O *SPAM* E O DIREITO BRASILEIRO*

Amaro Moraes e Silva Neto

RESUMO

Aduz que toda informação é passível de ser transformada em *bit,* o menor elemento atômico do DNA da informação, o que fez surgir o correio eletrônico, meio eficaz, mas inseguro de envio de mensagens. Algumas delas, com ou sem objetivos comerciais, são impostas, ou seja, para recebê-las, o destinatário não manifestou sua vontade mediante a disponibilização do seu endereço eletrônico, caracterizando-se o *spam*.

Ressalta que já existem grupos especializados em formar listas de endereços e comercializá-las sem autorização e que, para criá-las, são empregados vários artifícios, entre outros, pequenos textos gravados nos computadores de quem os acessam e funcionam como espiões de dados armazenados.

Ao final, salienta que, embora se argumente que o *spam* pode ser evitado por meio de filtros, estes correm o risco de funcionar como censores da informação; que, no Brasil, já estão em discussão projetos de lei para regulamentar as questões referentes à internet; bem como que o anonimato facilitado pela rede propicia a ocasião para a prática, inclusive, de crimes, destacando que, pelos embaraços criados, é preciso buscar meios de coibir o *spam* na legislação nacional.

PALAVRAS-CHAVE

Spam; Direito da Informática; Informática Jurídica; correio eletrônico; informação; internet.

* Conferência proferida no "Congresso Internacional de Direito e Tecnologias da Informação", realizado pelo Centro de Estudos Judiciários, nos dias 3 e 4 de outubro de 2002, no auditório do Superior Tribunal de Justiça, Brasília-DF.

OS ÁTOMOS SE DESVANECEM

Uma irreversível mudança se processou. O que era um grão de areia se tornou uma imensa praia. Devido a essa modificação, em vez dos átomos que costumeiramente são pegos, passou-se a manipular *bits*, que não podem ser pegos e que se tornam mais influentes na vida do *homo digitalis*, a cada dia.

O volume, o peso e a atomicidade não são expressões relevantes nos tempos digitais. *Softwares*, arquivos-textos ou meros dados de programas guardam valor, na maior parte das vezes, infinitamente superior ao de seu continente (o disquete, o CD ou o disco rígido de seu computador que mantêm registradas essas informações).

Essa nova máquina do choque dos milênios é, em verdade, qual a bolsa de Fortunatus. O que dela se tira é aparentemente impossível e inesgotável. Em se conectando à internet, aí é como se estivesse especificamente a usar o próprio chapéu de Fortunatus, eis que para "qualquer lugar" é possível ser levado[1].

A humanidade passou da era da valoração do aparente para a da valoração do invisível, do intangível, do imaterial, na qual, presentemente, destacam-se os *bits*.

Entretanto... o que é um *bit*[2]?

Um *bit* é algo que, como a água, não tem cheiro, não tem gosto e não tem cor. Porém seus (não) atributos são mais que esses. Um *bit*, como complementa Negroponte, também, não tem *tamanho ou peso e é capaz de viajar à velocidade da luz. Ele é o menor elemento atômico do DNA da informação. É um estado: ligado ou desligado, verdadeiro ou falso, para cima ou para baixo, dentro ou fora, branco ou preto*[3] – e é fragílimo...

Pode estar em tudo que for relativo à informação, visto que, em princípio, toda informação (escritos, desenhos, sons e imagens) é passível de ser digitalizada e, por conseqüência, transformada em *bits*.

Ele é o "papel", a "tinta", o "envelope", o "selo" e o "carteiro" da correspondência eletrônica.

Na internet, o homem desse *brave new world*[4] somente pode exercitar-se por meio de informações. E elas só podem ser alcançadas ou transmitidas de duas formas: por meio do acesso a um *website*[5] qualquer ou pelo recebimento de informações através do correio eletrônico, comumente conhecido como *e-mail* (ou *eletronic mail*), ou por intermédio de *softwares* de comunicação instantânea, *v.g.*, o *ICQ*[6].

E-MAIL, UM POPULAR – MAS INSEGURO – MEIO DE COMUNICAÇÃO.

Por certo os idealizadores da Arpanet (que se transformou na conhecida internet) não imaginaram que o correio eletrônico, o popular *e-mail*, tomaria as proporções que tomou. Todavia várias foram as razões a justificar sua popularização: rapidez, baixo custo (a transmissão de um milhar de mensagens pela internet tem um custo equivalente ao de uma "carta física"), desnecessidade de remetente e destinatário estarem simultaneamente disponíveis.

Em termos de comunicação, assim como os inquilinos do planeta são devedores de Morse e Bell[7], igualmente o são em relação a Ray Linson, o inventor do correio eletrônico, no final de 1971.

Entrementes, a par dessas vantagens, o correio eletrônico é um meio de comunicação bastante inseguro, porquanto, antes de uma mensagem eletrônica chegar a seu destino, ela realiza uma longa e tortuosa viagem. Parte do computador remetente para o computador de seu provedor de acesso à internet (*ISP*)[8] e, na seqüência, passa por incontáveis outros servidores até alcançar seu destinatário. Portanto, em primeiro lugar, constata-se que os administradores (*webmasters*) dos provedores de acesso podem, facilmente, vasculhar o conteúdo dos *e-mails* que retransmitem, que neles aportam durante a transmissão, ou que simplesmente recebem.

Além dos provedores que têm acesso direto às mensagens eletrônicas, outros podem interceptá-las em seu curso porque tais mensagens enviadas chegam a passar por centenas de pontos no planeta – aleatórios e sempre novos – antes de alcançarem seus destinatários. Daí a facilidade de serem adulteradas, acrescendo-lhes ou excluindo-lhes texto. Também podem ser interceptadas e sumariamente excluídas, apagadas. Afinal os *bits* (aquelas "coisas" que não são "coisas") se misturam sem qualquer esforço e os seus rastros não são tão facilmente identificáveis ou descobertos.

Enfim, a transmissão de *e-mails*, no que diz respeito à privacidade, não difere muito das transmissões mediante sinais de fumaça dos índios da América nortista (na época em que eram devastados) ou dos sons dos tambores de muitas tribos africanas (que ainda resistem à devastação). Ninguém se responsabiliza pela integridade dos *e-mails* remetidos. Não há a quem se queixar caso as mensagens eletrônicas não cheguem a seus destinatários. Não há como saber se foram alteradas ou não. Quanto aos remetentes, oxalá sejam quem dizem ser!

"*A única solução para a fragilidade do* e-mail *é a criptografia*"[9]*, afirma Gage, da Sun. Além de tornar as mensagens inescrutáveis, métodos de criptografia como o* PGP[10] *garantem duas outras coisas importantíssimas: a identidade do remetente, registrada por uma assinatura eletrônica, e a integridade da mensagem. Se ela for de alguma forma adulterada em seu trajeto, o* PGP *aponta. "Recomendamos aos nossos usuários que usem o* PGP"*, diz Caio Túlio Costa, diretor executivo do Universo Online, o serviço de informação via* internet *dos grupos Abril (que publica EXAME) e Folha*[11].

Se as informações eletronicamente transmitidas não forem protegidas e, concomitantemente, houver o objetivo de um trânsito sigiloso para a mensagem a ser transmitida, talvez seja mais prudente a utilização de um megafone em praça pública. Ele guarda menores riscos de indevida divulgação do que a transmissão convencional de *e-mails*. Ao menos não haverá a ilusão da preservação da privacidade.

MENSAGENS ELETRÔNICAS NÃO-SOLICITADAS, UMA VISÃO GERAL.

As mensagens eletrônicas não-solicitadas podem ser classificadas formalmente em duas categorias: as que não têm objetivos comerciais (*spam*[12] *lato sensu*) e as que os têm (*spam stricto sensu*)[13].

Materialmente, o *spam* pode ser típico (o envio massivo de *e-mails*) e atípico (o envio de um único *e-mail*). Para efeitos consumeristas e civis, pouco importa que se trate de um *spam stricto sensu* típico (remessa de *e-mails* comerciais a uma infinidade de destinatários) ou de um *spam lato sensu* atípico (um *e-mail* não-comercial enviado a um único destinatário). Frise-se que essas diferenças formais e materiais se prestam apenas para a determinação da tipificação penal.

O mero recebimento da correspondência eletrônica não caracteriza

o *spamming*[14]. Tampouco o seu volume. O que caracteriza sua ilicitude (contravencional, penal, consumerista ou civil) é o fato de a mensagem não ter sido solicitada pelo "webnauta". Portanto, caso o destinatário tenha, eventualmente, visitado algum *website* e se inscrito em determinada lista para receber informações sobre tais ou quais produtos (ou talvez se inscrito em um *newsgroup*[15]), não há que se falar em *spamming*.

O *spam* também se caracteriza quando os dados foram espontaneamente fornecidos, mas o volume de mensagens eletrônicas for excessivo ou divorciado de seus propósitos originais. Quando dados são cedidos a fornecedores de bens ou serviços, é lícito se pressupor que esses dados serão utilizados apenas nas situações objeto de contratação. Ressalte-se, outrossim, que se o responsável por tais informações cedê-las a terceiros, responderá solidariamente com aqueles que praticarem o *spam*.

(...) *mesmo que o usuário* motu proprio *e voluntariamente tenha cedido seus dados, não pode o receptor dar destinação para a qual recebeu. Assim, por exemplo, se os dados foram necessários para identificar o comprador, será ilícita a conduta de quem repassa esses dados a terceiros que têm como objetivo precípuo atulhar* e-mails *com suas mensagens publicitárias. Daí, haver responsabilidade solidária entre o fornecedor de dados e o remetente do* spam[16].

Como se vê, a par de, em princípio, ser indispensável a não-solicitação da mensagem recebida para a ocorrência do *spam*, existem exceções à regra.

Como não poderia deixar de ser, os vigaristas das três dimensões também migraram para o mundo virtual, pois viram, nos mares da *web*[17] muita água para fisgarem novos peixes, com seus eternos projetos para tornarem ricos alguns "escolhidos", *verbi gratia*, as tradicionais pirâmides[18], nas quais é oferecida a possibilidade de serem angariadas algumas dezenas de milhares de reais, sem trabalho e em exíguo espaço de tempo! Para tanto basta que sejam enviados alguns míseros reais a esses virtuais redentores digitais – e a algumas outras pessoas por eles indicadas – *et voilà! Tout le Monde est millionaire!* Só que não é bem assim...

A seu lado, mas sem tais ladinos mecanismos em mente, tipos desocupados e bisonhos seguem suas brumas nesses etéreos oceanos digitais, na busca de outros cardumes. Típico exemplo são aqueles que iniciam uma corrente[19], ou que indicam alguém para participar de alguma.

Seguindo-os vêm os que tentam convencer os "webnautas" que, em Taiwan, fetos e cérebros humanos são disputadas guloseimas, ou que um japonês radicado em Nova Iorque (EUA) vende gatos bonsai criados em garrafas, ou que aparelhos telefônicos celulares estão sendo distribuídos gratuitamente ou ... Eles são os responsáveis pelos boatos (*hoaxes*) da internet.

O *spam* também se caracteriza quando os dados foram espontaneamente fornecidos, mas o volume de mensagens eletrônicas for excessivo ou divorciado de seus propósitos originais. Quando dados são cedidos a fornecedores de bens ou serviços, é lícito se pressupor que esses dados serão utilizados apenas nas situações objeto de contratação.

No início de julho (de 2000), os proprietários do Motel Ilha de Capri, em São Bernardo, na grande São Paulo, levaram um susto. O telefone não parava de tocar. Os clientes, exaltados, queriam saber por que o motel filmava os casais que passavam por lá. A história da filmagem se espalhou rapidamente, na mesma proporção em que o movimento despencou. A causa: um e-mail*. O Ilha de Capri se tornou mais uma vítima dos* hoaxes*, os trotes que circulam pela internet. O caso está nas mãos do Setor de Investigação de Crimes de Alta Tecnologia e Meios Eletrônicos da Polícia de São Paulo. Embora a investigação não esteja concluída, o rastreamento dos* e-mails *apontou para quatro funcionários da Basf, que coincidentemente está localizada a poucos quilômetros do motel. A empresa não comenta o assunto, mas acredita que seus funcionários apenas receberam as mensagens. Ironicamente, em maio a Basf enviou a todos os funcionários um documento com orientações sobre o uso da internet, que prevê até demissões por justa causa. Todo mundo assinou*[20].

Os boatos divulgados na internet são, certamente, muito mais perigosos e perniciosos do que aqueles do mundo das três dimensões, dada a inequívoca facilidade de sua retransmissão. Certa feita, um boato sobre bactérias apresentadas em bananas custou às empresas que intermedeiam o produto, nos EUA, cerca de trinta milhões de dólares de prejuízos, pois que os consumidores deixaram de comprar a extravagante fruta oriunda dos trópicos. E esse não é um caso isolado.

A Emulex (EUA), em razão dos boatos enviados por um rapaz de vinte e três anos, perdeu, no ano 2000, cerca de dois bilhões de dólares da América nortista. Já o gatuno digital lucrou duzentos e quarenta mil dólares – o que foi um solar indício para ser preso pelo FBI[21] (que dispõe do mais sofisticado sistema de monitoramento e rastreamento das mensagens da rede).

No Brasil, é conhecido o episódio envolvendo o empresário Ricardo Mansur e um seu grande desafeto da época: o Banco Brasileiro de Descontos S/A (Bradesco). Consoante as investigações, esse empresário teria se valido de um falso *e-mail* do correio eletrônico baseado[22] *Hotmail* (http://www.hotmail.com), o qual teria sido criado em um cibercafé[23] londrino. Por meio dessa conta de correio eletrônico, ele teria enviado incontáveis informes a pessoas ligadas ao mundo financeiro, discorrendo sobre a fragilidade da saúde financeira do Bradesco. Mais tarde, já no Brasil, pelos computadores de suas empresas, ele teria acessado a conta de correio eletrônico que virtualmente criara. Em razão das provas indiciárias e da sua ingenuidade, ele acabou sendo preso. Foi um dos primeiros casos do gênero apurados no Brasil. A conduta foi enquadrada como atentado à segurança do mercado financeiro, que teria sido praticada mediante o envio de *e-mails* em massa, qual seja, *spam*[24].

Outro curioso boato que invadiu as caixas postais eletrônicas dos "cibernautas" brasileiros, no final do ano 2001, dizia respeito ao fim da soberania brasileira sobre a Amazônia. Diversos órgãos da imprensa nacional e estrangeira publicaram a mentira como sendo verdade.

Uma enxurrada de e-mails *inunda a internet brasileira há um mês denunciando o fim da soberania nacional. A mensagem informa, em tom raivoso, a existência de um livro didático nos Estados Unidos no qual a Amazônia não integra mais o mapa brasileiro. As crianças americanas apreenderiam, desde a década de 80, que a região está sob tutela americana e da Organização das Nações Unidas. A correspondência eletrônica refere-se ao vasto território como* Former International Reserve of Amazon Forest *(Finraf). Algo traduzido por Ex-Reserva Internacional da Floresta Amazônica.*

Domingo passado, dia 25 (de novembro de 2001), até a agência de notícias France Press registrou o boato, baseado em uma nota da coluna Hildegard Angel, de O Globo – desmentida pela própria colunista ontem. No mesmo dia, o Tribuna da Imprensa também caiu na esparrela. Antes, o Estado de S. Paulo havia publicado uma nota, em 23 de maio de 2000, com a história. Nos dias 12 e 14 de junho e em 6 de outubro do mesmo ano, desmentiu-a[25].

Por fim existem, também, as boas (e estúpidas) almas que sempre informam que alguém perdeu um cachorro, ou que a operação para a extração da hérnia de um sujeito foi um sucesso. No entanto, se a "boa alma" tivesse de pagar por seu precioso informe tão propalado e divulgado por meio da internet, será que ela o tornaria público, no mundo físico, com as mesmas arrebatadoras proporções a que se dispõe no mundo pós-arpanet? Remeteria centenas (ou milhares ou milhões) de cartas impressas, envelopadas e seladas que implicam custo? Teria tempo para realizar o mesmo número de telefonemas? Certamente não. As forças motrizes de sua despropositada ação residem na comodidade de um único procedimento para lograr seus objetivos, na ausência de despesas e na facilidade que o próprio código da rede autoriza.

Como é visto, no dia-a-dia, diversas são as mensagens que aportam nas caixas de correio eletrônico dos internautas. Das mensagens de amigos, amores, correspondentes ou procedentes de *spammers*[26] dos mais variados rincões do planeta e com os mais diversos objetivos.

Essas figuras podem-se enquadrar na Lei das Contravenções Penais, nos Códigos Penal, de Defesa do Consumidor e Civil e na Lei dos Crimes contra a Economia Popular, dependendo dos objetivos e do volume dos *spams*.

BANCOS DE DADOS: MALA DIRETA OU MALA *FIDEM*[27]?

Para um *spammer* remeter sua malfadada mensagem a milhares de pessoas é *conditio sine qua non* que ele disponha de uma base de dados, na qual conste, pelo menos, o *e-mail* dos cidadãos, vítimas de seu estorvo "bítico". E em tempos e termos de internet, os bancos de dados dos *spammers* (*lato sensu*), via de regra, são comprados (ou cedidos) ou formados ilicitamente.

CDs com e-mails *são vendidos livremente. Há diversos* sites *que, ilegalmente, vendem endereços de pessoas físicas e jurídicas em forma de CDs. O "Informática" falou com um dos vendedores, que se identificou como Geraldo e menosprezou a legislação. "Não há nada que proíba isso". A advogada Andrea Monteiro Affonso afirma que a atividade é ilegal porque a Constituição brasileira protege os dados pessoais. Os CDs têm até 1,5 milhão de* e-mails *e custam cerca de R$ 300,00. Vêm com um* software *para facilitar o trabalho de mala-direta. Herman Wecke, membro do movimento* Anti-Spam *diz que esses programas fazem a entrega do* e-mail *diretamente ao destinatário, sem passar pelo servidor de correio dele, e ainda ocultam o remetente.*

O publicitário Paulo Vogel, que criou o site NoSpam *repudia a prática. "Apesar de surtir algum resultado, é anti-ético"(K.A.)*[28].

A **compra (ou cessão) ilícita** pode-se processar mediante a aquisição de *e-mailing lists*[29] – que, no início do milênio, eram oferecidas aos borbotões na *web*. Sua ilicitude repousa no fato de que quem negocia os dados do cibernauta não possui qualquer autorização para tanto. A compra (ou cessão) ilícita também pode ocorrer quando os dados oferecidos *sponta sua* em um determinado *website* são cedidos a terceiros (a título gratuito ou oneroso), sem o seu consentimento.

Nas *e-mailing lists* **formadas ilicitamente**, seus autores (que podem ser *spammers* ou não) se valem de diversos expedientes. Participando de *chat-rooms*[30] ou *newsgroups*, eles se apropriam, dissimuladamente, dos endereços eletrônicos de seus partícipes. Visitando *websites* que disponibilizam endereços *on-line* (o que é bastante freqüente[31]), copiam-nos. Também se valem de *spiders*[32] para coletar *e-mails* na rede[33].

Nas hipóteses suscitadas (informações obtidas sem conhecimento e autorização dos destinatários), por provável a base de dados do *spammer* será ilegal, nos moldes da legislação consumerista. E, em sendo ilegal essa base de dados, o *spamming* também o será: se espúria é a causa, necessariamente espúria terá de ser a conseqüência. É a teoria da árvore envenenada[34].

COOKIES[35], A BOA MATÉRIA-PRIMA PARA A CRIAÇÃO DAS LISTAS DOS *SPAMMERS*.

Nos *websites* – e isso é uma regra – os *webmasters*[36] têm o discutível hábito de colocar em suas páginas pequenos arquivos-textos (*cookies*) que são gravados nos computadores dos que os acessam para, então, poderem obter informações de seus visitantes. Contudo, com as informações que obtêm, podem criar grandes bancos de dados (e, como a experiência informa, eles os criam), onde constam, evidente e invariavelmente, os *e-mails* indevidamente conseguidos.

Em 2001, o *website* Submarino (www.submarino.com.br) passou a utilizar *cookies* que, depois de analisados por um *software* específico desenvolvido por suas próprias equipes técnicas, passavam a enviar mais de meio milhão de *spams* para os seus clientes cadastrados, com ofertas estruturadas sobre os hábitos do destinatário. A empresa Lojas Americanas (www.americanas.com.br), entre outras companhias brasileiras, também adotou o sistema.

Por ser a privacidade protegida constitucionalmente (e, em parte, disciplinada pelos Códigos Penal, de Defesa do Consumidor e Civil), evidente resta que os *webmasters* têm de ter a autorização dos internautas quando de sua colocação.

Considere-se, outrossim, que o acúmulo de *cookies* em um computador faz com que ele perca velocidade, além de sujeitá-lo a mais invasões, haja vista que um *cookie* pode roubar até a sua senha de acesso à própria rede[37].

Por isso, no final do ano 2001, muitos donos de *websites* na Europa estavam deveras preocupados. A razão? A aprovação, pelo Parlamento da Comunidade Comum Européia (CCE), da proposta de restrição ao uso indiscriminado de *cookies* aos 21 de novembro de 2001 e, dessarte, a obrigação de seus países-membros proibirem o uso de *cookies* sem o consentimento explícito dos cidadãos europeus.

Como bem ponderou o Parlamento Europeu, quando Romano Prodi era presidente da Comissão Européia, os *cookies* são instrumentos para a espionagem dos hábitos dos usuários da internet e seu uso representa potencial ameaça para a utilização abusiva dos dados pessoais de seus cidadãos-membros.

Os deputados da CCE pretenderam, com essa medida, que os *websites* de seus albergados passassem a adotar a política de opção pelo recebimento de *cookies* por parte dos "cibernautas", antes que a turbação digital tivesse vez.

Tecnicamente, no que diz respeito a seu recebimento, os *cookies* podem ser enquadrados em duas categorias: *cookies opt-in* e *cookies opt-out*. No primeiro caso (*opt-in*), o internauta opta pela aceitação dos *cookies* de monitoramento. No segundo caso (*opt-out*), o cibernauta deverá manifestar seu desejo de **não receber** os *cookies*. A CCE, na resolução de 21 de novembro de 2001, só contempla a hipótese dos *cookies opt-out*.

Na defesa desses espiões digitais a *IAB* (*Interactive Advertising Bureau*)[38], conhecida sociedade inglesa defensora dessa mídia, argumentava serem os *cookies* são imprescindíveis para o bom e regular desenvolvimento do comércio eletrônico, pois facilitam as compras realizadas pelos usuários da internet, dando-lhes maior motivação e comodidade. Porém, facilitam mesmo? Se objetivamente for avaliado o argumento dos defensores dos *cookies* (a velha ladainha da importância da navegação personalizada para os internautas), será constado que tudo isso não passa de um embuste. Entrementes, a grande verdade – e a razão dos vociferares indignados – é que a proposta de lei da CCE provocará um prejuízo anual de aproximadamente setecentos milhões de reais para o setor de publicidade na internet. Assim, visando unicamente a seus interesses comerciais, a *IAB* lançou a campanha "salvem nossos *cookies*".

> (...) o acúmulo de *cookies* em um computador faz com que ele perca velocidade, além de sujeitá-lo a mais invasões, haja vista que um *cookie* pode roubar até a sua senha de acesso à própria rede. (...) os *cookies* são instrumentos para a espionagem dos hábitos dos usuários da internet e seu uso representa potencial ameaça para a utilização abusiva dos dados pessoais de seus cidadãos-membros.

No Brasil, os *cookies*, quando da colisão dos séculos, já eram objeto de discussão não apenas no Legislativo (sempre ávido em cristalizar desnecessárias leis), mas também no Ministério Público de São Paulo. Em razão da provocação n. 0071532/00 (protocolizada aos 11 de setembro de 2000), foram abertos três inquéritos civis para apurar as responsabilidades de *webmasters* de *sites* de grande notoriedade[39].

OUTRAS "CHOCADEIRAS" DE *SPAM*

Com a sofisticação dos *e-mails* com *HTML*[40], advieram novos riscos à segurança digital, visto que surgiu mais uma forma para devassar a privacidade.

Os *spammers* com vocações lombrosianas[41] se valem de meios tecnológicos de intrusão mais sofisticados. Com *spywares*[42] acessam os bancos de dados e acoplam-nos aos seus! Por meio dessa tecnologia, colocam programas de monitoramento no disco rígido do computador de suas vítimas.

Milhares de internautas que visitaram um site *de entretenimento estão descobrindo um emaranhado de componentes indesejados e potencialmente danosos em seus micros. É o resultado de uma campanha publicitária maliciosa organizada por uma empresa de Los Angeles, nos EUA.*

A história começa na página FlowGo (www.flowgo.com), que é capaz de plantar arquivos no PC.

Comprado pela IntelliTech (www.visitiws.com), o espaço publicitário trazia um recurso que redirecionava o navegador para um site *chamado "KoolKatalog", que atualmente está fora do ar.*

O visitante era convidado a fornecer seu endereço de e-mail *para participar de um jogo. A proposta era a seguinte: resolva o quebra cabeça e ganhe um prêmio.*

Mesmo que o usuário não clicasse em nada, o dano real já estaria quase consumado. Explorando falhas numa antiga versão da linguagem Java presente no navegador Internet Explorer, o site *secretamente colocava dez arquivos no disco-rígido do computador.*

O parasita, que foi considerado um dos cinco principais vírus de abril pela Symantec, monitora os hábitos de navegação da vítima na internet e pode fazer o micro travar[43].

Deploravelmente, a remessa de imagens transparentes junto com os arquivos *HTML* foi uma praxe que se tornou comum na virada do milênio. Quando lido o *e-mail*, *on-line*, o arquivo oculto na imagem transparente que ele trazia anexado entrava em ação e avisava ao *spammer* estar ativo o endereço da vítima/destinatária[44]. Daí para a frente, o internauta deveria se preparar para as ondas do maremoto de *e-mails* que eclodiriam nas praias de sua caixa de correio eletrônico.

Também existem os ataques *crackers,* que, após quebrarem as bases de segurança de determinado *website* (ou computador pessoal), acessam ilegalmente informações, delas se apropriam e formam suas *e-mailing lists*.

FILTRANDO OS *SPAMS*

O intrusivo "meio publicitário" de que sempre se valeram os *spammers* para lograr seus objetivos tende a alcançar proporções que não só incomodarão muitíssimo mais os usuários da rede como, ainda, aumentarão a gama dos riscos à combalida privacidade que pode ser desfrutada na *web*.

Os "bíticos" e abúlicos defensores do *spam* arriscam-se a dizer que ninguém deve preocupar-se com

essa mala direta digital por não ser ela nenhuma ameaça à privacidade dos internautas ou à rede como um todo. Aos que discordarem de sua argumentação, de pronto ripostarão: "Não lhe apraz *spams*? Então os apague ao recebê-los, ative um filtro que impeça seu recebimento ou remetanos um *e-mail* manifestando seu desejo de não ser destinatário". Descaradamente sugerem isso por terem a inabalável consciência de que somente essas são as alternativas tecnológicas disponíveis para evitar o recebimento dos *spams* – causadores de perda de tempo e de dinheiro, além de injustificados aborrecimentos derivados de suas indesejabilidade e inutilidade.

A possibilidade de "manifestação de não-recebimento" é uma "cibertapeação". Os primeiros defensores dessa "opção" foram os senadores Murkowsky e Torricelli (dos EUA), os quais criaram o instituto do *opt-out*.

De acordo com esse sistema, o *spammer* pode enviar *spams* desde que coloque a possibilidade de o internauta destinatário manifestar seu interesse por seu recebimento. Condensando a exposição: admitem que *spam* é crime, mas só depois da segunda vez... isso é uma leviandade legislativa! Na realidade, em vez de proibirem o *spam*, legalizaram-no.

Todavia, como bem alerta a Cauce[45], esse sistema não poderia funcionar, basicamente por dois motivos: existem muitos marqueteiros e excessivas listas de *e-mails* disponíveis na internet. Além disso, não pode ser esquecido que, a cada *spamming* o *spammer* pode mudar seu *e-mail* – o que não elide a conduta ilícita, mas que dificulta, sobremodo, sua apuração.

Quando do recebimento de um primeiro *spam*, o internauta terá de alterar as configurações do sistema de filtragem de seu correio eletrônico para, doravante, tal mensagem não ser mais recebida (ou melhor, lida), haja vista que o simples apagar ou o mero filtrar não solucionam o problema. E por diversas razões.

Pro primo porque, pelo menos em algum momento, a memória RAM[46] do disco rígido do computador do usuário da rede será vítima de um ataque por parte desses indesejáveis posseiros digitais, pois para o processo da filtragem da não-solicitada mensagem – e seu igualmente indesejável remetente – será necessário abri-la, copiar os detalhes que se prestarão para o critério de exclusão (normalmente o *e-mail* do remetente ou o assunto [*subject*] reportado), aplicar os filtros de *software* de correio eletrônico e, finalmente, apagar o indesejável *spam*. Algo que os *spammers* dizem "não custar nada", aos "cibernautas" é imposto muito trabalho... Considerando-se, ainda, que não se trata de pugnar pelo não-recebimento de um único e solitário *spam*, mas de centenas ou milhares de mensagens de *spammers* renitentes, constata-se que o trabalho e o conseqüente aborrecimento crescem na mesma proporção. Os serviços dos "webnautas" são unilateral e impositivamente contratados pelos *spammers* – mas sem carteira profissional de trabalho assinada, e com a obrigação de os destinatários arcarem com o pagamento de seus próprios salários e demais ônus do empreendimento dos *spammers*!

Pro secundo, sempre o recipiente de mensagens eletrônicas do destinatário (seja o do provedor de acesso à internet, seja o de um correio eletrônico baseado) guardará os *spams*, porquanto o filtro não impede o recebimento da mensagem. O filtro permite ao internauta ter em sua lista de *e-mails* recebidos apenas os que deseja receber, mas não evita que as mensagens indesejáveis permaneçam em seu computador ou em seu correio eletrônico baseado. Qual seja, os *spams* terão de ser recebidos e todos aqueles que dispõem de um correio eletrônico terão o dispensável trabalho de, em algum momento, apagá-los.

Em se abrindo o *software* de correio instalado em seu computador, as mensagens filtradas, por regra, não irão para a pasta "Lixeira". Logo, terão de ser apagadas. Se abrir seu correio eletrônico baseado, as mensagens estarão guardadas em uma pasta normalmente chamada "*e-mails"* em massa. Como se verifica, tanto num quanto noutro caso, a mensagem não-solicitada terá de ser apagada em algum momento.

Pro tertio, reste consignado haver um limite para as mensagens a serem filtradas, do mesmo modo que há um limite para as que podem ser recebidas. Haverá, dessarte, um momento em que ocorrerá a saturação e os novos *spams* não poderão ser "filtrados". Aí será atingido o *no return point*.

Nos correios eletrônicos baseados, o problema será sentido com mais ênfase – e mais dramaticamente –, pois o número de *e-mails* que podem ser bloqueados é bem menor. Deve também ser ponderado que, quanto maior for o número de filtros ativos, mais operações serão realizadas pelo computador para eliminar as mensagens pré-selecionadas (filtradas), o que reduzirá seu desempenho e provocará um indesejável e inútil aumento temporal nas atividades dos usuários dos serviços disponibilizados pela internet.

Além disso, o congestionamento decorrente do *spamming* afeta as comunicações (comerciais ou de negócios, amorosas ou de pesquisa) que têm vez na *web*, haja vista que mensagens não-solicitadas enviadas aos milhões ocupam considerável espaço na banda de transmissão, causando um sensível prejuízo aos cidadãos/usuários da grande rede de computadores.

FILTROS DAS PROVEDORAS DE ACESSO: RISCOS, INEFICIÊNCIA E ILEGALIDADE.

Por vezes, algumas empresas provedoras de acesso à internet agem por conta própria e sem o consentimento e o conhecimento do usuário/cidadão, filtram determinados *e-mails* que vêm em massa (mas que necessariamente não são *spams*), com o aparente objetivo de evitarem aborrecimentos aos que fruem de seus serviços. No entanto essa atitude, implica nítida censura à liberdade de expressão consolidada por todas as constituições ocidentais modernas e, ademais, pode ocultar escusos interesses.

Existem, outrossim, outros problemas corolários que não guardam características legais ou jurídicas, mas técnicas ou tecnológicas. Isso porque, quando é aplicado um filtro qualquer, necessariamente surgem efeitos colaterais. Como os antibióticos, além do alvo objetivado, os filtros das ISPs também atacam partes boas e saudáveis do sistema que pretendem preservar.

E-mails vindos de um mesmo endereço (www.mesmo-endereço.com.br), mas de remetentes diferentes (spammer@mesmo-endereço.com.br e boa-pessoa@mesmo-endereço.com.br) acabam tendo o mesmo destino se a ISP colocar a *URL*[47] www.mesmo-endereço.com.br como referência de bloqueio em suas listas de filtragem.

Algumas pessoas constataram que os e-mails *que enviam a um membro da AOL voltam porque a AOL os colocou em sua lista negra de remetentes que enviam um número excessivo de mensagens.*

Os administradores de redes empresariais podem adotar o sistema Real Time Black Hole List *(http://mail-abuse.org/rbl), que intercepta e elimina mensagens oriundas de um internauta ou provedora específicos e também permite o acesso a determinados* websites.

Mas toda vez que isso acontece, cria-se um conflito: a organização responsável pelo sistema é acusada de praticar censura e responde que está apenas oferecendo informações que os administradores usam por conta própria. Os usuários comuns normalmente não tomam conhecimento do que está acontecendo[48].

Um filtro obedece a um padrão lógico de seleção e, desse modo, apoiado nessa base, age. Porém os filtros não guardam os mesmos princípios lógicos das sinapses, o que acaba por criar indesejáveis confusões e descartáveis problemas. A Lei da Decência das Comunicações (*Communications Decency Act CDA*)[49], da América nortista, comprovou isso em 1996.

O Congresso norte-americano recentemente apreciou uma legislação obrigando todas as escolas e universidades que recebem verba federal a instalarem filtros de acesso à internet.

*Muitas organizações logo se opuseram a tal medida, alegando que, conforme já ficou decidido no julgamento que declarou a inconstitucionalidade da denominada Lei da Decência (*Decency Act*) nos Estados Unidos da América, é impossível se estabelecer um padrão para censurar as informações disponíveis na* NET.

Segundo a American Civil Libertation Union*, www.aclu.org, os programas-filtro são ainda muito incipientes e restringem inevitavelmente o acesso a muitas informações importantes, representando um claro impecilho à liberdade de expressão.*

Sites *da própria* American Civil Libertation *e até mesmo de entidades religiosas como a* American Family Association *já foram indevidamente bloqueadas por programas-filtro somente porque continham palavras consideradas atentatórias como sexo ou erótica, mesmo que em um contexto que nada tinha de atentatório.* Sites *educativos ou médicos, por exemplo, são vítimas freqüentes da ineficácia dos programas-filtro.*

Segundo a ACLU*, esses programas devem ser utilizados segundo critérios definidos pelos pais e educadores e não impostos pelo governo, até mesmo porque os programas filtro reduzem em muito a quantidade de informação disponível. Um exemplo clássico: por algum tempo a maioria dos programas filtro bloquearam o acesso ao* site *Exploração de Marte,* Mars Exploration*, simplesmente porque existia um número muito grande de letras s-e-x juntas no documento*[50].

AS *NEWSLETTERS*[51] E O *SPAM*

Do mesmo modo que existem filtros que barram o recebimento de *e-mails* em massa, também existem filtros impeditivos de envio de *e-mails* em massa que, necessariamente, não se confundem com *spam*. Ao aplicarem esses filtros, as ISPs, em tese, violam diversas prerrogativas civis e constitucionais daqueles que contrataram seus serviços. Mesmo assim, os provedores brasileiros não só aplicavam uma prévia censura em certas ocasiões, como publicamente declaravam fazê-lo no início do milênio.

Muitos usuários de e-mails *pensam que a culpa por eles receberem tantos* spams *é do provedor de acesso. Na verdade, o provedor é proibido de divulgar os* e-mails *de seus assinantes para fins de mala direta virtual. Alguns, para diminuir a quantidade de mensagens indesejadas, instalam filtros em seus servidores para que o internauta possa bloquear um determinado endereço e não receber mais* e-mails *dele. Outra opção adotada pelos provedores é a limitação dos destinatários.*

> Quando do recebimento de um primeiro *spam*, o internauta terá de alterar as configurações do sistema de filtragem de seu correio eletrônico para, doravante, tal mensagem não ser mais recebida (...), haja vista que o simples apagar ou o mero filtrar não solucionam o problema.

Foi o que fez o Terra Networks*. Segundo Sérgio Pretto, diretor de tecnologia do Terra, essa é uma forma de apenas minimizar o incômodo. "Os spammers são capazes até de mandar um* e-mail *por vez para burlar os provedores de acesso",* diz*. Nenhum deles divulga número limite de destinatário por mensagem para evitar que os* spammers *e empresas divulgando seus serviços descubram.*

Pretto conta que se o Terra Networks *perceber que algum usuário está enviando mensagens para vários destinatários de uma vez só, ele será advertido. Se ocorrer de novo, sua conta será suspensa. A maioria dos provedores atua dessa forma.*

A AOL*, além de delimitar destinatários, tem um filtro que avalia se um* e-mail *está sendo enviado para vários participantes da* AOL*. "Nesse momento, já percebemos se é* spam *e deletamos", conta Sílvia Rossi, diretora de conteúdo da* AOL*.*

O IG também tenta controlar o tráfego de spam *na rede, principalmente por ser um provedor de* e-mail *gratuito. Para isso, todo usuário deve fazer um recadastramento com o CPF.*

Guto Araújo, diretor de produção do Yahoo! Brasil afirma que foram incorporadas soluções técnicas para coibir a prática do spam *e diminuir o recebimento dessas mensagens. Entre elas está o uso de filtros, limitação de número de destinatários e os* e-mails *em massa recebidos são dirigidos a uma pasta separada na caixa de entrada.*

"Spam *é uma prática grave e incômoda para o usuário", diz Maria Ercília Galvão Bueno, diretora de conteúdo do* BOL*. Uma das medidas adotadas é que não é possível mandar* e-mail *sem ser usuário do* BOL*. Um* software *monitora a quantidade de destinatários e os* e-mails *suspeitos passam por uma triagem, feita por funcionários do portal. Todo usuário que pratica* spam *tem seu* e-mail *cancelado, invariavelmente, garante Maria Ercília.*

O UOL *também utiliza essas formas para conter o abuso e oferece filtro para que o assinante possa bloquear* e-mails *indesejados (C.G. e K. A.)"*[52].

GUERRA AO SPAM

Os spammers *estão na mira do* UOL. *Quem usa um servidor próprio de* e-mail *para enviar mensagens em massa via* Speedy *descobriu que a porta 25, usada pelo servidor* SMTP, *foi bloqueada. Como resultado, só* e-mails *enviados via servidor* UOL, *vigiado pelo provedor, chegam ao destinatário.*

EFEITO COLATERAL

De acordo com o diretor geral do UOL, *Caio Túlio Costa, a medida afeta apenas usuários identificados como* spammers. *Mas alguns usuários dizem que todos, sem distinção, sofreram o bloqueio. Curiosamente, o bloqueio da porta 25 não afeta o envio de mensagens de* e-mail *para a* sub-rede – *no caso para outros usuários do próprio* UOL[53].

Em princípio, a aplicação desses filtros fere o art. 5º da Lei n.7.716, de 5 de janeiro de 1989 (define os crimes resultantes de preconceitos de raça ou de cor), a saber:

Recusar ou impedir acesso a estabelecimento comercial, negando-se a servir, atender ou receber cliente ou comprador:

Pena: reclusão de um a três anos.

Uma provedora de acesso é um estabelecimento comercial e seus usuários são seus clientes. Logo, a negativa de atender suas solicitações de serviço (no caso o recebimento ou envio de *e-mails*), em tese, configura crime nos moldes da citada Lei.

O art. 163 do Código Penal dispõe que é crime inutilizar ou deteriorar coisa alheia[54]. Mas, seria o *e-mail* coisa? Em o não sendo, a conduta da ISP estaria enquadrada no art. 305, do CP, *ex vi*:

Art. 305 – Destruir, suprimir ou ocultar, em benefício próprio ou de outrem, ou em prejuízo alheio, documento público ou particular verdadeiro, de que não podia dispor:

Pena: reclusão, de dois a seis anos, e multa, se o documento é público, e reclusão, de um a cinco anos, e multa, se o documento é particular.

Nas brasíleas terras, no ano 2001, surgiram as primeiras questões nesse sentido. O Judiciário foi ágil e, liminarmente, aqueles que aparentemente foram vítimas de censura de seus provedores de acesso à internet restabeleceram seus direitos. Destacam-se, entre esses debutantes casos judiciais, o envio de *newsletters*, por parte de dois jornalistas brasileiros a seus assinantes.

> Para receber o *spam*, o internauta é forçado a pagar sua conta telefônica e seu provedor de acesso à internet, ter o dispensável trabalho de selecionar a mensagem que chegou em suas mãos e, por fim, ter de apagar o inútil arquivo recebido ou ativar um filtro para que a mensagem desse remetente não mais o aborreça.

O primeiro deles é relativo ao caso do jornalista Diego Casagrande, que enviava suas *newsletters* para cerca de 11.000 assinantes.

Ao ser proibido, por sua provedora de acesso (a Procergs) de enviar sua aparente *newsletter*, Casagrande ingressou com duas medidas judiciais contra ela: uma medida cautelar inominada e uma ação declaratória. Liminarmente a cautelar foi concedida.

Entrementes, quando da instrução processual da ação principal (a declaratória), Casagrande não logrou os êxitos esperados: não conseguiu provar que, efetivamente, seus destinatários eram apenas aqueles solicitantes de boletins. Também não conseguiu provar que, em seu *website* existiam mecanismos eficazes para o descadastramento dos destinatários da *newsletter*. Enfim, perdeu a demanda em primeira instância.

Como bem observou o promotor de Justiça Júlio César Finger, atuante no caso, *não condiz com a realidade a afirmação de Casagrande de que sua* newsletter *só é enviada mediante solicitação e é interrompida mediante mensagem para o endereço: descadastrar@opiniaolivre.com.br.*

Ao analisar esse julgado, o advogado Omar Kaminski consignou que *como parece não ter havido prova de solicitações de adesão ao* newsletter, *na prática o envio dos folhetins eletrônicos acabou sendo equiparado à prática de* spam *(envio sistemático de mensagens não-solicitadas). A propaganda não-solicitada só deixa de ser assim considerada quando há o cadastramento efetivo, explícito, que consiste no interesse concreto, na manifestação de interesse em receber mensagens por meio de cadastramento, quer seja no* site, *por* e-mail, *ou em formulários ou outros documentos impressos. Conforme noticiado nos autos, mesmo diante de um volume expressivo de reclamações, não estava havendo o descadastramento daqueles que se impuseram contra a prática*[55].

O segundo caso envolveu o jornalista Políbio Braga, que, por seu turno, enviava suas *newsletters* para mais de 15.000 assinantes, por meio de *e-mail*. Qual Casagrande, ele alegava que os folhetins eletrônicos somente eram enviados àqueles que haviam se cadastrado em seu *website* (http://www.baguete.com.br/polibio). Assim, partindo do pressuposto que seus destinatários optaram pelo recebimento da mensagem, não se haveria que falar em *spam*, liminarmente. No entanto a primeira instância da Justiça rio-grandense do sul não acatou suas pretensões. Recorreu e teve suas pretensões acolhidas pelo Tribunal de Justiça do Rio Grande do Sul.

Vistos em Gabinete.

1) Passo a apreciar a postulação de fls. 112 a 113, formulada pelo agravante.

Os autos do presente agravo me vieram conclusos ontem, depois de decorrido o prazo legal para a agravada manifestar-se sobre o recurso interposto. Postula o agravante a concessão de liminar anteriormente indeferida sob o fundamento de que não vai ser mais possível este agravo ser colocado em pauta este ano, sendo que isto lhe acarretará maiores prejuízos, considerando que "continua impossibilitado do envio de sua news letter *através do serviço contratado e pago pela requerida", sendo que o silêncio da agravada faz presumir a existência de verosimilhança quanto as suas alegações.*

É o sucinto relatório.

2) Passo a decidir.

Em juízo de cognição sumária, considerando a existência de fato novo surgido no curso do agravo, qual seja, o silêncio da recorrida (fl.

111), ao deixar escoar o prazo para sua manifestação sem nada objetar, e ainda levando em conta o fato de que o não-julgamento deste recurso poderá causar prejuízos maiores ao recorrente, susto os efeitos declaratórios negativos da r. decisão agravada, para conceder a liminar pleiteada, no sentido de que a agravada, de imediato, restabeleça ao recorrente os serviços de acesso à internet, conforme requerido em suas razões recursais. Comunique-se (art. 527, II, do CPC).

3) Intimem-se.

Porto Alegre, 14 de dezembro de 2001.

Des. Voltaire de Lima Moraes, Relator[56].

Além das razões apontadas no acórdão, a atitude censora das provedoras de acesso à internet viola frontalmente o disposto pelos arts. 5º, IX[57], e 220, §§ 1º e 2º[58], da Constituição Federal.

Nada obsta às vítimas desta censura (os jornalistas em questão) que processem suas ISPs civilmente por perdas materiais e danos morais além de, em tese, poderem processar as referidas ISPs como inclusas nos arts. 163 e 305 do Código Penal, desde que comprovada a ilicitude de suas ações.

O *SPAM* E O PODER LEGISLATIVO BRASILEIRO

A partir do final do passado milênio, começaram a surgir diversos projetos de lei objetivando a regulamentação das questões decorrentes da internet. Alguns chegaram a tratar de matérias relativas ao *spam* incidentalmente. Todavia o primeiro a tratar, exclusivamente, do assunto foi o de n. 6.210/02, de autoria do deputado federal Ivan Paixão, apresentado logo no início da legislatura de 2002. Posteriormente, aos 6 de agosto daquele ano, o referido parlamentar apresentou um substitutivo, consubstanciado no PL n. 7.093/02. Mais uma vez aflorou a incontível e patológica compulsão de legislalar sobre o já legislado, de tratar novamente de matérias já disciplinadas por outros diplomas legais, quando não pela própria Constituição.

O art. 3º do PL n. 7.093/02 diz que *Há direito de liberdade de expressão na internet*. O art. 5º, IV, da CF/88, dispõe que *é livre a manifestação do pensamento*. A mesma Magna Carta também ressalta que *A manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, processo ou veículo, não sofrerão qualquer restrição, observado o disposto nesta Constituição* (art. 220).

No art. 4º do PL n. 7.093/02, de novo a repetição se faz presente, quando é pontuado que *A mensagem eletrônica comercial não pode conter informação falsa, enganosa ou não obtida legitimamente*. Essa questão também se encontrava tratada por outros diplomas legais, dentre os quais o CDC (arts. 66[59] e 67[60]) e o CP (153[61] e 154[62]).

Em verdade esse projeto de Lei, em vez de boicotar o *spamming* (como aparentemente é seu objetivo), institucionaliza e legaliza essa indigesta prática publicitária, ao aceitar que o *spam* só pode ser considerado ilegal em sendo descumprido o art. 5º, §1º do PL n. 7.093/02[63].

Além disso, esse PL coloca o cidadão destinatário do *spam* em uma posição bastante desconfortável no momento em que se defrontar com a questão *probandi*, que muito interessa à prática forense e que não pode ser olvidada. Afinal, para que o destinatário do *spam* prove que recebeu um segundo *e-mail* ele terá de demonstrar, antes de mais nada, que recebeu um primeiro *e-mail*. Como essa prova se fará? Por meio de inspeção judicial em seu computador (caso **todos** os *e-mails* que tenham recebido estejam ali gravados)? Mediante registros existentes dos *spammers* e dos *bulkmaillers*? Interpelando-se a provedora de acesso à internet do *spammer* – ou a própria *ISP*[64] do destinatário – toda vez que receber um *spam*? Valendo-se da ata notarial?

A inspiração desses projetos, rios da mesma fonte, foi buscada em textos legais estrangeiros (especificamente as leis dos estados americano-nortistas que adotaram o sistema *opt-out* e as diretrizes da CCE), cujos resultados evidenciam que o vagalhão em que se transforma o *spamming* vai tornar bastante turbulentas as navegações nos mares da *web*. Destarte, já que inócuos os resultados colhidos com a legislação alienígena, por que adotá-la?

Ademais, o sistema de "desopção" adotado pelo arquiteto legal – virgem (o PL) no Direito pátrio – não reflete bons propósitos nem boas técnicas de legislar. Afinal, em última análise, é proposto que se tenha o direito de ter direitos[65]. Convenha: isso fere a boa *praxis* jurídica. Pondere, outrossim, que no Brasil essa prática é proibida pelo art. 39, III, do CDC[66] e por torrencial jurisprudência[67].

Quanto ao montante das multas (dada a possibilidade de ser aplicada em até 130 vezes o seu valor mínimo), ressalte-se que suplantou as máximas cinqüenta vezes de majoração de alguns estados dos EUA. Isso significa que a voracidade em relação à punição os crimes que têm a internet como pano de fundo reflete o espírito de tantos outros projetos aqui discutidos. Mas, ironicamente, a proporção pantagruélica de 1 para 130, absurdamente, é de menos; o que estarrece é que não há qualquer graduação para as infrações "previstas" pelo PL. A multa do PL vestibular era de, fixos, R$ 800,00 acrescidos, indefectivelmente, em um terço.

PAGANDO AS CONTAS DOS *SPAMMERS*

Para receber o *spam*, o internauta é forçado a pagar sua conta telefônica e seu provedor de acesso à internet, ter o dispensável trabalho de selecionar a mensagem que chegou em suas mãos e, por fim, ter de apagar o inútil arquivo recebido ou ativar um filtro para que a mensagem desse remetente não mais o aborreça. Some-se a isso a conta da companhia elétrica. E todos esses esforços para receber uma mensagem eletrônica comercial que ele não solicitou e que se caracteriza por suas **indesejabilidade** e **inutilidade**. Indesejável, pois não-solicitada; inútil, na quase totalidade das vezes, pois não sugere necessidades ou desperta interesse para o destinatário.

Contra o argumento do pagamento de eletricidade, alguns *spammers* aduzem: "Mas quem assiste televisão não paga pelos anúncios que vê e não solicitou? Não paga pela eletricidade? A questão não seria a mesma?" Isso é uma falácia. Em termos publicitários, tendo como pano de fundo o mundo físico, a coisa mais próxima a que o *spam* pode ser equiparado é, virtualmente, a mala-direta. E aí o fulcro da questão: a mala-direta, como o próprio nome ressalta, é direta e pessoal, enquanto o anúncio da televisão é abrangente, indireto e impessoal. Além disso, quando se trata de mala direta, quem arca com os custos são os remetentes. Já quando se trata de *spamming*, quem paga as contas são os destinatários. Por fim, é intrínseco ao ato de ver televisão pagar pela eletricidade utilizada, bem como faz parte se admitir que existam anunciantes. Sem eles,

a televisão comercial não existiria. Entrementes, caso os *spammers* desaparecessem da internet, por certo não apenas ela continuaria a existir como, inexoravelmente, seria mais rápida e menos custosa. Em outras palavras, muitíssimo mais eficiente.

Se em vez de uma mensagem eletrônica comercial se tratasse de uma ligação telefônica a cobrar realizada por um desconhecido vendedor, será que quem a recebe aceitaria a chamada? No entanto, com o *spam*, a questão é diferente. Afinal, ou é recebida a malfadada mensagem não-solicitada, ou não são recebidas as mensagens aguardadas, caso não tenha sido ativado algum filtro.

Há quem equipare o *spam* à prática do despejo de duas toneladas de correspondência não-solicitada na porta da casa de uma pessoa, de modo a impedi-la de entrar onde reside e mora.

Não é de se ir tão longe, nem propor o espancamento dos carteiros portadores dessas indefectíveis correspondências; contudo uma coisa é certa: o direito à privacidade merece mais proteção do que a liberdade que os publicitários alegam ter para invadir quaisquer caixas de correio eletrônico, ocasionando um furto de tempo e dinheiro[68]. Liberdade de expressão é uma coisa. Libertinagem publicitária é outra.

Se o número de *spams* recebidos diariamente equivalesse ao da correspondência comercial convencional que chega por meio do correio do mundo das três dimensões, poderia até ser considerado como tolerável, na maioria dos casos. Contudo a proporção dos *spams* supera, em muito, à debitada aos carteiros.

A Associação Brasileira de Provedores de Acesso, Serviços e Informações na Internet do Rio (Abranet) noticiou, no início do milênio, que *mais de um terço dos* e-mails *que circulam na internet brasileira não têm interesse para quem os recebe. Na maioria das vezes, são propostas para ganhar dinheiro fácil. Mas, além de significar perda de tempo, esses* e-mails *indesejados, conhecidos como lixo ou "*spam*", são também sinônimos de gasto extra. A Abranet fez um estudo estimando que, mensalmente, sejam gastos cerca de R$ 90 milhões por excesso de tais mensagens*"[69]; qual seja, mais de um bilhão de reais no ano 2000! Na Europa, nesse mesmo ano, o prejuízo causado pelos *spammers* naquelas plagas foi superior a US$ 9,000,000,000.00.

SITE ANTI-SPAM RECEBE 22 MIL QUEIXAS POR MÊS

O movimento anti-spam *(http://www.antispam.org.br) recebe um número enorme de reclamações de usuários, indignados com o recebimento de mensagens indesejadas. "São 22 mil queixas por mês", informa Hermann Wecke, membro do movimento. Na Europa, outro estudo apresentado na semana passada (a terceira semana de março de 2001) mostra que os* spams *causam prejuízos de US$ 9,36 bilhões aos usuários por ano, que gastam para receber mensagens indesejadas* (C.G.)[70].

Quando uma pequena porção de um gramado for contaminado por um "matinho" ou uma "pequena erva daninha", esse é o prenúncio de que todas belas e resistentes folhas rastejantes desse plano verde horizontal já estão contaminadas. É uma questão de prazo. Em outras palavras, quando o internauta recebe o primeiro *e-mail* de um *spammer*, isso prenuncia que, em breve, ele será vítima de centenas de inúteis mensagens a ser deletadas[71] ou filtradas. Mais uma piscadela da pálpebra do tempo e o que era um passou a ser um milhão. O significado disso é sua caixa postal ter problemas de saturação. Mensagens serão perdidas. Negócios talvez deixem de ser realizados. Quiçá até paixões se desfaçam.

OS PREJUÍZOS DECORRENTES DO *SPAM*

O *spam* causa prejuízos econômicos para o cibernauta vítima da ação, por perturbar sua rotina e molestá-lo.

Todavia os prejuízos não são só esses, uma vez que os *spammers* também atentam contra os provedores de acesso à internet, que, por feitas, gestam desnecessárias horas de trabalho para a exclusão (ou obstrução) de *spams* destinados a seus usuários. Em certas ocasiões, chegam a paralisar suas atividades, temporariamente[72]. Em casos mais graves, em decorrência de uma série de ataques de negação de serviço (DDoS), as provedoras acabam por transferir suas operações para outra empresa. Isso quando não encerram suas atividades. Foi o que aconteceu com um popular provedor britânico, *Cloud Nine* (*C9*), que oferecia serviços de acesso discado e de banda larga. Um ataque em massa levou-o à beira da falência[73].

Para sobreviverem aos *spammers*, as provedoras de acesso à internet têm de aderir a uma banda superior às suas necessidades (e às de quem as contrata) para a transmissão de dados, sob pena de congestionamento em decorrência do indesejado e desnecessário tráfico de mensagens comerciais não-solicitadas, o que implica mais gastos a serem repassados ao consumidor final.

De acordo com Roque Abdo, presidente da Abranet, que representa os provedores, há preocupação sobre o assunto. "Ao contrário do que se pensa, o grande ônus do spam *fica com o provedor, pois ele cobra o mesmo preço de quem envia um ou um milhão de* e-mails*. A cobrança não é por volume".*

Como o spammer *cria muito tráfego, para não comprometer a* perfomance *do sistema, o provedor precisa gastar recursos para aumentar sua banda na rede. Segundo Abdo, há uma forte mobilização dos provedores para acabar com a festa dos* spammers*. Existem duas propostas: limitar o número de* e-mails *diários e organizar uma lista negra, para que os provedores façam um bloqueio conjunto*[74].

Os pequenos comerciantes e os pequenos prestadores de serviços argumentam que esse meio de interligação de todas as pessoas do planeta lhes permite competir com os grandes em igualdade de condições. Afinal, em se valendo do *spamming*, podem atingir um potencial contingente de clientes inalcançáveis em outras circunstâncias e ocasiões – e, segundo sua ótica, em se gastando quase nenhum dinheiro! Estariam certos se não existissem respingos no campo da cidadania, se não ferissem prerrogativas constitucionais e se não enviassem ao destinatário as contas das despesas que ele não deu causa.

Em termos sociais, a questão se torna mais séria e delicada, pois dada a facilidade de utilização e o custo virtualmente nulo dessas mensagens, é comum um único *e-mail* do *spammer* ter milhares de internautas destinatários. Considerando-se, ainda, que os praticantes desse estorvo informático não se restringem a um, mas a uma legião de candidatos a posseiros de discos rígidos, não é desatino imaginar que poucos *bits* se transformem, incontinênti, em algo que supere os *terabytes*! É o milagre da multiplicação dos *bits* que provoca consideráveis prejuízos aos usuários da rede e aos provedores de acesso, em razão do congestionamento das linhas telefônicas e dos custos impostos.

Além disso, o *spam* não é um fenômeno estacionário, determinado, localizável e limitado. Ele tende a aumentar. É o "aquilo" mais entrópico que se manifestou na era digital.

O ANONIMATO DO *SPAMMER*

Sabedor de que, para a quase totalidade dos usuários da *web*, seus *spams* são um manifesto incômodo, o *spammer* prefere se ocultar sob o manto do anonimato. E, para se valer dessa anonímia na rede, basta abrir uma conta "fantasma" em um cibercafé qualquer (onde raramente é solicitada identificação ao usuário) e acesse a internet mediante provedores de *e-mails* baseados oferecidos na rede, como, por exemplo, Yahoo, Bol, IG etc. Aí poderá apresentar-se como bem lhe aprouver. Não olvide que nos próprios mares da *web* estão disponíveis todas ferramentas que autorizam um quase inexpugnável anonimato.

Em razão dessa pretensa invisibilidade, muitos *bits* terão de ser computados até que se descubra quem é, na verdade, o *spammer* qualificado como Jeremias Pitombesco Epaminondas de Assumpção, apátrida, polígamo, treinador de focas, residente e domiciliado não se sabe onde.

Não bastasse aos *spammers* levar o dinheiro de suas vítimas, eles ainda afetam o regular funcionamento da *web* – o que é igualmente sério, pois os *spams* ocasionam um tráfego desnecessário e prejudicial para todos os seus usuários regulares. De acordo com as estatísticas mais otimistas, no início do terceiro milênio, um terço da banda de transmissão para a internet (...) era utilizado por *spammers*.

Para complicar, posteriormente à criação de sua conta "fantasma", o *spammer* pode procurar um sistema "anonimizador" para dificultar, ainda mais, a possibilidade de ser identificado[75].

Uma vez que nada impede que o internauta interessado na anonímia acesse um serviço "anonimizador" através de outro serviço "anonimizador", temos que quantos mais "anonimizadores" forem utilizados no correr de uma navegação, mais difícil se tornará a localização daquele que quiser se ocultar na invisível cidade que é a internet [76].

Se o salafrário digital resolver se valer da utilização de *remaillers* [77] anônimos, virtualmente logrará um anonimato inexpugnável, o que tornará ainda maior o desafio de sua identificação, porque a combinação desses fatores (conta falsa, "anonimizadores" e *remaillers* anônimos) propicia uma anonímia aparentemente inquebrantável e perfeita para o *spammer*[78].

Entrementes, por mais anonimato que o internauta imagine fruir, ele sempre poderá ser descoberto. O típico exemplo foi a prisão do *cracker* mais famoso do mundo, na última década do passado milênio, o americano nortista Kevin David Mitnick, cujas ações inspiraram o filme Jogos de Guerra, além de diversos livros.

Acobertado pelo anonimato, ele invadiu a *Apple* e a Motorola; fraudou sistemas de telefonia e se apropriou das senhas de mais de vinte mil cartões de crédito. Em razão dos crimes cometidos, ficou preso durante quase cinco anos.

Foi descoberto graças à persistência, à capacidade e à obstinação do físico japonês Tsutomu Shimomura, o samurai cibernético. Sem o seu auxílio, o FBI não teria conseguido prender Mitinick.

Porém, posteriormente ao ataque às terras da América nortista, em 11 de setembro de 2001, o anonimato na *web* passou a ser visto com outros olhos e como um risco potencial para a segurança do planeta. Por essa razão, autoridades daquele país passaram a pressionar os fornecedores/prestadores dos serviços de anonímia para que deixassem de oferecê-los, temerosos que terroristas tivessem trânsito livre para a troca de suas mensagens.

A *SafeWeb* (EUA), que oferecia a possibilidade de uma navegação anônima, encerrou suas atividades, temporariamente, em outubro de 2001. Nessa mesma ocasião, a *Zero Knowledge Systems* (Canadá) também anunciou o fim de seus serviços de envio de *e-mails* anônimos.

Após as imperdoáveis aterrissagens de Osama Bin Laden nos EUA – e o não menos imperdoável massacre de milhares de civis afegãos – a questão censória atingiu patamares inimagináveis nas terras vizinhas do Canadá, a ponto de o *FBI* desenvolver um vírus chamado "lanterna mágica" para monitorar a internet.

Contudo, para lograr tal tento, esse órgão governamental dos EUA deveria contar com o apoio das companhias desenvolvedoras de *softwares* antivírus para que o seu vírus pudesse circular livremente pela rede e não ser acusado por seus programas. Esses espúrios propósitos não foram alcançados por duas razões: a) as *softwarehouses* que adotassem esse procedimento perderiam a confiança dos consumidores e b) estaria aberta uma nova porta "oficial" para que os *crackers* pudessem introduzir novos vírus.

CONSPIRAÇÕES: O DIREITO *VERSUS* A TECNOLOGIA

Na virada do milênio, os países com acesso à internet se viram às voltas com diversos problemas jurídicos aparentemente novos. Desse modo, em todo o planeta, buscaram-se soluções. Nos Estados Unidos, onde despontou a *web*, igualmente despontaram os primeiros problemas envolvendo a rede como meio para o cometimento de crimes já tipificados penalmente.

Uma das questões que consumiu especial atenção dos estudiosos da matéria foi o fato de a prática geometricamente crescente do *spam* poder levar a rede a um efetivo colapso.

Para regulamentar a matéria, em vez de se valerem da sempre tão desejável e rejuvenescedora *common law*, valeram-se de esforços legislativos. Inspirados na lei federal que regulamentava as transmissões de faxes comerciais não-solicitados (*junk fax*), vigente desde 24 de janeiro de 1994, adequaram-na à nova realidade dos *e-mails* não-solicitados.

Consoante os termos da Lei de Washington[79], é ilegal *usar qualquer aparelho telefônico fac-símile, computador ou outro serviço para enviar informações não-solicitadas para qualquer equipamento com capacidade de transcrever textos ou imagens (ou ambos), a partir de um sinal eletrônico recebido de uma linha telefônica, sobre papel*. A vítima do fax não-soli-

citado, naquelas terras, pode cobrar, judicialmente, do remetente, o equivalente a US$ 500.00 por cópia recebida. Na quase totalidade dos estados, as *small claims courts* (que se equiparam aos juizados especiais pátrios para pequenas causas) são competentes para o julgamento dessa matéria.

Os países-membros da Comunidade Comum Européia, como não poderia deixar de ser, também estavam profundamente preocupados com o crescimento geométrico do *spam*. A prova inconteste foram os esforços legislativos, que se mostraram expressivos.

Na América do Sul, a preocupação com o *spamming* também se manifestou. No Peru, talentosa doutrina entendia que o *spam* violava a privacidade das pessoas, nos moldes do art. 6º de sua Carta Constitucional de 1993[80]. Na Argentina, a busca de soluções para o problema também existiu. No Brasil, aparentemente, seus cidadãos tiveram mais sorte, haja vista que o legislador pátrio teve mais competência e visão atemporal (ou teria sido meramente sorte?). Afinal, o Código de Defesa do Consumidor[81] já previa em seu corpo a ilicitude do *spamming* (art. 43, por exemplo). O Código Penal, o mesmo fazia (art. 265, entre outros). A Lei das Contravenções Penais[82] (art. 65), não destoava da melodia da compreensão média. O Código Civil de 1916, idem (art. 159, revigorado pelos arts. 186 e 187 do Código Civil de 2002[83]).

Todavia, a tecnologia não só não propiciava meios efetivos para se evitar esse escatológico *marketing* digital, como, outrossim, conspirava a favor dos *spammers*, facilitando-lhes a ação e outorgando-lhes mecanismos para se entrincheirarem e não serem tocados pelas mãos da lei.

A ÉTICA COMERCIAL DOS *SPAMMERS*

Não bastasse aos *spammers* levar o dinheiro de suas vítimas, eles ainda afetam o regular funcionamento da *web* – o que é igualmente sério, pois os *spams* ocasionam um tráfego desnecessário e prejudicial para todos os seus usuários regulares. De acordo com as estatísticas mais otimistas, no início do terceiro milênio, um terço da banda de transmissão para a internet (para acesso a *websites* ou correio eletrônico) era utilizado por *spammers*. As mais pessimistas tinham uma estimativa de 45% de utilização da banda de tráfego dos dados. Essa saturação levava a rede das redes ao colapso e justificava a indignação das vítimas dos *spammers*.

Ademais, os *spammers* não assumem os custos de seus desatinos. Assemelham-se aos sorrateiros empreendedores que desejam dividir os prejuízos e concentrar os lucros. Apraz-lhes que suas despesas sejam assumidas por terceiros que não conhecem.

Para Vinton Cerf, o pai da internet, o spamming *pode causar sérias interferências na operação dos serviços da internet, isso sem se falar sobre os efeitos que isso pode causar num sistema de* e-mails *pessoais.* (...) *Os* spammers*, em verdade, estão sugando recursos da rede sem que seus usuários tenham quaisquer tipos de compensação – e sem a sua autorização*[84].

Ronald Coase, prêmio Nobel de Economia[85], muito antes do surgimento da internet, ressaltou ser perigoso para o mercado todo negócio ineficiente, qual seja, aquele que assume os riscos de terceiros para a realização de suas propostas. O *spammer*, *in casu*, adequa-se às idéias do laureado economista, uma vez que distribui o risco de suas atividades para um número incontável de vítimas.

Em síntese, a questão do *spam* é tão séria que o próprio Bill Gates, o mais convicto capitalista do planeta, descarta a sua utilização.

Desperdiçar o tempo de alguém me parece o cúmulo da grosseria. Nós temos um número limitado de horas por dia e nenhum tempo a perder.

É isso que faz da correspondência eletrônica não-solicitada, uma das trapaças via e-mail*, algo tão irritante.*

(...)

O custo básico para enviar essas mensagens é essencialmente zero.

Isso implica ações maravilhosas. Infelizmente faz com que a correspondência não-solicitada possa ser enviada a milhares de pessoas desperdiçando uma vasta porção de seu tempo – a custo praticamente nulo para os remetentes.

Quem arca com os ônus são os destinatários (...)[86].

Um correio eletrônico pessoal é propriedade de seu usuário, não dos *spammers*. Por seqüência, qualquer invasão implica algo prejudicial e atentatório à sua intimidade, porque o correio eletrônico não-solicitado (comercial ou não, formal ou materialmente) não se enquadra entre as propostas de fruição da internet, pelas quais os cibernautas pagam para a fruição de satisfações – não de aborrecimentos e molestações.

Os *spammers* usurpam o lídimo e inquestionável direito de os proprietários de caixas de correio eletrônico administrarem-nas segundo seus desejos. Eles se sentem no direito de dizerem o que os usuários da internet devem fazer, como devem se comportar e quais medidas podem ser tomadas, no que tange à sua correspondência pessoal eletrônica. Os *spammers* fazem tudo isso unilateralmente, impondo gastos que os destinatários de suas mensagens não estão dispostos a assumir e impingindo-lhes perda de tempo, além de aborrecimentos, para se livrarem de seus indesejados *e-mails*. São como os convivas que não foram convidados: palpiteiros, salientes e inoportunos.

Mesmo assim, sem pejo, sem dissimulações e sem desculpas, tentam a todos convencer que o *spamming* é um bem para a sociedade digital.

Apresentam "soluções" *anti-spam* que não funcionam. As técnicas mais conhecidas são um verdadeiro exercício de se somar "vazio" ao "vácuo" e multiplicar por zero.

Simplesmente apagar um *e-mail* não resolve a questão, eis que nunca se sabe quantas vezes se terá de apagar um *e-mail* por dia. Ademais, além de ser reduzida a produtividade do usuário receptor do *spam*, essa prática é um incentivo aos *spammers*.

A auto-regulamentação é uma falácia. É o mesmo que pedir aos lobos para que elaborem a Constituição dos Direitos das Ovelhas.

Sistema *opt-out* é igualmente uma farsa bastante defendida pelos *lobbies* dos *spammers*, notadamente na América nortista e na Comunidade Européia. Com esse sistema, admite-se que o *spammer* mande um primeiro *e-mail*, no qual, obrigatoriamente, deverá constar um mecanismo que permita ao destinatário manifestar seu desejo de que não lhe apraz pagar contas de terceiros. Já o envio de um segundo *e-mail* desautorizado caracterizaria uma infração. Isso é teratológico. Afora isso tudo, quantos não serão os *e-mails opt-out* que surgirão nas caixas de correio eletrônico do planeta diariamente?

As justificativas de seus atos igualmente não convencem. Eles alegam usar endereços eletrônicos de

suas vítimas porque "em algum lugar" da *web* esses *e-mails* estão disponíveis. Ou então que "houve sua indicação por parte de um amigo". Mas isso não é uma autorização, é usurpação! Endereços constam nas notas de cartórios e de registros públicos, de catálogos telefônicos (impressos ou virtuais) etc. No entanto, aqueles que se utilizam do *marketing* direto convencional não cometem o acinte de vasculharem informações nesses recipientes. Mesmo nos atos públicos a privacidade deve ser preservada. Por vezes por meio da lei[87]; em outras ocasiões, por *agreements*.

A seleção de *e-mails*, numa caixa de correio eletrônico, sob certo aspecto, equipara-se à seleção de ofertas de emprego na seção de classificados de um jornal qualquer. Quem passou por essa experiência sabe quanto tempo essa enfadonha tarefa exige. Separar os *e-mails* dos *spams* é igualmente bastante trabalhoso e tedioso. É o mesmo que separar o joio do trigo.

No início de 2002, metade dos *e-mails* processados pela *America OnLine* (uma grande provedora de acesso à internet) eram *spams*. O volume tornara-se tão assustador que alguns internautas deixaram de usar seus *e-mails*, em decorrência da nefasta e endêmica prática do *spamming*.

Como positivado resta, os danos sociais causados pelo *spammer* são imensuráveis, e esses ataques não são casos isolados, mas cumulativos. Seu crescimento é assustador por roubar toda a credibilidade que era emprestada aos *e-mails* e por ter um efetivo custo para seus destinatários.

Vale lembrar um curioso fato: o 105º Congresso Base das Normativas Internacionais sobre *Spam*, a moldura "legal" que muitos *spammers* colocam na pintura de gosto duvidoso que são as suas mensagens eletrônicas não-solicitadas[88].

Nessa apostasia jurídica consta que, *ex vi*:

Essa mensagem é enviada com a complacência da nova legislação sobre correio eletrônico, Secção 301, § (a) (2) (c) Decreto S 1618, Título Terceiro, aprovado pelo 105º Congresso Base das Normativas Internacionais sobre Spam. *Esse* e-mail *não poderá ser considerado* spam *quando inclua uma forma de ser removido. Para ser removido de futuros correios, simplesmente responda-o indicando no assunto: remover*.

Em verdade, o texto original não se refere ao 105º Congresso Base das Normativas Internacionais sobre *Spam*, porém à 105ª Legislatura do Congresso da América nortista.

*A tradução foi deliberadamente realizada de modo para dar a impressão de que se trata de algo específico sobre o tema e que está em vigor mas, por ignorância ou má-fé, não se explica em nenhum momento que este suposto "decreto" é apenas um projeto que tem o nome de "*Anti-Spamming Amendement Act*", proposta em 9 de fevereiro de 1998 pelo senador Robert McCain e que recebeu o número S. 1618, sendo o "S" a sigla de* Senate *e que visava a criar um* CFR – Code of Federal Regulations*, ou seja, um código de condutas para os* e-mails *e a proteção contra seus abusos. A proposta foi debatida e, realmente, continha a frase que hoje corre o mundo mas, em nenhum momento, foi aprovada ou entrou em vigor nos Estados Unidos*.

Porém há um outro "deslize" que cometem aqueles que enviam mensagens com o citado texto: ainda que houvesse sido aprovada esta legislação dos Estados Unidos, não poderia ser aplicada aqui como se pretende, uma vez que valeria apenas nos territórios norte-americanos e, como não é um tratado, não poderia nem ser ratificada pelo Brasil. Para valer em nosso território, deveríamos ter um projeto de lei nesse sentido que, após debatido, votado e aprovado, tornar-se-ia lei e assim tornaria legal a conduta dos spammers[89].

Todavia essa "advertência" é um verdadeiro nada jurídico, despido de qualquer validade para os diplomas legais brasíleos. A norma (com mais propriedade, *Code of Federal Regulations – CFR*) a que se referem os *spammers* brasileiros não existe. Porém, mesmo se existisse, não teria validade no território nacional, pois uma norma da América supra-equatorial vale apenas para os supra-equatorianos, não para o resto do mundo.

No Brasil, legislam os brasileiros!

NOTAS BIBLIOGRÁFICAS

1 As lendas dos países nórdicos noticiam um personagem chamado "Fortunatus". Ele possuía dois estranhos objetos de valor inestimável: uma bolsa que nunca se esvaziava de moedas de ouro e um chapéu mágico que transportava quem o usasse para qualquer sítio.
Uma das melhores narrativas, da qual ele é partícipe, é *A maravilhosa história de Pedro Schlemihl*, de autoria de *Adalberto Von Chamisso*, Editorial Estampa, Ltda. (Lisboa), 1983, fls. 23 *usque* 116 (*LIVRO B*).

2 *Bit* deriva de *binary unit* (unidade binária). É a menor unidade de processamento de informações.

3 NEGROPONTE, Nicholas. *A vida digital.* São Paulo: Cia. das Letras, 1997. p. 19.

4 HUXLEY, Aldous. *Admirável mundo novo.* Rio de Janeiro: Companhia Brasileira de Divulgação do Livro, 1968.
Nessa obra seu autor questiona os funestos efeitos de uma sociedade que, invasivamente, monitorava todos os hábitos e atos de seus membros.

5 *Website* (ou *site*) - Do latim *sitius*, sítio, lugar. É onde, na internet, estão disponibilizadas informações (na mais ampla acepção e extensão do termo) que podem ser acessadas pelos usuários da grande rede mundial de comunicações.

6 *ICQ* (em inglês, *I seek you*) que significa "eu procuro você". Foi desenvolvido pela *Mirabilis*, uma *softwarehouse* israelense.

7 Samuel Finley Breese Morse (1791/1872) foi inventor do telégrafo e Alexandre Graham Bell (1847/1922) foi o inventor do telefone.

8 *ISP* é a sigla de *Internet Service Provider*, ou seja, provedor de acesso à internet.

9 Criptografia é a ciência de se escrever em código.

10 *PGP* (ou *Pretty Good Privacy*, cujo significado é "privacidade razoavelmente boa") é um sistema criptográfico bastante popular que pode ser obtido gratuitamente na internet a partir do seguinte endereço: <http://www.pgp.com>.

11 Revista *Exame* n. 7, v. 30, março de 1997, p. 146.

12 Conta uma lenda urbana que esse termo teria sido inspirado no grupo inglês Monty Python que, em 1970, interpretou uma cena, numa taberna, onde tudo que era pedido era servido com *Spam* (um presunto enlatado da América nortista fabricado pela Hormel, desde 1930).

13 Nos *EUA,* o *spam* é, por vezes, referenciado como *UBE* (*usolicited bulked e-mail*, ou mensagem eletrônica em massa não-solicitada), por vezes como *UCE* (*unsolicited comercial e-mail*, ou mensagem eletrônica comercial não-solicitada).

14 *Spamming* é a ação de enviar *spams*.

15 *Newsgroup* é um grupo de discussão criado com o objetivo de trocar informações sobre um assunto específico. Apesar de sua intrínseca utilidade, por vezes se torna um estorvo para o cidadão/usuário da rede, particularmente quando é tentado o cancelamento de sua inscrição.

16 SANTOS, Antonio Jeová. *Dano moral na internet*. São Paluo: Método, 2001. p. 158.

17 *Web* (rede, em inglês) é uma das formas de se referir à *world wide web* (*www*).

18 "Pirâmide" é o nome de um conhecido golpe aplicado no mundo da corporalidade, no qual são beneficiários apenas o seu organizador e os primeiros partícipes, normalmente seus comparsas. Apóia-se no princípio da progressão geométrica (2, 4, 8, 16, 32...). A vítima envia alguns reais para determinados nomes indicados pelo infrator na esperança de lograr bons dividendos econômicos. Mas, em vez de lograr esses esperados benefícios, ela é quem acaba sendo lograda.

19 Corrente é algo como a pirâmide, só que, em vez do envio de dinheiro, o infrator solicita que seus incautos destinatários reenviem o malicioso *e-mail* para tantas e quantas pessoas, sob pena de serem vítimas de uma desgraça inimaginável caso seja quebrada (interrompida).

20 Revista *InfoExame* n. 175, out. 2000, p. 43.

21 *Federal Bureau of Investigations* (Escritório Federal de Investigações).

22 Correio baseado (ou correio eletrônico remoto) é aquele que permite o cidadão/usuário acessá-lo por meio de qualquer computador do planeta, depois de digitadas algumas informações solicitadas. Pode ser pago ou não. Dentre os gratuitos destacam-se o *Yahoo!* e o *Hotmail*.

23 Cibercafé (ou *cybercoffe*) é um local que oferece acesso à internet mediante pagamento. Normalmente podem ser encontrados em livrarias.

24 Posteriormente foi absolvido por falta de provas (cuja obtenção foi julgada irregular).

25 Extraído de *Golpe Geográfico na internet,* publicado pelo *Jornal do Brasil* na edição de 29 de novembro de 2001, p. 02.

26 *Spammer* é aquele que envia *spams*.

27 Má-fé, em latim.

28 Jornal *O Estado de S. Paulo*, edição de 26 de março de 2001, Caderno de Informática, p. 15.

29 *E-mailing list* é uma lista que contém diversos *e-mails* e, normalmente, outras informações sobre os seus possuidores.

30 *Chat-room* (ou apenas *chat*, que significa "papo", "papear", conversar) é um lugar para se comunicar com um grupo de usuários na internet.

31 O *website avocati locus* (administrado e mantido pelo autor desde junho de 1996 em http://www.advogado.com) é um exemplo disso. Nele existem inúmeras listas com os *e-mails* de diversos profissionais do Direito.

32 *Spiders* (aranhas, em inglês) são *softwares* que realizam buscas na *web* (teia, em inglês). Podem se prestar para todos os fins.

33 *Existem* softwares spiders *(aranhas) dedicados a vasculhar a* web *em busca de endereços de* e-mail *de modo a incluí-los em* e-mailing lists *que se prestarão para a prática de* spam (jornal *O Globo* de 8 de julho de 2002, Suplemento *Informática ETC*, p. 21).

34 *Se a árvore for envenenada, necessariamente envenenados serão seus frutos.*
A teoria da árvore envenenada (p*oisoned tree*) teve vez na década de 1960, quando a Suprema Corte de Justiça dos *EUA* apreciou o caso *Miranda* – julgamento esse que influenciou diversos posicionamentos jurídicos (entre os quais o do Brasil).
A questão jungia-se ao julgamento de um mexicano chamado Miranda que houvera confessado a prática de um delito no momento em que fora preso. Em razão dessa confissão, ele foi condenado judicialmente.
Quando da apresentação de recurso à Suprema Corte de Justiça da América nortista, essa o absolveu, decretando a nulidade do processo, uma vez que não fora dito ao acusado que ninguém é obrigado a depor contra si próprio. Dessarte, apesar de ser réu confesso, pelo fato de a prova ter sido obtida por meios não-jurídicos, ela seria decorrente e necessariamente ilegal.

35 De acordo com os desenvolvedores de *browsers*, *cookies são um mecanismo através do qual o lado do servidor de conexões de acesso à internet pode tanto armazenar como recuperar informações do lado cliente da conexão. A adição desse simples e persistente* status *do lado cliente/servidor amplia, significativamente, as capacidades de aplicações entre cliente e servidor, baseadas na* web. Traduzindo para o linguajar dos meros mortais (isto é, nós!), *cookies* são bisbilhoteiros arquivos de texto (com não mais que 1 Kb) que são gravados no disco rígido do *apparatus* do cidadão/usuário para serem utilizados pela memória *RAM* de seu computador quando tiverem vez novas navegações nos insondáveis – e turbulentos – mares da *web*. (*Privacidade na internet, um enfoque jurídico*. São Paulo: Edipro, 2001. p. 74/75).

36 *Webmaster* é o gerenciador, o responsável técnico pelos conteúdo, guarda, manutenção, apresentação das informações do *website*, bem como aquele que coordena sua estrutura.

37 Uma interessante matéria a respeito foi publicado na Gazeta Mercantil de 20 de novembro de 2001 chamado *A cada visita à rede, "cookies" ocupam disco.*

38 Departamento de Anúncios Interativos.

39 O parecer que determinou a abertura dos inquéritos encontra-se *in Privacidade na internet, um enfoque jurídico*. São Paulo: Edipro, 2001. p. 175/190.

40 *HTML* é a sigla de *HiperText Mark up Language.* É um modo pelo qual podem ser feitas as *webpages* existentes na w*eb*. Não se trata de uma linguagem, mas de uma marcação.

41 *Cesare Lombroso* (1835/1909) nasceu em Torino (Itália). Apesar de superadas, suas idéias foram um marco na história do Direito por sugerir uma abordagem biológica no estudo do crime. Sua teoria admitia que, a partir da presença de determinadas características biotípicas, poderia ser delineado o criminoso. Os cinco tipos por ele delineados são os seguintes: o criminoso nato, o criminoso louco (ou alienado), o criminoso profissional, o criminoso primário e o criminoso por paixão.

42 *Spywares* são *softwares* espiões inseridos furtivamente nos computadores por meio de determinados *softwares* (*freeware*, *shareware* ou mesmo *software* licenciado) ou por meio de *e-mail*.

43 Jornal *Folha de S. Paulo*, suplemento *Informática*, 22 de maio de 2002, p. 03.

44 Ativo é o endereço eletrônico considerado como válido.

45 A *Cauce (Coalisation Against Unsoliceted Comercial E-mail)* é uma sociedade americano-nortista defensora dos direitos civis. Suas posições e sua luta contra o *spam* podem ser constatadas em seu *website.* Disponível em: <http://www.cauce.org/problrm.html>.

46 *RAM (Random Acess Memory* – ou memória de acesso aleatório*)* é a memória principal do computador.

47 *URL* (*Uniform Resource Locator*) é a combinação de campos de dígitos separados por pontos que define a localização de um arquivo ou programa na internet. Cada um dos campos desse endereço guarda um significado próprio e é único. Não podem existir dois endereços *IP* idênticos. 200.201.133.12, por exemplo, é o endereço *IP* onde está situado o *website Avocati Locus*. A primeira dessas cadeias de dígitos (200) do endereço *IP* esclarece o país onde se encontram hospedado o *site* (*in casu*, no Brasil). As cadeias posteriores esclarecem quem é o hospedeiro do *site* ou o provedor de acesso ou o sistema de rede. Seu idealizador foi Vinton Cerf.

48 Extraído do artigo *Tecnologia elimina* e-mails *indesejados*, de *Esther Dyson*, publicado na *Folha de S. Paulo*, edição de 7 de novembro de 2001, suplemento de Informática, p. 02.

49 *Softwares* que obstam o acesso a determinados *websites*, ou palavras, sempre foram conhecidos por quaisquer neófitos em Informática. Contudo, esses programas informáticos – aptos para censurar determinados *websites* – somente vieram à tona nos oceanos digitais da w*eb* e se tornaram conhecidos pelo usuário/cidadão comum quando *Guilherme Clinton*, então presidente do Estados Unidos da América nortista, aos 8 de fevereiro de 1996, sancionou a Lei da Decência das Comunicações, aprovada por seu Congresso ao 1º de março seguinte. O objetivo maior dessa Lei era definir o significado de pornografia.
Entretanto, ela não chegou a viger, por causa do ativismo dos movimentos próliberdades civis (notadamente os ligados à liberdade de expressão e aos direitos democráticos e às novas tecnologias) daquele recanto planetário, dentre os quais se destacava a *American Civil Liberties Union (ACLU)*, que, na época, ingressou com uma ação de declaração de sua inconstitucionalidade perante a Corte Federal da Filadélfia.
De acordo com essa Lei, os *websites* deveriam adotar filtros que guardassem uma série de palavras consideradas obscenas como, por exemplo, "sexo", "nu", "peito" etc. Mas isso era inócuo e desastroso, como acabou por ficar comprovado. Depois das intrínsecas e esperadas delongas judiciais, essa Lei teve a sua inconstitucionalidade declarada por sua Suprema Corte por ferir a primeira emenda à Constituição, que autoriza a plena liberdade de expressão. Bastaram exatos e precisos setenta minutos para que o Juiz John Paul Stevens pontuasse que a Lei da Decência das Comunicações implicava censura estatal sobre a internet, que, segundo ele, é um *forum* público para o intercâmbio de idéias e informação.

50 GOIS JR., José Caldas. *A Liberdade e o delito no ciberespaço.* São Paulo: Edipro, 2001. p. 77.

51 *Newsletters* são boletins de informação, via de regra jornalísticos.

52 Jornal *O Estado de S. Paulo*, 26 mar. 2001, *Caderno de Informática*, p. 15.

53 Jornal *O Estado de S. Paulo*, 5 ago. 2002, *Caderno de Informática*, p. 12.

54 Art. 163, CP – *Destruir, inutilizar ou deteriorar coisa alheia*.
Pena – detenção, de um a seis meses, ou multa.

55 Vide *Spam x Newsletter*, artigo publicado pelo jornal eletrônico *Consultor Jurídico*. Disponível em: <http://cf6.com.br/consultor/view.cmf?id=11340&print=yes>.

56 Agravo de Instrumento n. 70003519782 – Décima Primeira Câmara Cível do Tribunal de Justiça do Rio Grande do Sul, proferido aos 14 de dezembro de 2001.

57 Art. 5º, IX, CF – *é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença*.

58 Art. 220, CF – § 1º *Nenhuma lei conterá dispositivo que possa constituir embaraço à plena liberdade de informação jornalística em qualquer veículo de comunicação social, observado o disposto no art. 5º, IV, V, X, XIII e XIV*.
§ 2º *É vedada toda e qualquer censura de natureza política, ideológica e artística*.

59 Art. 66, CDC: *Fazer afirmação falsa ou enganosa, ou omitir informação relevante sobre a natureza, característica, qualidade, quantidade, segurança, desemprenho, durabilidade, preço ou garantia de produtos ou serviços:*
Pena – Detenção de três meses a um ano e multa.
§ 1º Incorrerá nas mesmas penas quem patrocinar a oferta.
§ 2º Se o crime é culposo:
Pena – Detenção de um a seis meses ou multa.

60 Art. 67, CDC: *Fazer ou promover publicidade que sabe ou deveria saber ser enganosa ou abusiva:*
Pena – Detenção de três meses a um ano e multa.
Parágrafo único – (Vetado).

61 Art. 153, CP: *Divulgar alguém, sem justa causa, conteúdo de documento particular ou de correspondência confidencial, de que é destinatário ou detentor, e cuja divulgação possa produzir dano a outrem: Pena: detenção, de um a seis meses, ou multa*.

62 Art. 154, CP: *Revelar alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem:*
Pena – detenção, de três meses a um ano, ou multa.
Parágrafo único - Somente se procede mediante representação.

63 *§ 1º O remetente de uma mensagem eletrônica comercial não solicitada deve manter um endereço eletrônico em funcionamento, através do qual o receptor possa manifestar a recusa de não mais receber mensagens*.

64 *ISP* é a sigla de *Internet Service Provider*, ou seja, provedor de acesso à internet.

65 Art. 5º do Projeto de lei n. 7.093/02: *Para iniciar a transmissão de uma mensagem eletrônica comercial a um computador protegido, tal mensagem deve conter, de maneira clara e evidente, para o receptor:* III (...) *aviso ao receptor sobre a oportunidade de recusa a receber mais mensagens eletrônicas comerciais do remetente*.
§ 1º O remetente de uma mensagem eletrônica comercial não solicitada deve manter um endereço eletrônico em funcionamento, através do qual o receptor possa manifestar a recusa de não mais receber mensagens.
§ 2º O remetente, ou qualquer pessoa agindo em seu nome, tem o prazo de 24 horas do recebimento da recusa do receptor para encerrar a transmissão de correspondência eletrônica comercial.

66 Art. 39 – *É vedado ao fornecedor de produtos ou serviços*(...): *III - enviar ou entregar ao consumidor, sem solicitação prévia, qualquer produto, ou fornecer qualquer serviço;*

67 Na seqüência alguns acórdãos dos Tribunais de Justiça Distrito Federal e dos Territórios e do Rio de Janeiro que podem ser consultados na internet:
Acórdãos do TJRJ (Câmaras Cíveis): Apelação Cível n. 2000.001.23011, julgada pela Décima Terceira Câmara Cível aos 30/08/2001. Relator: Azevedo Pinto Disponível em: <http://www.tj.rj.gov.br/scripts/weblink.mgw?MGWLPN=JURIS&PGM=WJCAN04&LAB=JURIS&ORIGEM=1&TRIPA=58902,3120,1,79989170,2000,1,23011,1&PALAVRA=CREDITO%20E%20CARTAO%20E%20ENVIO>;
Apelação Cível n. 2000.001.18072, julgada pela Décima Sétima Câmara Cível aos 08/02/2001. Disponível em: <http://www.tj.rj.gov.br/scripts/weblink.mgw?MGWLPN=JURIS&PGM=WJCA N04&LAB=JURIS&ORIGEM=1&TRIPA=58902,3120, 3,79989792,2000,1,18072,1&PALAVRA=CREDITO%20E%20CARTAO%20E%20ENVIO>; Apelação Cível n. 2000.001.17463, julgada pela Décima Sétima Câmara aos 07/02/2001. Disponível em: <http://www.tj.rj. gov.br/scripts/weblink.mgw? MGWLPN=JURIS&PGM=WJCAN 04&LAB=JURIS&ORIGEM=1&TRIPA= 58902,3120,4,79989793,2000,1,17463, 1&PALAVRA=CREDITO%20E%20 CARTAO%20E%20ENVIO>; Apelação Cível n. 2000.001.13418, julgada pela Primeira Câmara Cível aos 05/12/2000. Disponível em: <http://www.tj.rj.gov.br/scripts/weblink. mgw?MGWLPN=JURIS&P GM=WJCAN04&LAB=JURIS&ORIGEM=1& TRIPA=58902,3120,5,79998795,2000,1,13418,1&PALAVRA=CREDITO%20E%20CARTAO%20E%20ENVIO>; Apelação Cível n. 1999.001.20971, julgada pela Sétima Câmara Cível aos 04/04/2000. Disponível em: <http://www.tj.rj.gov.br/scripts/weblink.mgw?MGWLPN=JURIS&PGM=WJC AN04&LAB=JURIS&ORIGEM=1&TRIPA=58902,3120,8,79999596,1999,1, 20971, 1&PALAVRA=CREDITO%20E% 20CARTAO%20E%20ENVIO> e Apelação Cível n. 1999.001.15718, julgada pela Terceira Câmara Cível aos 16/03/2000. Disponível em: <http://www.tj.rj.gov.br/scripts/weblink.mgw?M GWLPN=JURIS&PGM=WJCAN04&LAB=JURIS& ORIGEM=1&TRIPA=58902,3120,10,7 9999684,1999,1,15718,1&PALAVRA= CREDITO%20E%20CARTAO%20 E%20ENVIO>.
Acórdãos do TJDFT (Câmaras Cíveis): Apelação no Juizado Especial Cível ACJ75699 DF, publicada no DJU aos 8/5/2000 (p. 21, Secção 3) e Apelação no Juizado Especial Cível ACJ51998 DF, publicada no DJU aos 20/9/1999 (p. 26, Secção 3).

68 *O juiz distrital C. Weiner, no mês de novembro passado (referindo-se a autora ao ano 2000), deu parecer favorável à* America On Line*, maior provedor americano, que havia dado proteção aos próprios assinantes, bloqueando todos os emails que uma sociedade da* Philadelphia*, a* Cyber Marketing*, remetia a eles. O juiz estabeleceu que remeter correspondência sem solicitação é crime, pois a proteção da privacidade dos cidadãos é mais importante do que a liberdade dos publicitários de invadir as redes com suas correspondências-lixo (junk mail)* (PAESANI, Lilliana Minardi. *Direito e internet*, *Liberdade de informação, privacidade e responsabilidade civil*. São Paulo: Atlas S/A, 2000. p. 54).

69 *Jornal do Advogado*, publicado pela *OAB/SP*, fev. 2001, p. 22. Essa informação também pode ser obtida na *web*. Disponível em: <http://www.cnpi. com.br/03.htm>.

70 Jornal *O Estado de S. Paulo*, 26 mar. de 2001, Caderno de Informática, p. 13. Essa informação também pode ser obtida na *web*. Disponível em: <http://www.cnpi.com.br/04.htm>.

71 Anglicismo que significa "apagadas" (do inglês *to delete*, apagar).

72 Certo dia de março de 1998, os funcionários de uma provedora brasileira de acesso à internet notaram um movimento incomum em seus computadores. Avaliando o ocorrido, constataram que o problema se centrava na máquina responsável pelo trânsito dos *e-mails*. Praticamente não funcionava em decorrência de um ciclópico volume de idênticas mensagens eletrônicas. Tratava-se de uma típica invasão *spammer*. Como resultado dessa indesejável intrusão, a empresa despendeu incontáveis horas até conseguir obstar a distribuição dos *spams* a seus clientes. Em síntese, em prejuízo à regular distribuição de *e-mails* decorrente do sobretráfego na rede de computadores, esse servidor suspendeu temporariamente seus serviços em razão dos "espertos" virtuais que, como coelhos, produzem não-solicitada publicidade de proporções *gigabyticas*.
(Mais detalhes sobre esta questão podem ser encontrados no jornal *O Estado de S. Paulo*, de 3 de ago. 1998).

73 Disponível em: <http://www.infoguerra.com.br/infonews/viewnews.cgi?newsid1011889280,40375>.

74 *Jornal da Tarde* (suplemento de informática) 25 de abril 2002, p. 9, Caderno D.

75 Um dos mais famosos e respeitáveis serviços a propiciar um anonimato gratuito é oferecido pelo *Anonymizer* (www.anonymizer.com), mas traz o inconveniente de apresentar anúncios e outras limitações.

76 *Privacidade na internet, um enfoque jurídico*. São Paulo: Edipro, 2001, p. 110/113.

77 *Remaillers* são instrumentos de envio de mensagens mediante a internet sem que seja identificado o remetente.

78 Complicando um pouco mais a situação, caso o *spammer*, além de múltiplos anonimizadores para a sua navegação e de *remailers* anônimos para o envio de suas mensagens, resolva se valer da

identidade de terceiros, aí as dificuldades se tornarão exponencialmente maiores, porém não determinão a uma anonímia absoluta para o *spammer*.

79 A legislação *antispamming* do Estado de *Washington* (EUA) foi promulgada aos 25 de março de 1998 e publicada aos 2 de abril seguinte.

80 *Toda persona tiene derecho (...) a que los servicios informáticos, computadorizados o no, públicos o privados, no suministrem informaciones que efectúen la intimidad personal y falimiar.*

81 Lei n. 8.078, de 11 de setembro de 1990 (dispõe sobre a proteção ao consumidor e dá outras providências).

82 Lei n. 3.688, de 6 de outubro de 1941, atualizada pela Lei n. 9.521, de 27 de novembro de 1997.

83 Art. 186, CC: *Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito*.
Art. 187, CC: *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*.

84 Disponível em: <http://www.cauce.org/problrm.html>.

85 *Ronald Coase* nasceu em Londres em 1910. Em 1932 graduou-se em economia pela *London School of Economics*, onde lecionou nos anos 1930 e 1940. É um dos fundadores da dita "Nova Economia Institucional".
As principais obras desse autor são *The Nature of the Firm* (1937) e *The Problem of Social Cost* (1960). Sua proposta era simples: com os custos da oportunidade, podem ser solucionados os custos sociais por não se necessitar de meios que equilibrem as tensões sociais existentes.

86 Disponível em: <http://www.microsoft.com/billgates>.

87 Art. 155, CPC: *Os atos processuais são públicos. Correm, todavia em segredo de justiça os processos:*
I – em que o exigir o interesse público;
II – que dizem respeito a casamento, filiação, separação dos cônjuges, conversão desta em divórcio, alimentos e guarda de menores;
Parágrafo único – O direito de consultar os autos e pedir certidões de seu atos é restrito às partes e a seus procuradores. O terceiro que demonstrar interesse jurídico, pode requerer ao juiz certidão do dispositivo da sentença, bem como de inventário e partilha resultante de desquite.
(Vide arts. 815 e 841 do CPC.)

88 Só o número já é surpreendente: 105º congresso! Se realizassem um desses congressos a cada mês, no mínimo seriam necessários quase nove anos para que pudessem ter vez. Qual seja, existiam antes mesmo do surgimento da internet comercial.

89 *Verdade e mentiras sobre o e-mail e o spam*, de autoria do advogado paulista *Sérgio Ricardo*, publicada no boletim jurídico *Nada Consta*, n. 67 (março de 2002), do 1º Ofício do Registro de Distribuição do Rio de Janeiro, p. 03.

ABSTRACT

The author adduces that all information is liable to be transformed into bit, the smallest atomic element of the information DNA, which has aroused the electronic mail, an effective, but insecure way of sending messages. Some of them, with or without commercial purposes, are imposed, that is, to receive them, the addressee hasn't shown his will through the availability of his electronic address, which characterizes the spam.

He emphasizes that there are already specialized groups that form address lists and trade them without authorization and, in order to create them, several artifices are utilized, such as small texts which are recorded in the computers of those who access them and that function as spies of the stored data.

At the end, he points out that, although people argue that the spam can be avoided through filters, they run the risk of working as information censors; he also stresses that in Brazil, bills to regulate the subjects concerning the internet have been discussed; as well as that the anonymity facilitated by the network propitiates the opportunity to the practice of crimes inclusive, emphasizing that, due to the caused embarrassments, it is necessary to search ways to prohibit the spam in the national laws.

KEYWORDS – Spam; Informatics Law; Juridical Informatics; electronic mail; information; internet.

Amaro Moraes e Silva Neto é Advogado em São Paulo/ SP.