ESCOLA DA MAGISTRATURA DO ESTADO DO RIO DE JANEIRO

RESPONSABILIDADE CIVIL DOS PROVEDORES DE INTERNET PELA PRÁTICA DE *"SPAM"*

Adriana Maria Canuto Costa e Silva

Rio de Janeiro
2018

ADRIANA MARIA CANUTO COSTA E SILVA

RESPONSABILIDADE CIVIL DOS PROVEDORES DE INTERNET PELA PRÁTICA DE *SPAM*

Artigo científico apresentado como exigência de conclusão do Curso de Pós-Graduação *Lato Sensu* em Direito do Consumidor e Responsabilidade Civil da Escola de Magistratura do Estado do Rio de Janeiro.
Professores Orientadores:
Nelson C. Tavares Junior
Lucas Tramontano de Macedo

Rio de Janeiro
2018

RESPONSABILIDADE CIVIL DOS PROVEDORES DE INTERNET PELA PRÁTICA DE *SPAM*

Adriana Maria Canuto Costa e Silva

Graduada em Direito pela faculdade de Direito Universidade Presidente Antônio Carlos/ UNIPAC. Advogada.

Resumo – o reconhecimento geral de que o enorme desenvolvimento das tecnologias da informação nas últimas décadas alterou significativamente o comportamento e o hábito dos indivíduos, sem, contudo, que seus dados pessoais tenham vindo a receber, na mesma proporção, a devida proteção, como um corolário do direito da personalidade. O envio avassalador de *spams* aos usuários da rede mundial dos computadores – da qual o homem moderno hoje é praticamente dependente – visando ao lucro das empresas e a um aumento exagerado do consumo, vem causando aos consumidores danos de toda natureza. Minimamente, pela violação dos direitos informacional, à privacidade e à intimidade, em flagrante desrespeito à hipervulnerabilidade de muitos usuários, diante do desconhecimento da utilização de seus dados e, principalmente, da impossibilidade de coibir tal prática, à mingua da tutela efetiva do especial direito ao prévio consentimento pelo sistema jurídico brasileiro.

Palavras-chaves – Responsabilidade Civil. Provedores de Internet. Marco Civil da Internet.

Sumário – Introdução. 1. Marco Civil da Internet e direito fundamental à proteção de dados pessoais e à privacidade digital. 2. Comércio eletrônico no Brasil e na União Europeia e a violação ao consentimento livre, expresso e informado ao direito do consumidor. 3. Responsabilidade Civil e o envio de *SPAM* e mensagens de conteúdo ofensivo e/ou que caracterizam excesso de consumo. Conclusão. Referências.

INTRODUÇÃO

O presente estudo científico tem por escopo analisar a Responsabilização Civil dos Provedores de Internet diante da crescente utilização dos dados pessoais que hoje em dia alteraram, significativamente, as relações entre cidadão, Estado e mercado de molde a exigir a adaptação a diversas estruturas, entre elas a jurídica. Com efeito, é imprescindível alicerçar as novas formulações institucionais em uma sólida base jurídica e cultural, em reconhecimento do caráter fundamental do direito à privacidade e à proteção de dados e em contraposição às diversas dimensões da liberdade contemporânea, tão dependentes, hoje, da tecnologia.

O tema exige reflexão, tendo em vista que não há decisões judiciais suficientes a respeito, bem como a ausência de regulamentação específica no ordenamento jurídico pátrio, vindo, tão somente, em 2014, a Lei nº 12.965/14 – o Marco Civil da Internet, disciplinar a espécie, e que não coíbe, expressamente, a prática abusiva do envio excessivo de mensagens

indesejadas e/ou de conteúdo propagandístico, sob o entendimento doutrinário ainda de até mesmo não haver o direito, pelos usuários, à propriedade de seus dados pessoais.

Sob essa ótica, justamente em razão da ausência de instrumento eficaz para regular as relações jurídicas daí decorrentes, o envio, pelos Provedores de Internet, de *spams* invade avassaladoramente a liberdade individual e a proteção das informações pessoais. Nesse aspecto, há flagrante violação à norma protetiva do consumidor, bem como a direito erigido ao *status* de direito fundamental. Nesse aspecto, busca-se em tal estudo estabelecer um confrontamento e traçar um paralelo entre tais direitos, no intuito de se consolidar tal prática como abusiva, dentre as elencadas no CDC, a merecerem o repúdio e a reparação pelos danos causados, em nosso ordenamento jurídico, ainda que no sentido punitivo-pedagógico por violação ao direito da personalidade do qual a proteção de dados faz parte.

Assim é que, no primeiro capítulo iremos tratar, a partir dessa vivência institucional relativa à proteção da privacidade, sobre a possibilidade de se falar em um direito fundamental à proteção de dados pessoais no Brasil, seus limites e perspectivas para o exercício do consentimento, com vistas a fortalecer a proteção da personalidade do indivíduo nas relações de consumo ante o avanço tecnológico e contra os riscos ocasionados pela coleta, processamento e circulação de dados pessoais de molde a enquadrar a violação de dados como ofensa à direito fundamental e tal prática ser acrescida ao rol (meramente exemplificativo) do artigo 39 e incisos do CDC.

Pretende-se ainda discorrer acerca da vulnerabilidade do usuário-consumidor no que tange à captura de seus dados e perfis vinculados a um *spam* por meio de uso de suas senhas, perfis e dados privados, sem o seu livre e prévio consentimento, bem ainda na prática abusiva que acaba por culminar em um consumo excessivo e por vezes não desejado.

Segue-se, ponderando, no segundo capítulo, sobre a violação ao dever informacional, que tem sido observado pelo STJ e reconhecido pelo CDC como uma quarta modalidade de vulnerabilidade, ocorrendo em especial nas novas tecnologias e no comércio eletrônico – onde o uso da informática e a possibilidade de controle unificado das diversas atividades da pessoa humana, nas múltiplas situações de vida, permite o conhecimento de sua conduta pública e privada, nos mínimos detalhes, podendo chegar à devassa de atos pessoais, invadindo área que deveria ficar restrita à sua intimidade. O cidadão objeto dessa indiscriminada colheita de informações, muitas vezes, sequer sabe da existência de tal atividade, ou não dispõe de eficazes meios para conhecer o seu resultado, ratificá-lo ou cancelá-lo. Abordaremos, a esse respeito, o que estabelecem as diretivas europeias em defesa da proteção individual.

Por fim, no terceiro capítulo discorreremos sobre as consequências, sob outro enfoque, do prévio oferecimento, pelos Provedores, de pastas e ferramentas específicas baseadas em históricos de "*blacklist*" que permitem bloquear e direcionar e-mails de cunho ofensivo/propagandístico e de seus anexos, podendo-se ao revés, quando direcionados pelos *spamers* ao "lixo virtual", noutro passo, levar até mesmo à perda de uma oportunidade, informação ou um negócio jurídico desejado, e porque não dizer, à perda de uma chance.

Nesse sentido, propõe-se a pesquisa à Responsabilização Civil do Provedor de Internet, até mesmo por danos inclusive extrapatrimoniais decorrentes de tais práticas abusivas (a serem assim consideradas) e flagrante ofensa à direito da personalidade (da privacidade de seus dados) sob um ponto de vista da dogmática jurídica, levando-se em conta o Direito Comparado –modelos *opt in* e *opt ou* – e a Constituição Brasileira, que assegura a inviolabilidade da intimidade e da vida privada, bens do indivíduo tutelados contra os riscos advindos do processamento daqueles, objeto de nosso estudo.

1. O ENVIO EXCESSIVO DE MENSAGENS PELOS PROVEDORES DE INTERNET E A PROTEÇÃO DE DADOS DOS USUÁRIOS SOB A ÓTICA DE UM DIREITO FUNDAMENTAL CONSTITUCIONAL

Primeiramente, cumpre ressaltar que o tema proposto no presente estudo cuida da proteção de dados do indivíduo no que tange ao processamento ou a utilização de informações relacionadas a uma pessoa, "que a identificam e a caracterizam", e não por si só, à tutela, dentre outros direitos, quais o acesso à informação, à inviolabilidade, à intimidade e da vida privada, assim como o sigilo das comunicações de dados, telegráficas e telefônicas como direitos fundamentais elencados no artigo 5º incisos X e XII, respectivamente, da CRFB/88[1], de uma forma geral.

É indiscutível que com o avanço tecnológico e a concorrência empresarial, a infraestrutura de comunicação e da informação nos dias de hoje tornou-se indispensável para o exercício dos direitos fundamentais: a internet revolucionou a liberdade de expressão, a comunicação interpessoal e a comunicação social, assim como os sistemas informáticos transformaram o mundo do trabalho, da administração e do mercado, sem os quais se torna

[1] "Art. 5º, inc X: são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente da sua violação; Inc.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;" Retirado de: BRASIL, Constituição da República Federativa do Brasil. Disponível em: <http//www.planalto.gov.br>. Acesso em: 21 jun. de 2018.

impensável atualmente o livre exercício de qualquer trabalho, ofício ou profissão, tal como a livre expressão da atividade intelectual, artística, científica e de comunicação.

Todavia, em que pese o fato de que as garantias de sigilo e de inviolabilidade da intimidade e da vida privada configurarem mecanismos de proteção individual constitucional, certo é que eles se mostram insuficientes para lidar com os atuais efeitos do processamento e da utilização da informação sobre o indivíduo. Isto é, não abarcam a totalidade dos riscos aos quais o indivíduo está submetido na sociedade de informação.

Isso porque quando analisamos o âmbito de proteção de tais garantias constitucionais de sigilo, privacidade e intimidade, percebemos que ele se dá em um "âmbito específico de proteção", ou seja, das informações íntimas ou das comunicações, "diferentemente das informações que identificam uma pessoa". O que implica dizer que os dados e informações pessoais não são reconhecidos como "objeto imediato" de proteção constitucional, sendo despiciendo falar que o seu processamento e a sua utilização indevida venham acarretar a violação a inúmeros direitos fundamentais.

Assim é que, ao meu sentir, para manter a atualidade da proteção constitucional em face dos novos desafios sociais e tecnológicos, mister se faz interpretar a Constituição de modo a extrair uma garantia geral de proteção da informação pessoal, que complementaria o atual sistema de garantias específicas de sigilo e da intimidade e da vida privada. Somente o reconhecimento de um direito fundamental à "proteção de dados pessoais" poderia fazer jus aos atuais riscos aos quais os indivíduos se submetem, quando na qualidade de consumidores no uso das redes sociais e poderoso canal de comunicação e troca de informações – a Internet. Na interpretação corrente, "os dados não são objeto de proteção" da Constituição, mas somente a "comunicação de dados", nos moldes do inciso XII do seu artigo 5º, outrora citado, que assegura o sigilo da comunicação de dados, "mas não dos dados em si mesmos".

Logo, em ausência de norma protetiva específica, apesar de que muito em boa hora o Marco Civil da Internet tenha vindo estabelecer princípios, garantias e direitos e deveres para o uso da Internet no Brasil – eis que cada vez mais são crescentes as vantagens da facilidade e rapidez com o incremento da tecnologia, em especial o seu uso no comércio eletrônico – a proteção dos dados e informações que se referem a uma pessoa não foi tutelada de maneira efetiva. Sim, porque a responsabilização civil dos provedores por danos decorrentes de conteúdo gerado por terceiros dar-se-á somente após ordem judicial específica, para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível

o conteúdo apontado como infringente, a teor do artigo 19 da Lei nº 12.965/2014[2] – dispositivo cuja inconstitucionalidade vem sendo arguida perante a Corte Constitucional, o egrégio STF[3].

Assim, necessário se faz que a teoria do direito se reconstrua e se reinterprete a ponto de compreender e solucionar os problemas enfrentados pelo homem na era da informação quanto à violação e transmissão dos dados individuais, a exigir uma posição mais sólida de nossos Tribunais Superiores, bem como legislativa regulamentadora eficaz, ante a carência de efetividade da lei que disciplina a espécie.

Esse, pois, é o presente desafio, sobretudo no que tange aos Provedores de Internet e sua Responsabilidade Civil pela coleta de dados pessoais, muitas vezes à margem de qualquer conhecimento prévio do consumidor ou de instrumento capaz de impedi-lo, e como forma de gerar, consequentemente, um consumo excessivo e indesejado pelos indivíduos, e em especial por meio do envio de mensagens de cunho propagandístico – pelos conhecidamente *spamers.* Muitos consumidores desconhecem seu direito informacional nesse sentido, não tendo a Lei nº 12.965/2014[4] se harmonizado em favor de efetiva tutela desse direito, como mecanismo jurídico necessário e eficaz para o estabelecimento de um equilíbrio entre as relações de consumo e a proteção constitucional.

Objetiva-se, portanto, dar efetividade ao que assegura o Marco Civil da Internet, em especial seu artigo 10[5] e seguintes, relativamente ao respeito aos dados e sua confidencialidade, a fim de que essa prática venha a ser tutelada à luz da ordem constitucional e abarcada como conduta abusiva pela Lei nº 8.078/90 – pode-se afirmar que no tange aos direitos do consumidor a norma brasileira é das mais amplas e consistentes entre vários países –, nas quais enquadrar-se-ia a prática do não-consentimento livre e expresso da divulgação de dados da pessoa humana coletados pelas redes de comunicação e os Provedores de Internet.

Nesse diapasão, entende-se que é possível, a partir de uma interpretação sistemática da Constituição, fundamentar uma garantia geral de proteção de dados pessoais no sistema de direitos fundamentais, com o intuito de fortalecer a proteção da personalidade do indivíduo (aqui compreendidos o seu direito à privacidade e à intimidade), mormente diante do avanço

[2] Idem. *Lei nº 12.965*, de 23 de abril de 2014. Disponível em <http//www.planalto.gov.br>. Acesso em: 21 jun. 2018.
[3] Idem. Supremo Tribunal Federal.
[4] Idem. op. cit., nota 2.
[5] "Art.10: A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas." Ibidem.

tecnológico em face dos riscos ocasionados pela obtenção, processamento e circulação de seus dados e as novas formas de poder daí decorrentes, violando o direito informacional e o prévio, livre e expresso consentimento, assegurados efetivamente em outros países, principalmente da União Europeia.

Cabe ilustrar que a informação é sempre o resultado de uma ação interpretativa e depende do contexto em que surge, esclarecendo, nesse sentido, que "dados são símbolos ou sinais formais, que existem independentemente de interpretação e são armazenados em um suporte material[6]". A sua relevância jurídica reside no fato de que os dados são bases potenciais de informação por serem elementos formais e que podem ser facilmente armazenados e processados, razão pela qual revelam um alto valor informativo. Um dado pode ser qualificado como pessoal quando informações pessoais puderem ser extraídas a partir dele[7]".

Dessarte, podemos inferir que ainda que se diga que os dados pessoais não se enquadrem no inciso XII do artigo 5º da CRFB/88, anteriormente citado; eles se inserem, inequivocamente, no âmbito de proteção do direito à inviolabilidade da intimidade e da vida privada, tutelado pelo inciso X e interpretado de forma sistemática com o princípio da dignidade humana, atribuindo-se-lhe, consequentemente, o caráter de um direito fundamental, corolário dos direitos da personalidade.

Com efeito, nem se diga da vulnerabilidade do consumidor quanto ao uso de seus dados pessoais, indiscriminadamente – como sói acontecer por meio dos provedores de busca e de conteúdo da Internet, ávidos por tais informações –, tendo em vista que na grande maioria das vezes não lhe é assegurado tampouco o dever de informação, expressamente, como veremos adiante, em países da União Europeia, assim como meios de coibir ou suprir a ausência do livre e prévio consentimento do uso de seus dados pessoais em banco de dados, que constituem um risco constante e diário para todos os cidadãos.

Logo, isso vem a culminar, sem margem à dúvida, na enxurrada de e-mails indesejados, chamados de "lixo virtual" ou "pragas digitais" enviados aos usuários da rede mundial de computadores e violando sua privacidade e, porque não dizer, a sua liberdade de escolha. Ousa-se dizer que muitas vezes o consumidor se sente atraído pelo mercado eletrônico que lhe é posto à disposição de tal forma que acaba por consumir involuntária ou impulsivamente.

---

[6] VESTING, apud MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor, L*inhas gerais de um novo direito fundamental. São Paulo: Ed. Saraiva, 2014, p. 32

[7] BACKER, apud MENDES, op.cit., p. 32

Dito isso, dúvida não há de que a partir do art. 5º, inciso X da CRFB que garante a inviolabilidade da intimidade e da vida privada, é possível extrair a necessidade de uma tutela ampla da personalidade e da vida privada do cidadão nas mais diversas situações de risco a que se sujeita pela vasta e indistinta constelação de redes de processamentos de seus dados privados, oriundos de seus perfis, constantes de seus hábitos e preferências pessoais especificas com o fim de fidelização, compartilhamento e de comercialização – seja sob a ótica da tutela protetiva consumerista e levando-se em consideração a vulnerabilidade informacional reconhecida pelo egrégio Superior Tribunal de Justiça, seja à luz da proteção de sua integridade moral e a reparabilidade integral do dano, garantidas pela Constituição Brasileira e pelo Código de Proteção e Defesa do Consumidor[8], respectivamente.

Assim, a partir das experiências demonstradas e a vivência institucional relacionada à proteção de dados no Brasil, analisaremos no próximo capítulo como se dá a obtenção dos perfis dos usuários e a prática comercial exagerada oriunda dessa captação abusiva e até mesmo de modo ofensivo/lesivo e indesejado ou de conteúdo propagandístico pelos Provedores de Internet e os *spamers* dentro das relações de consumo, traçando-se um paralelo entre a norma legal e constitucional e as diretivas europeias de proteção individual a esse respeito.

2. A CAPTAÇÃO, PROCESSAMENTO E TRANSMISSÃO DE DADOS PESSOAIS DOS CONSUMIDORES VISTA PELO ORDENAMENTO JURÍDICO PÁTRIO E O DIREITO COMPARADO

Como visto, a comunicação de dados pessoais dos consumidores usuários da Internet, nessa qualidade, carece ainda de uma proteção legislativa mais específica no ordenamento jurídico pátrio, no sentido de lhes assegurar o direito à prévia informação de que seus perfis estarão sendo coletados e poderão vir a ser (como hodiernamente o são) objeto de um mercado publicitário, na maioria das vezes indesejado, pelos *spamers*, ou seja, o consumidor deve ser previamente avisado de que seus dados serão processados e compartilhados com uma vasta constelação de marketing direto e excessivo.

Considerado um fenômeno jurídico-naturalístico, o *spam* tecnicamente até então, era conceituado como “o envio não solicitado de e-mail com conteúdo comercial enviado para um

[8] BRASIL, *Lei nº 8.078*, de 11 de setembro de 1990. Disponível em: <http//www.planalto.gov.br>. Acesso em: 21 de junho de 2018.

grande número de pessoas[9]", ou seja, todo o correio eletrônico enviado de forma não autorizada a um usuário e cujo objetivo seja o oferecimento de produtos e/ou serviços. Contudo, modernamente, há que se entender que o *spam* hoje não está mais limitado apenas ao envio de e-mails de conteúdo comercial, devendo ser incluídas outras formas de envio como os *blogs*[10], sítios de relacionamento e mensagens *SMS* e até *Bluetooth*.

Com efeito, pode-se dizer que as principais fontes de dados dos consumidores são as transações comerciais, pesquisas de mercado e de estilo de vida, sorteios e concursos, censos e registros públicos, tecnologias de controle na Internet, entre outras.

Isso demonstra, induvidosamente, o fato de que o consumidor hoje é alvo fácil dessa prática abusiva que pode possuir, inclusive, conteúdo de cunho discriminatório, quando o tratamento dos dados é realizado de forma equivocada – como por exemplo, selecionando determinado nicho de consumidor – levando-se em conta sua condição financeira, econômica-social e até mesmo tendo em conta o grau de escolaridade, a cor, raça ou opção religiosa e sexual, acarretando sua "classificação" de forma a afetar o acesso a bens, serviços ou oportunidades sociais.

Sim, porque baseado nos perfis dos usuários, capturados por terceiros – pelas empresas, na busca de informações pessoais e com fim de se lhes diminuírem os riscos – ao examinar o tratamento de dados pessoais, no âmbito das relações de consumo e as demais informações extraídas a partir deles, constituem-se em uma representação virtual da pessoa perante a sociedade, ampliando ou reduzindo suas oportunidades no mercado, conforme sua utilização.

Daí infere-se que os dados de transações comerciais podem ser obtidos no momento da realização de uma compra ou de um serviço, quando da efetivação do cadastro do usuário, e consequentemente, de um registro e no qual é comum constar não somente os dados pessoais relativos àquela transação, mas também seus hábitos de consumo, entre outros, assim como a partir de cartões de fidelização, que possibilitam às empresas conhecer os dados comportamentais dos usuários da rede de Internet e, assim, classifique-os, podendo os consumidores passarem a receber ofertas e promoções de seu interesse (ou não).

---

[9] "*Spam* é o termo usado para referir-se aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas. Quando o conteúdo é exclusivamente comercial, esse tipo de mensagem é chamada de UCE (do inglês *Unsolicited Commercial E-mail*)". NÚCELO DE INFORMAÇÃO E COORDENAÇÃO – NIC.BR. *O que é spam?*. Disponível em < http//www.antispam.br/conceito/>. Acesso em: 30 jan. 2007.

[10] *Blog* é a contração de *web log*, ou diário da web, numa tradução literal. O *blog* é um *site* que surgiu com formato de um diário, em que o usuário tem a liberdade de inserir textos, fotos, vídeos e sons. In CAPANEMA, Walter Aranha, *O Spam e as Pragas Digitais*, Uma visão Jurídico-Tecnológica. São Paulo: Ed.LTr, 2009, p. 21

Vale dizer que "a *Amex*, por exemplo, que é uma empresa americana que oferece serviços financeiros e de viagens (*travelers cheques*) em todo o mundo, possui mais de trinta e quatro milhões de nomes no seu cadastro de consumidores internacional, no qual estão registrados dados sobre o que os seus clientes compram, para onde viajam e onde comem[11]".

As consequências, contudo, dessa classificação pelas empresas dos perfis dos consumidores podem ser indesejáveis, notadamente quanto à classificação pelo endereço, frequência e até mesmo data e horário em que os usuários utilizam-se do serviço, ou pelo valor monetário (*recenty, frequency and monetary value* – RFMV), ensejando, por exemplo, a possibilidade de exclusão daqueles de menor capacidade financeira. Assim, uma vez que não se sabe quais informações fornecidas pelos usuários estão sendo capturadas, bem como o momento em que as tecnologias de controle (*cookies*[12] e *spywares*[13]) estão a restringir a liberdade do consumidor, é essencial o prévio consentimento do processamento de seus dados para que o mesmo possa ser legítimo.

Analise-se, pois, a tutela desse direito no âmbito das diretivas europeias, nesse sentido.

É inequívoco, portanto, que para que a utilização de dados pessoais na Internet e/ou seu compartilhamento sejam válidos, necessário se faz que o seja autorizado pelo seu titular, salvo expressa previsão legal, constante da lei de acesso às informações (ou no caso em que a transação econômica assim o requeira, para sua efetivação), sob pena de violar-se o princípio da finalidade.

Assim é igualmente o previsto na Lei Federal de Proteção de Dados Alemã[14] (§4º, 1 do BDSG), devendo esse consentimento ser expresso, livre, específico e informado. "Isso implica a necessidade de que a declaração de vontade seja manifesta e clara, não podendo ser oculta, subentendida ou implícita. Dessa forma, compreendemos que, em regra, somente o modelo de consentimento *opt in* confere validade ao consentimento e torna legítimo o tratamento de dados[15]".

---

[11] GANDY, Oscar, apud MENDES, op. cit., p. 97.

[12] Os *cookies* são marcadores digitais que são automaticamente inseridos por *websites* visitados, nos discos rígidos do computador do consumidor, em sua casa ou no seu local de trabalho, para possibilitar a sua identificação e a memorização de todos os seus movimentos. In: BELLEIL, Arnaud, *@privacidade*, *O mercado de dados pessoais*: proteção da vida privada na idade da Internet. Trad. Paula Rocha Vidaline. Lisboa: Instituto Piager, 2002, p.65.

[13]Tipo de *software* que tem o objetivo de monitorar atividades de um sistema e enviar as informações coletadas para terceiros, podendo comprometer a privacidade do usuário e a segurança do computador. Algumas de suas funções são, por exemplo, o monitoramento de URLs acessadas enquanto o usuário navega na Internet e captura de senhas bancárias e números de cartões de crédito. Ibidem, p.68.

[14] BDSG, §4º, (1)

[15] BUCHNER, apud MENDES, op.cit., p. 205.

Noutro passo, “entende-se que caixas previamente assinaladas em uma página na internet, configurações de *browser* que são instaladas por *default*, ou cláusulas de autorização em contratos de adesão sem o devido destaque não constituem um consentimento válido. Já uma assinatura adicional em um contrato acerca da autorização do processamento de dados pode ser considerada uma manifestação de vontade clara[16]”.

Como destacado no parecer do “Grupo de Trabalho do art. 29[17]”, “o consentimento válido pressupõe uma manifestação de vontade, isto é, uma indicação, uma ação no sentido de consentir, o que dificilmente poderia ser pressuposto de uma inação ou da ausência de comportamento[18].

“O modelo *opt out* não se coaduna, a princípio, com o requisito do “consentimento expresso” e pode ser considerado legítimo apenas em casos excepcionais, quando o tratamento de dados não acarretar riscos à personalidade do consumidor e se o sistema de *opt out* disponibilizado for realmente efetivo para a proteção da personalidade do consumidor. Além disso, para que o sistema *opt out* seja considerado legítimo, ele precisa se fundar numa relação entre empresa e cliente já existente, a partir da qual o consumidor já tenha fornecido, voluntariamente os seus dados e pode ter a expectativa de receber, eventualmente, ofertas publicitárias dessa empresa[19]”.

Uma breve análise comparativa é capaz de demonstrar como esse direito já foi reconhecido, de diferente formas, pelas jurisdições constitucionais de outros países: Na Alemanha, o direito à autodeterminação informativa foi extraído pela Corte Constitucional alemã a partir do direito ao livre desenvolvimento da personalidade (art. 2.1 da Lei Fundamental) no clássico julgamento da Lei do Censo de 1983 (BVerGE 65,1, “*Volkszählung”).* Em Portugal, a Constituição regulamenta expressamente, em seu art. 35, relativo à “Utilização da Informática”, as condições de processamento e utilização de dados pessoais. Já a Constituição espanhola traz, em seu art. 18, a limitação do uso da informática para o pleno exercício dos seus direitos e, por fim, a Carta de Direitos Fundamentais da União Europeia prevê, em seu art. 8º, de forma bastante detalhada, a proteção de dados pessoais como um direito fundamental e prescreve a necessidade do consentimento ou outro fundamento legal

[16] Ibidem, p. 205-205

[17] O Grupo de Trabalho foi estabelecido com base no art. 29 da Diretiva 95/46/EC e consiste num órgão europeu de aconselhamento sobre os assuntos relativos à privacidade e à proteção de dados pessoais.

[18] Opinião 15/2011 sobre a definição de consentimento do Grupo de Trabalho do art. 29, p.11. Disponível em: <http//ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2011_ en.htm>. Acesso em. 21 jun. 2018.

[19] Ver art. 13 da Diretiva 2002/58/EG, com a modificação efetuada pela Diretiva 2009/136/EG, que prevê para comunicações eletrônicas não solicitadas o sistema *opt in* como regra, permitindo o modelo *opt out* em casos excepcionais.

para o tratamento dos dados pessoais, bem como a necessidade de uma autoridade de supervisão para exercer o controle dessa atividade.

Com efeito, diante do ora exposto, à saciedade, contrariamente ao sistema europeu, a inocuidade da norma legislativa brasileira no que tange ao envio de *spams,* bem como a pouca insurgência de vozes na doutrina em defesa desse tema e à míngua de entendimento jurisprudencial a respeito de forma suficiente a coibir essa prática pelos *spamers* no ordenamento jurídico pátrio, é que uma avalanche de mensagens, cotidianamente, tornou-se uma febre na rede mundial de computadores, por meio de MSN – *Messenger* –, sítios de relacionamento e *blogs*, tendo em vista o fato de que essas páginas permitem a inserção de comentários acerca dos textos publicados, utilizando-se assim, o espaço para a divulgação de produtos e serviços não solicitados, levando-se a um consumismo excessivo e indesejado.

Diferentemente – vale reafirmar – se diz quanto ao fato de as empresas que divulgam e enviam aos seus usuários e-mails para fins de marketing direto aos seus próprios clientes desde que disponibilize um meio eficiente, único, e "sem qualquer ônus" no caso de recusa do recebimento de tais e-mails, o que definitivamente não funciona, na prática, no Brasil.

Além disso, vale ressaltar que "surgiram nos últimos tempos as mais lesivas formas de *spams*. Seriam aqueles que, anexados à mensagem, trazem um *link* para o usuário obter um programa, ou ainda, fornecem em anexo ao e-mail tal *software*, cujo objetivo é diverso, como o de apagar os dados do computador da vítima: utilizar seu computador como instrumento de prática de crimes; ou apropriar-se dos seus dados pessoais para a obtenção de valores depositados em contas bancárias[20] (entre outras fraudes).

Tal prática, no mundo tecnológico, recebe a denominação de *phishing scam*, e se traduz numa forma de "pescar" os dados pessoais de um usuário de computador através da sugestão de o *download* e a execução de um programa de computador que se aproprie de tais dados[21]".

Posto isso, lamentavelmente, em que pesem as inúmeras possibilidades, segundo, inclusive, entendimento jurisprudencial no sentido de que tais mensagens possam vir a ser "deletadas" pelos usuário, não há que se negar o imenso transtorno que essa comercialização dos dados dos usuários venha acarretar, inclusive, danos de ordem extrapatrimonial – ainda que não se tenha no ordenamento jurídico pátrio um posicionamento firmado a respeito.

---

[20] CAPANEMA, Walter Aranha, *O Spam e as Pragas Digitais*, Uma Visão Jurídico-Tecnológica. São Paulo: Ed. LTr, 2009, p. 21.
[21] Ibidem, p. 22.

Ao meu ver, não se trata de mero aborrecimento causado ao consumidor que assim não o deseja – e, por vezes, é levado a um consumismo absurdo atraído pelas facilidades e ofertas publicitárias tentadoras que invadem seus computadores – e que é capaz até de ocasionar o superendividamento do indivíduo, tema esse já enfrentado por boa parte da doutrina e por renomados autores consumeristas.

Isso sem se levar em conta o desrespeito pelo mercado eletrônico diante da ausência de mecanismo obrigatório a fim de evitar tal prática lesiva, que, ainda que assim o fosse, repise-se, o consumo exacerbado pelos usuários hipervulneráveis suplanta, em muito qualquer sanção pecuniária, resultando na inocuidade da norma, haja vista o vultoso ganho das empresas de *marketing* de massa com essas mensagens publicitárias.

Logo, ainda que o usuário das redes possa se valer dos mecanismos para "deletarem" tais mensagens, é inegável o transtorno causado pelos *spams*, que transborda, em muito, a seara do mero aborrecimento, correspondentes a praticamente 90% de todo o tráfego de mensagens eletrônicas e ocasionando um verdadeiro "engarrafamento de dados", cujos efeitos são caixas de e-mails lotadas, mensagens perdidas, tempo despendido em apagá-las. Essa prática hoje poder-se-ia ser abarcada pela Teoria do Desvio Produtivo, que, em que pese a sua inovação no ordenamento jurídico, é reconhecidamente adotada pelo Tribunal de Justiça de São Paulo e a propósito, bem condizente e adequada ao tema em comento, diante da perda de tempo pelos consumidores e prejuízos sofridos advindos da circulação de seus dados de molde até mesmo a lhe trazer danos extrapatrimoniais, cujo tema será tratado no capítulo seguinte.

3. A NECESSIDADE DA PROTEÇÃO DOS DADOS PESSOAIS NO SISTEMA JURÍDICO BRASILEIRO E DO RECONHECIMENTO DA RESPONSABILIDADE CIVIL OBJETIVA DOS PROVEDORES DE INTERNET

Como vimos nos capítulos anteriores, a vulnerabilidade do consumidor no processo de coleta de seus dados pelos Provedores de Internet é tão patente que anteriormente se cunhou a expressão "consumidor de vidro"[22] para denotar a sua extrema fragilidade e exposição no mercado de consumo, diante de inúmeras burocracias privadas que tomam decisões e influenciam as suas oportunidades, a partir das informações pessoais armazenadas em bancos de dados.

[22] LACE, apud MENDES, op. cit., p. 93
.

Pode-se concluir que os riscos a que os usuários estão sujeitos consistem tanto na diminuição do consumidor como no risco de ser discriminado no mercado de consumo, uma vez que a vigilância de todos os seus comportamentos, pelas empresas, enseja a perda de controle sobre suas informações que circulam na sociedade, já que o consumidor não consegue determinar quais informações sobre si são conhecidas e que podem ser utilizadas na tomada de decisões que influenciem a sua vida.

Ou seja, ele terá sua capacidade de autodeterminação reduzida. Assim é que pode estar "sujeito ao risco de ser discriminado no mercado de consumo, caso lhe venha a ser negado acesso a bens e serviços ou tenha suas oportunidades diminuídas, em razão de informações armazenadas em banco de dados e que sejam utilizadas de forma discriminatória[23]".

Tanto assim o é que a partir da associação entre as tecnologias da informação e o armazenamento de enorme quantidade de dados pessoais, formas de discriminação, como por exemplo, a estatística, venham a ocorrer e segundo a qual grupos de consumidores recebem tratamentos diferenciados – preços ou condições de contratação diferentes – em razão de atributos aparentemente inofensivos, como dito anteriormente, a saber: idade, gênero, nacionalidade ou endereço e condição financeira. Tal prática baseia-se em informações que associam esses atributos a outras características, cuja identificação pelo fornecedor seja mais difícil como o nível de renda, risco de inadimplência, etc.

Vale lembrar ainda que o armazenamento dos dados pessoais uma vez capturados pelas empresas os sujeitam à disponibilização por lapso de tempo indeterminado, não havendo como saber por quanto tempo dar-se-á tal armazenamento e, assim, não possuem os consumidores nenhum controle dos mesmos quanto ao prazo e à probabilidade de futuros danos à sua personalidade, haja vista que que não há uma limitação temporal, gerando, assim, uma insegurança jurídica.

Assim, desde mensagens contendo fornecimento ou promoção de produto ou serviço aos seus destinatários, bem como as que oferecem um negócio ou uma oportunidade, cujos dados foram coletados pelos Provedores de Internet, fato é que os mesmos se perpetuam, vinculando o consumidor, e seu banco de dados circula facilmente na rede mundial de computadores.

[23] A respeito da relação entre proteção de dados, discriminação estatística e direitos fundamentais, ver de forma pioneira BRITZ, Gabrielle, apud MENDES, op. cit., p. 92

Cumpre ressaltar que, sob uma outra ótica, de acordo com a *Abrahosting* (Associação Brasileira das Empresas de Infraestrutura e Hospedagem na Internet)[24] o fenômeno é preocupante principalmente por acarretar maiores riscos de segurança e mais custos improdutivos de manutenção e ampliação da infraestrutura de serviços dessas empresas, detectando-se um crescimento espantoso do tráfego de *spam*, que triplicou em um período de dois anos no Brasil. De acordo com a entidade, concluiu-se que a taxa atual de *spam* no fluxo de mensagens que chegam diariamente nas redes dos seus associados atinge a média de 90% dos e-mails, os quais são prontamente bloqueados antes mesmo de chegarem aos níveis internos da estrutura.

Além disso, dos 10% de mensagens que recebem licença para entrar nos servidores das empresas de *hosting* do país, apenas 50% (ou 5% do total) são entregues ao endereço do usuário final com *status* de mensagem lícita. Os outros 5%, por sua vez, mesmo sendo encaminhados ao destino, recebem do Provedor, uma espécie de "carimbo" de suspeição e, quase sempre, acabam caindo na caixa de "lixo eletrônico" do usuário.

De acordo com Vicente Neto[25], presidente da *Abrahosting*: "a taxa de mensagens bloqueadas por serem identificadas como *spam* ainda é superior em provedores de hospedagem que atuam em nichos de mercado corporativos e oferecem serviços". Assim é que, em outra perspectiva, uma mensagem ou até mesmo uma oportunidade esperada pode ser reconhecida como *spam* e direcionada à "lixeira", podendo levar o consumidor à perda da celebração de um contrato ou de um negócio jurídico desejado, ou até mesmo de uma oportunidade de trabalho.

Sim, porque no levantamento da *Abrahosting*, pode-se citar a *Locaweb* que diariamente bloqueia cerca de 320 milhões de mensagens, e, "enquanto não houver uma diretiva internacional para coibir a banalização de registros (muitos deles anônimos ou sem uma personalidade jurídica comprovada) não haverá contenção do *spam*", conforme comenta o presidente da *Abrahosting*. Ou seja, é necessário formalizar uma autorregulação que seja implementada por todos os prestadores de *hosting* e que seja observada em comum acordo com os emissores de e-mail de marketing.

Na avaliação de muitos Provedores, as autoridades brasileiras de registro de domínio deveriam também repensar o nível de liberalidade para a criação de endereços IP que, muitas

[24]BRASIL, *Spam atinge até 97% dos e-mails no Brasil*, Disponível em: <http//www.convergenciadigital.com.br/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=44909&sid=4. Acesso em: 04 jun. 2018.
[25] Idem. op. cit., nota 24.

vezes, são feitos a partir de informação fraudulenta e/ou pouco consistente, como já dito em capítulos anteriores.

Daí porque uma enorme avalanche de *spams* e as consequentes medidas de segurança a que os Provedores se obrigam, acabam por ocasionar, por outro lado, certos efeitos indesejáveis. Um deles é o bloqueio acidental de remetentes lícitos de e-mail cujas características confundem os bloqueadores das empresas que acabam por classifica-los como *spam*.

Dessa forma, mensagens por vezes desejadas ou legitimamente esperadas podem ser objeto de *blacklists*, que são as listas com aquelas que mais praticam *spam*. Contudo, alguns remetentes legítimos acabam por "cair nessas listas" por erros básicos, e os usuários podem ser enormemente prejudicados com a perda de uma mensagem deletada, cujo conteúdo venha a ser de seu interesse e que, em virtude de tal fato, pode ser induzido tratar-se de *spam*.

Enfim, o *spam* é um problema mundial, que atinge graves proporções e que deve ser visto pelo mundo jurídico como um tema relevante tendo em vista o acúmulo de mensagens enviados pelos *spamers*, responsáveis pela maioria do tráfego na Internet e acarretando prejuízos aos Provedores e usuários, que vão desde o desnecessário tempo por parte do destinatário de tais e-mails em apagar as mensagens não solicitadas, bem como o esgotamento da caixa postal ou limite de recebimento dessas pelo usuário, provocando o não recebimento de mensagens por vezes desejadas. Isso sem falar no fato de que pode ocorrer, inevitavelmente, situações em que um menor de idade, usuário de serviço de Internet como e-mails ou *blogs*, por exemplo, receba mensagens de conteúdo inadequado, incentivando a lascívia e o acesso a tais sítios.

E por fim, pode haver a destruição de mensagens importantes, tendo em vista que o ato de triagem de mensagem pode se dar pela utilização de um programa *anti-spam* que classifica a mensagem com base em banco de dados, como já dito anteriormente, inseridas pelos usuário, e de forma manual em que o destinatário apaga o *spam* por si mesmo, mediante uma seleção das quais assim se lhe pareçam.

Dito isso, inegavelmente, o envio de mensagem eletrônica publicitária não solicitada, o excesso de e-mails de conteúdo comercial/ofensivo, sobretudo, sem o consentimento de seu usuário, configura, inexoravelmente, conduta abusiva à luz do CDC, bem ainda o processamento e a circulação de dados pessoais generalizado de modo a acarretar riscos à personalidade dos indivíduos e à proteção de sua privacidade. Isso somado ao abuso das empresas em relação à utilização dos mesmos ou à sua omissão em instituir sistemas de

proteção daquela (princípio do risco da atividade), caracterizam, sim, sem sombra de dúvida, danos morais a ensejar o dever de reparação.

Demais disso – vale repisar – a conduta deve pautar-se no cumprimento dos princípios da finalidade, esquecimento, transparência e, sobretudo, do consentimento, de maneira consentânea com a experiência internacional. E mister se faz para a reparação de danos morais e materiais oriundos da violação a direito fundamental, a constituição de um sistema de responsabilidade objetiva e solidária.

Assim, o reconhecimento do caráter objetivo dos direitos fundamentais enseja um dever de proteção do Estado (*Schutzpflicht)*, direcionado tanto ao Estado-legislador como ao Estado-juiz. O Poder Judiciário é o destinatário do dever de proteção que, na ausência do legislador, deve assegurar a devida proteção, a partir das normas já existentes.

Traz-se à baila – a título de ilustração, um julgado da lavra do Tribunal de Justiça de São Paulo, de um caso envolvendo repasse indevido de dados cadastrais de um consumidor e de seus rendimentos por uma loja de departamentos que ensejou o ajuizamento de uma ação de alimentos em face do mesmo, cujo teor da ementa, *verbis*:

> RESPONSABILIDADE CIVIL - Ação de indenização por danos morais - Cerceamento de defesa – Inocorrência - Ré que repassou dados cadastrais acerca dos rendimentos do autor a terceira estranha e com fins sem qualquer ligação a outra relação de consumo - Abuso do objeto cadastral em detrimento da privacidade do autor - Dano moral *in re ipsa* - *Quantum* que não merece reparo - Correção monetária, por outro lado, que deve incidir a partir da data em que o valor foi arbitrado - Incidência de juros mantida a partir da citação - Encargos da sucumbência- Reciprocidade - Inocorrência - Gratuidade processual que não pode ser revogada com base em futura indenização - Litigância de má-fé - Inocorrência- Recurso provido em parte [26].”

Posto isso, à vista da inequívoca necessidade de uma maior proteção dos dados pessoais a partir de sua obtenção, circulação e divulgação pelos *spamers* e suas maléficas consequências aos usuários, é que impõe-se a Responsabilização Civil dos Provedores da Internet em face da já reconhecida hipervulnerabilidade dos consumidores, especialmente informacional, demonstrada, *ex abundantia*, no presente estudo, sendo imperativo que medidas mais enérgicas sejam tomadas, e a cuja observância se faz necessário: i) o desenvolvimento de um novo direito à privacidade, consubstanciado na proteção e no controle das próprias informações pessoais; ii) a proteção do direito fundamental a ser tutelado na esfera privada do indivíduo em diversas dimensões em sua maior abrangência; iii) o direito à proteção de dados deve pautar-se no cumprimento dos seguintes princípios: finalidade,

[26] BRASIL, Tribunal de Justiça do Estado de São Paulo. *Apelação Cível nº 355.607.4/0-00*, rel. Des. De Santi Ribeiro. Disponível em: <www.planalto.gov.br>. Acesso em: 21 jun 2018.

esquecimento, qualidade dos dados, transparência e consentimento; iv) o direito geral de informação, amplo direito de acesso aos dados, direito de notificação, direito de retificação, cancelamento e bloqueio dos dados; v) a proibição ou limitação do armazenamento de informações sensíveis e excessivas e em especial por tempo indeterminado.

Em assim sendo, o presente estudo busca chamar a atenção dos órgãos públicos para a coibição e a punição do abuso das empresas em relação à utilização dos dados individuais dos consumidores que são objeto de *spams* – ou sua omissão em instituir sistemas de proteção de privacidade –, sem a qual, é forçoso reconhecer a necessidade de uma ação urgente dos Poderes Legislativo e Judiciário quanto à existência de danos morais e sua reparabilidade, sendo que para tanto, imprescindível a constituição de um sistema de responsabilidade objetiva e solidária.

Afirme-se ainda que vale demonstrar o aspecto punitivo-pedagógico o qual fundamentou inúmeros julgados que se traduziram em resultados positivos, como podemos analogamente e a título de exemplificação, citar a conduta abusiva dos "fornecedores" ao enviar, sem solicitação prévia, cartões de crédito aos consumidores exigindo-se-lhes a posterior cobrança como forma de elevar e facilitar o consumo de bens e serviços, restando hoje pacificado o posicionamento dos Tribunais ante o reconhecimento, inclusive, da existência de danos morais que levou praticamente à erradicação dessa prática nos dias de hoje.

Contudo, muito há que se aprimorar em termos de uma proteção dos consumidores usuários da internet em termos da responsabilização dos Provedores, que atualmente devem ser vistos dentro da norma protetiva dos direitos do consumidor – a Lei nº 8.078/90[27] – a abarcar a conduta sob a ótica da responsabilidade civil pelo envio de mensagens como prática abusiva, sem nos olvidarmos que os dados, objeto do presente artigo, devem ser erigidos ao *status* de direitos fundamentais a serem tutelados de forma específica, como direitos da personalidade tutelados pela Constituição da República Federativa Brasileira.

CONCLUSÃO

Esse estudo buscou, pois, demonstrar a importância da proteção dos dados pessoais e sua tutela pela Constituição Brasileira, como consectário dos direitos da personalidade e que devem ser protegidos pelo ordenamento jurídico brasileiro, em especial o CDC, uma vez que

[27] BRASIL. *Lei n° 8.078,* de 11 de dezembro de 1990. Disponível em: <http//www.planalto.gov.br>. Acesso em: 21 jun. 2018.

o princípio da vulnerabilidade (e aqui a reconhecidamente “informacional”) é um dos mais relevantes já consagrados, na medida em que é patente o reconhecimento do estado de risco e a fragilidade do sujeito de direitos inseridos no mercado de consumo, especialmente quando usuários da Internet.

Logo, configuradas a ausência da transparência e do dever informacional pelos Provedores de acesso e de busca/pesquisa da Internet, impõe-se o dever de reparar os danos, à luz do CDC, nos termos do que determina o seu art. 6º, VI, oriundos da coleta, processamento e divulgação dos dados da pessoa humana sem que os mesmos concedam, para tanto, prévia e legítima autorização ou se lhes faculte instrumento hábil a impedir tal circulação.

Assim, a relevância dos *spams* no mundo jurídico – e seu considerável aumento, descrito minuciosamente nos capítulos dessa pesquisa – decorre do fato de que o acúmulo de mensagens não solicitadas ocasiona, comprovadamente, diversos malefícios aos provedores e seus usuários, sendo responsável pela maioria do tráfego de e-mails de conteúdo ofensivo e propagandístico indesejados.

Isso, aliado ao verdadeiro sistema objetivo de reparação integral do dano previsto tanto na legislação protetiva do consumidor quanto na Constituição de 1988, impõe que a violação do direito à proteção de dados pode gerar dano patrimonial quanto dano moral. Aquele, *verbi gratia*, em uma contratação de um crédito mais caro pelo consumidor; esse, pela comprovada violação dos dados pessoais do consumidor sem o seu consentimento ou base legal.

Dúvidas não há, portanto, sob o aspecto da Lei nº 8.078/90 de que a Responsabilidade Civil dos Provedores de Internet enseja o dever de reparação e a cujo entendimento muitos Tribunais vêm se rendendo, em homenagem a um atributo maior, qual seja o direito da personalidade e em respeito à dignidade da pessoa humana.

Encerra-se aqui o tema com as sábias palavras da eminente autora Cláudia Lima Marques: “a igualdade perante a lei e a igualdade na lei só podem realizar-se, no direito privado brasileiro, se existir a distinção entre fracos e fortes, entre consumidor e fornecedor...”

REFERÊNCIAS

BENJAMIN, Antônio Herman; MARQUES, Cláudia Lima; BESSA, Leonardo Roscoe. *Manual de Direito do Consumidor*. São Paulo: Revista dos Tribunais, 2016.

BRASIL. *Constituição da República Federativa do Brasil*. Disponível em: <http//www.planalto.gov.br>. Acesso em 21 jun. 2018.

_____. *Lei nº 12.965*, de 23 de abril de 2014. Disponível em: <http//www.planalto.gov.br>. Acesso em: 21 jun. 2018.

_____. *Lei 8.078*, de 11 de setembro de 1990. Disponível em: <http//www.planalto.gov.br>. Acesso em: 21 jun. 2018.

_____. *Spam atinge até 97% dos e-mails no Brasil*, Disponível em: <http//www.convergenciadigital.com.br/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=44909&sid=4. Acesso em: 04 jun. 2018.

CAPANEMA, Walter Aranha. *O Spam e as Pragas Digitais*: Uma Visão Jurídico-Tecnológica. São Paulo: LTR, 2009.

DONEDA, Danilo. *Da Privacidade à proteção de dados pessoais*. Disponível em: <www.renatoleitemonteiro.com.br/.../Danilo-Doneda-Da-privacidade-a-protecao-de-dados.pdf>.Acesso em: 11 dez. 2017.

MARQUES, Cláudia Lima. *Comentários ao Código de Defesa do Consumidor*. São Paulo: RT, 2006.

MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor*: Linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.