# ESTUDO SOBRE A REGULAMENTAÇÃO JURÍDICA DO SPAM NO BRASIL

*Trabalho comissionado pelo Comitê Gestor da Internet no Brasil*
*ao Centro de Tecnologia e Sociedade (CTS),*
*da Escola de Direito do Rio de Janeiro / Fundação Getúlio Vargas*

Ronaldo Lemos
Danilo Maganhoto Doneda
Carlos Affonso Pereira de Souza
Carolina Almeida A. Rossini

Abril/2007

**Ronaldo Lemos**

Doutor em Direito pela Universidade de São Paulo. Mestre em Direito pela Harvard University. Coordenador do Centro de Tecnologia e Sociedade (CTS) da Escola de Direito da FGV-RJ. Diretor do Creative Commons no Brasil. Membro da Comissão de Proteção ao Consumidor no Comércio Eletrônico, do Ministério da Justiça. Professor da Fundação Getúlio Vargas. Organizador dos livros *Comércio Eletrônico* (Revista dos Tribunais/2001) e *Conflitos sobre Nomes de Domínio e outras Questões Jurídicas na Internet* (Revista dos Tribunais/2003). Autor do livro *Direito, Tecnologia e Cultura* (Editora FGV/2005).

**Danilo Maganhoto Doneda**

Doutor e Mestre em Direito Civil pela Universidade do Estado do Rio de Janeiro - UERJ. Pesquisador na *Garante per la protezione dei dati personali* (2003-2005). Pesquisador visitante na *Scuola di Specializzazione in Diritto Civile dell´Università degli Studi di Camerino*. Membro da Comissão de Proteção ao Consumidor no Comércio Eletrônico, do Ministério da Justiça. Professor dos cursos de pós-graduação do CEPED/UERJ. Autor do livro *Da Privacidade à Proteção de Dados Pessoais* (Renovar/2006), e co-autor dos livros *Problemas de Direito Civil-Constitucional* (Renovar/2001), *A Parte Geral do Novo Código Civil* (Renovar/2002) e *Código Civil Interpretado Conforme a Constituição da República* (Renovar/2004). Autor da dissertação "O Correio Eletrônico e o Direito à Privacidade", aprovada com louvor, e da tese "Da Privacidade à Proteção de Dados Pessoais", aprovada com nota 10, com distinção e louvor, nos exames de mestrado e doutoramento, respectivamente, na Universidade do Estado do Rio de Janeiro.

**Carlos Affonso Pereira de Souza**

Mestre e Doutorando em Direito Civil na Universidade do Estado do Rio de Janeiro – UERJ. Coordenador Adjunto do Centro de Tecnologia e Sociedade (CTS), da Escola de Direito da Fundação Getúlio Vargas-RJ (DIREITO RIO). Professor dos cursos de graduação e pós-graduação da DIREITO RIO e da Pontifícia Universidade Católica – PUC-Rio. Professor dos cursos de pós-graduação do CEPED/UERJ. Membro da Comissão de Direito do Autor e do Entretenimento da Ordem dos Advogados do Brasil (OAB/RJ). Co-autor dos livros *Direito da Informática e da Internet* (Esplanada-Adcoas/2001), *Comentários à Lei de Imprensa* (Editora Forense/2004) e *Código Civil Interpretado Conforme a Constituição da República* (Renovar/2004). Autor da dissertação "Privacidade e Imagem: a Tutela dos Direitos da Personalidade na Internet", aprovada com nota 10, com distinção e louvor no exame de mestrado na Universidade do Estado do Rio de

Janeiro. Membro da Comissão de Proteção ao Consumidor no Comércio Eletrônico, do Ministério da Justiça.

**Carolina Rossini**

Advogada. Bacharel pela Universidade de São Paulo. Formada em Relações Internacionais pela Pontifícia Universidade Católica de São Paulo - PUCSP. MBA em E-Business pelo Instituto de Empresas de Madri. Especialista em Negociações Econômicas Internacionais pelo Programa Santiago Dantas - UNESP, UNICAMP e PUC/SP. Ex-advogada do Grupo Telefônica, atuante na área de Tecnologia da Informação e Direito Empresarial.

## *Sumário*

## 1. Apresentação:

O presente estudo, elaborado pelo Centro de Tecnologia e Sociedade (CTS), da Escola de Direito da Fundação Getúlio Vargas, mediante solicitação formulada pela Comissão de Trabalho sobre *Spam* (CT-Spam), do Comitê Gestor da Internet no Brasil (CGI), tem por escopo analisar as possibilidades de regulamentação jurídica no Brasil da questão do *spam*.

Para essa finalidade, o estudo ora apresentado encontra-se dividido em quatro partes: (i) o *spam* e a tutela dos dados pessoais; (ii) análise dos modelos estrangeiros; (iii) análise do substitutivo apresentado pelo deputado federal Nelson Proença ao projeto de lei nº 2186, de 2003, de autoria do deputado federal Ronaldo Vasconcellos; e (iv) proposta de anteprojeto sobre *spam*.

Na primeira parte acima mencionada, a questão do combate ao *spam* é inserida no cenário atual de proteção aos dados pessoais a partir da legislação brasileira já existente. Nesse sentido, é preciso perceber que a repressão à prática de envio de *spams* deve por um lado respeitar os parâmetros sobre a matéria inseridos na Constituição Federal e, por outro lado, inovar perante a legislação infraconstitucional. Nesse particular, é importante analisar as relações que eventualmente poderão ser criadas entre a nova legislação proposta e certos diplomas legais como o Código Civil (mais especificamente o seu art. 21) e o Código de Defesa do Consumidor (com respeito ao seu art. 43).

A segunda parte do estudo é dedicada à análise dos modelos adotados na legislação internacional para o combate ao spam. Ganharam destaque nesse sentido as soluções adotadas pela União Européia, através de sucessivas Diretivas, e pelos Estados Unidos, através do chamado CAN-SPAM Act.

A terceira parte do estudo trata de uma análise focada nos principais dispositivos de projetos de lei recentemente propostos no Congresso Nacional sobre a matéria. Maior atenção foi dedicada ao Projeto de Lei Substitutivo oferecido pelo Deputado

Nelson Proença ao Projeto de Lei nº 2.186/2003, originalmente apresentado pelo Deputado Ronaldo Vasconcellos.

Após o debate sobre a legislação projetada no cenário nacional, o estudo encerra com uma proposta de anteprojeto de lei para o combate efetivo do *spam* no País. A proposta aqui encaminhada representa uma sugestão que leva em consideração os diversos fatores mencionados neste estudo e, sobretudo, visa à aprovação de uma legislação que, ao invés de simplesmente criminalizar condutas, proporcione um desestímulo ao envio de *spams* como ferramenta de publicidade ou promoção de qualquer espécie.

É nesse sentido que o presente estudo espera prestar uma contribuição ao debate sobre a repressão e a regulamentação jurídica do *spam* no Brasil, atendendo às solicitações feitas pelo CGI, através de sua CT-Spam.

## 2. O *spam* e a tutela de dados pessoais:

### *2.1. A tutela de dados pessoais na legislação nacional*

O debate sobre o modelo normativo mais eficaz de combate ao *spam* passa, inicialmente, por uma análise de um cenário mais abrangente. Esse cenário consiste no estudo da tutela dos dados pessoais prevista na legislação brasileira em vigor. A importância de remeter a discussão sobre *spam* à proteção concedida aos dados pessoais reside no fato de que, independentemente do modelo que se adote para combater a proliferação do *spam* no País, a sua positivação legal repercutirá necessariamente na aplicação de diversos outros diplomas legais. Os referidos impactos dessa nova legislação sobre o tema poderão repercutir desde o texto constitucional até à aplicação de leis infraconstitucionais como o Código Civil e o Código de Defesa do Consumidor.

Adicionalmente, a análise isolada do problema do *spam* perde de vista a percepção de que o spam é, muitas vezes, o elo final de uma corrente que poderia ser interrompida anteriormente. O envio de mensagem eletrônica, muitas vezes, só é possível porque os dados pessoais que identificam o destinatário foram coletados de alguma forma. Um estudo, ainda que breve, sobre as formas de coleta e tratamento desses dados pessoais, bem como a sua respectiva legislação torna-se, portanto, peça fundamental para a introdução do debate ora proposto.

O direito à privacidade é garantido constitucionalmente no Brasil. A Constituição Federal brasileira contempla não apenas o direito à privacidade com respeito à preservação da vida privada e da intimidade da pessoa, como também garante a inviolabilidade da correspondência, do domicílio e das comunicações, em consonância com o previsto no artigo 5º, X e XII:

> *Artigo 5º, X: "São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação."*
> *Artigo 5º, XII: " É inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso,*

*por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal."*

Buscando situar o conteúdo normativo do artigo 5º, X, da Constituição Federal, acima referido, enuncia Celso Bastos que:

> *"O inciso oferece guarida ao direito à reserva da intimidade assim como ao da vida privada. Consiste na faculdade que tem cada indivíduo de obstar a intromissão de estranhos na sua vida privada e familiar, assim como impedir-lhes o acesso a informações sobre a privacidade de cada um, e também impedir que sejam divulgadas informações sobre esta área da manifestação existencial do ser humano."*[1]

A tutela concedida pela Constituição brasileira ao direito à privacidade não se esgota na declaração de direitos dos incisos X e XII, municiando ainda o indivíduo, através seu artigo 5º, LXXII, com a possibilidade de recorrer ao Poder Judiciário para que lhe seja garantido o acesso aos seus dados pessoais armazenados por entidades governamentais ou de caráter público. O preceito constitucional encontra-se redigido da seguinte forma:

> *"Artigo 5º, LXXII: Conceder-se-á habeas data:*
> *a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constante de registros ou bancos de dados de entidades governamentais ou de caráter público;*
> *b) para retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo."*

À luz dos dispositivos constitucionais acima referidos, cumpre destacar o entendimento de Tercio Sampaio Ferraz Junior, segundo o qual o sistema instituído pela Constituição para a proteção da privacidade de dados pessoais não visa a proteger exatamente um direito de propriedade de certo indivíduo sobre as suas informações, tal qual um direito de propriedade clássico. O viés da tutela constitucional encontrar-se-ia, portanto, no processo de comunicação de tais dados, fornecendo aos interessados meios de impedir a manipulação estratégica de dados (grampeamento e violação de circuitos informáticos), a

1 Celso Bastos e Ives Gandra da Silva Martins. Comentários à Constituição do Brasil, vol 2. São Paulo, Saraiva, 1989; p.63.

divulgação de informação inexatas (tutela do direto à imagem) ou ainda que firam a privacidade pessoal (coleta e armazenamento de dados pessoais em bancos de dados).[2]

Cumpre ressaltar ainda que a tutela do direito à privacidade no ordenamento jurídico nacional não se limita aos termos da Constituição Federal. Existem outras leis que regulamentam a privacidade em áreas específicas, como, por exemplo, a Lei nº 5.250/67, a chamada Lei de Imprensa, que estabelece penalidades para pessoas que, no exercício da atividade jornalística, revelarem fatos que violem a privacidade e a intimidade alheias; e a Lei nº 9296/96, que estabelece as condições necessárias para a interceptação telefônica.

O Código Civil, por seu turno, contempla o direito à privacidade no art. 21, da seguinte forma:

> *"Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma."*

Pela leitura da redação do art. 21, percebe-se de imediato que o legislador optou por restringir a titularidade do direito à privacidade no Brasil apenas para as pessoas físicas, estando implicitamente excluída a possibilidade de se tutelar a privacidade de pessoas jurídicas.

Adicionalmente, o art. 21 refere-se ao fato de que, em atendimento à solicitação da parte prejudicada, caberá ao Poder Judiciário adotar "as providências necessárias" para garantir a tutela da privacidade. A redação abrangente do dispositivo, que não se limita apenas a hipóteses de responsabilização civil pelo dano causado, poderá gerar efeitos salutares para o desenvolvimento da proteção à privacidade. Conforme expõe Danilo Doneda, em comentário ao artigo:

> *"Ao clamar pela criatividade do magistrado para que tome as providências adequadas, o Código Civil dá mostras da necessidade de uma atuação*

2 Tercio Sampaio Ferraz Junior. "A Liberdade como Autonomia Recíproca no Acesso à Informação" In, Marco Aurélio Greco e Ives Gandra de Silva Martins, Direito e Internet. São Paulo, Revista dos Tribunais, 2001, p. 247.

*específica de todo o ordenamento na proteção da privacidade da pessoa humana, que seja uma resposta eficaz aos riscos que hoje corre."*[3]

Deve-se lembrar, ainda, da pouco mencionada Lei nº 9454, de 07.04.1997, que institui o número único de Registro de Identidade Civil pelo qual cada cidadão brasileiro, nato ou naturalizado, será identificado em todas as suas relações com a sociedade e com os organismos governamentais e privados. Tal lei, ainda não regulamentada, poderá acarretar sérios entraves para a defesa da privacidade, uma vez que o estabelecimento de um cadastro único facilita o controle social e, unificando as informações de diversos bancos de dados então dispersos, poderá simplificar a construção indevida de perfis individuais.[4]

No que se refere especificamente à privacidade na Internet, o Projeto de Lei nº 4.906, de 2001, do Deputado Júlio Semeghini, ao consolidar outros dois projetos de lei em trâmite no Congresso Nacional, visa a regulamentar a atividade do comércio eletrônico no Brasil, contendo algumas disposições relativas à privacidade dos dados informados pelo consumidor nas transações *online*.

O artigo 33, ao regular a questão da privacidade dos dados fornecidos pelos consumidores, estabelece que o ofertante apenas poderá solicitar do consumidor informações de caráter privado necessárias à efetivação do negócio, devendo mantê-las em sigilo, salvo se prévia e expressamente autorizado a divulgá-las ou cedê-las.

O *caput* do presente artigo positiva a vedação da prática, recorrente no meio de Internet, da venda de cadastros dos consumidores sem o seu prévio conhecimento ou aceitação. Essa prática alcançou amplo desenvolvimento com a facilidade de comunicação

3 Danilo Doneda. "Os direitos da personalidade no novo Código Civil", in Gustavo Tepedino (coord). A Parte Geral do Código Civil. Rio, Renovar, 2003; pp. 52/53.

4 Severas críticas à referida lei são feitas por Marco Aurélio Greco em seu artigo "E todos tinham um número..." (in Internet e Direito. São Paulo, Dialética, 2000, pp. 175/197). Tem-se notícia de que a Comissão de Constituição e Justiça e de Redação, da Câmara Federal, aprovou em 29.03.2001 o projeto de lei nº 1.931/99, que revoga a Lei nº 9454/97, sendo a proposta encaminhada para o Plenário da Câmara, conforme divulgado pelo site da Câmara (http://www.camara.gov.br/sileg/Prop_Detalhe.asp?id=17414).

dos fornecedores com os potenciais consumidores através do correio eletrônico, proporcionando o envio de mensagens publicitárias não autorizadas (*spams*).

O comércio de dados pessoais estabelecido na Internet afronta o tratamento concedido aos bancos de dados pelo CDC em seu artigo 43, abaixo comentado, o qual estabelece que o consumidor deverá ter acesso às informações armazenadas sobre o mesmo, além de ser comunicado da abertura de banco de dados contendo suas informações pessoais.

O parágrafo segundo estabelece que, sem prejuízo da sanção penal, responde por perdas e danos o ofertante que solicitar, divulgar ou ceder informações em contrariedade com o dispostos no artigo 33 do projeto de lei.

Para lograr maior proteção aos dados pessoais dos consumidores, à parte da imputação de sanções, poder-se-ia inserir um parágrafo no artigo 33 do projeto de lei ora comentado, estabelecendo que o endereço eletrônico constitui dado de caráter pessoal para fins de controle da coleta, armazenamento e comunicação dos mesmos, enquadrando-se, assim, na proteção do *caput*. Essa medida contribuiria para coibir a proliferação de listas públicas de endereços eletrônicos, fonte precípua de coleta de dados pessoais para a propagação de *spams*, bem como a atividade de empresas que vendem os endereços eletrônicos de terceiros para o mesmo fim. Essa questão será melhor debatida no tópico abaixo.

### *2.2. A tutela dos dados pessoais na Internet*

As ameaças ao direito à privacidade foram severamente incrementadas na medida em que o progresso tecnológico permitiu que novas formas de violação à privacidade alheia fossem desenvolvidas. A rede mundial de computadores, por sua vez, constitui um ambiente favorável para incursões em afronta à privacidade, pois parcela significativa de seus usuários desconhece os meios pelos quais informações pessoais são coletadas através do hábito de navegação por páginas eletrônicas.

Nesse sentido, é importante notar que o tratamento da informação por computadores permite não apenas seu célere processamento para fins idôneos, mas também para o cruzamento indevido de dados pessoais e a interceptação de comunicações. Diversas são as formas de invasão à privacidade atualmente discutidas, podendo-se destacar, para os fins desse estudo, algumas considerações sobre a utilização de *cookies* para o monitoramento e personalização da navegação, e posteriormente, o envio reiterado de mensagens eletrônicas (*spams*), como objeto do debate ora proposto e conseqüência por vezes imediata da coleta desautorizada de dados pessoais.

O debate sobre a legalidade da coleta de informações pessoais pelos *cookies* tem-se mostrado como uma das questões mais controvertidas no que tange à tutela dos direitos da personalidade na Internet. Para que se compreenda corretamente a ameaça representada pela sua utilização indiscriminada na rede mundial de computadores, faz-se necessário conjugar conhecimentos tecnológicos e jurídicos. A análise da questão exclusivamente através de um desses aspectos conduzirá a um entendimento equivocado, não raramente radical, que falha em perceber a complexidade do debate.

Os *cookies* são pequenos arquivos de texto, que são enviados pelo servidor de um *site* acessado na Internet diretamente para o disco rígido do computador do usuário. O arquivo, uma vez inserido no computador, servirá então como repositório de informações que dizem respeito à pessoa do usuário, bem como aos seus hábitos de navegação na Internet (quais páginas foram visitadas e com que freqüência; quais compras foram efetuadas; anúncios visualizados, etc).[5]

Segundo definição de Antonio Jeová Santos, os *cookies*:

> *"[s]ão arquivos de dados gerados toda vez que a empresa que cuida da manipulação de dados, recebe instruções que os servidores web enviam aos programas navegadores e que são guardadas em diretório específico do computador do usuário."*[6]

5 Para maiores explicações sobre o funcionamento dos cookies, vide o verbete "cookies" na enciclopédia Wikipedia (http://pt.wikipedia.org/wiki/Cookie, acessado em 12.05.2007), além de outras informações constantes no site da Unicamp, in http://www.dicas-l.com.br/dicas-l/19970711.php (acessada em 30.08.2006).
6 Antonio Jeová Santos. Dano Moral na Internet. São Paulo, Método, 2001; p. 196.

A tecnologia dos *cookies* desempenhou uma função de grande relevo para o sucesso da Internet, na medida em que é o *cookie* que permite ao usuário obter uma navegação mais personalizada pelas páginas eletrônicas da rede. O desenvolvimento dessa tecnologia foi impulsionado pelo desejo de tornar mais agradável, e prática, a utilização da Internet.

Dessa forma, não necessariamente o *cookie* representa uma tecnologia projetada com fins exclusivos de invadir ilicitamente a privacidade dos usuários da rede mundial de computadores, como mencionam, equivocadamente, alguns autores.[7] O que deverá ser observado é como essa tecnologia será utilizada, não se condenando previamente um programa de computador, em si, por permitir que o seu uso seja realizado de forma a violar direitos de terceiros.[8]

Diversas práticas ilícitas, que representam séria ameaça à privacidade, têm sido praticadas na Internet por intermédio da utilização dos *cookies*,[9] mas é preciso analisar

7 Sonia Aguiar do Amaral Vieira. Inviolabilidade da Vida Privada e da Intimidade pelos Meios Eletrônicos. São Paulo, Juarez de Oliveria, 2002; p. 95; e Antonio Jeová Santos. Dano Moral na Internet, cit.; pp. 196/197.

8 Conforme tese exposta por Lawrence Lessig, em seu parecer apresentado no processo judicial movido por A&M Records Inc. contra Napster Inc., por conta de infração a direitos autorais decorrentes da utilização do programa de computador de troca de arquivos na Internet, desenvolvido pela Ré (in http://www.lessig.org/content/testimony/nap/napd3.doc.html - acessada em 30.08.2006).

9 Para que se possa mensurar a possível ameaça à privacidade representada pela utilização indevida dos cookies, cumpre lembrar o caso da tecnologia DART, desenvolvida pela empresa DoubleClick, cuja repercussão a transformou no expoente de toda a discussão sobre os limites do marketing direcionado e suas implicações relativas à privacidade do usuário na Internet.

A DoubleClick fornece para os sites afiliados à sua rede, a DoubleClick Network, ferramentas para que a publicidade exposta por tais sites (geralmente mediante a utilização de banners) possa estar diretamente relacionada às preferências de seus usuários, através do desenvolvimento de cookies gerados nos computadores individuais.

Por vários anos a DoubleClick coletou dados dos usuários dos sites pertencentes à sua rede comercial, tendo depositado um cookie nos computadores sempre que eles se deparavam com uma publicidade nas páginas eletrônicas. Através da denominada tecnologia DART, a DoubleClick é então capaz de disponibilizar publicidade direcionada para o perfil do usuário, tendo por base a leitura dos cookies arquivos previamente depositados no computador pessoal.

A atenção dos grupos de defesa da privacidade perante os novos meios de comunicação foi centrada na DoubleClick quando a empresa anunciou que iria cruzar os dados coletados de seus usuários com os colhidos por outra empresa, a Abacus Direct Corporation, cujos bancos de dados reportam informações sobre hábitos de consumo de 88 milhões de pessoas, resultantes de transações realizadas fora do ambiente de Internet. Esse fato ocasionou uma investigação por parte do FTC – Federal Trade Comission, nos Estados Unidos, tendo a DoubleClick desistido, em março de 2000, de prosseguir em seu projeto de relacionar os dados pessoais que possuía com os colhidos pelos cookies para fins de publicidade.

sempre o interesse por trás da manipulação da tecnologia. Assim será possível perceber se o programa de computador é capaz de promover algum bem-estar de forma lícita, ou se apenas foi desenvolvido para a realização de condutas ilegais.

Uma vez inserido no disco rígido do usuário, o *cookie* permite que, em retornando a uma página previamente visitada, o usuário possa ter acesso a informações que são do seu interesse, uma vez que o arquivo pode armazenar as preferências de navegação da pessoa, definindo um perfil que será utilizado pela empresa que explora o *site*, tanto para direcionar notícias que possam ser do seu interesse, como para oferecer produtos que se enquadram no seu perfil de consumo. A questão é: como essa empresa teve acesso às informações pessoais do usuário?

O *cookie* pode coletar tanto as informações que a pessoa voluntariamente fornece quando preenche um cadastro, por exemplo, como organizar um perfil do usuário com base no tipo de páginas eletrônicas visitadas.

Pode o usuário optar por não fornecer seus dados, ou mesmo impedir que *cookies* sejam instalados em seu computador, através de medidas técnicas usualmente simples, pois basta configurar o seu programa de navegação (*browser*) para que o recebimento de *cookies* seja proibido. Todavia, essas providências podem eventualmente resultar em problemas para se acessar as páginas eletrônicas na rede mundial de computadores.[10]

---

Para maiores detalhes sobre o caso, vide http://www.epic.org/doubletrouble/ (acessada em 30.08.2003).

10 Reporta Christiano German uma dificuldade encontrada pelo usuário da rede mundial de computadores quando configura o seu browser para que não seja permitida a colocação de cookies em seu disco rígido: "O provedor de acesso brasileiro UOL (www.uol.com.br) reage com insistência especialmente desagradável se o usuário não aceita nenhum dos seus cookies em seu computador. Nesse tocante, ele praticamente não se distingue dos seus pendants nos Estados Unidos e na Europa. Inicialmente, o acesso a homepage sofre um retardamento. Depois disso, o usuário precisa rejeitar 14 (quatorze) tentativas de se colocar um cookie. Se ele quiser em seguida chamar uma das janelas na oferta do UOL, o procedimento inicia uma vez mais da estaca zero." (in O Caminho do Brasil rumo à Era da Informação. São Paulo, Fundação Konrad Adenauer, 2000, p. 87).

O debate sobre a violação da privacidade do usuário deve então ser analisado em três momentos distintos da utilização dos *cookies*: (i) a coleta; (ii) o armazenamento; e (iii) a utilização dos dados pessoais.

Com relação à coleta dos dados, é importante notar que deve o usuário da Internet estar ciente de que algumas informações pessoais podem ser coletadas quando do acesso a um *site* na rede mundial de computadores. No Direito brasileiro, a questão está regulada, no âmbito das relações de consumo. Dentre outras medidas protetoras, o Código de Defesa do Consumidor contempla, em seu capítulo V, seção VI, uma regulamentação especial em relação aos bancos de dados e cadastros formados a partir de informações dos consumidores. Como previsto no artigo 43, muitas obrigações são impostas aos administradores dos bancos de dados, como, por exemplo, revelar a cada consumidor a informação coletada a seu respeito. É a redação do artigo 43, do CDC:

> *Art. 43. "O consumidor, sem prejuízo de disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.*
>
> *§1.º Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.*
>
> *§2.º A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.*
>
> *§3.º O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas."*

Dessa forma, não é possível, no Direito brasileiro, que informações pessoais sejam coletadas sem o consentimento do consumidor. Todavia, essa prática tem sido descumprida reiteradamente, em ostensiva violação ao comando do CDC.

Victor Drummond, por seu turno, entende que não haveria qualquer infração à privacidade na simples coleta de dados dos usuários pelos *cookies*. Esse entendimento se baseia na hipótese de que a lesão à privacidade decorre apenas da utilização indevida das informações coletadas:

> "Reputamos como correta a interpretação de que o grande problema dos *cookies* decorre das utilizações que se faz após a coleta dos dados, sendo que, em geral, a coleta em si, acaba por não representar violação de privacidade."[11]

Esse entendimento pode encontrar alguma oposição quando se observa diversas práticas desenvolvidas na Internet e, principalmente, se for levado em conta que a legislação consumerista demanda que a pessoa cujos dados são ingressados em banco de dados seja comunicada não apenas do fato, mas também de quais informações foram objeto dessa conduta. Não basta, portanto, simplesmente dar notícia da coleta dos dados pessoais, mas também esclarecer o conteúdo dos dados obtidos. Assim, caso a comunicação tenha sido realizada de forma clara, a coleta de dados pessoais torna-se legítima.

Com relação ao armazenamento, é importante notar que o consumidor, por força do art. 43 do CDC, deverá ter acesso aos seus dados constantes do banco de dados da empresa que explora o *site*, sendo-lhe ainda permitido exigir a sua correção, caso encontre alguma inexatidão. O não cumprimento da requisição encaminhada pelo usuário submete o infrator às disposições do art. 84 do Código de Defesa do Consumidor, podendo o mesmo ser condenado a cumprir a sua obrigação de fazer sob pena de multa, ou mesmo pagar indenização por perdas e danos causados.

Finalmente a utilização das informações armazenadas tem por escopo proteger a pessoa cujas informações foram coletadas contra o manuseio indevido de seus dados pessoais. É especialmente relevante nesse contexto a prática disseminada na Internet de venda de cadastros, sem que seja feita qualquer notificação do fato ao usuário que forneceu os dados.

À luz do art. 43 do CDC, pode-se perceber que as exigências feitas pelo Código são similares àquelas propostas pela maioria das diretrizes de privacidade *online*, como as da OPA – *Online Privacy Alliance*, de acordo com a qual:

> "A política de privacidade deve deixar claro quais informações estão sendo coletadas, o uso destas, o possível acesso de terceiros a elas, as opções disponíveis ao indivíduo quanto à coleta, uso e distribuição das informações;

11 Victor Drummond. Internet, Privacidade e Dados Pessoais. Rio, Lumen Juris, 2003; p. 103.

> uma declaração de compromisso quanto à segurança das informações por parte da organização e quais os passos tomados por ela para assegurar a qualidade e o acesso às informações."[12]

Embora os tribunais venham aplicando largamente o CDC no que se refere a diversos assuntos, as exigência específicas do art. 43 não têm sido, ainda, totalmente observadas, especialmente no que diz respeito à revelação ao consumidor dos dados coletados sobre ele.

Em junho de 2000, a Fundação Vanzolini, em cooperação com a Universidade de São Paulo - USP, emitiu uma Norma Padrão para adequar os sites brasileiros a níveis internacionais de políticas de privacidade. A elaboração da NRPOL – Norma de Referência da Privacidade Online foi patrocinada por diversas empresas e gradualmente vem alcançando efeitos positivos no mercado brasileiro da Internet.

A NRPOL estabelece vários princípios éticos a serem aplicados pelos sites brasileiros a fim de se preservar a privacidade do usuário da Internet, tais como: (i) o acesso completo do usuário às informações coletadas ao seu respeito; (ii) a garantia de que a informação recolhida é adequada e de que não será usada para propósitos diversos daqueles que motivaram o seu recolhimento; e (iii) a adoção, pela empresa recolhedora dos dados, de procedimentos que previnam danos e o uso, sem autorização de tais informações, e assim por diante.[13]

Em síntese: a tecnologia dos *cookies* não representa em si uma violação ao direito da privacidade. Todavia, a forma pela qual irá se estruturar a coleta, o armazenamento e a utilização das informações pessoais é que irá determinar a licitude, ou ilegalidade, da conduta do administrador do banco de dados.

Uma das utilizações que podem ser manejadas depois da coleta dos dados pessoais é a compilação de e-mails para a finalidade de envio de spams. Nesse sentido, é importante definir o que se entende por spam para que então seja perceptível como o seu

12 (trad. aut.) www.privacyalliance.org/resources/ppguidelines.shtml
13 NRPOL – Norma de Referência da Privacidade Online, Fundação Vanzolini, 2000; p.06.

combate passa por esse enquadramento maior sobre a tutela dos dados pessoais (e da privacidade como um todo) erguida no ordenamento jurídico nacional.

### *2.3 Conceito e problematização do spam*

O termo "*spam*" é um neologismo surgido na esteira da popularização da Internet. Originalmente, refere-se a uma determinada marca de alimento enlatado[14]. Não é possível precisar quando foi empregado pela primeira vez no contexto que agora examinamos: talvez em meados da década de 1980, quando um usuário de um sistema informatizado causou problemas técnicos com a repetição automática da palavra "*spam*" em um ambiente multi-usuário[15]; ou então, na mesma época, alguns grupos de discussão da USENET[16] começavam a enfrentar mensagens enviadas em massa. O que parece certo é que o termo foi inspirado em um célebre quadro do grupo humorístico Monty Python[17].

Uma definição "utópica" do *spam* poderia apontá-lo como todo *e-mail* que não seja útil ao destinatário, ou que este tenha preferido não haver recebido. Uma definição "prática" seria aquela que identificasse objetivamente no *spam* elementos que o qualificassem como inútil e indesejado e pudesse orientar os mecanismos de repressão à sua prática. Entre estes dois pólos, porém, há uma série de incertezas e inconsistências.

---

14 O termo *SPAM*™ (em letras maiúsculas) refere-se a um produto, uma espécie de carne enlatada (provavelmente uma espécie de contração a partir das palavras *SPiced hAM*), produzida pela Hormel Foods Corporations, que detém os direitos sobre a marca. <http://www.*spam*.com/ci/ci_in.htm>.

15 Este usuário participava em um MUD (*Multi-User Dungeon* - uma espécie de jogo no qual vários participantes interagem *on-line*), e criou um pequeno programa que fazia com que a palavra "*Spam*" aparecesse incessantemente na tela dos demais participantes, impedindo sua participação. J. D. Falk. *The Net abuse FAQ revision 3.2*, §2.4. <http://www.cybernothing.org/faqs/net-abuse-faq.html#2.4>, cf. David Sorkin. "Technical and legal approaches to unsolicited eletronic mail". 35 *U.S.F. Law Review* 325 (2001).

16 A USENET reúne grupos de discussões sobre variados temas, nos quais os inscritos podem postar *mensagens* que ficam a disposição de todos os interessados. Um forte traço da origem da utilização do termo "*spam*" na USENET é oferecido por algumas das definições do termo *spam* presentes no *Jargon file:* "2. to cause a newsgroup to be flooded with irrelevant or inappropriate messages; (...); 4. To bombard a newsgroup with multiple copies of a message. ". O *Jargon File* é um popular glossário de termos técnicos referentes à Internet e sua cultura. V. < http://www.catb.org/jargon/html/S/*spam*.html>.

17 Neste *sketch*, que se passa em um restaurante, uma garçonete tentava dar informações sobre o menu - no qual todas as opções incluíam *spam*, o que irrita um cliente. Ao mesmo tempo, um grupo de vikings que se encontra no restaurante canta, ao fundo: "*Spam*, *spam*, *spam*, *spam! Lovely spam! Wonderful spam*!" – com vigor cada vez maior, até o ponto de tornar impossível o trabalho da garçonete. Deste quadro o termo "*spam*" foi tomado de empréstimo para representar algo que seja absolutamente irrelevante para uma determinada discussão e que tire a atenção do seu foco principal.

Uma primeira definição, a partir da qual se pode trabalhar, é aquela adotada pela Cartilha de Segurança para Internet, elaborada pelo CERT – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, a qual define spam como "termo usado para se referir aos e-mails não solicitados, que grealmente são enviados para um grande número de pessoas. Quando o conteúdo é exclusivamente comercial, esse tipo de mensagem é também referenciada como UCE (do Inglês, Unsolicited Commercial E-mail)."[18]

Já de início, a maior parte das tentativas de definição parecem muito mais motivadas pela conveniência do que propriamente refletir uma determinada acepção em si. É comumente aceita sua sinonímia com "correio eletrônico comercial não solicitado", a qual abrange o núcleo central das mensagens percebidas como *spam*, porém carrega um certa inconsistência que se evidencia pelo fato de que há diversas mensagens geralmente percebidas como *spam* que não possuem caráter comercial, bem como, sob determinados enfoques, é possível identificar mensagens "não solicitadas", com caráter comercial, que podem não merecem esta qualificação.

Note-se ainda que o âmbito de aplicação do termo não é somente o *e-mail* da Internet, pois sua utilização vem se propagando para outros protocolos de comunicação eletrônicos (SMS, *chat on-line* e outros)[19] e sistemas informáticos nos quais não há propriamente a troca de mensagens[20]. Em um limite extremo, são englobadas até mesmo algumas modalidades de comunicação que independem de redes de computadores[21], não obstante que a tendência à utilização do termo *spam* esteja associado com maior

[18] CERT. *Cartilha de Segurança para Internet*. Versão 3.0 (in http://cartilha.cert.br, acessado em 14.12.2006).
[19] Na União Européia, a Diretiva 2002/58/CE do Parlamento Europeu e do Conselho (Diretiva relativa à privacidade e às comunicações eletrônicas) endereça o problema sem referir-se diretamente ao termo "*spam*", preferindo uma referência genérica como "comunicações eletrônicas não solicitadas". Assim, são abrangidas outras formas de comunicação eletrônica.
20 Cite-se como exemplo o "vandalismo" do qual são vítimas certos sites que permitem a elaboração coletiva de seu conteúdo, como os sitemas Wiki (v. <http://en.wikipedia.org/wiki/Wikipedia:Vandalism> ); ou então a utilização indiscriminada de *meta-tags* para fazer com que um site apareça com maior destaque nos mecanismos de busca na Internet, ambas práticas que são também eventualmente rotuladas como "*spam*".
21 Algumas chamadas telefônicas realizadas automaticamente, em regra para fins de marketing direto, são eventualmente denominadas *phone spam*.

propriedade com as variadas formas de abusividade identificadas no âmago das comunicações eletrônicas de uma forma geral.

Na busca de um denominador comum, mesmo uma tentativa de generalização que considere os *e-mails* comerciais não solicitados como o "núcleo duro" do *spam* não é capaz, por si só, de proporcionar um patamar jurídico ou mesmo técnico[22] dentro do qual tratar a questão de maneira completamente segura - visto que o *spam*, nesta ótica, não se diferenciaria qualitativamente de diversas práticas de marketing direto.

Para enquadrarmos a questão, é necessário identificar alguns elementos básicos que o *spam* pode apresentar de forma mais ou menos acentuada: (i) o caráter comercial; (ii) o envio em massa; (iii) a uniformidade de seu conteúdo; e (iv) o fato de não ter sido solicitado pelo destinatário.

Sobre o caráter comercial do *spam*, já foi aludida a freqüência com que esta sua característica é mencionada como essencial. Salta aos olhos, no entanto, o fato de que não é impossível nem mesmo raro que *e-mails* sem caráter comercial direto ou até indireto acabem por ser considerados como *spam* – e, mais importante, que o tratamento que eles mereçam seja idêntico àquele dos *e-mails* comerciais tidos como *spam*. Nesta grande categoria do *spam* não-comercial estariam incluídas, por exemplo, as mensagens com conteúdo fictício elaboradas com a intenção de fraudar de alguma maneira o destinatário. Tal fraude poder-se-ia processar seja através da instalação de vírus, *trojans*, *spyware* ou congêneres no computador do destinatário, seja pela tentativa de obter dados pessoais de forma ilícita ou então por inúmeros outros meios – todos dificilmente reconduzíveis a qualquer aspecto licitamente "comercial". Assim, malgrado a finalidade comercial direta ou indiretamente verificável em um *spam* "clássico", é de se ter em conta que esta não é uma característica a ser tomada como absoluta.

O envio em massa e a uniformidade do conteúdo do *spam* são características da sua própria modalidade de propagação. Como a taxa de resposta é baixíssima, o *spam*

22 Como é confirmado pela arquitetura dos principais filtros desenvolvidos para bloquear o *spam*. Estes filtros não tem como seu pressuposto de funcionamento qualquer definição estática sobre o *spam* (seu caráter comercial, por exemplo), porém se baseiam em regras (linguísticas, heurísticas e outras) que estabelecem uma alta probabilidade de uma mensagem ser do gênero que uma pessoa preferiria "não ter recebido").

somente se justifica quando realizado em um determinado volume que garanta um mínimo de respostas positivas para o intento do seu remetente. Portanto, é uma prática quase sempre massificada, que tem como conseqüência a impossibilidade de personalização de seu conteúdo – que é uniforme e padrão ou, em casos específicos, pode compreender modificações mínimas realizadas justamente para que o destinatário, por conta destas, não perceba tratar-se propriamente de um *spam*. Estas, porém, são regras apenas qualitativas, por não se concentrarem no conteúdo da comunicação. Como conseqüência, apesar de praticamente todo *e-mail* considerado abusivo e classificado como *spam* apresentar estas duas características, ainda resta o fato de que, em poucos e raros casos, uma única mensagem, ainda que dirigida a um só destinatário, possa ser considerada como *spam*.

A idéia de que um *e-mail* não foi "solicitado" pelo seu destinatário deve ser examinada com a devida cautela. Em uma interpretação excessivamente literal, a grande maioria dos *e-mail*s (e das comunicações em geral) não é estritamente "solicitada" pelo destinatário, porém lhe são dirigidos no âmbito de contatos anteriores ou de interesses específicos. Talvez a expressão "não solicitada" fosse melhor traduzida por algo que representasse o fato de que o destinatário, tendo sabido do teor da mensagem, tivesse preferido não tê-la recebido – que, por sua vez, peca pelo extremo subjetivismo. Fato é que a expressão "não solicitado" é de uso generalizado, e cabe a integração de sua interpretação, que deve ser realizada sob a ótica da boa-fé no sentido de que o *e-mail* deva apresentar algum interesse objetivo potencial para seu destinatário. É relevante ainda que, nas perspectivas de abordagem da matéria a partir de regras de proteção de dados pessoais e também de regras de *opt-in*, o conteúdo da referida solicitação integrar-se-á essencialmente pela verificação do consentimento prévio do destinatário ao recebimento do *e-mail*.

Uma definição que procura equilibrar os elementos apresentados é fornecida pelo *Jargon File*:

> *"Enviar e-mails em massa, não solicitados, idênticos ou quase idênticos, geralmente contendo publicidade. Utilizado em particular*

> *quando os endereços foram extraídos do tráfego de rede ou de bancos de dados sem o consentimento dos destinatários. (...)"*[23].

Conclui-se, enfim, que o atual estado da matéria não recomenda que o tema do *spam* seja encerrado em uma definição abstrata fechada, pelo motivo que qualquer uma destas apresenta o risco de excluir da sua esfera de abrangência *e-mails* que sejam percebidos como *spam* e que mereçam ser tratados como tal. Feita esta consideração, a classificação de uma mensagem como *spam* deve (i) levar em conta a presença (ainda que não de todas) das quatro características acima delineadas e (ii) ponderar se o envio da mensagem pode responder a algum interesse do remetente ou mesmo que não possa lhe acarretar um dano, concreto ou potencial.

Na ausência de uma legislação específica que coíba a prática de envio reiterado de mensagens não solicitadas, busca a doutrina nacional responsabilizar o *spammer*, civil e criminalmente, pela sua atitude. Assim, os mais diversos dispositivos legais são invocados, sem que se alcance um entendimento coerente sobre o assunto.

Um dos dispositivos mais referidos pela doutrina para buscar-se enquadrar a prática de *spam* é o artigo 39, III, do CDC, que assim está redigido:

> "Art. 39. É vedado ao fornecedor de produtos ou serviços, dentre outras práticas abusivas:
>
> (...) III - enviar ou entregar ao consumidor, sem solicitação prévia, qualquer produto, ou fornecer qualquer serviço."[24]

Vale destacar que o art. 84, do CDC, que prevê a possibilidade de se obter em juízo uma ordem que obrigue a parte contrária à observância de uma obrigação de fazer ou não fazer, também poderá ser acionado para que se impeça o *spammer* de prosseguir com o envio de mensagens não solicitadas.

---

[23] O mencionado *Jargon File* trata o termo "*spam*" como verbo transitivo, verbo intransitivo e substantivo. Entre as 6 definições que ele fornece para o termo, destacamos a de número 5: "5. To mass-mail unrequested identical or nearly-identical email messages, particularly those containing advertising. Especially used when the mail addresses have been culled from network traffic or databases without the consent of the recipients. Synonyms include *UCE*, *UBE*. As a noun, '*spam*' refers to the messages so sent.". *The Jargon File*, in: <http://www.catb.org/~esr/jargon/html/S/*spam*.html>.

24 Nessa direção, vide Sonia Aguiar do Amaral Vieira. Inviolabilidade, cit.; p. 121; e Amaro Moraes e Silva Neto. E-mails Indesejados à luz do Direito. São Paulo, Quartier Latin, 2002; p. 156.

No aspecto penal, Amaro Moraes e Silva Neto chega a propor que, em sendo a Internet um serviço de utilidade pública, a prática do envio de *spam* poderia ser enquadrada no artigo 265 do Código Penal, segundo o qual será aplicada pena de reclusão de 1 (um) a 5 (cinco) anos, além de multa, a quem atentar contra o funcionamento e segurança de serviços de utilidade pública.[25]

De toda sorte, para que se logre êxito em responsabilizar o envio reiterado de mensagens eletrônicas, deverá ser comprovado dano causado. Nesse ponto, interessa pouco o debate travado na doutrina sobre o melhor artigo de lei a ser utilizado para a condenação do *spammer*. O próprio artigo 186, do Código Civil, ofereceria base para que se buscasse indenização contra o remetente das mensagens, ao dispor que:

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

Em se entendendo que o envio de *spam* representa violação à privacidade, poder-se-ia, inclusive, acionar o dispositivo do art. 12, do Código Civil, que, de forma genérica, garante a tutela dos direitos da personalidade.

Todavia, no que concerne à prova do dano, é importante notar que a sua apresentação poderá ser dificultada pelas circunstâncias do encaminhamento de *spam*. É comum, nesse sentido, alegar-se que o dano causado pelo *spam* adviria da perda de tempo resultante da constante exigência de se apagar mensagens não solicitadas da caixa postal eletrônica.

No Brasil, a primeira decisão proferida sobre a matéria esposou o entendimento de que com relação ao envio de propaganda não solicitada na Internet "não

25 Amaro Moraes e Silva Neto. Privacidade na Internet, cit.; p. 97. Neste sentido, vale ressaltar, com base nas informações de Robert B. Gelman e Stanton McCandlish, que o grande fluxo de mensagens não solicitadas não está, de forma alguma, congestionando o tráfego de informações na Internet, uma vez que a maior parte de tais mensagens são apenas arquivos de texto. Todavia, lembram os referidos autores, os spams podem congestionar o servidor de e-mails de uma pessoa, ou mesmo fazer com que o espaço máximo reservado para suas mensagens seja ultrapassado (In Protecting Yourself Online, cit.; p. 123/125).

há o que se falar em violação à intimidade, à vida privada, à honra e à imagem de alguém ou prejuízos de ordem material."[26]

Como a lesividade do spam individualmente considerado é bastante reduzida, poder-se-ia pensar em trazer para o debate sobre a melhor forma de combater o envio de spam algumas experiências bem sucedidas no Brasil para o atendimento de outros casos em que o dano individualmente considerado é pequeno ou de difícil percepção. Trata-se, nesse particular, da tutela coletiva de direitos.

O melhor de exemplo de atuação da tutela coletiva de direitos pode ser buscada nas disposições do Código de Defesa do Consumidor. Os artigos 81, III, e 82, ao regular a possibilidade de proteção coletiva dos direitos previstos naquele diploma legal, assim estão redigidos:

> *"Art. 81. A defesa dos interesses e direitos dos consumidores e das vítimas poderá ser exercida em juízo individualmente ou a título coletivo.*
>
> *Parágrafo único. A defesa coletiva será exercida quando se tratar de:*
>
> *(...)*
>
> *III - interesses ou direitos individuais homogêneos, assim entendidos os decorrentes de origem comum.*
>
> *Art. 82. Para os fins do art. 81, parágrafo único, são legitimados concorrentemente:*
>
> *I - o Ministério Público;*
>
> *II - a União, os Estados, os Municípios e o Distrito Federal;*
>
> *III - as entidades e órgãos da Administração Pública, direta ou indireta, ainda que sem personalidade jurídica, especificamente destinados à defesa dos interesses e direitos protegidos por este Código;*
>
> *IV - as associações legalmente constituídas há pelo menos um ano e que incluam entre seus fins institucionais a defesa dos interesses e direitos protegidos por este Código, dispensada a autorização assemblear.*
>
> *§ 1° O requisito da pré-constituição pode ser dispensado pelo juiz, nas ações previstas nos arts. 91 e seguintes, quando haja manifesto interesse social*

26 Trecho da sentença da juíza Rosângela Leiko Kato, da 6.ª Vara do Juizado Especial Cível de Micro Empresas, de Campo Grande, Mato Grosso do Sul (processo nº 2001.166.0812-9). Segundo informa Victor Drummond, a decisão foi confirmada em segunda instância (in Internet, Privacidade e Dados Pessoais, cit.; p. 115).

*evidenciado pela dimensão ou característica do dano, ou pela relevância do bem jurídico a ser protegido.*

A proposta de anteprojeto de lei ao final deste estudo apresentada procura se valer da experiência desenvolvida na última década pelo Direito brasileiro na seara da tutela coletiva dos direitos individuais homogêneos, facultando às pessoas constantes do art. 82 da Lei nº 8078/90 (Código de Defesa do Consumidor), mover a competente ação coletiva para a defesa dos interesses violados pelo envio de spam. Esse dispositivo possibilita que instituições como o Ministério Público ou entidades de defesa dos direitos dos consumidores possam inserir a repressão ao spam em suas atuações, além de se valer de uma infra-estrutura já montada por tais entidades para a defesa de direitos e interesses que em tudo se assemelham àqueles violados pelo fenômeno do spam.

A partir desses dados, é preciso localizar a discussão sobre a melhor forma de regulamentação jurídica e combate ao *spam* no mundo, para que, em seguida, e à luz das propostas já em vigor, possa ser enunciada uma alternativa ao problema aqui suscitado.

.

## 3. Análise dos modelos estrangeiros:

Quando confrontados com a magnitude a que chegou o problema do *spam*, alguns dos países mais sensíveis aos seus efeitos iniciaram a propor e a testar diversas possibilidades de solução. As medidas para afrontá-lo podem ser divididas em, basicamente, três categorias: a auto-regulação e o recurso a normas sociais; as medidas técnicas e, finalmente, a via jurídica[27]. Nos últimos anos, após experiências pouco satisfatórias com as duas primeiras categorias de medidas, a via judicial e em particular a via legislativa passou a ser utilizada com cada vez maior freqüência.

O objetivo deste estudo é a apresentação das linhas gerais de ação no combate ao *spam* na Europa e nos Estados Unidos, com ênfase na via legislativa e em sua eficácia.

O fenômeno do *spam* na Europa se manifestou com certa defasagem em relação aos Estados Unidos, bem como foi percebido de maneira um pouco diferenciada. Esta diferença de dinâmicas pode ser justificada pelo fato de ter sido primeiramente nos Estados Unidos que o e-mail se tornou uma ferramenta amplamente utilizada, bem como foi ali que a Internet começou a ser utilizada para finalidades comerciais de forma massificada.

Tais motivos justificam um certo retardo na percepção econômica e social do fenômeno do *spam* na Europa, ao que se soma também um retardo na prospectiva de soluções de certa forma típico dos ordenamentos jurídicos de bases romano-germânicos: nestes, não raro é necessário que uma determinada demanda esteja razoavelmente estabelecida antes que o ordenamento passe a propor remédios para atendê-la.

[27] A referência a estes diferentes tipos de respostas ao problema do *spam* é freqüente na doutrina, como por exemplo em Daniel Sorkin. "Technical and legal approaches to unsolicited electronic mail", in: 35 *University of San Francisco Law Review* 325 (2000-2001), p. 326. É interessante notar, como aliás o faz o próprio Sorkin, uma certa similitude entre estas categorias e as formas de regulação do comportamento no espaço virtual que aponta Lawrence Lessig: a lei, os mercados e a arquitetura do ciberespaço (que ele denomina "código"). Lawrence Lessig. *Code and other laws of cyberspace.* Basic Books: New York, 1999.

Consideradas certas diferenças básicas, hoje se pode dizer que a percepção do *spam* como um grave problema a ser imediatamente enfrentado, capaz de comprometer a utilização de redes de comunicação eletrônica em sua eficiência e confiabilidade, é comum tanto aos Estados Unidos quanto à Europa. A seguir nos ocuparemos do desenrolar deste enfrentamento, basicamente através da via legislativa.

### *3.1. O sistema europeu*

O tratamento do tema do *spam* a partir de um prisma europeu justifica-se pelo fato de este ser um tema que foi sendo paulatinamente transferido para a esfera de influência direta do direito comunitário.

A União Européia não editou uma normativa exclusivamente do problema do *spam*, porém o tema foi tratado em algumas importantes diretivas[28], as quais a principal é a Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrônicas (Diretiva relativa à privacidade e às comunicações eletrônicas).

A tendência do desenvolvimento da matéria demonstra que ela foi conduzida para o campo da proteção de dados pessoais, sendo que a sua problemática é freqüentemente traduzida nos termos das normativas referentes a dados pessoais[29], matéria que já conta com um razoável tempo de maturação no espaço jurídico europeu[30].

---

28 A Diretiva é um instrumento normativo típico da União Européia, em cujo sistema de fontes legislativas coexistem os tratados que a instituem (fonte primária), ao lado da normativa diretamente derivada deles; e as fontes secundárias, que são basicamente os regulamentos, as diretivas e as decisões, além das recomendações e pareceres. A função básica da Diretiva é de uniformização legislativa. A aprovação de uma diretiva implica que cada país-membro adapte, em um certo período de tempo, seu próprio ordenamento jurídico aos moldes estabelecidos pela diretiva, em um processo que leva o nome de transposição. Caso um país-membro não o faça tempestivamente, o país poderá responder pela mora perante a Corte Européia de Justiça, além do que a matéria disciplinada passa a contar com um certo grau de eficácia direta. v. Klaus-Dieter Borchardt. *O ABC do direito comunitário.* Bruxelles: Comissão Européia, 2000.

29 Em particular a Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

30 v. Viktor Mayer-Schönberger. "General development of data protection in Europe", in: *Technology and privacy: The new landscape*. Phillip Agre; Marc Rotenberg. (orgs.). Cambridge: MIT Press, 1997, pp. 219-242 e Danilo Doneda. *Da privacidade à proteção de dados pessoais.* Rio de Janeiro: Renovar, 2006.

Pode-se afirmar que o enfoque dado pela legislação comunitária ao *spam* compreende dois objetivos: o primeiro, prático, de reduzir o volume global de *spam*, e o segundo, ético, de procurar garantir o controle individual sobre o fluxo de informações, seja este em entrada ou em saída[31].

Passando ao tratamento específico da matéria, a primeira disposição normativa no direito comunitário que veio a produzir efeitos sobre a prática do *spam* é a mencionada Diretiva 95/46/CE, de 1995, que institui a disciplina geral de proteção de dados pessoais. Ainda que não tenha visado especificamente ao problema do *spam*, entre outras disposições ela especifica que, no tratamento informatizado de dados pessoais, estes devem ser coletados por meios lícitos e para finalidades precisas e determinadas[32]. Esta diretiva ainda não abordava diretamente o problema do *spam*, porém forneceu o patamar jurídico de base sobre o qual viriam a se estabelecer as futuras previsões normativas referentes ao tema.

Após a Diretiva 95/46/CE, alguns países europeus procuraram tratar do problema do *spam* em seu direito interno, antecipando o que viria a se tornar a solução padrão no espaço comunitário, qual seja, a introdução do princípio do consentimento preliminar para o envio de mensagens comerciais - o *opt-in*.

Os primeiros traços de uma normativa européia que aborde diretamente o tema do *spam* estão na Diretiva sobre contratos à distância, de 1997[33], que ao tratar do marketing direto estabelecia a regra do *opt-in* para as comunicações realizadas por fax e por

31 Nicola Lugaresi. "European Union vs. *spam*: A legal response", in: *Spam 2005: Technology, law and policy.* Washington: Center for Democracy and Technology, 2005 , p. 45.

32 Uma dúvida suscitada por esta diretiva foi se os endereços de e-mail seriam ou não identificadores do seu titular - pois, em caso afirmativo, as disposições sobre proteção de dados da Diretiva aplicar-se-iam ao e-mail e, consequentemente, ao *spam*. A tendência que se revelou mais forte foi a que considerava o e-mail, efetivamente, como identificador da pessoa. John Magee. "The law regulating unsolicited commercial e-mail : An international perspective", 19 *Santa Clara Computer & High Technology Law Journal* 333 (2002-2003), p. 365.

33 Diretiva 97/7/CE do Parlamenteo Europeu do Conselho de 20 de Maio de 1997, relativa à proteção dos consumidores em matéria de contratos à distância

chamadas telefônicas automáticas[34], e um sistema de *opt-out* para as demais[35] (que incluíam, portanto, o e-mail).

A Diretiva sobre Telecomunicações, de 1997[36], não inovou as disposições da diretiva sobre vendas à distância ao proibir de forma geral a utilização de fax e de chamadas telefônicas automáticas com o propósito de marketing direto sem o consentimento do destinatário[37]. Em relação a "chamadas não solicitadas" realizadas por outros meios de comunicação[38], a diretiva proporciona aos estados membros optarem entre regimes de *opt-in* ou *opt-out*. Esta diretiva novamente não tratou diretamente do e-mail[39], porém proporcionou a base para que alguns países (Itália, Finlândia, Áustria e Dinamarca) incluíssem em seu direito interno, ao transpor a diretiva, normas específicas para o e-mail que instituíram um regime de *opt-in*[40].

A primeira menção direta ao e-mail no direito comunitário veio com a Diretiva sobre Comércio Eletrônico, de 2000[41]. A técnica adotada para afrontar o problema previa um sistema de identificação da mensagem comercial não-solicitada no campo do assunto do e-mail[42], técnica esta conhecida como *labelling*. Ela também prevê a possibilidade de medidas que obrigam aos remetentes de e-mails comerciais a consultarem listas de usuários que optaram por não receber tal gênero de mensagens – as conhecidas

34 Art. 10(1).
35 Art. 10(2).
36 Diretiva 97/66/CE do parlamento Europeu e do Conselho de 15 de Dezembro de 1997 relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das telecomunicações
37 Art. 12(1).
38 Art. 12(2).
39 De fato, o texto da Diretiva trata de "chamadas não solicitadas", dando azo às diversas interpretações que incluíram ou não no espírito destas "chamadas" o e-mail.
40 Por outro lado, outros países europeus interpretaram de forma mais literal o termo "chamada", excluíndo o e-mail do campo de aplicação da diretiva e evidenciando a desarmonia entre as diversas legislações nacionais da União Européia em uma área na qual a necessidade de normas similares se fazia sentir com intensidade cada vez maior.
41 Diretiva 2000/31/CE do Parlamento Europeu e do Conselho de 8 de Junho de 2000 relativa a certos aspectos legais dos serviços da sociedade de informação, em especial do comércio eletrônico, no mercado interno (conhecida como "Diretiva sobre comércio eletrônico")
42 Art. 7.1. "Além de outros requisitos de informação constantes da legislação comunitária, os Estados-Membros que permitam a comunicação comercial não solicitada por correio electrónico por parte de um prestador de serviços estabelecido no seu território assegurarão que essa comunicação comercial seja identificada como tal, de forma clara e inequívoca, a partir do momento em que é recebida pelo destinatário."

listas de *opt-out*[43], assim evitando o envio de mensagens às pessoas que inscreveram seus e-mails em tais listas. No entanto, alguns problemas minaram a eficácia destas medidas, entre eles o fato de que a técnica de *labelling* necessita de elevada harmonização entre todas as partes envolvidas para que possa ser minimamente efetiva - algo com o que a diretiva não se preocupou; além do que as próprias listas de *opt-out* não existiam à época e nem sequer foram implementadas posteriormente. Em relação ao *opt-in* a diretiva não o impôs nem o incentivou de modo especial, mantendo a política de deixá-lo como uma opção a ser considerada livremente por cada estado membro no seu direito interno.

A abordagem definitiva do problema do *spam* pelo direito comunitário veio à luz com a Diretiva sobre Privacidade nas Comunicações Eletrônicas, de 2002[44]. Esta diretiva foi preparada em um momento no qual os efeitos do *spam* já se faziam sentir com bastante nitidez e crescia a demanda por barreiras, inclusive de cunho legislativo[45]. Assim, foi este o primeiro instrumento legislativo que se ocupou diretamente deste problema no direito comunitário[46].

A técnica utilizada pela mencionada diretiva resume-se basicamente à adoção de um sistema de *opt-in*[47], conforme instituído pelo seu art. 13(1):

> *"A utilização de sistemas de chamada automatizados sem intervenção humana (aparelhos de chamada automáticos), de aparelhos de fax ou de*

43 "Art. 7.2. Sem prejuízo da Directiva 97/7/CE e da Directiva 97/66/CE, os Estados-Membros deverão tomar medidas que garantam que os prestadores de serviços que enviem comunicações comerciais não solicitadas por correio electrónico consultem regularmente e respeitem os registos de opção negativa ("opt-out") onde se podem inscrever as pessoas singulares que não desejem receber esse tipo de comunicações."

44 Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrônicas (Diretiva relativa à privacidade e às comunicações eletrônicas).

45 Note-se que, de toda sorte, o termo "*spam*" não está presente na normativa comunitária, que prefere utilizar um termo mais genérico como "comunicações eletrônicas não solicitadas". Uma conseqüência desta postura é a utilização da mesma técnica legislativa para outras formas de comunicação eletrônica como, por exemplo, as mensagens SMS (*Short Message Service*) enviadas através de telefones celulares.

46 Seu considerando (40) afirma que: "Devem ser previstas medidas de proteção dos assinantes contra a invasão da sua privacidade através de chamadas não solicitadas para fins de comercialização directa, em especial através de aparelhos de chamadas automáticas, aparelhos de fax e de correio electrônico, incluindo mensagens SMS (...)".

47 Ainda no texto do considerado (40), ressaltamos: "(...) No que diz respeito a essas formas de comunicações não solicitadas para fins de comercialização directa, justifica-se que se obtenha, antes de essas comunicações serem enviadas aos destinatários, o seu consentimento prévio e explícito. (...)".

*correio eletrônico para fins de comercialização direta apenas poderá ser autorizada em relação a assinantes que tenham dado o seu consentimento prévio".*

Entre as razões para a adoção do regime de *opt-in* estão o crescimento exponencial do volume de *spam* na União Européia que se verificou durante o período de maturação da proposta que resultou na diretiva em tela, bem como a avaliação de que era o sistema de *opt-in* que poderia proporcionar uma proteção mais eficaz contra o *spam*. Também foi levado em consideração que um sistema de *opt-in* poderia ser implementado com maior facilidade e a partir de um quadro normativo mais simples do que os de *opt-out*[48].

O sistema de *opt-in* da diretiva é temperado por exceções, que lhe valeram por parte da doutrina a denominação de sistema de "*opt-in* modificado" ou simplesmente "*soft opt-in*"[49]. A primeira exceção, prevista no art.13(2), prevê que quando o endereço de e-mail foi obtido no contexto da venda de produto ou serviço[50], o fornecedor poderá utilizar este endereço para o envio de mensagens proporcionais referentes a produtos ou serviços "análogos". Esta exceção vem acompanhada, nestes casos, da instituição de um regime de *opt-out*, na previsão de que uma pessoa deve dispor de meios fáceis e gratuitos para recuar o envio destas mensagens. A diretiva dispõe com clareza que ao consumidor deverá ser oferecida a opção do *opt-out*, seja no momento em que o seu endereço eletrônico for colhido, seja por ocasião de cada uma das mensagens que podem ser posteriormente enviadas caso o consumidor não tenha recusado o seu envio já de início.

A exceção do art. 13(2) legítima o interesse dos fornecedores em manter um contato de natureza pós-contratual para fins de marketing, presumindo interesse do

48 Um dos problemas freqüentemente relacionados à criação de uma lista de *opt-out* é o conjunto de dificuldades administrativas e técnicas para a criação e manutenção de uma verdadeira lista universal do gênero. A estes, somam-se também as questões de privacidade relacionadas à própria existência da lista e à divulgação de seus integrantes, bem como, e não de menos importância, a necessidade de vincular efetivamente os *spammers* a observar a referida lista. v. David Sorkin, "Tecnhical and legal approaches ...", cit., pp. 353-354; Nicola Lugarese. "European Union ...", cit., p. 47.

49 John Magee, "The law…" , cit., p. 371.

50 Como "contexto da venda" hão de ser compreendidas somente as hipóteses nas quais houve efetivamente a venda de um produto ou serviço, sem compreender eventuais relacionamentos de caráter pré-contratual que não se desenvolveram ao ponto da efetiva venda. John Magee, "The law ...", cit., p. 372.

consumidor em produtos ou serviços análogos. Na discussão que precedeu a diretiva, fortes críticas foram feitas à adoção do sistema do *opt-in*, sendo esta exceção uma das vias encontradas para a conciliação de interesses.

A segunda exceção é de ordem subjetiva e se encontra no art. 13(5), que prevê a proteção dos interesses legítimos das pessoas jurídicas. A distinção parece fundamentada pela *ratio* declarado da lei de proteger os interesses e a privacidade dos indivíduos, juntamente com a intenção de manter livre de qualquer amarra a comunicação *business to business*.

Esta distinção entre pessoas físicas e jurídicas, porém, pode gerar complicações. Nem sempre é simples distinguir, a partir de um endereço de e-mail, se este pertence a um indivíduo ou a uma pessoa jurídica, o que faz com que, em casos de dúvida, a opção recomendável seja tratá-lo como se fosse um e-mail individual. Um erro nesta avaliação pode tornar ilícito o e-mail enviado[51]. Além disto, tal distinção entre pessoa física e jurídica não auxilia uma desejada e simplificadora adoção de um regime único para todo o tráfego de e-mail, assim como dificulta a concretização de uma das finalidades da luta contra o *spam*, que é excluir da rede o tráfego ocioso e indesejado, reduzindo custos e aumentando a eficiência das comunicações eletrônicas.

A verificação do direito comunitário não pode prescindir do exame da sua incidência no âmbito dos ordenamentos nacionais, a partir da internalização das normativas comunitárias no espaço jurídico de cada estado. O direito comunitário, segundo autorizada doutrina, acaba se desdobrando em tantos direitos quantos sejam os países nos quais suas normas são aplicadas, proporcionando que não exista um sistema comunitário, porém tantos sistemas quanto resultem da integração das normas comunitárias com as de cada país[52]

51 Nicola Lugarese. "European Union ...", cit., p. 48

52 Pietro Perlingieri lembra que, além de uma normativa primária, que é o Tratado de Maastrich, existe uma normativa secundária que não se aplica autonomamente, porém em conjunto com o direito dos países membros. Pietro Perlingieri. "Normativa comunitaria e ordinamento interno", in: *I giuristi e l'Europa*. Luigi Moccia (org.). Laterza: Bari, 1997, p. 110.

A Itália foi um dos países que enfrentaram o problema do *spam* mesmo antes da Diretiva 2002/58/CE, tendo estabelecido regras bastante aproximadas ao que posteriormente veio a sedimentar-se com a internalização da norma comum européia, observando como base legal para tal construção a norma existente sobre proteção de dados pessoais.

Pode-se também ter uma idéia do perfil destas regras através da observação de alguns provimentos da Autoridade Garante para a Proteção de Dados Pessoais italiana. A coleta de endereços de e-mail disponibilizada em uma página na Internet foi reconhecida como inválida para fins de envio posterior de e-mails de conteúdo comercial ou publicitário[53]; da mesma maneira o envio de e-mails a endereços eletrônicos gerados de forma randômica por um programa de computador especialmente concebido para tal finalidade foi considerada ilícita[54]. Igualmente a partir desta normativa, foram tomadas medidas como o bloqueio de 11 operações de tratamentos de dados pessoais para fins de *spam*, determinado por via administrativa em 2001[55].

Posteriormente, a normativa comunitária sobre o tema foi transposta no ordenamento italiano pelo *Código em matéria de proteção de dados pessoais* (decreto legislativo n. 196, de 30 de junho de 2003)[56], que substituiu a lei anterior sobre proteção de dados[57] e incluiu a transposição da Diretiva 2002/58/CE.

---

53 Cf. provimento de 11 de janeiro de 2001, no qual se lê que: "A disponibilidade na *Internet* dos endereços de correio eletrônico publicados através de sites da *web* deve ser relacionada à finalidade para a qual tais endereços foram disponibilizados pelos sujeitos que administram os referidos sites. Os dados pessoais que são publicados relativamente aos eventos e finalidades desta forma determinados não são livremente utilizáveis para o envio generalizado de e-mails de conteúdo comercial e publicitário".

54 Provimento de 4 de julho de 2002.

55 Giovanni Buttarelli. "La atività del garante in materia di prevenzione dello *spam*", in: *La rete contro lo spam, che cos'è, come combatterlo*. Laura Abba e Giorgio Giunchi (coord.). Società Internet: Lucca, 2004, p. 26.

56 Conhecido também como *Codice in materia di protezione di dati personali.* Sobre a lei, v. Danilo Doneda. "Um Código para a proteção de dados pessoais na Itália", in: *Revista Trimestral de Direito Civil,* v. 16, 2003, pp. 78-99.

57 Lei n. 675, de 31 de dezembro de 1996, resultado da transposição para o ordenamento italiano da Direitiva sobre proteção de dados pessoais 95/46/EC.

A lei italiana mantém o teor da diretiva, com alterações pontuais (como a menção às mensagens do tipo SMS ou MMS[58]) e especificações na forma de tutela (como a possibilidade da Autoridade Garante de dados pessoais italiana prescrever aos provedores de serviços de comunicação eletrônica a filtragem ou outras medidas que possam impedir o envio de *spam* por parte de sujeitos que tenham violado reiteradamente a lei).

A atuação da Autoridade Garante italiana serve como uma boa ilustração do papel que instituições deste gênero vêm desempenhando no combate ao *spam* em vários países da União Européia. Podemos mencionar, ainda a partir da situação italiana, quais são as principais medidas que estas autoridades tomam para afrontar o problema: (i) o bloqueio e posterior interrupção, por via administrativa, do tratamento de dados pessoais para fins de *spam*; (ii) a definição de cláusulas contratuais comuns a contratos entre usuários, provedores de acesso e demais entes envolvidos, com o fim de vedar práticas que favoreçam o *spam*; (iii) a inclusão de práticas anti-*spam* nos códigos deontológicos redigidos em conjunto com associações de classe[59].

Em outros dos maiores países europeus, a solução observada não foi muito diferente. A França, por exemplo, estabeleceu em sua lei de 21 de junho de 2004[60] a proibição da utilização comercial do correio eletrônico "utilizando-se das coordenadas de uma pessoa física" caso esta pessoa física não exprima seu consentimento prévio para receber mensagens de tal natureza". Na Espanha, ainda em 2002, a Lei 34/2002 expressamente proibia o envio de "comunicações comerciais não autorizadas" por meios eletrônicos[61].

---

[58] *Multimedia Messaging System,* um padrão técnico para o intercâmbio de objetos multimídia através de telefones celulares.

[59] Giovanni Buttarelli. "La attività del garante ...", cit., pp. 26-27.

[60] Loi du 21 juin 2004 pour la confiance dans l'économie numérique (artigo L 34-5 do Código dos correios e telecomunicações).

[61] A Lei 34/2002, de 11 de julho (Lei de serviços da sociedade da informação e comércio eletrônico (LSSICE), prevê em seu art. 21: "*Prohibición de comunicaciones comerciales no solicitadas realizadas a través de correo electrónico o medios de comunicación electrónica equivalentes.*

Queda prohibido el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas."

### *3.2. O sistema norte-americano*

Os Estados Unidos acumulam o que é provavelmente a maior experiência judicial de qualquer país em matéria de *spam*[62], o que se justifica basicamente pela dimensão e importância que a Internet ali passou a apresentar, além de outros fatores como o fato do país possuir uma forte tradição de marketing direto, um tanto mais agressivo que em outros países.

São freqüentes no país as tentativas de resolução do problema através de métodos técnicos[63] e da auto-regulação[64] que, no entanto, não se demonstraram eficazes na sua tentativa de diminuir o volume de *spam*[65].

Em relação ao patamar legislativo, desde uma fase que poderíamos situar como anterior ao grande impacto proporcionado pela Internet nas comunicações eletrônicas, podem ser mencionadas algumas normas que interessam ao tema como a legislação federal existente desde 1991 sobre chamadas telefônicas e por fax comerciais com fins de marketing, o TCPA[66], além de importantes decisões sobre o envio de publicidade pelo correio[67].

---

[62] A primeira ação judicial relacionada a um caso de *spam* nos Estados Unidos data de 1995 (*Robert Arkow* v. *CompuServe*). Seu fundamento era a analogia entre o *spam* que recebia e a lei federal que proibia o envio não autorizado de fax (TPCA, *infra*). Este caso específico foi encerrado por uma composição entre as partes, sem que o mérito tivesse sido julgado. David Sorkin, "Technical and legal approaches ...", cit., pp. 357-358.

[63] Como medidas técnicas entendam-se todas aquelas que atuam diretamente no processamento e nas interfaces de comunicação dos e-mails, desde a mera eliminação manual do *spam* pelo usuário até os complexos mecanismos para sua avaliação e bloqueio, entre tantos outros.

[64] Diversos modelos de auto-regulação foram e são propostos nos Estados Unidos; muitos deles estão em vigor no presente momento. Entre os mais conhecidos, mencionamos a proibição dos membros da DMA (*Direct Marketing Association*), baseado em seu *Privacy Promise*, de enviar *spam* para os e-mails presentes no banco de dados compilado pela associação para este fim.

[65] A auto-regulação e as medidas técnicas inibitórias do *spam*, em extrema síntese, atingiram focos específicos do problema e fizeram com que o *spam* e os próprios *spammers* mudassem de perfil – mudando, por exemplo, as técnicas de envio ou a sua localização geográfica. Porém, até o momento, não se demonstraram capazes de debelar o problema.

66 *Telephone Consumer Protection Act*.

67 Entre as quais se destaca *Rowan v. United States Post Office Department*, 397 U.S. 728 (1970), decisão da Suprema Corte norte-americana que garantia ao destinatário o poder de solicitar a remoção de seus nomes dos cadastros de empresas que realizam marketing direto através do correio.

A jurisprudência norte-americana possui uma experiência bastante razoável em relação ao *spam*. As causas que ela habitualmente enfrenta são as ações de operadores de serviços de telecomunicações e provedores de Internet contra *spammers* pela utilização não autorizada de seus sistemas (através da *tort* de *trespass to chattels*)[68]; as ações contra operadores de *open relays*[69]; ações contra *spammers* que utilizam falsas identidades para obter acesso a sistemas ou para enviar mensagens não autorizadas e, finalmente, ações de provedores de acesso contra usuários que se utilizam de seus serviços para enviar *spam*[70].

Apesar da profusão de decisões e regras de natureza sempre um pouco restrita, compreendendo diversos aspectos do *spam*, começava a se fazer sentir a opinião de que a via legislativa seria a abordagem mais adequada para o tema, sob o argumento de que o combate ao *spam* é algo muito diverso de outros temas tratados anteriormente pela *common law*, a ponto de impossibilitar uma solução realmente eficiente para muitos de seus problemas, como por exemplo, a prova do dano[71].

O primeiro estado a promulgar uma lei contra *spam*[72] foi Nevada[73], imediatamente seguido pela Califórnia, Washington e Virginia[74], todos entre 1997 e 1998.

---

[68] A *tort of trespass to chattels* é um remédio judicial típico da *common law* para casos em que uma pessoa utiliza a propriedade privada de outra pessoa sem autorização. O ofensor é responsável pela deterioração do valor da referida propriedade ou pele fato da diminuição da sua utilidade para o proprietário por algum período de tempo. David Sorkin, "Technical and legal approaches ...", cit., pp. 359-360. A tese do *trespass to chattels* foi utilizada em tribunal, com sucesso, ainda em 1997, no caso *CompuServe* v. *Cyber Promotions* (962 F. Supp. 1015 S. D. Ohio 1997). Nele, o provedor de acesso *CompuServe* acusou a empresa *Cyber Promotions* de utilizar sua rede para enviar *spam* aos seus clientes, algo expressamente vetado nas suas políticas de uso da rede. Na fundamentação de sua sentença, o juiz reconheceu que os sinais eletrônicos gerados por computadores seriam, fisicamente, tangíveis o suficiente para fundamentar a referida ação de *trespass to chattels* .

[69] Os *open relays* são servidores de e-mail que permitem sua utilização indiscriminada por usuários da Internet; eles costumam ser utilizados com o fim de disseminar *spam* ao mesmo tempo que dificultam a localização de sua origem.

[70] David Sorkin, "Technical and legal approaches ...", cit., pp. 357-367.

71 John Magee, "The law…" , cit., pp. 355-356.

72 Coletâneas atualizadas das leis estaduais anti-*spam* podem ser consultadas em <www.*spam*laws.com> ou em <www.cauce.org/legislation>.

73 A lei de Nevada, posteriormente emendada, obriga a mensagem comercial a se identificar claramente como tal e a incluir endereço e nome verdadeiros do remetente, bem como meios para realizar o *opt-out*.

74 A legislação contra *spam* da Virgínia, após suas últimas modificações, é uma das mais agressivas de todo o país: entre previsões que visam a facilitar que *spammers* baseados em outros estados sejam processados segundo este estatuto, é de se destacar a pena de prisão de um a cinco anos para quem envie mais

Estas leis apresentam um conjunto de medidas bastante variadas para o combate ao *spam*, que assim podem ser sintetizadas basicamente: repressão à falsificação da identidade do remetente nos cabeçalhos do e-mail; requisição de uma indicação de que se trata de uma mensagem comercial no campo "Assunto:" do e-mail (a técnica do *labelling*); reconhecimento formal das políticas anti-*spam* dos provedores de acesso; na necessidade de previsão de um mecanismo de *opt-out* em todo e-mail comercial; previsão de ressarcimento por cada mensagem recebida caracterizada como *spam* em valores que variam entre 10 dólares e o infinito e até mesmo, no caso do estado de Delaware, na obrigatoriedade da pré-existência de um relacionamento comercial entre remetente e destinatário para legitimar o envio do e-mail - uma previsão que se aproxima bastante da política de *opt-in* tipicamente européia. Até o momento 38 estados norte-americanos possuem suas próprias leis sobre *spam*[75].

A edição de uma legislação federal sobre *spam* é defendida por muitos como um passo absolutamente necessário para enfrentar o problema do *spam*, visto que a co-existência de várias legislações estaduais, diversas e eventualmente antitéticas, reduz em muito o efetivo alcance deste conjunto normativo. O problema do *spam* sugere uma solução global e não localizada, conseqüentemente tanto mais parece necessário que o seu tratamento seja uniformizado dentro de um único país.

A edição desta legislação federal era dificultada, no entanto, por limitações de ordem constitucional, como a primeira emenda constitucional e a sua proteção ao chamado *commercial speech*, parte integrante do *free speech* da primeira emenda, referenciado por ampla jurisprudência que fundamenta a liberdade de expressão publicitária

---

de dez mil e-mails considerados como *spam* em um dia. O motivo desta particularidade pode ser o impacto econômico do *spam* na economia local, devido ao fato do maior provedor de acesso norte-americano (AOL) ter sede no estado e que cerca de 50% do tráfego da Internet nos Estados Unidos passe pela Virgínia. Reagan Smith. "Eliminating the *spam* from your Internet diet: The possible effects of the Unsolicited Commercial Electronic Mail Act of 2003", in: 35 *Texas Law* Review 411 (2004), p. 426.

[75] Remeta-se novamente à compilação atualizada das leis sobre *spam* realizada por David Sorkin em <www.*spam*laws.com>.

na previsão constitucional de proteção à liberdade de expressão[76]. Um outro inibidor é a chamada *commercial clause* constitucional que, por conta das tensões que cria entre as legislações estaduais sobre a matéria e qualquer tentativa de ação legislativa federal, acaba por dificultar a possibilidade do governo federal regular este setor bem como contribui para a fragmentação da legislação estadual a respeito.

Após uma série de ensaios para uma lei federal[77], foi finalmente aprovado em 2003 o *CAN-SPAM Act*[78]*,* normativa que prescreve um sistema de *opt-out* como padrão para o envio de mensagens comerciais não solicitadas, bem como fortalece o papel da *Federal Trade Commission* – FTC – como o ente com a função de combater o *spam* em um nível nacional.

O *CAN-SPAM Act* estabelece a necessidade do e-mail conter um endereço eletrônico válido ou outro mecanismo para que o destinatário possa solicitar não receber outras mensagens - um mecanismo de *opt-out*. Entre suas medidas de tutela, estão mecanismos de tutela inibitória, assim como ressarcitória (com penalidades para o *spammer* que o desrespeitar estipuladas em até U$ 250,00 por e-mail, até o limite de dois milhões de dólares).

A viabilidade de um sistema baseado no *opt-in* nos EUA é, em síntese, bastante questionável (i) pela dificuldade de implementação de uma legislação a seu respeito na estrutura federalista norte americana e (ii) pela já mencionada dificuldade de harmonizá-lo com a proteção constitucional ao chamado *commercial speech,* aliada a uma

---

[76] Determinados *spammers* chegaram inclusive a buscar na primeira emenda uma espécie de guarida que lhes permitisse exercer sua atividade sem que fossem impedidos pelos provedores de acesso, seja por meios contratuais ou técnicos. Elizabeth Alongi, "Has the U.S. canned *spam*?", in: 46 *Arizona Law Review* 263 (2004), p. 278.

[77] Apenas como ilustração podemos mencionar alguns títulos de leis propostas nesta matéria no mesmo ano de 2003: a *Criminal Spam Act*; *Wireless Telephone Spam Protection Act*; *REDUCE Spam Act*; *SPAM Act*; *RID Spam Act*; *Anti-Spam Act.*

78 O acrônimo se refere a *Controlling the Assault of Non-Sollicited Pornography and Marketing Act*, codificado como 15 U.S.C. §770, que se auto-define como "An Act to regulate interstate commerce by imposing limitations and penalties on the transmission of unsolicited commercial electronic mail via the Internet". Esta norma foi aprovada pelo senado em 25/11/2003, pelo Congresso em 8/12/2003, assinada pelo presidente em 16/12/2003 e entrou m vigor em 1º de janeiro de 2004.

alegada situação de desvantagem pela qual passariam empresas que não contam ainda com uma base de consumo já formada.

Destarte, a opção regulatória pelo *opt-out* obedeceu a vários juízos, inclusive os de viabilidade e oportunidade, dentro de um sistema jurídico específico. E, mesmo assim, não deixou de ser alvo de severas críticas, das quais algumas das mais veiculadas foram que: (i) mesmo de uma forma mais branda, o *CAN-SPAM Act* continuava regulando o discurso comercial – e, portanto, subsistiam seus conflitos potenciais com a primeira emenda; (ii) ele criava conflitos e mesmo ab-rogava diversas leis estaduais em matéria de *spam* que, não raro, eram mais severas que o próprio *CAN-SPAM Act*. Outras críticas genéricas também ecoaram, como a de que a lei surgiu antes que houvesse consenso para uma regulação federal, ou então as próprias críticas genéricas à eficácia de sistemas baseados no *opt-out*.

O perfil do sistema instituído pelo *CAN-SPAM Act* permite, conforme constatou um de seus críticos, um "tiro livre" em cada caixa postal norte-americana[79] e, ao legitimar esta prática, mantém inalterada a necessidade do recurso a meios técnicos para a filtragem e eliminação de e-mails indesejados porém lícitos e pouco contribuindo para minimizar estes custos.

Além da adoção do sistema de *opt-out,* o *CAN-SPAM Act* solicitou expressamente à *Federal Trade Commission* uma investigação sobre a viabilidade da criação de uma lista do gênero *Do-Not-Call List*[80], contendo os endereços eletrônicos de pessoas que, declaradamente, não desejassem receber mensagens comerciais não solicitadas nestes endereços. A FTC, após analisar a questão, declarou-se contrária à criação de uma

79 *CAUCE Statement on CAN-SPAM Act*, in: <www.cauce.org/news/ 2003.shtml>.

80 A *Do-Not-Call List*, que com efeito veio a ser posteriormente implementada, é uma lista mantida pela *Federal Trade Commission* para regular a utilização do marketing direto telefônico nos Estados Unidos. Os números telefônicos registrados nesta lista (que em novembro de 2005 chegavam a 109 milhões) não podem ser utilizados para fins de envio de mensagens publicitárias.

lista do gênero, ao menos até que fossem implementados meios capazes de autenticar com exatidão a origem do e-mail considerado como *spam*[81].

Em termos quantitativos, a eficácia da norma ainda está para ser demonstrada. De forma geral, ela serviu para definir e unificar o patamar legal do *spam* e estabelecer com clareza um patamar de legalidade: de acordo com a FTC, a totalidade das grandes empresas envolvidas no comércio eletrônico norte-americano opera de acordo com suas normas[82]. Por outro lado, a lei pouco modificou a situação referente ao *spam* proveniente de fora dos Estados Unidos nem, de forma geral, os grupos ou indivíduos que estariam, por diversos motivos, mais afastados do alcance da lei norte-americana.

Na tentativa de coibir o *spam* proveniente destas e de outras fontes pouco atingidas pelo *CAN-SPAM Act*, certas medidas foram tomadas. Algumas já estão presentes na própria normativa da qual tratamos, como a determinação para a FTC interagir e colaborar com entidades internacionais com a finalidade de definir estratégias e normativas contra a ação de *spammers*, fora e dentro dos Estados Unidos[83]. Outras dependem, além do necessário patamar legal, de uma ação positiva e bem planejada da própria FTC em identificar sujeitos-chave que são responsáveis pelo envio de *spam* em escala massificada e propor ações judiciais que sirvam como desestímulo a estes e aos demais grandes *spammers*.

Este modelo de combate ao *spam* implica em uma ação cada vez mais acentuada da FTC. Para favorecer esta ação, fornecendo à comissão as permissões e instrumentos mais adequados para tal fim, foi proposto o *U.S. Safe Web Act*, que sinteticamente proporciona à comissão poderes para aliar-se a entidades estrangeiras e realizar intercâmbio de informações para o combate ao *spam* para elevar o nível de

[81] Para chegar a este juízo, a FTC considerou basicamente as dificuldades técnicas devidas ao atual estado tecnológico da rede que tornam plenamente possível ao *spammer* dificultar, forjar ou mesmo impossibilitar a sua localização. Também foram levados em conta outros fatores, entre eles o risco à privacidade dos próprios integrantes da lista. Federal Trade Comissiom. *National do not email registry. A report to the Congress.* Washington: FTC, 2005.
[82] Federal Trade Commission, *Top etailer's compliance with CAN-SPAM's opt-out provisions.* Washington: FTC, 2005.
83 *CAN-SPAM Act*, §2 (12).

confidencialidade de suas próprias informações e aumentar a sua autoridade na área penal e sua possibilidade de atuar no exterior.

### *3.3. Algumas conclusões sobre os modelos estrangeiros*

Verificadas as linhas gerais das respostas européia e norte-americana ao problema do *spam*, é possível traçar algumas considerações gerais a respeito.

O enfoque europeu para o *spam* foi, desde seu início, limitado, tanto é que o debate acabou por se concentrar na adoção do *opt-in* ou do *opt-out*, sem que fossem consideradas com tanta ponderação outras opções e outras vias que não a legislativa. Por outro lado, as bases do estatuto jurídico do *spam* no ordenamento jurídico comunitário (e, portanto, nos diversos ordenamentos nacionais) estão mais solidamente fundadas, mesmo por estarem vinculados a uma experiência relacionada à proteção de dados pessoais que já é razoavelmente madura.

As alternativas para o combate ao *spam* parecem ter sido exploradas com maior avidez e criatividade nos Estados Unidos, o que pode ser demonstrado pela riqueza de abordagens e tentativas de enfrentar o problema, seja pela via legislativa ou não. Não hão de ser deixados de lado, porém, importantes fatores que impediram que, como um todo, a solução norte-americana viesse efetivamente a apresentar resultados mais interessantes do que a européia.

Um fator latente que inibe a adoção de medidas concretas sobre o *spam* pela via legislativa é o fato de que qualquer normativa que procure regulá-lo corre o risco de, ao vedar determinadas práticas e outras não, acabar por estabelecer um patamar de licitude para certo tipo de *spam* e, desta forma, legitimá-lo – com o risco de fomentar um enorme fluxo de *spam* "lícito", comprometendo ainda mais a confiabilidade e a gestão do tráfego na rede[84]. Neste ponto, pode-se dizer que o legislador europeu forneceu uma resposta mais

[84] É este o dilema típico de determinadas técnicas de regulação, como por exemplo a que se baseia na etiquetação da mensagem como comercial em seu assunto – a mencionada técnica do *labelling*.

firme, ao idealizar um sistema de *opt-in* com restrições limitadas e não extensíveis, muito embora isto não signifique necessariamente o sucesso do seu inteiro sistema.

O risco cada vez mais presente é que o e-mail, dentro de alguns anos, deixe de ser o meio de comunicação simples, eficiente e acessível que é hoje, caso a tendência ao seu crescimento exponencial não seja revertida. Neste intento, uma correta avaliação e integração no plano internacional de combate ao *spam* não é somente um auxílio precioso - é uma necessidade de primeira ordem.

**4. Análise do projeto de lei:**

O crescimento da utilização e aplicação comercial da Internet no Brasil, a partir do final dos anos de 1990, fez inundar com inúmeros projetos relacionados ao tratamento de mensagens eletrônicas não solicitadas às Casas Civis. Nesse sentido citamos passagem do parecer proferido pelo Deputado Nelson Proença ao projeto 2.186/2003:

> *As propostas ora submetidas ao exame desta douta Comissão referem-se a uma prática que se tornou generalizada na Internet. Empresas ou pessoas que têm algum produto ou serviço a oferecer encaminham mensagens eletrônicas de forma indiscriminada, sobrecarregando as caixas de entrada dos usuários da rede. O volume dessas mensagens não solicitadas representa, hoje, mais da metade do total do tráfego da rede.*

Entre os tantos projetos apresentados, e como mais abaixo serão concentrados esforços de análise, merecido destaque deve ser conferido ao projeto de Lei Substitutivo oferecido pelo mesmo Deputado Nelson Proença ao Projeto de Lei nº 2.186/2003 apresentado pelo Deputado Ronaldo Vasconcellos.

Três projetos encontram-se apensos ao Projeto nº 2.186/2003 e a seu substitutivo. São eles:

> *a) Projeto de Lei nº 2.423, de 2003, do Deputado CHICO DA PRINCESA, que autoriza o envio, por uma única vez, de mensagem eletrônica não solicitada e que tipifica o crime de enviar mensagem com arquivo ou comando destinado a inserir ou a capturar dados, código executável ou informação do destinatário, punível com reclusão de até quatro anos e multa.*
>
> *b) Projeto de Lei nº 3.731, de 2004, do Deputado TAKAYAMA, que admite o envio de "spam" por uma única vez e sujeita o infrator à detenção de seis meses a dois anos e multa de quinhentos reais por mensagem enviada.*

*c) Projeto de Lei nº 3.872, de 2004, do Deputado EDUARDO PAES, que admite o envio, por uma única vez, de mensagem não solicitada e sujeita o infrator à pena de multa de duzentos reais, bem como obriga o provedor de acesso a dispor de recurso para bloquear tais mensagens.*

Como mencionado, no início da presente exposição, focar-se-á no conteúdo proposto pelo 2.186/2003 e seu substitutivo.

O texto oferecido pelo então Deputado Ronaldo Vasconcellos dispõe sobre o envio de mensagem não solicitada por meio de redes de computadores destinadas ao uso do público. Desta forma, já explicita em sua proposta o conceito central base para discussão aqui desenvolvida.

Determina, desta forma, como conceito de *spam* a mensagem não solicitada por meio de redes de computadores destinadas ao uso do público, como pode ser auferido de seu artigo segundo:

> *Art. 2º Para os efeitos desta lei, considera-se mensagem não solicitada ("spam") qualquer mensagem eletrônica recebida por rede de computadores destinada ao uso do público, inclusive a Internet, sem consentimento prévio do destinatário.*

A previsão contida em seu artigo 3º apresenta quatro pressupostos que, quando atendidos em seu conjunto, tornariam permitida uma mensagem eletrônica não previamente solicitada.

Dessa forma, para que qualquer mensagem possa ser enviada sem o consentimento prévio, deverá obedecer aos seguintes quatro critérios:

(i) ser enviada **uma única vez**;

(ii) **conter** no campo do assunto, no cabeçalho e em seu primeiro parágrafo **identificação** clara que se trata de **mensagem não previamente solicitada**;

(iii) **conter identificação** do **remetente** válida e apta de ser confirmada e, por fim,

(iv) que, na mesma mensagem, exista um **procedimento simples** para que o usuário receptor da mensagem possa **optar por receber novas mensagens** daquela fonte.[85]

Mais três importantes pontos são abordados nos artigos 4º, 5º e 6º do projeto de Ronaldo Vasconcellos, quais sejam, a criminalização da prática de envio do que considera *spam*, a definição de infrações de natureza civil e, por fim, qual o papel a ser cumprido pelos provedores de serviços de acesso e correio eletrônico como sujeitos ativos e contribuidores do sistema de regulação proposto no projeto.

O citado artigo 4º determina que constituirá crime, punível com detenção de 06 (seis) meses a 01 (um) ano e multa de até R$ 500,00 (quinhentos reais) por mensagem enviada, a ação de utilizar, de forma não autorizada, endereços de terceiros para o envio de mensagens. Destaca-se, para fins de comentários posteriores, que o núcleo deste delito é **"utilizar endereços"**.[86]

O dispositivo seguinte, artigo 5º, traz em seu bojo a caracterização de outra forma de violação, dessa vez com natureza civil. Caracteriza como infração **o envio de mensagem não solicitada** e **sua reincidência**, sendo que para o primeiro envio será devida pena de multa de até R$ 200,00 (duzentos reais) por mensagem enviada, acrescida de um terço em caso de reincidência. Neste, existem dois núcleos caracterizadores de condutas infracionais: a ação de **"o envio de mensagem não solicitada"** e **"sua reincidência"**.

---

[85] *Art. 3º Será admitido o envio de mensagem não solicitada nas seguintes condições:*
*I – a mensagem poderá ser enviada uma única vez, sendo vedada a repetição, a qualquer título, sem o prévio consentimento pelo destinatário;*
*II – a mensagem deverá conter, no cabeçalho, no primeiro parágrafo e na identificação do assunto, identificação clara de que se trata de mensagem não solicitada;*
*III – o texto da mensagem conterá identificação válida e confirmável do remetente;*
*IV – será oferecido um procedimento simples para que o destinatário opte por receber outras mensagens da mesma origem ou de teor similar.*

[86] Art. 4º Constitui crime, punido com detenção de seis meses a dois anos e multa de até quinhentos reais por mensagem enviada, a utilização não autorizada de endereços de terceiros para o envio de mensagens.

O que chama atenção no citado artigo 5º, a seguir transcrito, em relação à caracterização da infração, é a não expressa exceção ao conteúdo do artigo 3º que permite, quando preenchidos determinados requisitos, o envio da primeira mensagem não solicitada.

> *Art. 5º As infrações no envio de mensagem não solicitada sujeitarão o infrator à pena de multa de até duzentos reais por mensagem enviada, acrescida de um terço na reincidência.*

Tal problemática, capaz de gerar confusão quando da interpretação e aplicação da letra da norma, poderia ser resolvida com a utilização do conceito completo apresentado no artigo 2º do projeto que agrega ao "não solicitado" a não existência de "consentimento prévio". Desta maneira, ajudaria a cristalizar, ao longo da lei, o entendimento do conceito de *spam*.

Por fim, o artigo 6º estabelece:

> *Art. 6º Os provedores de acesso a redes de computadores destinadas ao uso do público, inclusive a Internet,* ***manterão*** *cadastro com os dados dos titulares de endereços eletrônicos, sítios, contas de correio eletrônico ou quaisquer outros meios* ***por eles operados que possam*** *ser utilizados para o envio de mensagens não solicitadas.*
>
> *Parágrafo único.* ***Os dados*** *de que trata este artigo serão* ***preservados*** *por um período não inferior a* ***um ano****,* ***contado do encerramento*** *do sítio, endereço ou conta de correio eletrônico.*

Apresentado um panorama geral do referido projeto, seguem-se os comentários sobre cada um de seus pontos e a análise crítica relativa à alternativa apresentada pelo então projeto substitutivo do Deputado Nelson Proença.

Primeiramente, a abrangência proposta pela norma resultado do Projeto de Lei 2.186/2003 e prevista em seu artigo primeiro que determina que "Esta lei dispõe sobre as limitações ao envio de mensagem não solicitada ("spam") por meio de correio eletrônico, veiculado em redes de computadores destinadas ao uso do público, inclusive a Internet." Esse é um dos primeiros aspectos que despertam atenção e questionamento sobre

sua atualidade e suficiência, tendo em vista o atual estado da tecnologia disponível socialmente.

Referimo-nos a tecnologia móvel, a tecnologia de comunicação disponível para aparelhos celulares e similares.

Desta forma, não há mais como caracterizar a Internet como somente uma rede de computadores. Esse conceito foi ampliado a fim de determinar que a Internet seja uma rede de quaisquer dispositivos, como computadores, *palms* e celulares, entre outros, passíveis de utilização para comunicação. Nesse sentido, e para evitar que um dispositivo legal perca a sua efetividade frente ao avanço tecnológico, a proposta de anteprojeto de lei ao final sugerida optou por mencionar apenas "redes de comunição", não utilizando expressões atualmente populares como "redes de comuncação digital" ou mesmo o termo "Internet".

Ademais, há que se destacar que novos meios de comunicação, como os celulares mais modernos, possibilitam novos meios de se atingir a privacidade de um indivíduo por meio do envio de mensagens não solicitadas. Destacam-se, a título exemplificativo, serviços que oferecem dados de localização de pessoas, os chamados LBS (*Location Based Services*), para o envio de mensagens publicitárias por comerciantes e prestadores de serviço dos mais diversos tipos, ademais das próprias operadoras de celular. Os LBS já são comuns na Europa e Japão e já se encontram disponíveis no Brasil principalmente para fins coorporativos.

Citados serviços, baseados na capacidade de triangulação das torres de sinal de celulares, utilizam os dados de posição geográfica de determinado dispositivo móvel para serviços *business-to-consumer* e *business-to-business*, dos mais variados, como envio de publicidade relativa ao local (como por exemplo, ao entrar num shopping e receber uma mensagem com as promoções de suas lojas) ou que possam gerar interesse a um cliente com determinado perfil (como serviços de relacionamento pessoal que indicam que alguém com o perfil pelo usuário selecionado se aproxima), serviços de localização em viagem,

associação com serviços de GPS para controle de frotas, entre outros mais ou menos invasores de privacidade.

Destarte, tornam-se comuns mensagens como: "bem-vindo ao shopping 'tal', promoções nas lojas 'x', 'y' e 'z' esperam por você." ou "bem-vindo à cidade 'abc', chuvas são esperadas para esta tarde". Outros tipos de serviços que vem ganhando destaque são os serviços de alerta sobre localização de filhos para os pais mais preocupados.

Esclarece-se que citados serviços, agrupados baixo o chamado marketing móvel ou serviços corporativos, já se encontram operantes em diversas partes do mundo e tecnologicamente viáveis no Brasil, como acima citado, não são serviços baseados na comunicação via Internet (ou WAP – *Wireless Application Protocol* – a Internet do celular), mas sim serviços baseados em mensagens de texto, os SMS (*short message service*), ou mensagens multimídia, os MMS (*multimidia message service*) que utilizam outras linguagens e protocolos.

Acredita-se, assim, que temas como o acima apresentado devem ser retidos para consideração para determinar a adequada abrangência de uma norma como a que é proposta.

Ressalta-se, entretanto, que esse objetivo somente poderá ser atingido quando reste claro qual o bem jurídico que se pretende proteger. Ou seja, a **privacidade**, o **bem estar**, **bens de caráter material** como os próprios bens utilizados para a comunicação (a rede, o aparato, a caixa de e-mail) ou **outros** interesses que podem ser prejudicados indiretamente, como, por exemplo, no eventual caso de uma importante mensagem que deixa de ser recebida por falta de espaço ocasionada pelo excesso de spams recebidos.

Dessa forma, o primeiro passo para construir um instrumento jurídico adequado é determinar qual o bem e sua natureza a serem protegidos, para, num segundo momento, pensar em formas eficazes preventivas e repressivas de regular a ação considerada potencialmente lesiva.

Essa prévia definição do bem jurídico a ser tutelado determinará os alicerces para que se possam definir os conceitos aplicáveis e o quão flexíveis deverão ser para abranger novas práticas que possam surgir com o avanço tecnológico e capazes de atingir o mesmo bem jurídico foco de regulação.

Para que isso seja possível, entretanto, há que se apresentar o rigor técnico legislativo necessário e ser capaz de aplicar a hermenêutica jurídica na construção de uma nova legislação que tem como pretensão regular os efeitos do abuso da tecnologia.

Tendo em vista o acima exposto, acredita-se que tanto o projeto 2186/2003 como seu substitutivo que, apesar de deixar expresso a finalidade de "proteção ao usuário", não foram completamente capazes de tornar transparente o bem jurídico tutelado, correndo o risco de tornarem-se restritos a uma atividade herança de uma época especifica.

Dessa forma, em seu substitutivo, Nelson Proença determina como abrangência da norma em análise o que segue:

> *"Art. 1º Esta lei dispõe sobre a* ***proteção ao usuário*** *de redes de computadores destinadas ao público em geral, inclusive a Internet, em face do recebimento de* ***grandes volumes*** *de* ***mensagens não solicitadas*** *("spam")."*

Em relação à delimitação do conceito de spam, o projeto substitutivo, em seu artigo 2º [87], acabou por restringir ainda mais o conceito ao fazer uma simples alteração de localização da palavra "eletrônica".

Acredita-se que alguns pontos devem ser levados em consideração para um adequado desenho do conceito de spam como atividade potencialmente indesejada ou lesiva, quais sejam:

[87] Art. 2º Para os efeitos desta lei, considera-se mensagem eletrônica não solicitada qualquer mensagem recebida por rede de computador destinada ao uso do público, inclusive a Internet, sem consentimento prévio do destinatário.

- A clareza de finalidade da utilização de dados pessoais quando fornecidos pelos usuários futuros receptores a um organizador e detentor de banco de dados pessoais ou cadastros;
- Quantidade de e-mails enviados;
- A expressão da vontade dos receptores;
- O momento da expressão dessa vontade;
- A identificação das mensagens enviadas em relação a seu propósito;
- O conteúdo das mensagens enviadas e sua compatibilidade com os demais pontos;
- A existência e natureza da relação estabelecida previamente entre o remetente e o receptor;
- A forma de identificação do receptor;
- As formas para expressar a vontade de o receptor querer ou não receber mais mensagens;
- Os passos e atores envolvidos que tornam possível tal prática e os níveis e formas de sua responsabilização;
- A ação de organização e comercialização de cadastros de dados pessoais de usuários, potencialmente ofensiva, inclusive a direitos constitucionais e de consumidor.

Diferentemente do projeto do Deputado Ronaldo Vasconcellos, que se propõe, em seu artigo 3º, a estabelecer requisitos formais para que uma mensagem não se caracterize como *spam*, o artigo 3º do projeto do Deputado Nelson Proença preocupa-se com a forma de relação entre remetente e receptor ao determinar que:

> *Art. 3º O envio de grande volume de mensagens eletrônicas não solicitadas, nas condições e limites referidos na regulamentação desta lei, será admitido sempre que:*

*I – os destinatários tenham optado por receber mensagens comerciais; ou*

*II – haja relação comercial pré-existente entre o remetente e os destinatários.*

O artigo acima citado acaba por trazer ao corpo do projeto o debate sobre o melhor sistema para o regramento do envio de mensagens eletrônicas. Embora esses conceitos já tenham sido trabalhados na análise dos modelos estrangeiros, cumpre trazer à tona algumas definições que possibilitam a análise das propostas legislativas.

O primeiro dos sistemas em comento é o denominado *opt-in,* o qual é definido pela Cartilha de Segurança para Internet, elaborada pelo CERT – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, como sendo "regra de envio de mensagens que define que é proibido mandar e-mails comerciais/spam, a menos que exista uma concordância prévia por parte do destinatário."

Em oposição ao sistema opt-in, conforme já visto, existe o sistema opt-out que, no mesmo documento, é definido como "regra de envio de mensagens que define que é permitido mandar e-mails comerciais/spam, mas deve-se prover um mecanismo para que o destinatário possa parar de receber as mensagens."

Por fim, uma derivação do sistema opt-in, denominado "soft opt-in", é também bastante utilizado nas proposições legislativas, sendo o mesmo definido como "regra semelhante ao opt-in, mas nesse caso prevê uma exceção quando já existe uma relação comercial entre remetente e destinatário. Desta forma, não é necessária um permissão explícita por parte do destinatário para receber e-mails desse remetente."[88]

O texto do art. 3º do substitutivo apresentado pelo deputado Nelson Proença parece trabalhar com conceitos que o aproximam do sistema "*opt-in modificado*" ou "*soft opt-in*". Entretanto não estabelece, como foi a opção realizada no caso da União Européia, se as mensagens seguintes devem ser estritamente relacionadas a prestação de serviços ou

[88] Todas as definições foram extraídas de CERT. *Cartilha de Segurança para Internet*. Versão 3.0 (in http://cartilha.cert.br, acessado em 14.12.2006).

produto contratados, se relacionadas a análogos ou quaisquer outros serviços ou produtos das partes.

A opção de Nelson Proença é justificada na seguinte passagem de seu parecer:

> *Optamos, no texto, por limitar as restrições aos casos em que grandes volumes de mensagens não solicitadas, nos quais o remetente utiliza-se de um programa automático de expedição. Em tais casos, deve prevalecer o critério de limitar-se o envio a aqueles destinatários que optem por receber esse tipo de correspondência ("opt-in") ou que mantenham relação comercial com o remetente. Por se tratar de parâmetro variável, que depende do estado-da-arte das redes de computadores, deixou-se à regulamentação a tarefa de definir em que quantidades e condições caracteriza-se tal volume.*

O texto de Ronaldo Vasconcellos determina que a primeira mensagem deverá conter mecanismo para que o receptor expresse sua vontade em continuar recebendo e-mails da mesma origem ou teor semelhante. Entretanto abre uma brecha que pode gerar risco de tornar ineficiente a proposta de regulação, ao permitir o envio da primeira mensagem.

Chamamos atenção nesse ponto, pois hoje já se é sabido que os meios tecnológicos existentes possibilitam alteração de remetente por meio de atribuição de "máscaras" ou e-mails de envio rotativos, ademais de outros mecanismos que, ademais de contribuírem com a prática de ações fraudulentas, impedem a identificação do real remetente do e-mail.

Ademais, merece ser ressaltado que ambos os projetos acabaram por não prever mecanismos para que o destinatário manifeste a sua vontade de não mais receber as mensagens que, até então, se enquadravam na normatização, ao não determinar, em qualquer de seus dispositivos, a obrigação de apresentar ao receptor a opção de ser automática e definitivamente excluído de determinada lista de endereços eletrônicos ou banco de dados eletrônico utilizados para o envio daquelas mensagens.

Outro aspecto merecedor de destaque em relação ao comentário de Nelson Proença em relação à adoção do sistema "*opt-in*" acima transcrito diz respeito à questão da necessidade de regulamentação posterior de dois de seus aspectos: "*grande volume de mensagens"* e *"relação comercial pré-existente"*.

Primeiramente questiona-se a quem caberia essa regulamentação infralegal? Não é expressar como letra da lei um conceito de tamanha subjetividade que possa ter como conseqüência a inviabilizaçao de sua interpretação e aplicação? Nesse sentido, lembra-se o claro exemplo de dificuldade de interpretação do trecho "pequenos trechos" presente no artigo 46, inciso II, da Lei 9610/1998, a Lei de Direitos Autorias[89] e todos os resultados sociais daí advindos.

Ademais, *relação comercial pré-existente* não parece justificar todos e quaisquer envios de comunicações, mas somente aquelas relativas especificamente ao conteúdo daquela relação comercial e sua execução e concretização, se interpretada restritivamente.

Desta forma, haver-se-á que fazer uma opção sobre o conteúdo abrangido por citadas expressões.

Por fim, cabe mencionar, em relação ao artigo 3º, o Projeto de Lei nº 2.186/2003, que o Código de Defesa do Consumidor já prevê, em seu artigo 36[90] que a publicidade deve ser veiculada de tal forma que o consumidor, fácil e imediatamente identifique como tal. Desta forma, mesmo que se opte por uma legislação especifica, sua aplicação deverá ser realizada em conjunto com o código do consumidor, concluindo-se que toda a mensagem enviada com fins comerciais deverá identificar claramente seus fins.

---

[89] LDA - *Art. 46. Não constitui ofensa aos direitos autorais: (...) II - a reprodução, em um só exemplar de pequenos trechos, para uso privado do copista, desde que feita por este, sem intuito de lucro;*

[90] CDC – *Art. 36. A publicidade deve ser veiculada de tal forma que o consumidor, fácil e imediatamente, a identifique como tal. Parágrafo único. O fornecedor, na publicidade de seus produtos ou serviços, manterá, em seu poder, para informação dos legítimos interessados, os dados fáticos, técnicos e científicos que dão sustentação à mensagem.*

Em seguida, já em seu artigo 4º, o Projeto de Lei nº 2.186/2003, criminaliza a pratica de *spam* como acima citado. Em relação a tal opção, merece destaque o prudente comentário de Nelson Proença.

> *Há que se proceder, no entanto, com extremo cuidado no exame da matéria. Não cabe dúvida de que tal prática seja inconveniente. Também é inegável que representa um custo para a rede como um todo. Mas enquadrá-la como infração ou crime é um passo agigantado, que não guarda, a nosso ver, proporção com o desconforto provocado.*
>
> *Não compete ao relator desta Comissão discorrer sobre princípios de direito penal, sob pena de prejudicar o parecer ora proferido. Mas não se pode deixar de reconhecer que deve existir uma correlação entre a relevância atribuída a um bem jurídico e a punição aplicada a quem causar lesão a esse bem.*
>
> *A mensagem comercial não solicitada, embora esteja sendo usada abusivamente, não coloca em risco nosso sistema social e não implica na violação de qualquer direito fundamental do cidadão. Agregue-se que o "spam" que contenha apenas informações comerciais ou propaganda não compromete o ambiente virtual da rede de computadores em que trafega. Não vemos, portanto, razão para que o mero envio da mensagem seja tratado como infração.*
>
> *Entendemos, pois, que a proposição principal é demasiadamente rigorosa no tratamento da matéria. Vemos, ainda, como desnecessária a tipificação do crime de fazer-se passar por outrem ao enviar a mensagem, objeto do seu art. 4º. A prática caracteriza, de fato, crime de falsa identidade, já previsto no art. 307 do Código Penal, sendo este preferível.*

O posicionamento do Deputado Nelson Proença merece acolhida e aqui apresentar-se-á as bases jurídicas para tanto.

O poder punitivo do Estado, o *jus puniendi*, regulado pelo conjunto de normas que tipificam fatos e os atribuem penas, formando o Direito Penal, é limitado pelos princípios que regem esse ramo do Direito, que abaixo serão sucintamente comentados.

Por sua vez, a "pena criminal é a sanção imposta pelo Estado e consistente na perda ou restrição de bens jurídico do autor da infração, em retribuição a sua conduta e

para prevenir novos atos ilícitos"[91]. Seu fundamento jurídico é a culpabilidade do autor, sendo sua finalidade a prevenção e repressão de condutas ilícitas e culpáveis socialmente.

Para os fins do aqui tratado, em relação aos princípios que regem o *jus puniendi,* faz-se referência aos princípios da subsidiariedade, da fragmentariedade, da pessoalidade ou individualização[92] e, por fim, da proporcionalidade[93].

Os dois primeiros princípios vão determinar que o Direito Penal somente entre em ação, englobando em sua esfera de regulação determinadas condutas, como ultimo recurso – *ultima ratio*. Assim, somente com o esgotamento de outras esferas, como a administrativa e a civil, poderia o Direito Penal ser aplicado.

Ademais, a concretização da conduta de enviar mensagens não desejadas envolve uma cadeia de ações e atores, que, como muito se questiona nos crimes de natureza ambiental, contrariaria o princípio de pessoalidade e individualização da pena, dificultando a caracterização pessoal da conduta e o nexo causal.

Portanto, ao apresentar o substituto, bem fez o Deputado Nelson Proença em não acolher o artigo 4º, o Projeto de Lei nº 2.186/2003.

Sem embargo, acredita-se desnecessária a especificação da conduta proposta pelo Deputado Nelson Proença constante do artigo 5º do projeto substitutivo[94].

---

[91] Dotti, René Ariel. O Sistema Geral das Penas. P 66. in Penas Restritivas de Direito – Criticas e comentários às penas alternativas. São Paulo, 1999.

[92] Por esse princípio, a pena deve ser individualizada nos planos legislativo, judiciário e executório, evitando-se a padronização a sanção penal. Para cada crime tem-se uma pena que varia de acordo com a personalidade do agente, o meio de execução etc. Veja art. 5º, inc. XLVI, 1ª parte, da Constituição Federal.

[93] Segundo Aury Lopes o principio da proporcionalidade refere-se a uma ponderação que permita encontrar um equilíbrio entre o interesse punitivo estatal (jus puniendi) e o direito de liberdade (jus libertatis), dando-lhe efetividade, dessa forma, "deverá ponderar a gravidade da medida imposta com a finalidade pretendida, sem perder de vista o fumus commissi delicti e o periculum libertatis. Deverá valorar se esses elementos justificam a gravidade das conseqüências do ato e a estigmatização jurídica e social que irá sofrer o acusado. Jamais uma medida cautelar poderá se converter em uma pena antecipada, sob pena de flagrante violação à presunção de inocência." (Introdução Crítica ao Processo Penal. Rio de Janeiro: Lumen júris, 2004. p.200). Para um conceito mais abrangente de principio da proporcionalidade ver: Suzana de Todelo Barros - O Principio da proporcionalidade e o controle de constitucionalidade das leis restritivas de direitos fundamentais. 3 ed. Brasília: Brasília Jurídica, 2003, p. 214.

[94] Art. 5º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940, Código Penal, passa a vigorar com as seguintes modificações:

A presente crítica justifica-se pela existência e suficiência do artigo 307 do Código Penal ser amplo o suficiente para abarcar tal conduta, cabendo ao juiz interpretá-lo e aplicá-lo ao caso concreto.

O artigo 307 do Código Penal Brasileiro determina:

> *Art. 307. Atribuir-se ou atribuir a terceiro falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem.*
>
> *Pena – detenção, de três meses a um ano ou multa, se o fato não constituir elemento de crime mais grave.*

Desta forma, o que vai determinar a abrangência de aplicação do tipo previsto no artigo 307 é o preenchimento de significado do núcleo **"atribuir falsa identidade"**.

Utilizar-se, dolosamente, de nome, marca ou qualquer símbolo identificativo que não próprio, expresso por meio de, por exemplo, um documento, uma direção de correio eletrônico ou, mesmo, uma assinatura eletrônica são exemplos que podem configurar práticas que, *per se*, já poderiam ser encaixadas no tipo objetivo.

Isto por que para a consumação do crime de falsa identidade basta a simples ação de atribuição, independentemente de efetivo benefício ou dano, de identidade que não a sua.

Finalmente, ambos os projetos fazem referência aos provedores de serviços de Internet.

Antes de uma análise mais detida, é importante estabelecer alguns conceitos.

Os provedores de Internet podem ser classificados em três tipos fundamentais, os provedores de acesso, provedores de serviço e provedores de conteúdo.

---

"(...) Art. 307 (...) Parágrafo único. Incorre na mesma pena quem utilizar o endereço eletrônico de terceiro para o envio de mensagem eletrônica, ou reproduzir, em qualquer campo do cabeçalho ou do corpo de mensagem eletrônica, o nome, endereço eletrônico, marca ou logomarca de terceiro com a intenção de atribuir-lhe a autoria."

- O **provedor de acesso** é responsável pela conexão de um usuário à rede mundial de computadores;

- Os **provedores de serviços** desempenham atividades de diversas naturezas na Internet, podendo-se destacar o provimento de serviços de correio eletrônico, de hospedagem e de chave de busca;

- **Provedores de informações**, ou conteúdo, são todas as pessoas que disponibilizam informações na Internet através de uma página eletrônica.

Citadas definições importam para a delimitação de quais atribuições lhes poderiam ser imputadas e daí as responsabilidades advindas.

O Deputado Ronaldo Vasconcellos trata da questão no artigo 6º de seu projeto de lei nº 2.186/2003, determinando que:

> *Art. 6º Os provedores de acesso a redes de computadores destinadas ao uso do público, inclusive a Internet,* ***manterão cadastro com os dados dos titulares*** *de endereços eletrônicos, sítios, contas de correio eletrônico ou quaisquer outros meios por eles operados que possam ser* ***utilizados para o envio de mensagens não solicitadas.***
>
> *Parágrafo único. Os dados de que trata este artigo serão* ***preservados por um período não inferior a um ano, contado do encerramento*** *do sítio, endereço ou conta de correio eletrônico.*

Por sua vez, o Deputado Nelson Proença vai tratar a questão no artigo 4º de seu projeto substitutivo, estabelecendo que:

> *Art. 4º Os provedores de serviços de acesso a redes de computadores destinadas ao uso do público, inclusive a Internet, ou quaisquer entidades que ofereçam serviço de hospedagem de caixas de correio eletrônico ou similar,* ***ficam obrigados a****:*
>
> *I –* ***manter registro das transações de envio*** *de* ***grandes volumes*** *de mensagens eletrônicas;*
>
> *II –* ***manter e divulgar relação dos usuários atendidos que optarem por receber mensagens comerciais*** *("opt-in");*

> *III – **colocar gratuitamente à disposição** dos usuários atendidos programa de computador **destinado a bloquear e eliminar mensagens eletrônicas não solicitadas, bem como a combater vírus e demais códigos maliciosos** incorporados a tais mensagens.*

As propostas apresentam fortes diferenças de conteúdo, imposições de obrigações e resultados. Ambas, entretanto, demonstram mais uma vez uma realidade a qual todos estão submetidos atualmente: a crescente possibilidade de perda de controle das informações pessoais frente à capacidade crescente de coleta, armazenamento e processamento de dados.

Especificamente em relação à primeira, a do Deputado Ronaldo Vasconcellos, esta somente determinada que os provedores de acesso manterão o cadastro dos dados dos titulares e os preservarão por um período não inferior a um ano, contado do encerramento do contrato de prestação de serviços para acesso, hospedagem de site, registro de endereço e/ou serviço de correio eletrônico.

A finalidade de dispositivos dessa natureza é clara por relacionar-se com a construção da prova quando necessária à verificação da concretização de condutas reguladas pela proposição.

Entretanto, a interpretação desse dispositivo faz crer que dados de titulares são somente os dados de caráter pessoal que identificam as partes contratantes de um determinado serviço de comunicação, o que não parece ser suficiente se não preservadas as ações desenvolvidas ao longo da relação estabelecida.

O proposto pelo deputado Nelson Proença vai ao encontro dessa preocupação ao determinar que os provedores de serviços ficam obrigados a manter registro **das transações** de envio. Mas, ao qualificar o envio, determina que somente seriam abrangidos os **de grandes volumes** de mensagens eletrônicas.

Dessa forma, acredita-se peca ao acabar por desviar a proteção que deveria ser a fundamental, ou seja, a proteção do usuário de Internet e a segurança social na utilização da rede, visto que o potencial ofensivo de um e-mail não decorre do envio de grandes quantidades de e-mails, mas sim de seu conteúdo e recebimento indesejados.

Portanto, acredita-se que a especificação de envio de "grades volumes" não coincidente com o bem jurídico a ser protegido pela norma oferecida.

De qualquer forma, tendo em vista os custos envolvidos na preservação e manutenção desse tipo de registro, a limitação do registro a ações que envolvam grandes volumes de e-mails originados por um determinado remetente seria mais bem acolhida pelo mercado, pois os provedores poderiam descartar e-mails individuais ou pequenos grupos.

Entretanto, poderia gerar insegurança jurídica ao, como já anteriormente comentado, ser um conceito abstrato e subjetivo. Quando restaria configurado um "grande volume"?

Por sua vez, considera-se inconstitucional o inciso II do artigo 4º apresentado ao determinar a divulgação da relação de usuários atendidos que optarem por receber mensagens comerciais, ferindo o artigo 5º, inciso X e o inciso XII, da Constituição Federal. Visto que ambos dispositivos foram objeto de comentários anteriores, somente ressalta-se que o inciso X faz referência, especificamente, ao sigilo dos dados, enquanto que o inciso XII faz referência ao sigilo da comunicação de dados. Nesse sentido, Tercio Sampaio Ferraz Junior assevera:

> *"O sigilo, no inciso XII, está referido à comunicação, no interesse da defesa da privacidade. Isto é feito, no texto, em dois blocos: a Constituição fala em sigilo 'da correspondência e das comunicações telegráficas, de dados e das comunicações telefônica'. Note-se, para a caracterização dos blocos, que a conjunção e une correspondência com telegrafia, segue-se uma virgula e, depois, a conjunção de dados com comunicação telefônica. Há simetria nos dois blocos. Obviamente o que se regula é comunicação por correspondência e telegráfica, comunicação de dados e telefonia."*[95] *(grifo nosso)*

Ademais, uma previsão como esta constante no inciso II tampouco pode receber guarida quando analisamos o disposto no § 2º, do artigo 43[96], do Código de Defesa

[95] Tercio Sampaio Ferraz Junior. Sigilo de Dados: o direito à privacidade e os limites à função fiscalizadora do Estado. Cadernos de Direito Constitucional e Ciência Política. São Paulo, ano 1, p. 82, out-dez. 1992.

[96] CDC - *Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes. (...)*

do Consumidor, que determina que a abertura de cadastro, ficha, registro e dados pessoais e de consumo, deverá ser comunicada por escrito ao consumidor, quando não solicitada por eles.

Cabe, lembrar, por fim, que o Código Civil de 2002[97] realça o aspecto preventivo vinculado ao denominado caráter extrapatrimonial do direito à privacidade previsto constitucionalmente ao determinar, em seu artigo 12, que o titular do direito pode exigir que cesse a ameaça a direito de personalidade e, em seu artigo 21, complementar ao primeiro, ao prescrever que o juiz, a requerimento do interessado, adotara providencias necessárias para impedir ou fazer cessar ofensa ao direito.[98]

Por todo, acredita-se que, somente mediante ordem judicial, os registros deveriam ser abertos, nos termos já tratados no inicio do presente estudo.

Acredita-se, por fim, na grande dificuldade em execução do inciso III do proposto por Nelson Proença, visto que a constante evolução tecnológica faz com que mecanismos de proteção e combate a *spam*, vírus e códigos maliciosos como é o caso dos conhecidos cavalos de Tróia, o que sempre deixaria as empresas provedoras de Internet em estado de descumprimento da lei.

Adicionalmente, e retomando à problemática da responsabilidade dos provedores, em nenhum dos projetos apresentados faz-se menção aos contornos que essa poderia assumir ou, se fica excluída a responsabilidade do provedor por ações realizadas pelos meios que provê aos seus usuários. Ressalta-se tal problemática visto que a prescrição de muitas ações se dá em tempo maior ao previsto para a guarda das informações, como é o caso de 10 anos para ações contra danos morais. Há que se estabelecer alguns critérios de abrangência para se evitar uma tão grande disparidade jurisprudencial sobre

---

*§ 2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.*

[97] Lei 10406/2002 (NCC)

[98] NCC - *Art. 12. Pode-se exigir que cesse a ameaça, ou a lesão, a direito da personalidade, e reclamar perdas e danos, sem prejuízo de outras sanções previstas em lei. (...)*
*Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.*

responsabilidade de provedores, como a que observamos atualmente nos tribunais brasileiros.

Ainda em relação a essa temática, há que se deixar claro que os provedores, antes de revelar qualquer informação relativa à transação realizada pelos meios que provê, deve respeitar a privacidade de seus usuários e da correspondência, devendo observância aos art. 5º, inciso XII, da Constituição Federal; aos artigos 151 e 154 do Código Penal brasileiro[99] e aos estabelecido na Lei 9.262/96 sobre interceptação de comunicações, no que aplicável.

As ações dos provedores de serviços de Internet são reguladas por, ademais dos contratos firmados e legislação aplicável, pelo principio da boa-fé e da função social do contrato, devendo, ademais serem respeitados os direitos fundamentais previstos na Constituição. Ademais há que se questionar a eficácia e economia das medidas previstas para que a possibilidade de prestação de serviços de Internet não fique restrita às empresas com grande fôlego econômico. Havendo, ademais, que se optar por qual o tipo de responsabilidade assumirá o provedor de serviços de Internet. Obrigações de meio ou de resultado? E se isso vai depender da possibilidade e capacidade de intervenção do provedor nas atividades e ações executadas por seus usuários quando se utilizam dos serviços contratados do primeiro.

Por fim, ressalta-se que dois pontos considerados importantes acabaram por não constar em qualquer dos projetos ora em análise. Faz-se referência à limitação de propósito da mensagem a ser enviada e o tratamento de dados por prestadores de serviços, seja em território nacional ou estrangeiro.

---

[99] CPB - *Art. 151 - Devassar indevidamente o conteúdo de correspondência fechada, dirigida a outrem:*
*Pena - detenção, de 1 (um) a 6 (seis) meses, ou multa.*
*Art. 154 - 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 3 (três) meses a 1 (um) ano, ou multa.*

## 5. Proposta de anteprojeto sobre *spam*:

### EXPOSIÇÃO DE MOTIVOS

O envio indiscriminado de mensagens eletrônicas não solicitadas pelos seus destinatários se tornou uma constante na Internet mundial. A maioria das pesquisas indica que mais da metade dos e-mails que circulam atualmente na Internet configuram-se como "*spam*".

O recebimento de uma mensagem eletrônica não solicitada não representa apenas um mero aborrecimento para o seu destinatário. Apesar de muitas vezes o valor dano individual ser pequeno, considerado coletivamente, o problema do *spam* representa danos significativos para as redes de informação, empresas, provedores e também para usuários individuais. O caráter coletivo desse problema demanda uma solução jurídica que considere os efeitos difusos do *spam*.

Para alcançar essa finalidade foram adotados os seguintes pressupostos: (i) a adoção do sistema chamado "opt-in" como modelo para a qualificação das mensagens eletrônicas na Internet brasileira, conforme o exemplo adotado pela União Européia; (ii) a possibilidade de tutela coletiva de direitos para o combate ao *spam*, considerado o caráter difuso do dano provocado pelo mesmo; (iii) a explicitação de parâmetros para a aferição do dano por parte do juiz no âmbito da ação judicial relativa ao *spam*; e (iv) a extensão do crime de falsidade ideológica para abranger as mensagens enviadas através de redes digitais ou análogas com a finalidade de obter vantagem econômica ou causar dano.

O presente anteprojeto de lei tem como objetivo principal fornecer uma legislação que não legitime o *spam* como meio de comunicação de massa na Internet, independentemente de seu escopo ser comercial ou não.

A adoção do sistema *opt-in* no Brasil se justifica pela análise da experiência européia, em com comparação com o modelo de *opt-out* adotado pelos Estados Unidos. O

sistema *opt-out* legitima o envio da primeira mensagem ao destinatário, sendo posteriormente facultado ao mesmo solicitar a sua exclusão da lista de envio do remetente. Esse sistema não contribui de forma significativa para a redução do número de mensagens não solicitadas, além de abrir caminho para fraude e outros artifícios que reduzem a eficácia do modelo. Como exemplo, ao permitir o envio da primeira mensagem abre-se a possibilidade do remetente mudar freqüentemente o endereço eletrônico utilizado, tornando-se, na prática, um novo remetente e estando assim legitimado para o envio de nova mensagem.

Dessa forma, o anteprojeto aqui apresentado adota o sistema *opt-in* em detrimento do sistema *opt-out*, uma vez que o seu reconhecimento levaria à legitimação do *spam* como meio de comunicação, principalmente comercial. O anteprojeto também prima por sua neutralidade tecnológica, sendo aplicável para qualquer sistema de informação, como computadores, celulares e outras mídias para o relacionamento e comunicação pessoal. Sendo assim, o presente anteprojeto não permite, salvo as exceções mencionadas, o envio do primeiro e-mail como ferramenta de comunicação.

A introdução da tutela coletiva para o combate ao *spam* é aqui tratada como uma medida necessária para que se alcance resultados práticos no combate ao envio indevido de mensagens eletrônicas. A motivação de uma única vítima para a propositura da ação de reparação de danos é pequena, em vista de ser o dano pequeno em se considerado apenas uma vítima individual. A tutela do *spam* deve ser assim coletiva, inserida no âmbito da tutela dos direitos do consumidor. A redação do anteprojeto expressa, em seu artigo 6º, que se aplica ao envio indevido de mensagens eletrônicas o disposto no Código de Defesa do Consumidor sobre a tutela coletiva de direitos (artigos 81, III, e 82 da Lei 8.078, de 11 de setembro de 1990).

São legitimados assim para a propositura de ações contra o envio de *spam* as entidades de tutela coletiva de direitos. Essas entidades incluem o Ministério Público, a União, os Estados, os Municípios e o Distrito Federal, as entidades e órgãos da Administração Pública, direta ou indireta, e as associações legalmente constituídas há pelo

menos um ano e que incluam entre seus fins institucionais a defesa dos interesses e direitos protegidos pela presente lei.

O projeto mantém assim a coibição do *spam* no âmbito do direito civil, evitando a expansão do direito penal e a criminalização da atividade do *spam*. O projeto parte do princípio de que o direito penal deve ser utilizado como ferramenta regulatória apenas como *ultima ratio*, não devendo se aplicar ao *spam*. E, sobretudo, reconhece que o caminho da tutela coletiva de direitos no âmbito civil produzirá maior efetividade como ferramenta para se coibir o *spam* na prática do que sua criminalização.

O oferecimento de parâmetros para o julgador no caso concreto é outra inovação trazida pelo anteprojeto. Esses parâmetros atendem à demanda por balisamentos que possam auxiliar o juiz quando confrontado com situações técnicas e guiar a quantificação do valor indenizatório. Se um dos principais questionamentos hoje sobre responsabilidade civil é justamente como o juiz chega ao valor da indenização, a essa redação proposta assegura alguns fatores fundamentais que direcionam a atividade do julgador.

Conforme mencionado acima, o anteprojeto apresentado não se filia à corrente pela criminalização do envio indevido de mensagens eletrônicas. O artigo 8º do anteprojeto, no entanto, estende o dispositivo do Código Penal sobre falsidade ideológica àquelas mensagens que se valham desse expediente para obter vantagem ou causar dano. Isto se dá sem a necessidade de se alterar a redação do Código Penal, mas apenas expressando que o tipo penal também passa a abranger as mensagens enviadas em redes de comunicação digital ou análoga.

Dessa forma, procurou-se inovar no tratamento legislativo da importante matéria que é o envio indevido de mensagens eletrônicas sem a necessidade de se promover alterações na redação de outros dispositivos legais, mas inserindo o combate ao *spam* dentro do âmbito dos instrumentos legais da tutela coletiva, já existentes e bem sucedidos no Brasil.

**PROPOSTA DE REDAÇÃO DO ANTEPROJETO DE LEI**

*Dispõe sobre o envio indevido de mensagens eletrônicas (spam) em redes de comunicação.*

## .I.

## CARACTERIZAÇÃO E PROIBIÇÃO DO ENVIO INDEVIDO DE MENSAGENS ELETRÔNICAS:

**Art. 1º -** Considera-se indevido o envio de mensagens eletrônicas (*spam*) em redes de comunicação quando, independentemente de sua finalidade, seja realizado de forma massificada, com conteúdo uniforme ou praticamente uniforme, não tendo sido solicitado previamente por seu destinatário.

**Parágrafo primeiro.** É permitido, contudo, o envio de mensagem eletrônica em redes de comunicação quando houver contato social ou relação comercial prévia entre remetente e destinatário, observado que a mensagem deve estar relacionada estritamente com o contato social ou a relação comercial mantida.

**Art. 2º -** As mensagens eletrônicas enviadas em redes de comunicação devem prezar pela facilidade de identificação do remetente e respeitar a vontade de seus destinatários em recusar o recebimento futuro de tais mensagens, observada a proibição do art. 1°.

**Art. 3º -** Os princípios da boa-fé e da proteção dos dados pessoais devem informar toda relação comercial mantida através do envio de mensagens eletrônicas em redes de comunicação.

**Art. 4º -** É vedada a utilização, especialmente a cessão, comercial ou gratuita, de endereços eletrônicos de terceiros sem a prévia e expressa autorização de seu titular.

## .II.

**RESPONSABILIZAÇÃO E PENALIDADES PELO ENVIO INDEVIDO DE MENSAGENS ELETRÔNICAS:**

**Art. 5º -** A defesa dos interesses e direitos das vítimas do envio indevido de mensagens eletrônicas poderá ser exercida em juízo individualmente ou a título coletivo.

**Art. 6º** - Aplica-se ao envio indevido de mensagens eletrônicas a tutela coletiva de direitos, conforme disposto nos artigos 81, III, e 82 da Lei 8.078, de 11 de setembro de 1990.

**Art. 7º -** Para a quantificação da indenização correspondente aos danos causados pelo envio indevido de mensagens eletrônicas, o juiz deverá apreciar, especialmente, os seguintes critérios:

I. os prejuízos causados ao funcionamento das redes de comunicação;

II. a quantidade de mensagens enviadas em discordância com o previsto nesta lei;

III. a reincidência do agente do dano na prática de condutas previstas nesta lei;

IV. a finalidade que se buscou alcançar com o envio indevido das referidas mensagens; e

V. a extensão do dano experimentado pela vítima individualmente considerada; e

VI. o valor do benefício auferido através do envio indevido de mensagens.

**Art. 8º -** Aplica-se à atribuição de falsa identidade através do envio de mensagens eletrônicas, para a obtenção de vantagem, em proveito próprio ou alheio, ou para causar dano a outrem, o disposto no art. 307 do Decreto-Lei nº 2848, de 07 de dezembro de 1940.

**Art. 9º** - Esta Lei entra em vigor na data de sua publicação.