu um documento onde são listados os 12 tipos de golpes mais comuns na rede, de acordo com uma análise feita em e-mails recebidos de consumidores. Os chamados *Dirty Dozen* não estão obsoletos. A lista da FTC inclui os seguintes tipos de golpes, a saber: a) oportunidades de negócio; b) venda de malas diretas; c) correntes; d) propostas para trabalho em casa; e) golpes

[12] Disponível em: http://www.ftc.org. Acesso em: 14 dez. 2007.

da dieta ou da melhoria de saúde; f) esquemas para ganho de dinheiro fácil (get-rich-quick); g) produtos gratuitos; h) oportunidades de investimento; i) kits para decodificação de sinal de TV a Cabo; j) garantia de crédito e empréstimo facilitados; l) recuperação de crédito; e m) promoções de viagens.

Como exemplo de golpes que circularam na Internet brasileira: a) o e-mail sobre uma nova vulnerabilidade identificada em um sistema operacional e a veiculação do endereço para download da correção (um código malicioso); b) a "raspadinha virtual", que oferece como prêmio um carro, mas o usuário ganha como brinde um keylogger cm seu computador, gravando tudo que é digitado, e c) o e-mail em busca de participantes para o realio, show da Rede Globo, o Big Brother Brasil 4. Segundo a mensagem não solicitada, a Rede Globo estaria selecionando participantes para o BBB4 e, para se inscrever, bastaria fazer download de um formulário (arquivo anexado com código malicioso) e preenchê-lo. Apesar dos esclarecimentos feitos pela Rede Globo, o e-mail ainda circulou muito tempo e com tipos diferentes do código malicioso.[13]

Dentre os novos golpes, o que mais se destaca é o *phishing*, também conhecido como *phishing scam*. O termo foi originalmente criado para descrever o tipo de fraude que se dá através do envio de mensagem não solicitado, que se passa por comunicação de uma instituição conhecida, como um banco, empresa ou site popular, e que procura induzir o acesso a páginas fraudulentas (falsificadas), projetadas para furtar dados pessoais e financeiros de usuários.

A palavra *phishing* (de "fishing") vem de uma analogia criada pelos fraiidadores, onde "iscas" (e-mails) são usadas para "pescar" senhas e dados financeiros de usuários da Internet (NIC.BR, 2007).

Atualmente, este termo vem sendo utilizado também para se referir aos seguintes casos: a) mensagem que procura induzir o usuário à instalação de códigos maliciosos, projetados para furtar dados pessoais e financeiros; e b) mensagem que, no próprio conteúdo, apresenta formulários para o preenchimento e envio de dados pessoais e financeiros de usuários.

Novas formas de *phishing* podem surgir, portanto é muito importante que você se mantenha informado sobre os tipos de *phishing* que vêm sendo utilizados

[13] Terra. Vírus e Cia. Disponível em: http://informatica.terra.com.br/interna/0„01148562-E1559,00.html. Acesso: 23 dez. 2007.

pelos fraudadores, através dos veículos de comunicação, como jornais, revistas e sites especializados.

Também é muito importante que o usuário, ao identificar um caso de fraude via Internet, notifique a instituição envolvida, para que ela possa tomar as providências cabíveis.

6 ATUAÇÃO DOS SPAMMERS

Numa realidade em que cada vez mais pessoas consideram os spams uma praga a ser combatida a todo custo, os spammers utilizam técnicas no mínimo duvidosas, para não dizer mentirosas, para colocar seu lixo eletrônico na caixa postal eletrônica de suas vítimas.

A primeira delas é a obtenção de listas de endereços de suas vítimas. Os endereços constantes em tais listas, apesar de serem apregoados como de pessoas que autorizaram o recebimento de e-mails comerciais, são coletados utilizando-se de técnicas nem sempre éticas, às vezes ilegais.

As demais estão elencadas nos itens a seguir, demonstrando os ardilosos artifícios usados pelos spammers, bem como as ferramentas utilizadas por eles para a elaboração e envio das mensagens eletrônicas não solicitadas.

6.1 ARTIFÍCIOS DOS SPAMMERS

São muitos os artifícios usados pelos spammers, além de usar a engenharia social para convencer o usuário da veracidade da mensagem enviada e ganhar sua confiança. Utilizam técnicas para dificultar a busca de sua verdadeira identidade, garantindo o anonimato.

O objetivo do spammer é fazer com que os seus e-mails sejam lidos e não descartados imediatamente pelo usuário, usando desculpas para o convencimento do usuário que sua mensagem é legítima e ainda a enviar algum tipo de resposta.

As desculpas mais comuns são:

a) E-mails enviados uma única vez (one-time e-mails): certas mensagens dizem que serão enviados somente uma vez e que você não precisa se preocupar, pois, não será importunado novamente. Trata-se de spam e é bem provável que você receba outras cópias do mesmo tipo de e-mail;

b) "Caso não tenha interesse em continuar recebendo este tipo de mensagem, por favor solicite sua retirada de nossa lista de distribuição, enviando e-mail para remove-me-from-list@...". Este é um dos artifícios mais frequentes usados atualmente. São os spams do tipo "remove me". A recomendação é não responder, na verdade, ao responder o usuário estará confirmando a legitimidade de seu e-mail e este possivelmente será inserido em malas direta de spammers pelo mundo afora.

c) "Se este assunto não lhe interessa, apenas delete este e-mail (*Just hit delete*)": são os que pedem para serem removidos ou ignorados, caso não sejam de seu interesse. Neste caso, antes de removê-lo, reclame. Simplesmente deletar e não reclamar, ignorando o sparn, pode torná-lo conivente, pois o spammer continuará atuando tranquilamente.

d) "Você se cadastrou em nosso site e, portanto, está recebendo esta mensagem. Caso queira sair de nossa lista de divulgação...". Uma variação do tipo *remove me*. Alguns spams se utilizam dos recursos válidos de cadastro on-line de determinados sites para dar legitimidade ao e-mail. Da mesma forma, o usuário não deve responder e deve reclamar.

e) "Você foi indicado por um amigo e por isso estamos contatando-o. Caso queira sair de nossa lista de divulgação...". Outra variação do tipo *remove me*... De fato, pode ser que o usuário tenha sido indicado por um amigo. Neste caso, um amigo spammer ;-).

f) "De acordo com a lei xxxx, este e-mail não pode ser considerado spam...": Uma das perguntas mais frequentes sobre spam na rede foi com relação a esta suposta lei citada no final de vários spams. Não existe lei nem decreto que regulamente o sparn. Basta consultar o site: http://www.spambr.org/congresso.html.

g) "Consultamos sua Nome page, e sua empresa foi selecionada para participar de ... Esperamos não ter importunado com nosso contato..."

Decididamente, qualquer das desculpas acima configuram o spam.

6.2 FERRAMENTAS DOS SPAMMERS

Alguns sites são utilizados pelos spammers para o envio de grandes quantidades de e-mails e outros que permitem falsificar o remetente, dificultando a investigação posterior de sua verdadeira identidade. São os anonimizadores que são encontrados livremente na rede.

Um dos sites mais conhecidos é o *anonymizer*[14] que permite o anonimato para navegação na rede e o envio de mensagens, no caso não solicitadas.

Existem também ferramentas que permitem a elaboração do texto do spam, mantendo um codificador e deeodificador para a composição de mensagens, bastando que o spammer digite algumas palavras, como por exemplo "caro leitor". O site spammimic[15] permite a elaboração de textos de e-mails anônimos, bem como o seu envio em massa. Como se pode verificar a própria rede oferece um verdadeiro "kit de ferramentas" para a atuação do spammer.

7 PROBLEMAS CAUSADOS PELO SPAM

O spam pode afetar os usuários do serviço de correio eletrônico, os provedores de serviço, o tráfego de dados pela rede, enfim compromete toda a estrutura do envio e recebimento de mensagens eletrônicas. Os exemplos a seguir mostram os alguns problemas causados pelo spam:

a) Não recebimento de e-mails: boa parte dos provedores de Internet limita o tamanho da caixa postal do usuário no seu servidor. Caso o número de spams recebidos seja grande, ele corre o risco de ter sua caixa postal lotada com mensagens não solicitadas. Se isto ocorrer. passará a não receber e-mails e, até que possa liberar espaço em sua caixa postal, todas as mensagens recebidas serão devolvidas ao remetente. Outro problema é quando o usuário deixa de receber e-mails nos casos em que regras anti-spam ineficientes são utilizadas, por exemplo, classificando como spam mensagens legítimas.

b) Gasto desnecessário de tempo: para cada spam recebido, o usuário necessita gastar um determinado tempo para ler, identificar o e-mail como spam e removê-lo da caixa postal.

c) Aumento de custos: independentemente do tipo de acesso à Internet utilizado, quem paga a conta pelo envio do spam é quem o recebe. Por exemplo, para um usuário que utiliza acesso discado à Internet, cada spam representa alguns segundos a mais de ligação que ele estará pagando.

d) Perda de produtividade: para quem usa o e-mail como ferramenta de trabalho, o recebimento de spams aumenta o tempo dedicado à tarefa de leitura de

[14] Disponível em: http://www.anonymizer.com. Acesso em: 12 dez. 2007.
[15] Disponível cm: http://www.spammimic.com. Acesso em: 12 dez. 2007.

e-mails, além de existir a chance de mensagens importantes não serem lidas, serem apagadas por engano ou lidas com atraso.

e) Conteúdo impróprio ou ofensivo: como a maior parte dos spams é enviada para conjuntos aleatórios de endereços de e-mail, é bem provável que o usuário receba mensagens com conteúdo que julgue impróprio ou ofensivo.

f) Prejuízos financeiros causados por fraude: o spam tem sido amplamente utilizado como veículo para disseminar esquemas fraudulentos, que tentam induzir o usuário a acessar páginas clonadas de instituições financeiras ou a instalar programas maliciosos, projetados para furtar dados pessoais e financeiros. Como vimos anteriormente, esse tipo de spam é conhecido como *phishing scam*. O usuário pode sofrer grandes prejuízos financeiros, caso forneça as informações ou execute as instruções solicitadas nesse tipo de mensagem fraudulenta.

8 PREJUÍZOS DECORRENTES DO SPAM

O spam causa prejuízos econômicos para o internauta, por perturbar sua rotina, tomar seu tempo de acesso pago ao provedor e molestá-lo.

Mas os prejuízos não são só contra o intemauta, os spammers também atentam contra os provedores de acesso à internet, que gastam desnecessárias horas de trabalho para exclusão ou obstrução de spams destinados a seus usuários.

Em certas ocasiões chegam a paralisar suas atividades temporariamente, para manutenção.

Para sobreviverem aos spammers, os provedores dc acesso têm que aderir a uma banda superior às suas necessidades para transmissão dc dados, sob pena de congestionamento em decorrência do indesejado e desnecessário tráfego de mensagens comerciais não solicitadas, o que implica em mais gastos a serem repassados ao consumidor final.

9 O SPAM ZOMBIE

O termo inglês *zombie* pode ser traduzido para o vernáculo como zumbi. Com a evolução tecnológica e ousadia dos *crackers*, as denominadas "máquinas zumbis" tornaram-se grandes aliadas na aplicação de golpes virtuais.

O nome se refere a computadores controlados remotamente por um invasor para a prática de ilícitos, sem que seu proprietário desconfie.

A expressão spam *zombie* é uma particularização dos "computadores zumbis", com o propósito específico de disseminar spams, que pode ser assim definida:

> Spam zombies são computadores de usuários finais que foram comprometidos por códigos maliciosos em geral, como worms, bois, vírus e cavalos de tróia. Estes códigos maliciosos, uma vez instalados, permitem que spammers utilizem a máquina para o envio de spam, sem o conhecimento do usuário. Enquanto utilizam máquinas comprometidas para executar suas atividades, dificultam a identificação da origem do spam e dos autores também. Os spam zombies são muito explorados pelos spammers, por proporcionar o anonimato que tanto os protege (NIC.BR, 2007).

Destarte, como os spammers estão cada vez mais se valendo de computadores alheios para a prática do spam, como se poderia imputar a responsabilidade a esses verdadeiros "laranjas informáticos", que eventualmente poderão ser identificados como agentes em uma perícia, mas que tampouco sabem que seus computadores estão infectados por códigos maliciosos e que automaticamente realizam o envio dessas execráveis mensagens.

Uma solução seria disciplinar legalmente a obrigatoriedade de proteção dos computadores, através de softwares antivírus ou similares, como meio de coibir que tais equipamentos, de imenso potencial danoso, pudessem ser indevidamente utilizados.

O spammer que realmente deveria ser apontado como causador do ato ilícito poderá permanecer anônimo, dadas as dificuldades impostas por esses novos softwares de disseminação de spam.

Não há como rastrear esse agente, visto que simplesmente distribui os códigos maliciosos pela grande rede, a exemplo dos vírus, que se disseminam rapidamente, instalando-se nos computadores de terceiros, restando praticamente impossível prever o poder de alastramento dessas ferramentas de envio de mensagens e os correlatos danos que poderão ocasionar.

10 TÉCNICAS DE COMBATE AO SPAM

O combate ao spam nunca foi e nunca será uma tarefa fácil. Desde que o problema do envio de mensagens não solicitadas começou, diversos sistemas,

métodos, técnicas, etc., foram desenvolvidos com a pretensão de acabar, senão minimizar o sofrimento dos usuários na rede.

Bill Gates, dono da Microsoft, em um encontro com executivos do Fórum Econômico Mundial em 2004, chegou a prometer em "um mundo livre do spam até 2006", afirmando que sua empresa vem trabalhando em uma solução contra o spam, que será baseada no conceito de "provar" ou identificar o verdadeiro e-mail do remetente. Entre os métodos envolvidos está um que envolve trabalho humano. Por exemplo, exigir que o usuário desvende algum código, que só poderá ser descoberto com a presença humana de forma que o spam seja economicamente inviável para o remetente. A principal ideia, diz Gates, é "atingir o bolso do spammer" (FOLHA ONLINE, 2004).

O objetivo de um sistema anti-spam é reduzir o número de spams recebidos por um usuário, classificando as mensagens para, então, depois filtrá-las.

Esses sistemas estão em constante evolução já que para cada novo sistema, tenta-se criar técnicas para enganá-lo e permitir a passagem dos spams.

As principais propriedades de um sistema anti-spam são a sua taxa de falsos positivos e de falsos negativos, ou seja, a taxa de mensagens legítimas classificadas como spams e vice-versa. Em geral, a taxa de falsos positivos tem um valor mais importante, já que uma mensagem legítima acaba sendo filtrada, o que pode gerar grandes transtornos e atrasos no processo de comunicação. Já os falsos negativos têm um impacto menor, já que o usuário irá receber o spam, mas provavelmente acabará apagando-o.

Outro aspecto importante de um sistema anti-spam é a sua interferência com o usuário, seja ela por necessidade de configuração, manutenção, atualização ou desafios que são feitos ao usuário e que devem ser respondidos. Quanto maior o nível de interação com o usuário, mais complexo e menos amigável o sistema acaba se tornando, dificultando sua adoção em grande escala.

Os métodos de filtragem de uma forma geral são divididos em duas classes: filtros de conteúdo c filtros de bloqueio, a saber: a) Filtros de conteúdo: são aqueles que trabalham analisando o conteúdo do e-mail, procurando padrões, indícios que a mensagem seja um spam. Os mais conhecidos são: filtros baseados em regras; filtros estatísticos e filtros baseados em desafio e resposta; e b) Filtros de bloqueio: são aqueles baseados na filtragem direta de e-mails originários de reconhecidas

fontes de spam. Muitos provedores têm listas negras de domínios, redes, servidores que mantém *relay* ou *proxy* abertos.

Os métodos de filtragem descritos acima, possuem vantagens e desvantagens e nenhum deles tem eficácia total, gerando outros problemas para os provedores de serviço dc correio eletrônico como processos judiciais questionando suas listas negras, chegando até ao encerramento de atividades de muitos deles.

10.1 PERSPECTIVAS FUTURAS

Mesmo com todas as técnicas anti-spam, ativistas dos movimentos anti-spam, campanhas educativas, etc. não existe hoje nenhum indício que permita afirmar que a atividade de enviar spams diminuirá nos próximos anos. Ao contrário, os spammers vêm se especializando e em contra-ataque usando técnicas cada vez mais elaboradas para burlar os sistemas anti-spam.

Vale ressaltar que os sistemas anti-spam estão em constante evolução já que para cada novo mecanismo criado, novas técnicas são desenvolvidas pelos spammers para enganá-los e permitir a passagem das mensagens não solicitadas.

Uma nova forma de mensagem não solicitada que está surgindo é o spam através de serviços de voz sobre IP (VoIP). Os spams de VoIP, também chamados de spits (*Spam over Internet Telephony*), consistem de mensagens, em sua maioria de conteúdo publicitário, enviadas em difusão através de serviços de telefonia IP e a tendência é que o volume de spams dessa natureza cresça em virtude do aumento do número de usuários dos sistemas de telefonia sobre IP. O combate a este tipo de spam ainda é mais difícil, devido a necessidade do desenvolvimento dc algoritmos de reconhecimento de voz, que demandam hoje um alto custo financeiro e até agora não são muito eficientes, devido a dificuldades técnicas, não podendo esquecer que a mensagem não solicitado VoIP é similar a uma ligação telefônica comum, em tempo real e até que algum trecho seja ouvido, analisado, o mecanismo torna-se ainda mais ineficiente.

As mensagens não solicitadas em forma dc vídeo também estão surgindo e assim como os spams de VoIP são difíceis de ser classificadas, já que para analisar o conteúdo das mensagens de vídeo são necessárias técnicas de processamento e reconhecimento de padrões de imagem. Os spams de vídeo estão começando a aparecer em sites da Internet que, sem a permissão do usuário, carregam e mostram um determinado vídeo, que na maioria das vezes possui um conteúdo

publicitário. Dessa forma, durante a exibição do vídeo, a atenção do usuário é desviada para o anúncio, devido aos sons e aos movimentos. A identificação dos spams de vídeo é complexa, pois em muitas ocasiões um site contém um vídeo que é do interesse do usuário e, portanto, não deve ser considerado como um spam.

Outra forma indireta de spam corresponde à manipulação do resultado de mecanismos de busca na Internet, como o Google. A finalidade desses spams é fazer com que um determinado produto ou site apareça como uma das primeiras referências retornadas pelos mecanismos de busca, quando é realizada a busca de determinadas palavras. Para manipular os mecanismos de busca, os spammers se aproveitam do fato de que esses mecanismos, geralmente, dão mais importância a sites que são referenciados por outros sites da Internet. Dessa forma, um spammer cria vários sites que contém apenas atalhos para um determinado site do seu interesse. Neste site, que na maioria das vezes tem conteúdo pornográfico ou comercial, são inseridas palavras com as quais se deseja manipular o resultado dos mecanismos de busca. Geralmente, estas palavras estão camufladas e não têm qualquer relação com o conteúdo do site. Assim, como o site do interesse do spammer contém a palavra buscada e é muito referenciado por outros sites, ele acaba tendo um resultado de destaque na busca e, conseqüentemente, atrai um grande número de usuários que somente após acessar o site descobrem o seu real conteúdo.

Na luta contra os spams, deve-se levar em consideração que a maioria dos usuários da Internet não tem formação técnica em informática, possuindo uma capacidade limitada para gerenciar e configurar seus computadores. Portanto, é fundamental que se construam sistemas o mais independentemente possível da intervenção humana. Uma das propostas nesse sentido é a proposição de sistemas autônomos para combater os spams. A ideia é fazer com que os sistemas anti-spam sejam capazes de se adaptar, sem a intervenção humana, às novas técnicas que vão sendo criadas pelos spammers. Tais sistemas devem possuir, além da característica de auto-aprendizado já encontrada cm alguns sistemas atuais, as propriedades de auto-gerenciamento, automanutenção, auto-configuração e auto-recuperação.

Assim, ficou claro que o envio dc spams se tornou uma atividade financeira atrativa para os spammers tanto para anunciar produtos e serviços quanto pela possibilidade dc enriquecimento ilícito através de fraudes. Para tanto, os spammers

estão se especializando cada vez mais. Neste sentido, prevê-se uma batalha interminável entre os spammers e os desenvolvedores de sistemas anti-spam, o que torna ainda mais necessária, a criação de medidas legais para punir os infratores.

11 O SPAM E O DIREITO

Na falta de uma definição doutrinária, unânime, acerca do assunto, a definição mais aceita do spam é o envio não solicitado, indesejável, de mensagens eletrônicas, ao destinatário. O spam engloba todo tipo de mensagem, seja particular ou comercial.

A grande controvérsia sobre o spam não é a sua definição, sua conceituação, mas a sua legalidade.

Basicamente duas correntes podem ser identificadas, sendo que a primeira argumenta que a inexistência de uma legislação específica e proibição expressa do envio de mensagens eletrônicas não solicitadas, não autorizadas pelo destinatário, legitima o envio do spam, inclusive sustentam que essas mensagens não trazem nenhum prejuízo ao mesmo, unia vez que a ele assiste a possibilidade de descartar ou desconsiderar tais mensagens (Stacchini, 2007).

Os adeptos da outra corrente sustentam que o spam além de facilitar e propagar atividades ilegais (muitos spams contém correntes de dinheiro, racismo, pornografia, discriminação religiosa, difamação, etc.), causa prejuízos ao destinatário (que paga o serviço de acesso à rede, além do tempo utilizado para receber, abrir, filtrar ou deletar essas mensagens) e também ao provedor (além dos riscos de vírus e pragas virtuais aos seus clientes, congestionam o tráfego dc dados na rede), não podendo esquecer que a obtenção do endereço eletrônico e envio da mensagem não solicitada também afronta o direito constitucional do destinatário à privacidade.

11.1 O DIREITO BRASILEIRO

Não existe uma legislação específica no Brasil sobre o spam, as mensagens eletrônicas não solicitadas, ou o spamming, a prática do envio de spam.

Muitos projetos de lei foram apresentados nas duas casas legislativas, a Câmara dos Deputados e o Senado Federal, projetos estes que serão analisados na segunda parte deste trabalho.

A inexistência de legislação específica não impede que o ordenamento jurídico vigente seja acionado para coibir os abusos desta prática indiscriminada, o envio de mensagens eletrônicas não solicitadas.

O spam viola a intimidade das pessoas que têm proteção constitucional como disposto no art. 5° da CRFB/88:

> [...]
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
> [...]
> XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal (Brasil, 1988).

Como visto acima o spamming é uma conduta que fere a inviolabilidade da privacidade dos internautas, desrespeitando seus direitos personalíssimos, também previstos no art. 21 do CC: “Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma” (Brasil, 2002).

Muitos são os danos provocados pelos spammers, ao lotar as caixas de mensagens dos internautas, ocasionando gastos de tempo e dinheiro, sem contar os incontáveis prejuízos causados aos provedores dc acesso a rede mundial de computadores que são obrigados a aumentar a banda para tráfego das informações, congestionadas pelos milhões e milhões de mensagens indesejadas enviadas por eles.

O Código Civil é claro no comando do art. 186: “Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito” (Brasil, 2002).

Além de permitir no art. 12 que cesse imediatamente a ameaça ou lesão a direito da personalidade: “Art. 12. Pode-se exigir que cesse a ameaça, ou a lesão, a direito da personalidade, e reclamar perdas e danos, sem prejuízo de outras sanções previstas em lei” (Brasil, 2002).

Seguramente o spamming também é considerado abuso de direito, previsto no art. 187 do CC: “Art. 187. Também comete ato ilícito o titular de um direito que,

ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes" (Brasil, 2002).

Da nossa melhor doutrina, Rosenvald e Farias (2007, p. 525), ao exemplificarem o abuso de direito em concreto:

> Efetivamente, é possível destacar ampla aplicação em sede civil, valendo enunciar, para fins de fixação da matéria, algumas hipóteses concretas: (...) envio de mensagens eletrônicas não solicitadas, por e-mail (Internet), apresentando produtos ou serviços para comercialização, periodicamente e, não raro, em grande quantidade (o chamado spam);

Para Tartuce (2004, p. 89),

> O spam consiste no envio de e-mails ou mensagens eletrônicas sem solicitação, prática que se tomou comum no meio cibernético. Para nós, consiste em modalidade de abuso de direito. Primeiro, porque há quebra da boa-fé objetiva, já que nenhuma mensagem é solicitada. Segundo, porque há um desvio na finalidade sócio-econômica da internet.

Sobre a responsabilidade civil nos meios eletrônicos, Gonçalves (2007, p. 105) menciona que,

> A responsabilidade extracontratual pode derivar de inúmeros atos ilícitos, sendo de destacar os que dizem respeito à concorrência desleal, à violação da propriedade intelectual, ao indevido desrespeito à intimidade, ao envio de mensagens não desejadas e ofensivas da honra, à divulgação de boatos infamantes, à invasão da caixa postal, ao envio de vírus, etc.

O art. 927, sacramenta a obrigação de indenizar: "Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo" (Brasil, 2002).

Outros diplomas trazem dispositivos perfeitamente aplicáveis ao spam, como pontua Vidonho Júnior (2003), a saber: a) art. 65 da LCP (revogado pela lei 14.132/21); b) arts. 146, 265 e 266 do CP; e c) arts. 4°, I e III, 6°, II e IV, 33, 36, 37, 39, II, III, IV, V e parágrafo único, 43, §§ 2° e 3°, 51, III, IV e XV, 66, §§ 1° e 2°, 67, parágrafo único (vetado), 72 e 73 do CDC.

Ao contrário do que é propalado pela imprensa em matérias sensacionalistas que a internet é uma terra sem lei, o ordenamento jurídico atual é perfeitamente aplicável ao mundo virtual, dependendo por obvio de alguns ajustes necessários devido a evolução tecnológica.

Ressalte-se por fim, que vários outros dispositivos do ordenamento jurídico brasileiro podem ser aplicados, dependendo do ilícito praticado juntamente com o spamming.

11.2 A LEGISLAÇÃO NORTE-AMERICANA

Preocupado com as avassaladoras estatísticas sobre o spam, o governo norte-americano propôs o *Can-Spam Act*[16], uma abreviação de *Controlling the Assault of Non-Solieited Pornography and Marketing Act*[17], que é a lei que veda as mensagens eletrônicas de cunho comercial não solicitadas.

A norma legal entrou em vigor em 01/01/2004 e representa o primeiro estatuto federal dos Estados Unidos que regulamenta o spam, muito embora se tenha conhecimento da existência de várias leis estaduais editadas em tempo anterior, todas com a finalidade de impor sanções aos spammers.

Apesar dos méritos da nova legislação, doutrinadores já estão antevendo problemas futuros advindos de alguns de seus dispositivos. Como exemplo, o critério do *opt-out*, adotado pela lei, permite que todo comerciante possa enviar mensagens eletrônicas para qualquer destinatário, até que seja informado de que não deseja mais recebê-las.

Não se sabe ainda quais serão os efeitos que tal lei acarretará fora do território norte-americano, como no Brasil, onde sabidamente há uma grande quantidade de spammers e ainda não existe uma legislação específica sobre o assunto.

Conforme observado com a vigência do *Can-Spam Act*, o governo norte-americano encontra-se empenhado em resolver de uma vez por todas os transtornos que o spam vem causando.

11.3 A LEGISLAÇÃO EUROPEIA

Atualmente os países europeus dispõem já de legislação sobre atividade de caráter informático, proteção de dados e inclusive relacionados com o problema do spam.

---

[16] Site norte-americano Spam Laws. Disponível em: http://www.spamlaws.com/f/pdf/p1108-187.pdf. Acesso em: 10 fev. 2008.

[17] Pode ser traduzido como "lei que controla o ataque de pornografia e do marketing não solicitados".

Inclusive alguns países apresentam leis que promovem a modalidade *opt-in* (ex: Alemanha, Áustria, Dinamarca, Finlândia, Grécia, Itália, Noruega, etc.), enquanto noutros países como a Espanha e a Bélgica se encontra em fase de discussão.

A abordagem definitiva do problema do spam pelo direito comunitário veio à luz com a Diretiva sobre Privacidade nas Comunicações Eletrônicas, de 2002[18].

Esta diretiva foi preparada em um momento no qual os efeitos do spam já se faziam sentir com bastante nitidez e crescia a demanda por barreiras, inclusive de cunho legislativo. Assim, foi este o primeiro instrumento legislativo que se ocupou diretamente deste problema no direito comunitário.

A norma atual da União Europeia que protege os dados pessoais, privacidade nas comunicações eletrônicas e as comunicações eletrônicas não solicitadas é a Diretiva Comunidade Europeia 2002/58/EC.

12 CONCLUSÃO

O fenômeno do spam representa um dos maiores desafios da era digital, afetando diretamente a segurança da informação, a privacidade dos usuários e a eficiência das comunicações eletrônicas. A evolução das tecnologias de internet, ao mesmo tempo em que proporcionou avanços significativos na troca de informações, também facilitou a proliferação do envio massivo de mensagens eletrônicas não solicitadas, trazendo consigo diversos impactos negativos. O estudo demonstrou que o spam não se limita a um mero incômodo, mas se configura como um problema complexo que envolve questões técnicas, econômicas, sociais e jurídicas.

A análise histórica do spam evidencia sua rápida transformação ao longo dos anos, desde sua origem até sua sofisticação atual, em que novas técnicas e ferramentas são utilizadas para ludibriar usuários e burlar filtros de segurança. Os spammers adotam artifícios cada vez mais engenhosos, explorando vulnerabilidades e desenvolvendo estratégias de disfarce para disseminar suas mensagens de forma massiva e indiscriminada. O impacto dessas práticas é evidente tanto para os usuários individuais, que sofrem com caixas de entrada sobrecarregadas e

[18] No site http://www.euro.cauce.org pode ser encontrada uma sistematização detalhada por país, e onde se procura promover o trabalho de sensibilização face à má utilização da Internet, particularmente do spam, defendendo a promulgação de leis que defendam abordagens *opt-in*.

exposição a conteúdos indesejados, quanto para as empresas e provedores de serviço, que enfrentam altos custos para gerenciar e mitigar os efeitos dessa prática abusiva.

Os prejuízos causados pelo spam vão além da mera perturbação no recebimento de mensagens. O artigo demonstra que há implicações econômicas significativas, pois empresas precisam investir em infraestrutura para lidar com o fluxo excessivo de e-mails não solicitados. Além disso, o spam é frequentemente utilizado como veículo para disseminação de fraudes, golpes financeiros e ataques aos sistemas de informação, como phishing e propagação de malware, aumentando a vulnerabilidade dos usuários e das instituições. Dessa forma, o combate ao spam se torna não apenas uma questão de conveniência, mas um aspecto essencial da segurança digital global.

No âmbito jurídico, a ausência de uma legislação específica sobre spam no Brasil evidencia um vácuo normativo que dificulta a repressão efetiva dessa prática.

Embora existam dispositivos constitucionais e infraconstitucionais que possam ser aplicados para coibir o envio indiscriminado de mensagens eletrônicas não solicitadas, como normas de proteção à privacidade e ao consumidor, a falta de uma regulação clara e objetiva favorece a impunidade dos infratores. A experiência de países como os Estados Unidos e as nações da União Europeia demonstra a importância de legislações específicas para estabelecer critérios e sanções aplicáveis ao envio de spam, bem como mecanismos de proteção aos usuários.

A dificuldade na regulamentação do spam decorre, em grande parte, da necessidade de equilibrar a proteção dos direitos fundamentais, como a liberdade de expressão e o direito à informação, com a imposição de restrições ao uso indevido das ferramentas de comunicação digital. Modelos regulatórios como o opt-in e o opt-out foram analisados ao longo do artigo, destacando-se a necessidade de uma abordagem equilibrada, que impeça abusos sem inviabilizar o uso legítimo da internet para fins comerciais e informativos. Além disso, o debate sobre a responsabilidade dos provedores de serviço no controle do spam continua sendo um tema central na formulação de políticas públicas e regulatórias.

O combate ao spam exige uma abordagem multidisciplinar, combinando esforços legislativos, avanços tecnológicos e conscientização dos usuários.

Soluções tecnológicas, como filtros de conteúdo, listas de bloqueio e sistemas de autenticação de remetentes, são fundamentais para mitigar o impacto

do spam, mas não são suficientes para eliminá-lo completamente. A participação ativa dos usuários na adoção de boas práticas, como o uso de softwares de proteção e a não divulgação indiscriminada de endereços de e-mail, é igualmente essencial para reduzir a disseminação de mensagens não solicitadas.

Além das medidas regulatórias e tecnológicas, a conscientização da população sobre os riscos do spam e a importância da segurança digital deve ser incentivada por meio de campanhas educativas. Muitas fraudes e ataques aos sistemas de informação ocorrem devido à falta de conhecimento dos usuários sobre os perigos do spam e sobre como identificar mensagens maliciosas. A implementação de programas educativos, tanto no âmbito acadêmico quanto corporativo, pode contribuir significativamente para a redução dos danos causados pelo spam e para o fortalecimento da cultura de segurança digital.

Outro aspecto relevante é o impacto global do spam e a necessidade de cooperação internacional para seu combate. Como a internet não possui fronteiras, o envio de mensagens não solicitadas pode ser realizado de qualquer lugar do mundo, tornando desafiadora a aplicação de legislações nacionais. Dessa forma, iniciativas de colaboração entre países, como a adoção de padrões internacionais de segurança e o compartilhamento de informações sobre práticas fraudulentas, são essenciais para enfrentar esse problema de forma mais eficaz.

Diante do exposto, conclui-se que o combate ao spam deve ser tratado como uma prioridade no âmbito jurídico, tecnológico e social. A criação de uma legislação específica no Brasil, alinhada às melhores práticas internacionais, aliada ao fortalecimento das políticas de segurança da informação e à educação digital, pode contribuir para a mitigação dos impactos negativos dessa prática. A evolução constante das técnicas utilizadas pelos spammers exige uma resposta igualmente dinâmica e adaptável, garantindo a proteção dos usuários e a manutenção da integridade da comunicação eletrônica.

Por fim, destaca-se que a luta contra o spam não pode ser conduzida de forma isolada. A cooperação entre governos, empresas de tecnologia, provedores de internet e usuários é essencial para a construção de um ambiente digital mais seguro e confiável. Somente com esforços conjuntos e estratégias bem estruturadas será possível reduzir os danos causados pelo spam e garantir que a internet continue sendo um espaço democrático, seguro e eficiente para a troca de informações.

REFERÊNCIAS

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Brasília, DF: Presidência da República, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 10 dez. 2007.

BRASIL. **Constituição da República Federativa do Brasil**: promulgada em 5 de outubro de 1988: atualizada até a Emenda Constitucional nº 56, de 20.12.2007. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 23 dez. 2007.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: Presidência da República, 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/Leis/L8078.htm. Acesso em: 10 dez. 2007.

BRASIL. **Decreto-Lei nº 3.688, de 3 de outubro de 1941**. Lei das Contravenções Penais. Brasília, DF: Presidência da República, 1941. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3688.htm. Acesso em: 10 dez. 2007.

BRASIL. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940**. Código Penal. Brasília, DF: Presidência da República, 1940. Disponível em: https://www.planalto.gov.br/CCIVIL_03/Decreto-Lei/Del2848.htm. Acesso em: 10 dez. 2007.

BRASIL. **Lei nº 8.069, de 13 de julho de 1990**. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Brasília, DF: Presidência da República, 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 10 dez. 2007.

CAMPOS, Ivan Moura. Futuro da internet: entre o elitismo e o computador popular, abr. 2002. Disponível cm: http://www.cg.org.br/infoteca/artigosientrevista7.htm. Acesso em: 01 dez 2007.

CASTELLS, Manuel. **Fim de milênio**. 2. ed. São Paulo: Paz e Terra, 1999. p. 411-438. (A era da informação: economia, sociedade e cultura, v. 3).

CORRÊA, Gustavo Testa. Aspectos jurídicos da internet. 2. Ed. São Paulo: Saraiva, 2002.

DRUCKER, Peter. O futuro já chegou. Disponível em: http://www.fea.usp.br/ead451/pd/pd1.htm. Acesso em: 01 out. 2007.

FERNANDES, Dilson Bastos. **O Estatuto jurídico do spamming no Brasil**. 2008. 144 f. Dissertação (Mestrado em Direito) - Faculdade de Direito do Vale do Rio

Doce, Governador Valadares, 2008, Universidad Politécnica y Artistica del Paraguay, Maestria em Derecho, Assunção, abr. 2008.

FERNANDES, Dilson Bastos (org.). Dicionário de tecnologia. Governador Valadares, abr. 2003. (Notas de aula)

FERRAZ Jr., Tercio Sampaio. "Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado", em 24 ago. 2006 Disponível em http://www.terciosampaioferrazjr.com.br/?q=/publicacoes-cientificas. Acesso em: 10 jan. 2008.

FOLHA ONLINE. Notícias. Gates promete um mundo sem spam em 2006. **Folha de S. Paulo**, 26 jan. 2004. Disponível em: http://www1.folhamol.com.br/folha/informatica/ult124u15034.shtml. Acesso em: 15 jan. 2008.

GANDELMAN, Henrique. **De Gutenberg à internet**: direitos autorais na era digital. 4. ed. amp. e atual. Rio de Janeiro: Record, 2001. p. 221.

GATES, Bill. **A empresa na velocidade do pensamento com um sistema nervoso digital**. São Paulo: Companhia das Letras, 1999. p. 391.

GONÇALVES, Carlos Roberto. **Direito civil brasileiro**. São Paulo: Saraiva, 2007. v. 4.

HALEMBECK, Luiz Fernando Amaral. **Arranjos societários usuais em negócios de intemet**. *In*: SCHOUERI, Luís Eduardo (org.). Internet o direito na era virtual. Rio de Janeiro: Forense, 2001. p. 9.

KAKU, William Smith. **Internet e comércio eletrônico**: pequena abordagem acerca da regulação da privacidade. *In*: ROVER, Aires José (org.). Direito, sociedade e informática: limites e perspectivas da vida digital. Florianópolis: Fundação Boiteaux, 2000. p. 82.

KAMINSKI, Omar. A Esfinge do cyberespaço desafia o mundo jurídico. Disponível em: http://www.neofito.com .br/artigos/art03/eletronico_pdf015_neo to.pdf. Acesso em: 29 dez. 2007.

LORENZETTI, Ricardo L. **Comércio Eletrônico**. São Paulo: Revista dos Tribunais, 2004.

MUSEU do Computador, 2004. Disponível em: http://www.museudocomputador.com.bdinternet.php. Acesso em: 04 dez. 2007.

NIC.BR. Núcleo de Informação e Coordenação. Tipos de spam. Propagandas. Disponível em: http://www.antispam. br/tipos/#2. Acesso em: 20 dez. 2007a.

NIC.BR. Núcleo de Informação e Coordenação. O que é spam? Disponível em http://www.antispam. br/conceito/. Acesso em 15 dez. 2007b.

PAESANI, Liliana Minardi. **Direito e internet**. 2. ed. São Paulo: Atlas, 2003.

PECK, Patricia. **Direito digital**. São Paulo: Saraiva, 2002.

PEREIRA, Josecleto Costa de Almeida. **Ciberespaço e o direito do trabalho**. *In*: ROVER, Aires José (org.). Direito, sociedade e informática: limites e perspectivas da vida digital. Florianópolis: Fundação Boiteaux, 2000. p. 52.

QUATROCANTOS.COM. As lendas, as verdades e as meias-verdades. Meias-mentiras pela ordem de análise e inserção. Disponível em: http://www.quatrocantos.com/LENDAS/index_crono.htm. Acesso: 20 dez. 2007.

ROSENVALD, Nelson; FARIAS, Cristiano Chaves de. **Direito civil**. Teoria geral. 6. ed. Ed. Lumen Juris, 2007.

RUIZ, Osvaldo López. Manuel Castells e a "era da informação", abr. 2002. Disponível em: http://www.comciencia.br/reportagens/internet/frameset/net16.htm. Acesso em: 01 nov. 2007.

SANTOS, Antônio Jeová. **Dano moral na internet**. São Paulo: Método, 2001. p. 13.

SCHULTZ, Peter A. B. A internet é um sistema autosustentável? abr. 2002. Disponível em: http://www. comciencia.br/reportagens/internetlnetl4.htm. Acesso em: 01 dez. 2007.

STACCHINI, Fernando Farano. Aspectos do lixo eletrônico ou spam. Disponível em http://www.abdi.org.br/artigos.php?artigo=7. Acesso em: 28 dez. 2007.

TARTUCE, Flávio. "**Considerações sobre o abuso de direito ou ato emulativo civil**". Questões Controvertidas no Novo Código Civil. Belo Horizonte: Ed. Método, 2004. v. 2.

VIDIGAL, Geraldo Facó. "infocrimes e responsabilidade na Internet", **Jornal Folha de São Paulo**. 15 abr. 2000. Disponível em http://www1.folha.uol.com.brifsp/dinheiro/fil504200015.htm. Acesso em: 15 dez. 2007.

VIDONHO JÚNIOR, Amadeu dos Anjos. O spam sob a ótica jurídica da dignidade. **Jus Navigandi**, Teresina, ano 7, n. 63, mar. 2003. Disponível em: http://jus2.uol.com.bridoutrina/texto.asp?id----3798. Acesso em: 07 fev. 2008.

VOGT, Carlos. O futuro da internet - Parábola do cão digital, abr. 2002. Disponível em http://www.comeiencia.br/reportagens/framereport.htm. Acesso em: 01 dez. 2007.

ZANETTI, Robson. A internet em beneficio do acesso a informação jurídica. **Jornal O Estado de São Paulo**, seção Economia, São Paulo. Disponível em http://www.estado.estadao.com.br. Acesso em: 27 jan. 2008.