Universidade de Brasília – UnB

Faculdade de Direito

ALICIA YUKARI LIMA AKAMINE

REGULAÇÃO RESPONSIVA DA PRÁTICA DE *E-MAIL MARKETING* NO BRASIL

Responsive Regulation applied to the e-mail marketing in Brazil

Brasília

2018

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE DIREITO

REGULAÇÃO RESPONSIVA DA PRÁTICA DE *E-MAIL MARKETING* NO BRASIL

Autor: Alicia Yukari Lima Akamine

Orientador: Prof. Dr. Márcio Iorio Aranha

Monografia apresentada como requisito parcial à obtenção do grau de Bacharel, na Graduação da Faculdade de Direito da Universidade de Brasília.

Brasília, ___ de _____ de ____.

FOLHA DE APROVAÇÃO

ALICIA YUKARI LIMA AKAMINE

Regulação Responsiva da prática de *e-mail marketing* no Brasil

Monografia apresentada como requisito parcial à obtenção do grau de Bacharel, na Graduação da Faculdade de Direito da Universidade de Brasília.

Aprovada em: ___ de _____ de _____.

BANCA EXAMINADORA

_____

Prof. Dr. Márcio Iorio Aranha

(Orientador – Presidente)

_____

Prof. Dr.

(Membro)

_____

Prof. Dr.

(Membro)

_____

Prof. Dr.

(Suplente)

Em memória dos meus avós, Teresinha e Oneildo,

que estejam em paz.

AGRADECIMENTOS

A Deus, por tudo, e Maria, pelo cuidado.

Ao meu orientador, professor Márcio Iorio Aranha, pela oportunidade de ser sua orientanda, pelos ensinamentos e admirável atenção durante a elaboração e revisão deste trabalho.

Aos meus pais, Mercedes e Harehiko, pela vida, amor, paciência e dedicação. Aos meus irmãos, Aline, Larissa e Welington, pela compreensão e carinho, que nossos caminhos nunca nos separem. Aos meus cunhados, Asari e Raphael, por agregarem-se tão bem à nossa família.

A Welington e Asari, novamente, pelo compartilhamento de conhecimentos da Engenharia e Ciência da Computação nos meus momentos de dúvida.

Por fim, ao querido Thiago, pelas preciosas sugestões e revisões, além do compartilhamento de conhecimentos da Ciência da Computação e do Direito nas nossas frequentes conversas, que foram fundamentais para o êxito deste trabalho. Não poderia deixar de agradecer, também, a sua parceria ao longo de toda a graduação, que espero levar para a vida.

FICHA CATALOGRÁFICA

Akamine, Alicia Yukari Lima
Ar Regulação Responsiva da prática de e-mail marketing no Brasil / Alicia Yukari Lima Akamine; orientador Marcio Iorio Aranha. -- Brasília, 2018.
53 p.

Monografia (Graduação - Direito) -- Universidade de Brasília, 2018.

1. O e-mail marketing e a privacidade na sociedade em rede: estudo sobre o estágio atual da regulamentação dos EUA, União Europeia e Brasil. 2. Proposta de regulação responsiva da prática de e-mail marketing no Brasil. I. Aranha, Marcio Iorio, orient. II. Título.

RESUMO

Este trabalho analisa o *e-mail marketing* como a forma legítima de *e-mail* comercial, mas que pode se tornar *spam*, se realizado de forma abusiva. Inicia-se a discussão com a contextualização da privacidade no ambiente digital, para compreender a importância da proteção de dados pessoais e do consentimento do seu titular para a sua utilização. Após, são abordados o objeto de estudo deste trabalho, o *e-mail marketing*, e a prática abusiva do *spam*. Apresentam-se, também, os sistemas de consentimento *opt-in* e *opt-out*, que, se cumpridos, legitimam o envio de uma comunicação comercial eletrônica como o *e-mail marketing*. Os Estados Unidos, a União Europeia e o Brasil adotam regulamentos que implementam esses sistemas, o *Controlling the Assault of Non-Solicited Pornography and Marketing Act* (CAN-SPAM), a Diretiva 2002/58/CE e o Código de Autorregulamentação para a prática de *E-mail Marketing* (CAPEM), respectivamente, os quais são discutidos ao longo deste trabalho. Propõe-se a regulação responsiva da prática de *e-mail marketing* no Brasil pela Autoridade Nacional de Proteção de Dados, para aprimorar e tornar eficaz a regulação dessa prática e, assim, garantir a privacidade dos cidadãos. Em resumo, após a análise, conclui-se que a cooperação entre regulador e regulados, incentivada pela regulação responsiva, pode compelir as empresas e indivíduos que realizam *e-mail marketing* no Brasil a tornarem-se responsáveis pela execução dessa prática em conformidade com o CAPEM e a Lei Geral de Proteção de Dados.

Palavras-chave: *e-mail marketing*; privacidade; consentimento; CAPEM; regulação responsiva.

ABSTRACT

This final project analyzes the use of commercial e-mail as spam when it violates individuals' privacy. The discussion begins by an overview of privacy in the digital environment to understand the importance of data protection and consent. Afterwards, the object of this research, e-mail marketing, and the abusive practice of spam are discussed. The systems of opt-in and opt-out consent are presented as a marker to categorize an electronic commercial communication as e-mail marketing. United States, European Union and Brazil adopt regulations that implement those systems: Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM), Directive 2002/58/CE, and Self-regulation Code of E-mail Marketing Practice (CAPEM). These regulations are discussed throughout this paper. Responsive regulation of e-mail marketing adopted in Brazil by the National Data Protection Authority is proposed in order to improve and make the regulation of this practice effective, thus guaranteeing citizens' privacy. After the analysis, this final project concludes that cooperation between regulator and those it regulates, encouraged by responsive regulation, may compel companies and individuals who do e-mail marketing to comply with CAPEM and the General Data Protection Law.

Keywords: e-mail marketing; privacy; consent; CAPEM; responsive regulation.

LISTA DE FIGURAS

LISTA DE ACRÔNIMOS

ABRADi	Associação Brasileira das Agências Digitais
ABRADi-RS	Associação Brasileira dos Agentes Digitais – Regional Rio Grande do Sul
ABRADi-SP	Associação Brasileira dos Agentes Digitais – Regional São Paulo
ABRANET	Associação Brasileira dos Provedores de Internet
ABRAREC	Associação Brasileira das Relações Empresa Cliente
ANATEL	Agência Nacional de Telecomunicações
ANPD	Autoridade Nacional de Proteção de Dados
APD	Autoridade de Proteção de Dados
CAN-SPAM	*Controlling the Assault of Non-Solicited Pornography and Marketing Act*
CAPEM	Código de Autorregulamentação para a Prática de *E-mail Marketing*
CDC	Código de Defesa do Consumidor
CF	Constituição Federal de 1988
CGI.br	Comitê Gestor da *Internet* no Brasil
CT *Spam*	Comissão de Trabalho *Anti-Spam*
FECOMÉRCIO-RS	Federação do Comércio do Estado do Rio Grande do Sul
FECOMÉRCIO-SP	Federação do Comércio do Estado de São Paulo
FEDERASUL	Federação das Associações Comerciais e de Serviços do Rio Grande do Sul
IAB	*Interactive Advertising* Bureau do Brasil
IMAP	*Internet Message Access Protocol*
INTERNETSUL	Associação dos Provedores de Acesso, Serviços e Informações da Rede *Internet*
LGPD	Lei Geral de Proteção de Dados
MCI	Marco Civil da *Internet*
ONU	Organização das Nações Unidas
POP3	*Post Office Protocol version 3*
PRO TESTE	Associação Brasileira de Defesa do Consumidor
RGPD	Regulamento Geral sobre a Proteção de Dados
RICE	Regimento Interno do Conselho de Ética
Senacon	Secretaria Nacional do Consumidor
SEPRORGS	Sindicato das Empresas de Informática do Rio Grande do Sul

SMTP	*Simple Mail Transfer Protocol*
TCP	*Transmission Control Protocol*

SUMÁRIO

INTRODUÇÃO

Na sociedade contemporânea, a centralidade assumida pelos meios de comunicação em rede, tais como *e-mail*, *Facebook* e *Instagram*, atraiu diferentes agentes econômicos para divulgação de seus produtos e serviços nessas plataformas. A mensagem eletrônica enviada por *e-mail* para fins comerciais denomina-se *e-mail marketing*, bastante utilizado por possuir os benefícios desse ambiente digital, quais sejam: agilidade para o envio, baixo custo em comparação com a correspondência física e fácil visualização pelos seus destinatários nos dispositivos conectados à *internet* (PANIGRAHI, 2016).

Pequenas empresas e pessoas físicas também podem utilizar essa espécie de comunicação comercial eletrônica a partir de *softwares* que realizam *e-mail marketing*, como o *Sendinblue, E-goi, SendBlaster* e *1and1Mail*. Além disso, a prática de *e-mail marketing* também é comum no setor público, para comunicação com o público de interesse na divulgação de eventos e realização de campanhas em geral, por exemplo, como se verifica pelo Pregão Eletrônico nº 19 de 2014, promovido pelo Conselho Federal de Medicina (CFM), e o Pregão Eletrônico nº 30 de 2016, efetuado pelo Conselho Regional de Engenharia e Agronomia do Rio de Janeiro (CREA-RJ), para contratar empresas que realizam esse serviço.

Por outro lado, essa forma de *marketing* deve se atentar para as especificidades desse ambiente em rede, tendo em vista que o endereço eletrônico é um dado pessoal e sua utilização indevida viola a privacidade do seu titular. Nesse caso, há o chamado *spam*, um *e-mail* enviado por códigos maliciosos para obter informações pessoais (CERT.BR, 2012), ou por um anunciante que coletou o endereço eletrônico do destinatário sem seu consentimento ou não ofereceu a possibilidade de ele cancelar o envio de novos *e-mails* (BRASIL, 2010).

Por isso, é preciso estabelecer e tornar efetivos parâmetros mínimos de privacidade dos cidadãos na *internet*, que devem ser respeitados pelas empresas, órgãos públicos e indivíduos que realizam *e-mail marketing* de modo a torná-lo benéfico para toda a coletividade, enquanto consumidores e destinatários desse serviço.

Essa preocupação fez com que os Estados Unidos da América criassem, em 2003, uma lei federal para regulamentar a prática de *e-mail* comercial não solicitado, denominada *Controlling the Assault of Non-Solicited Pornography And Marketing Act* (CAN-SPAM). Por sua vez, a União Europeia elaborou a Diretiva 2002/58/EC, com contornos mais restritivos que o norte-americano para a regulação dessas correspondências (MUTCHLER, 2010). No Brasil,

foi elaborado, em 2010, o Código de Autorregulamentação para a Prática de *E-mail Marketing* (CAPEM), com anuência do Comitê Gestor da *Internet* no Brasil (CGI-br).

Tendo em vista esse cenário, observa-se a preocupação dos países em tornar legítima essa prática de *marketing* a partir da sua regulamentação. Sendo assim, o presente estudo será guiado pela seguinte pergunta de pesquisa: como a teoria da regulação responsiva pode orientar as empresas e indivíduos que realizam *e-mail marketing* a preservarem a privacidade dos usuários da *internet* no Brasil?

A pesquisa limitar-se-á ao *e-mail*, pois essa plataforma antecede as demais redes sociais utilizadas na atualidade, o que proporciona mais tempo de estudo acerca de sua utilização comercial, e a existência de regulamentação no Brasil e no exterior. Além disso, este trabalho poderá ser aproveitado para auxiliar os estudos de proteção à privacidade dos usuários nas demais plataformas de comunicação na *internet*, observadas as suas especificidades.

Por sua vez, a teoria da regulação responsiva servirá como parâmetro para o aperfeiçoamento da regulação utilizada no Brasil para a prática de *e-mail marketing*. Essa teoria propõe que o Estado, ao regular, procure, em primeiro lugar, cooperar com o ente regulado, ao invés de proceder diretamente às sanções, em caso de infração às normas (AYRES e BRAITHWAITE, 1992).

Assim, para entender melhor o que é o *e-mail marketing*, o primeiro capítulo do presente trabalho iniciará com contextualização da privacidade na sociedade conectada à *internet*, para depois explicar essa prática comercial e apresentar a regulamentação utilizada nos Estados Unidos e na União Europeia, referida acima, e sua influência no modelo brasileiro, representado pelo CAPEM.

No segundo capítulo, será abordada a essência da teoria da regulação responsiva e apresentados os princípios responsivos elaborados pelo coautor da teoria, John Braithwaite (2011), para, em seguida, definir quem poderá exercer o papel de regulador responsivo do objeto de estudo do presente trabalho no Brasil. Após a definição, será proposta uma regulação responsiva da prática de *e-mail marketing* no Brasil a partir da aplicação dos princípios responsivos.

Por fim, no último capítulo, serão apresentas as conclusões obtidas ao longo da pesquisa.

1 O *E-MAIL MARKETING* E A PRIVACIDADE NA SOCIEDADE EM REDE: estudo sobre o estágio atual da regulamentação dos EUA, União Europeia e Brasil

Na primeira seção deste capítulo, serão abordadas a privacidade e a proteção de dados na sociedade conectada à *internet*, a fim de evidenciar a amplitude das questões que perpassam o tema do presente trabalho. Observa-se que o estudo irá se limitar à garantia da privacidade dos indivíduos e à importância do consentimento do titular do dado pessoal para o seu legítimo tratamento.

No ambiente digital criado pela rede mundial de computadores, está inserido o objeto de estudo deste trabalho, o *e-mail marketing*, que será apresentado na segunda seção. Além de conceituá-lo e demonstrar sua atual relevância para o setor econômico, esse recurso será distinguido do *spam*, que constitui um dos principais desafios enfrentado pelas regulamentações estatais e privadas (autorregulamentação).

Em seguida, apresentam-se as regulamentações adotadas nos Estados Unidos e na União Europeia para preservar a privacidade dos seus cidadãos e garantir que a prática de comunicação comercial eletrônica possa existir, respeitando o controle do indivíduo sobre seu dado pessoal, qual seja o endereço eletrônico.

Por último, analisa-se a regulamentação adotada no Brasil, verificando a sua inspiração no modelo europeu de legitimação do *e-mail marketing*. Conhecer a regulamentação brasileira e sua efetividade será fundamental para entender como aperfeiçoá-la com a aplicação da teoria da regulação responsiva, no segundo capítulo do presente trabalho.

1.1 A privacidade na sociedade conectada à *internet*

Com a evolução da tecnologia e a disseminação da *internet*, as pessoas passaram a disponibilizar cada vez mais diversas informações pessoais, como nome, endereço residencial e eletrônico (*e-mail*), número de telefone, seus familiares e amigos, que podem, inclusive, serem facilmente encontradas nos perfis das redes sociais. Essas informações são denominadas dados e, se identificarem um indivíduo ou o tornarem identificável, são classificados como dados pessoais (MENDES, 2014).

Assim, conscientes ou não, os seres humanos conectados à *internet*, por meio das mais diversas tecnologias[1], produzem uma vasta quantidade de dados. Esses dados possuem grande valor estratégico para as empresas, pois, aliados a ferramentas de tratamento, como *data mining*[2] e *profiling*[3], com auxílio de algoritmos de inteligência artificial e outras técnicas computacionais estatísticas, podem identificar indivíduos, revelar seus padrões de consumo, tendências de comportamento e decisões (ALLEN, 2016).

É certo que o *Big Data* e as novas tecnologias trouxeram benefícios para a sociedade. Pesquisadores da Universidade de Stanford, por exemplo, montaram um banco de dados com 130.000 imagens de lesões de pele e treinaram um algoritmo, com auxílio de inteligência artificial, para identificar visualmente um potencial câncer de pele, classificando-o como maligno ou benigno[4]. Em todos os testes realizados, o diagnóstico do algoritmo foi compatível com o dos dermatologistas (KUBOTA, 2017).

Por outro lado, a depender da forma de coleta dos dados e da finalidade para a qual se destina o seu tratamento, poderá haver violação da privacidade do indivíduo e, em alguns casos, a sua discriminação. Como exemplo, citam-se as propagandas comerciais ou *marketing*. Se antes era preciso enviar cupons para o consumidor com uma propaganda e um desconto para saber quais anúncios funcionavam de acordo com os respectivos cupons utilizados, hoje, com o *Big Data*, é possível direcionar as ofertas de produtos e serviços aos potenciais compradores com muita precisão (AKERLOF e SHILLER, 2016).

Como já mencionado anteriormente, isso ocorre porque a vasta quantidade de dados pessoais aliada a algoritmos que utilizem técnicas computacionais estatísticas e inteligência artificial dá acesso aos anunciantes a informações como hábitos, desejos e tendências de consumo dos indivíduos. Além disso, o *marketing online* possibilita a resposta rápida e

---

[1] A proliferação de aparelhos com sensores e conectados à internet, como *smartphones*, carros e relógios, fenômeno denominado *Internet* das Coisas (*Internet of Things*), enseja uma coleta expressiva de dados de indivíduos. Brinquedos também têm sido alvos dessa prática, originando categoria específica chamada "*Internet of Toys*", o que despertou a preocupação do Conselho do Consumidor Norueguês, ante a maior vulnerabilidade dos consumidores envolvidos, os quais são crianças (NORWEGIAN CONSUMER COUNCIL, 2016).

[2] *Data mining* "consiste na busca de correlações, recorrências, formas, tendências e padrões significativos a partir de quantidades muito grandes de dados, com o auxílio de instrumentos estatísticos e matemáticos" (DONEDA, 2006, p. 176).

[3] *Profiling* é uma técnica de tratamento de "elaboração de perfis de comportamento de uma pessoa a partir de informações que ela disponibiliza ou que são colhidas" (DONEDA, 2006, p. 173).

[4] Para melhor entender a precisão do algoritmo, colaciona-se a definição de maligno e benigno: "neoplasias malignas são, genericamente, conhecidas como 'câncer', apresentando capacidade de crescimento invasivo e de disseminação por vasos sanguíneos ou linfáticos, sobrevivendo e crescendo como novas lesões em linfonodos ou órgãos distantes, caracterizando as metástases. [...] De modo simplificado, as neoplasias benignas tendem a se apresentar como massas teciduais de crescimento lento e expansivo, comprimindo e não propriamente infiltrando o tecido vizinho. Assumem, assim, aspecto circunscrito, capsulado ou pseudocapsulado, com limites claramente identificados." (HOFF, 2013, p. 10)

rastreável do consumidor, que, ao clicar em um determinado *link* e ser direcionado para a loja eletrônica do anunciante, por exemplo, já informa que a propaganda foi eficaz, despertando seu interesse (O'NEIL, 2016).

O que, à primeira vista, aparenta ser positivo, pois estaria poupando o tempo dos consumidores na busca de um produto ou serviço, na realidade, pode consistir em uma violação a sua privacidade, caso não haja o consentimento do titular na coleta dos seus dados ou na venda deles para outras empresas.

Por sua vez, a discriminação surge quando as pessoas são ranqueadas a partir de seus dados e algumas, devido à raça, gênero, sexualidade ou recursos financeiros disponíveis, formam um grupo de vulneráveis, ao qual são direcionas publicidades predatórias, cujo objetivo é arrecadar dinheiro às custas de sua posição não privilegiada na sociedade (O'NEIL, 2016).

Para ilustrar, cita-se o *AdFisher*, uma ferramenta de *machine learning* desenvolvida para analisar a influência da visualização de *websites* associada à configuração de anúncios do Google nas propagandas que são apresentadas aos seus usuários. Um dos experimentos foi uma pesquisa de emprego, dividida em grupos masculinos e femininos, que visitavam os mesmos *websites*, com a configuração de anúncio especificando seu gênero. Comparando os resultados, descobriu-se que poucas ofertas de emprego com cargo e remuneração maior eram apresentadas para o grupo feminino (DATTA, TSCHANTZ e DATTA, 2015).

Além do potencial discriminatório, não se pode esquecer dos efeitos concorrenciais ocasionados por determinados agentes econômicos com maior qualidade e velocidade no processamento de dados, que abusam de seu poder econômico ao impossibilitar a entrada de novos agentes no mercado, demandando a intervenção da autoridade de defesa da concorrência (FRAZÃO, 2017).

Esses fenômenos da sociedade conectada à *internet* demonstram o quanto a vida privada do indivíduo encontra-se cada vez mais exposta, pois as suas "pegadas digitais", deixadas após a compra de um produto ou serviço, por exemplo, pode revelar mais do que a soma de suas partes para empresas que realizam o tratamento de dados (CASTELLANO, 2016). Proteger a privacidade do indivíduo e, por conseguinte, seus dados, é fundamental para garantir a sua autodeterminação informativa e coibir abusos por parte de setores privado e público.

A privacidade é reconhecida pela Organização das Nações Unidas (ONU) como um direito fundamental do ser humano no artigo 12[5] da Declaração Universal dos Direitos do

[5] "Art. 12. Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito à protecção da lei."

Homem, de 1948, e no artigo 17[6] do Pacto Internacional dos Direitos Civis e Políticos, de 1966. No ordenamento jurídico brasileiro, a Constituição Federal de 1988 (CF) também elenca a privacidade como um direito fundamental, no artigo 5º, incisos X[7] e XII[8].

O direito à privacidade também aparece em outros dispositivos legais: artigo 43[9], do Código de Defesa do Consumidor (CDC); artigo 5º[10] da Lei do Cadastro Positivo (Lei nº 12.414 de 2011); artigo 31[11] da Lei de Acesso à Informação (Lei nº 12.527 de 2011 – LAI); artigo 3º,

---

[6] "Art. 17. Ninguém será objecto de ingerências arbitrárias ou ilegais na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem de ataques ilegais à sua honra e reputação. Toda a pessoa tem direito a protecção da lei contra essas ingerências ou esses ataques."

[7] Art. 5º, inciso 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;".

[8] Art. 5º, inciso 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;".

[9] "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.

§ 1° 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° 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 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.

[...]"

[10] "Art. 5º São direitos do cadastrado:

I - obter o cancelamento do cadastro quando solicitado;

II - acessar gratuitamente as informações sobre ele existentes no banco de dados, inclusive o seu histórico, cabendo ao gestor manter sistemas seguros, por telefone ou por meio eletrônico, de consulta para informar as informações de adimplemento;

III - solicitar impugnação de qualquer informação sobre ele erroneamente anotada em banco de dados e ter, em até 7 (sete) dias, sua correção ou cancelamento e comunicação aos bancos de dados com os quais ele compartilhou a informação;

IV - conhecer os principais elementos e critérios considerados para a análise de risco, resguardado o segredo empresarial;

V - ser informado previamente sobre o armazenamento, a identidade do gestor do banco de dados, o objetivo do tratamento dos dados pessoais e os destinatários dos dados em caso de compartilhamento;

VI - solicitar ao consulente a revisão de decisão realizada exclusivamente por meios automatizados; e

VII - ter os seus dados pessoais utilizados somente de acordo com a finalidade para a qual eles foram coletados."

[11] "Art. 31. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.

§ 1º As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem:

I - terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem; e

II - poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem.

[...]

§ 4º A restrição de acesso à informação relativa à vida privada, honra e imagem de pessoa não poderá ser invocada com o intuito de prejudicar processo de apuração de irregularidades em que o titular das informações estiver envolvido, bem como em ações voltadas para a recuperação de fatos históricos de maior relevância."

§ 5º Regulamento disporá sobre os procedimentos para tratamento de informação pessoal.

incisos II e III[12], e incisos do artigo 7º[13] do Marco Civil da *Internet* (Lei nº 12.965 de 2014 – MCI). Esses dispositivos trouxeram novos contornos para a discussão ao possibilitar que o indivíduo exercesse uma posição mais ativa em relação aos seus dados, seja com a possibilidade de corrigi-los ou consentir com a sua coleta, uso, armazenamento e tratamento.

Com a recente sanção da Lei 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados (LGPD), consolidou-se no Brasil o entendimento acerca da necessidade de respeito à privacidade do indivíduo no ambiente digital e, também, da importância da sua postura ativa no que diz respeito ao tratamento dos seus dados. Dentre os vários dispositivos que abordam esse entendimento, destaca-se o artigo 2º, incisos I e II[14], e artigo 17[15], da referida Lei.

Verifica-se, então, a evolução do conceito de privacidade anteriormente concebido de forma individual e patrimonialista, como o direito a ser deixado só (*right to be let alone*), ou seja, a não intervenção na esfera individual, para acrescentar a necessidade de controle do cidadão sobre suas informações, ou seja, o fluxo dos seus dados pessoais (RODOTÀ, 2008).

Esse controle se traduz na autodeterminação informativa do cidadão, que é a possibilidade de decidir quais dados pessoais podem ser tratados, ter ciência da finalidade do

---

[12] "Art. 3º A disciplina do uso da *internet* no Brasil tem os seguintes princípios: […]
II - proteção da privacidade;
III - proteção dos dados pessoais, na forma da lei; [...]"

[13] "Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
[...]
III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;
[...]
VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
a) justifiquem sua coleta;
b) não sejam vedadas pela legislação; e
c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;
IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;
X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;
[...]
XIII - aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet."

[14] "Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
I - o respeito à privacidade;
II - a autodeterminação informativa;
[...]"

[15] "Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei."

processamento e das etapas e órgãos envolvidos (MENDES, 2014). O exercício dessa autonomia privada é realizado por meio do consentimento do titular ao autorizar o tratamento de seus dados pessoais (MENDES, 2015).

Segundo o artigo 4, parágrafo 11[16], da norma europeia de proteção de dados pessoais, o Regulamento Geral sobre a Proteção de Dados (RGPD), o consentimento, para ter eficácia, precisa ser livre, específico, informado e explícito. Essas características também foram adotadas pela LGPD, no artigo 5º, inciso XII[17], e em dispositivos separados, quais sejam: artigo 8º, *caput*, §3º, §4º[18], e artigo 9º, *caput*, incisos I a VII, e §1º[19].

Entende-se por livre, a manifestação de vontade em que não haja vício de consentimento, como dolo, erro, simulação ou fraude (RIZZARDO, 2015). Por sua vez, se o indivíduo sabe para que fim será destinado os seus dados, entende o que está consentindo e seus riscos, pois há transparência no processamento, e expressa sua permissão de forma indubitável, há o consentimento específico, informado e explícito, respectivamente (ARTICLE 29 WORKING PARTY, 2018).

Além disso, deve ser sempre possibilitada a revogação do consentimento pelo titular dos dados, tendo em vista que o tratamento pode não estar mais beneficiando o indivíduo ou pode não estar sendo realizado de forma adequada, caso ocorra desvio de finalidade, por exemplo (MENDES, 2015). A LGPD prevê que o consentimento pode ser revogado a qualquer momento

---

[16] Artigo 4, parágrafo 11, do RGPD: "«Consentimento» do titular dos dados, uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento."

[17] "Art. 5º Para os fins desta Lei, considera-se:

[...]

XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;" (Grifos da autora)

[18] "Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.

[...]

§ 3º É vedado o tratamento de dados pessoais mediante vício de consentimento.

§ 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas." (Grifos da autora)

[19] "Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:

I - finalidade específica do tratamento;

II - forma e duração do tratamento, observados os segredos comercial e industrial;

III - identificação do controlador;

IV - informações de contato do controlador;

V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;

VI - responsabilidades dos agentes que realizarão o tratamento; e

VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.

§ 1º Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca." (Grifos da autora)

pelo titular dos dados pessoais, de forma gratuita e acessível, conforme o artigo 8º, §5º[20], sendo um dos direitos do titular, previsto no artigo 18, inciso IX[21], da referida Lei.

Por outro lado, conforme evidenciado por Daniel Solove (2013), há dois tipos de problemas que dificultam a obtenção do consentimento com todos esses requisitos: (i) os cognitivos, pois poucas pessoas entendem as consequências da coleta de dados para ler e compreender os termos de privacidade, alterar a configuração de privacidade dos *websites* ou optar por não disponibilizar seus dados, quando há escolha; e (ii) os estruturais, que surgem devido à enorme quantidade de entidades que coletam, armazenam e processam os dados, o que dificulta o gerenciamento do cidadão sobre seus dados.

Ainda assim, o consentimento é necessário, pois é a forma de exercício da autonomia da vontade do particular. No entanto, apenas informar a população acerca das consequências da disponibilização de dados pessoais ou tornar os termos de privacidade mais inteligíveis não é suficiente. É preciso criar uma base sobre a qual os indivíduos acreditem que seus dados estão sendo protegidos, o que é desenvolvido a partir de políticas públicas e regulação (NISSENBAUM, 2011).

Nesse ponto, surge o papel do Estado na elaboração de normas sobre privacidade e proteção de dados pessoais e na regulação das atividades que os utilizam. No Brasil, o primeiro passo já foi dado com a recém aprovação da LGPD. Por sua vez, uma regulação estatal desenvolvida de forma específica sobre determinada atividade pode atender as suas peculiaridades e, ao mesmo tempo, garantir que o consentimento do titular seja observado e seus dados resguardados.

1.2 O *e-mail marketing* e a prática abusiva do *spam*

---

[20] "Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.

[...]

§ 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei."

[21] "Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

[...]

IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei."

Dentre os diversos meios de comunicação na *internet*, o *e-mail* destaca-se por ser bastante disseminado, mais antigo e perene que as redes sociais, utilizado para envio de correspondências formais de trabalho, ensino, pesquisa e outras comunicações restritas a determinadas pessoas, tendo em vista que as correspondências eletrônicas não são abertas ao público. Representa, em parte, a substituição da correspondência física enviada pelos correios.

Observa-se que *e-mail* pode ser compreendido tanto como a correspondência enviada pela *internet* para outras pessoas, por intermédio de plataformas de *webmail* como o *Gmail* do *Google* e o *Outlook* da *Microsoft*, quanto o endereço eletrônico utilizado para o envio e recebimento dessas correspondências.

Para fins comerciais, há modalidade específica chamada de *e-mail marketing*, que se direciona a um público alvo consumerista, com o objetivo de: adquirir novos clientes; enviar promoções para os consumidores continuarem comprando produtos da mesma marca; e estreitar os laços de relacionamento e confiança com os atuais clientes (PANIGRAHI, 2016).

O último objetivo é também conhecido como *newsletter* e possui mais do que uma simples divulgação de produtos e serviços, pois tem a finalidade de agregar valor à sua relação com o destinatário, sendo comum o envio de mensagens que informam, entretêm e beneficiam, de um modo geral, o receptor (PANIGRAHI, 2016).

O *e-mail marketing* conta com os benefícios de uma comunicação digital, dentre os quais se destacam: agilidade no envio; baixo custo em comparação com a versão física de envio de anúncios pelo correio, denominada mala direta; e fácil visualização pelos destinatários por meio de dispositivos conectados à *internet* (PANIGRAHI, 2016). Em relação à finalidade comercial, essa modalidade conta com rápida e fácil atualização dos anúncios, além da possibilidade de averiguar sua efetividade a partir de quantos *e-mails* foram abertos, quantos foram excluídos e quantas vezes os *links* das mensagens foram clicados (O'NEIL, 2016).

Essa prática se desenvolveu tanto que existem empresas que se dedicam a gerir e realizar o serviço de *e-mail marketing* para seus clientes, como a *Qualitare* Agência de *Internet* Ltda. Ademais, é uma prática acessível para pequenos empreendimentos e, até mesmo, para pessoas físicas, pois também estão disponíveis, na *internet*, *softwares* voltados para esse fim, por exemplo: *Sendinblue*, *E-goi*, *SendBlaster* e *1and1Mail*.

O setor público também utiliza o *e-mail marketing*, como se verifica nos pregões da Administração Pública para contratação de empresas que realizam esse serviço, listados a seguir: Pregão Eletrônico nº 19 de 2014, realizado pelo Conselho Federal de Medicina; Pregão Eletrônico nº 4 de 2014, promovido pelo Conselho Regional de Administração do Rio de Janeiro (CRA-RJ); Pregão Eletrônico nº 30 de 2016, efetuado pelo Conselho Regional de

Engenharia e Agronomia do Rio de Janeiro (CREA-RJ); e Pregão Eletrônico nº 18 de 2017, realizado pelo Conselho Regional de Enfermagem de Santa Catarina (Coren/SC).

Destaca-se que as questões sobre privacidade e proteção de dados, tratadas na seção anterior, estão fortemente presentes na prática do *e-mail marketing*, tendo em vista o fato de o endereço eletrônico ser um dado pessoal, que carece de proteção contra abusos (BRASIL, 2010).

Para entender melhor o objeto de estudo, é interessante conhecer, de forma simplificada, a arquitetura computacional envolvida no funcionamento do *e-mail*. Afinal, a interface gráfica com que o indivíduo interage para receber, organizar, responder e enviar *e-mails* é apenas uma parte desse meio de comunicação, conhecido como agente do usuário ou leitor de *e-mail* (TANENBAUM e WETHERALL, 2011).

Agentes de transferência de mensagens ou servidores de correio, localizados no servidor de *e-mail*, como o *Gmail* do *Google* e o *Microsoft E-mail Exchange*, são responsáveis pelo deslocamento das mensagens até o seu destino (TANENBAUM e WETHERALL, 2011).

Esses agentes se comunicam por meio de protocolos, que são regras convencionadas para possibilitar a comunicação entre máquinas. A linguagem humana utilizada para conversar seria uma analogia e, assim como existem vários idiomas, há também diversos protocolos, dentre os quais o *Simple Mail Transfer Protocol* (SMTP) é o utilizado para enviar *e-mails* (TANENBAUM e WETHERALL, 2011).

A figura 1, a seguir, ilustra a arquitetura computacional envolvida para a transferência (envio e recebimento) de *e-mails*.

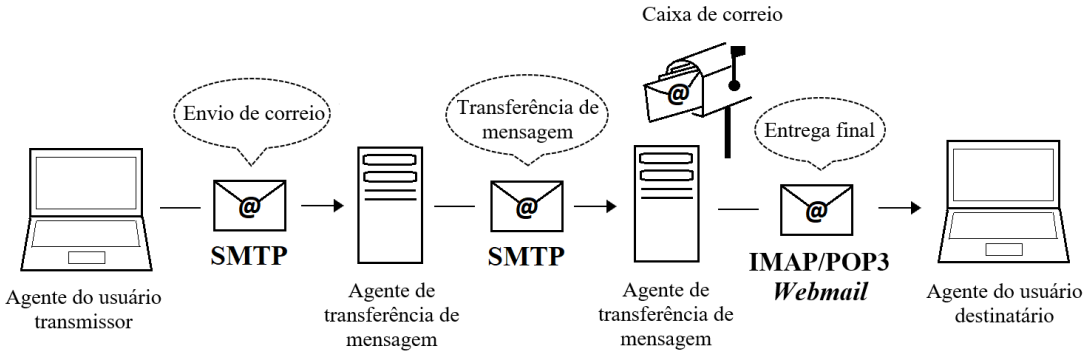

Figura 1: Arquitetura computacional para o envio e recebimento de *e-mail*.[22]

[22] A figura 1 tem como base a ilustração 7.4 do livro "Rede de Computadores" dos autores Andrew Tanenbaum e David Wetherall (2011, p. 392).

Na figura 1, o agente do usuário transmissor envia um correio eletrônico para o agente do usuário destinatário, através do protocolo SMTP, que é igualmente utilizado para transferência entre os servidores de correio. Observa-se que todos os agentes conectam entre si por meio do protocolo *Transmission Control Protocol* (TCP) com a Porta 25, a fim de assegurar que a mensagem seja entregue corretamente (TANENBAUM e WETHERALL, 2011).

Para que a mensagem possa ser enviada, é preciso ter um endereço eletrônico de destino que o agente de transferência possa reconhecer, por exemplo, fulano@gmail.com. Assim, após realizada a conexão TCP com a Porta 25, o agente de transferência de mensagem destinatário verifica a existência do endereço no destino, caso exista, a mensagem pode ser enviada pelo protocolo SMTP (TANENBAUM e WETHERALL, 2011).

No servidor de *e-mail* existe uma caixa de correio que armazena as mensagens recebidas, que podem ser baixadas para o agente do usuário destinatário, caso a remessa final seja feita pelo protocolo *Post Office Protocol version* 3 (POP3), ou apenas visualizadas pelo indivíduo, quando é utilizado o protocolo *Internet Message Access Protocol* (IMAP) ou *webmail*, como *Gmail* do *Google* (TANENBAUM e WETHERALL, 2011).

Observa-se que o acesso à caixa de correio no início desse meio de comunicação era realizado por programas isolados no computador que utilizavam os protocolos IMAP ou POP3. Atualmente, é comum o acesso do *e-mail* através da *web* (*World Wide Web*), o que possibilita aos indivíduos utilizarem qualquer navegador, Google Chrome e Firefox, por exemplo, para entrar no seu *e-mail*.

Nessa arquitetura computacional, destaca-se o fato do SMTP não verificar a autenticidade do endereço eletrônico do remetente das mensagens, de forma que ele, mesmo sendo falso, pode enviar *e-mails* para qualquer endereço eletrônico (TANENBAUM e WETHERALL, 2011). Por isso, milhares de mensagens indesejadas pelos destinatários podem ser enviadas por um *botnet*, ou seja, uma rede de computadores infectados por um código malicioso, que abusa de agentes do usuário para entregar a mensagem diretamente para o agente de transferência do destinatário (HOEPERS, STEDING-JESSEN e KUHL JR, 2008).

Essas mensagens indesejadas, decorrentes do abuso na utilização de um dado pessoal, qual seja o endereço eletrônico do destinatário, são conhecidas como *spam*[23] ou *e-mail* comercial não solicitado[24], caso tenha conteúdo exclusivamente comercial (CERT.BR, 2012).

> [...] 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 (BRASIL, 2010, p. 93).

A segunda denominação "*e-mail* comercial não solicitado" evidencia o fato de os *spams* não serem enviados somente por códigos maliciosos para infectar o computador de indivíduos e coletar suas informações pessoais. A própria arquitetura computacional do *e-mail*, que possibilita o envio de mensagens em massa, sem necessidade, a princípio, do consentimento dos destinatários e com um custo muito inferior à postagem física, tornou a prática do *spam* útil para anunciar produtos e serviços (BRASIL, 2010).

Os *spams* mostram-se frequentes no Brasil, que se encontra na 3ª posição da lista de países que apresentaram a maior taxa de *e-mails* considerados *spam* no ano de 2017, de acordo com o 23º Relatório de Ameaças à Segurança da *Internet* da empresa *Symantec* (SYMANTEC, 2018).

Para impedir o envio de *spams* de *botnet* e de códigos maliciosos em geral, o Comitê Gestor da *Internet* no Brasil criou a Comissão de Trabalho *Anti-Spam* (CT *Spam*), em dezembro de 2004, que atuou na implementação da Gerência da Porta 25 no Brasil. Essa Gerência é um conjunto de medidas tecnológicas que substituem a conexão do agente de usuário transmissor com o agente de transmissão por meio da Porta 25/TCP pela Porta 587/TCP, que utiliza serviço de autenticação de *e-mails* (HOEPERS e STEDING-JESSEN, 2009).

Por outro lado, há *spams* que são provenientes de endereços eletrônicos autênticos, como os *e-mails* comerciais não solicitados de empresas que existem no mercado. Para combatê-los, servidores de *e-mail* utilizam *softwares*, que filtram automaticamente os *e-mails* da caixa de correio para identificar os *spams*, excluí-los ou colocá-los em quarentena (TANENBAUM e WETHERALL, 2011). No caso da quarentena, o destinatário precisará

---

[23] Também é denominado s*pam* mensagens indesejadas enviadas por outros meios digitais, por exemplo: mensagens para celulares, conhecidas como SMS; mensagens diretas para usuários de redes sociais; ou mensagens em aplicativos de conversa instantânea, como *Whatsapp* e *Telegram*.

[24] Além da finalidade comercial, os *spams* "estão diretamente associados a ataques à segurança da Internet e do usuário, sendo um dos grandes responsáveis pela propagação de códigos maliciosos disseminação de golpes e venda ilegal de produtos." (CERT.BR, 2012, p. 34)

revisar as mensagens para ter certeza de que nenhuma delas foi classificada erroneamente como *spam* (BRASIL, 2010).

O *Gmail* do *Google* também fornece um botão intitulado "denunciar *spam*", o que auxilia e aperfeiçoa a filtragem a partir dos dados coletados das correspondências denunciadas pelos usuários.

Além das técnicas de filtragem, outra ferramenta para o bloqueio de *spams* é a criação de uma lista com os servidores que os enviam, denominada *blacklist*[25], que impede que os *e-mails* enviados por esses servidores sejam encaminhados para os destinatários (RAO e REILEY, 2012). Porém, a eficiência da *blacklist* é questionável, pois pode ocorrer de um determinado domínio[26] ser totalmente bloqueado, o que impediria a passagem de *e-mails* legítimos (BRASIL, 2010).

Ao contrário do *spam*, o *e-mail marketing* não viola a privacidade do destinatário, pois ele não tem seu endereço eletrônico coletado de forma indevida, além de ser oferecida a oportunidade de recusar o recebimento de novas mensagens comerciais (RAO e REILEY, 2012). Não obstante, os anunciantes devem ser diligentes para evitar que seu *e-mail marketing* torne-se um *spam* e, assim, tenha seu envio vedado.

1.3 A regulamentação aplicável ao *e-mail marketing* dos Estados Unidos, União Europeia e Brasil

Com o objetivo de garantir a proteção à privacidade dos indivíduos, evitando o uso abusivo de seus endereços eletrônicos, alguns países têm adotado como requisito o consentimento do destinatário para o envio de mensagens, que se divide em dois sistemas: *opt-in* e *opt-out*.

O sistema *opt-in* caracteriza-se pelo consentimento prévio, ou seja, nenhum *e-mail* pode ser enviado para o indivíduo, sem que, anteriormente, ele autorize (KUMAR, ZHANG, & LUO,

[25] No setor das telecomunicações do Estado de São Paulo foi implementada ideia semelhante pela Lei 13.226 de 2008, denominada Cadastro para o Bloqueio do Recebimento de Ligações de *Telemarketing* ou "Não perturbe", cuja execução e fiscalização ficaram a cargo da Fundação de Proteção e Defesa do Consumidor (PROCON/SP). No caso, o consumidor cadastra seu número de telefone e as empresas de *telemarketing* ficam proibidas de ligar para esse número, salvo se houver autorização escrita (art. 1º, parágrafo único, e art. 5º, caput, §2º e 3º, ambos da referida lei).

[26] Domínio é o nome utilizado para identificar um endereço de sítio eletrônico, como "amazon.com" e "saraiva.com.br". O termo domínio também é utilizado para se referir ao ".br", por exemplo, é por esse motivo que a inserção do ".br" em uma determinada *blacklist* poderia bloquear todos *e-mails* com esse domínio.

2014). Nesse caso, a empresa ou sujeito deve requerer a permissão do titular do dado pessoal para envio de *e-mail marketing*, quando uma conta é criada no seu sítio eletrônico, por exemplo, além de oferecer a possibilidade de retirar seu consentimento a qualquer momento.

Por sua vez, no sistema *opt-out* é possível enviar *e-mails* sem ter o consentimento prévio do destinatário, mas o remetente deve sempre oferecer a opção do destinatário vedar o envio de novos *e-mails*, a partir de um *link* para o descadastramento, por exemplo (KUMAR, ZHANG, & LUO, 2014).

Em ambos os sistemas a prática de *e-mail marketing* é viável e não corre o risco de ser taxada como *spam* por ser uma mensagem de teor comercial. Ao mesmo tempo é respeitada a privacidade do indivíduo, que pode exercer o controle do seu dado pessoal, o endereço eletrônico, ao consentir o envio dos *e-mails* ou, posteriormente, ter cumprida sua solicitação de vedação de novos envios.

Os Estados Unidos, no ano 2003, e a União Europeia, em 2002, adotaram o sistema *opt-out* e *opt-in*, respectivamente, para garantir a privacidade e proteção de dados dos seus cidadãos e, ao mesmo tempo, permitir o exercício da publicidade na *internet*. O Brasil, por sua vez, apresentou uma regulamentação mais tardia, em 2010, e específica para o *e-mail marketing*, seguindo as diretrizes europeias.

Ainda assim, cada território supracitado adotou uma forma distinta de regulamentação do seu sistema de consentimento, o que será visto com mais detalhes nas subseções a seguir.

1.3.1 A regulamentação aplicável ao *e-mail marketing* dos Estados Unidos

Por pressão do consumidor, para dar uma resposta ao problema dos *spams*, e do setor industrial, para evitar que leis estaduais mais severas regulassem essa prática, os Estados Unidos editaram a lei federal *Controlling the Assault of Non-Solicited Pornography and Marketing Act* (CAN-SPAM) de 2003, com vigência a partir de janeiro de 2004 (MAGGS, 2006).

Na exposição de motivos do Congresso para elaboração da lei, foi ressaltada a importância do *e-mail* para o dia a dia do cidadão e a ameaça que sua efetividade e conveniência poderiam sofrer com o crescimento do volume de *e-mails* comerciais não solicitados. O Congresso ainda esclareceu que a lei federal sozinha não iria resolver o problema do *spam*,

soluções tecnológicas e cooperação com outros países seriam fundamentais para o êxito dessa tarefa.

O direito preservado na lei federal é o do destinatário poder recusar o recebimento de novas correspondências do mesmo remetente. Verifica-se, então, que o CAN-SPAM considera legal o envio de *e-mails* comerciais não solicitados, pois não os proíbe, mas, sim, cria vedações para o envio quando há certas circunstâncias (MUTCHLER, 2010). Por isso, o legislativo norte-americano escolheu o sistema *opt-out*, em que é lícito o envio de mensagens comerciais, desde que haja possibilidade de o destinatário cancelar o recebimento de novos *e-mails*.

Além do recurso do descadastramento, também chamado *opt-out*, as demais circunstâncias que vedam o envio de *e-mail* comercial não solicitado no CAN-SPAM são: informações de remetente falsas ou enganosas; informações enganosas no cabeçalho de assunto; não identificação explícita da mensagem como anúncio; endereço físico inválido do remetente; endereço eletrônico do remetente inválido para receber pedido de *opt-out* ou que não inclui na mensagem recurso *opt-out*; e após dez dias úteis da solicitação de *opt-out*, é vedado o envio de novos *e-mails*.

Essas circunstâncias aplicam-se a todos os *e-mails* comerciais, sejam eles solicitados ou não pelos seus destinatários. Ao contrário dos *e-mails* pessoais, em que se proíbe, tão somente, informações falsas ou enganosas na mensagem (LORENTZ, 2011). Essa é uma forma de a lei evitar a proliferação de *spams* cujo objetivo não é comercial, mas, sim, fraudulento.

A lei federal também contém disposições penais sob o título "Fraudes e outras atividades relacionadas à correspondência eletrônica", cujos delitos envolvem a transmissão intencionada de múltiplas mensagens eletrônicas por meios fraudulentos. As penas podem chegar até cinco anos e serem cumuladas com multa. O Departamento de Justiça é responsável por realizar a execução dessa parte da lei.

A agência reguladora de comércio norte-americana, denominada Comissão Federal de Comércio (*Federal Trade Commission* – FTC), é responsável pela regulação da lei e pela prevenção da sua violação, podendo utilizar os meios, poderes, deveres e jurisdição presentes no seu estatuto, o *Federal Trade Commission Act*. Assim, as penas civis que a Comissão pode aplicar em caso de descumprimento do CAN-SPAM podem chegar até o valor de 41.484 dólares (FEDERAL TRADE COMMISSION, 2018).

Para evitar essas violações, o CAN-SPAM e a Comissão incentivam a conformidade com a lei, a partir do respeito às circunstâncias que vedam o envio de *e-mail*, mencionadas anteriormente. Acresce-se a elas o dever de monitorar a empresa contratada para realizar o *e-*

mail marketing, pois a lei prevê que quem tem seu produto promovido e a empresa que realiza o anúncio são igualmente responsáveis no caso do seu descumprimento.

Outras condutas proibidas pela lei são: coleta de endereços eletrônicos por meio de varreduras em *sites* sem permissão; ataque a dicionários, ou seja, a criação de possíveis endereços eletrônicos através da combinação de letras, números e nomes; criação de múltiplas contas de *e-mail* para transmissão de correspondências eletrônicas vedadas pela lei; e retransmissão de *e-mails* proibidos pela lei. Além disso, há requerimento para inserção de etiqueta de advertência em *e-mails* que contenham conteúdo sexual.

Em junho de 2017, por meio do *Federal Register*, volume 82, número 123, a Comissão requisitou comentários públicos de quaisquer interessados sobre a eficiência, custos, benefícios e impactos regulatórios da sua regulação do CAN-SPAM. Ao todo, foram encaminhados noventa e quatro comentários, dentre eles oitenta e dois são de pessoas físicas.

Roger Ford (2017, p. 2), professor da Universidade de *New Hampshire*, no seu comentário público, observou que o CAN-SPAM e sua regulamentação pela Comissão proporcionaram proteção ao consumidor, no que diz respeito ao uso de seu endereço eletrônico para *marketing*, quando a empresa ou pessoa física cumpre a lei. O professor destacou, ainda, a necessidade de padronizar a opção de cancelar o recebimento de novos *e-mails*, para facilitar a identificação desse recurso pelo consumidor (FORD, 2017, p. 6).

Em contrapartida, para Roger Ford (2017, p. 12), a lei federal se revelou pouco eficaz para o combate de *e-mails* de empresas e pessoas físicas que não cumprem a lei, razão pela qual a Comissão deveria buscar outras formas de exercer sua autoridade. Para tanto, o professor sugeriu que empresas de tecnologias, em parceria com a Comissão, desenvolvessem novas técnicas de filtragem, para impedir que mensagens que violem o CAN-SPAM sejam enviadas desde o início (FORD, 2017, p. 13).

1.3.2 A regulamentação aplicável ao *e-mail marketing* da União Europeia

A Diretiva Europeia 95/46/CE (*Data Protection Directive*), de 1995, já abordava o tema da proteção de dados pessoais e privacidade dos cidadãos. Porém, a manifestação específica da União Europeia para a questão dos *spams* foi na Diretiva 2002/58/EC (*E-Privacy Directive*), que se refere à privacidade e às comunicações eletrônicas.

Essa Diretiva, na seção de considerações, abordou a facilidade e baixo custo das comunicações comerciais eletrônicas não solicitadas e a preocupação com o volume dessas comunicações, que poderia ocasionar diversos ônus aos seus destinatários. A Diretiva incluiu no rol de comunicações comerciais não solicitadas as realizadas por meio de: aparelhos de chamadas automáticas (excluído, pois, o telemarketing realizado por pessoa física); aparelhos de fax; e correio eletrônico (*e-mails* e mensagens SMS).

Assim, a Diretiva europeia manifestou-se pela necessidade de os Estados-membros da União Europeia implementarem medidas de proteção aos indivíduos contra a invasão de sua privacidade decorrentes dessas comunicações. A medida principal estabelecida foi a implementação do sistema *opt-in,* ou seja, a imprescindibilidade do consentimento prévio e explícito do destinatário da comunicação comercial.

Nesse caso, o consentimento seguia as diretrizes da Diretiva 95/46/CE e da Diretiva 2002/21/CE (artigo 2º da Diretiva 2002/58/CE), sendo válida qualquer manifestação de vontade, desde que livre, específica e informada, pela qual o indivíduo aceitava o tratamento de seus dados pessoais. Não era considerado válido o consentimento originado pela inércia do titular, o que ocorre quando aparece uma caixa previamente selecionada para o recebimento de *e-mail marketing* nos termos de uso de determinado serviço (ARTICLE 29 WORKING PARTY, 2004).

Por outro lado, era permitida a comunicação comercial sem prévio consentimento, caso houvesse relação comercial anterior entre o destinatário e o anunciante, além de ser oferecida ao destinatário oportunidade de recusar a utilização dos seus dados pessoais para contato, de forma gratuita e clara (artigo 13, item 2, da Diretiva 2002/58/CE). Nas mensagens posteriores, sempre deveria haver recurso *opt-out*. Essa exceção ficou conhecida como "*soft opt-in*" (DONOVAN, 2004).

Da mesma forma que o CAN-SPAM, a Diretiva vedou o envio de *e-mail* cuja identidade do remetente estava oculta ou dissimulada, ou cujo endereço eletrônico não era válido, o que impediria o encaminhamento de mensagem do destinatário para recusar novas comunicações comerciais (artigo 13, item 4, da Diretiva 2002/58/CE).

O *Article* 29 *Working Party*[27], na Opinião 5/2004 sobre o tema, argumentou que a Diretiva 95/46/CE possuía outros requisitos para a legalidade dos *e-mails* comerciais, como a

[27] *Article 29 Working Party* é um grupo de trabalho composto por um representante de cada Autoridade de Proteção de Dados dos países-membros da União Europeia, que foi criado pela Diretiva 95/46/CE, no artigo 29. É um grupo independente e tem caráter meramente consultivo, a fim de aconselhar a Comissão Europeia acerca de temas relativos ao tratamento de dados pessoais. Esse grupo foi substituído pelo *European Data Protection Board*, com a entrada em vigor do Regulamento Geral sobre a Proteção de Dados, em maio de 2018.

necessidade de informar, no momento da coleta do dado pessoal, a identidade do controlador e a finalidade da coleta (ARTICLE 29 WORKING PARTY, 2004). Ademais, a colheita automática de *e-mails* seria proibida pela Diretiva 95/46/CE por ser uma forma ilegal de processamento de dados pessoais, que não observa os requisitos mencionados acima (ARTICLE 29 WORKING PARTY, 2004).

Observa-se que os outros meios de comunicação comercial não contemplados pela Diretiva ficaram sujeitos à regulação específica por cada Estado-membro, que poderia definir se seria necessário o consentimento anterior e, caso fosse, a forma em que ele se daria, conforme o artigo 13, item 3, da Diretiva 2002/58/CE.

Em 2009, houve uma emenda à Diretiva, que acrescentou o direito de indivíduos prejudicados por *spams* entrarem com ações judiciais contra os *spammers*. Aos Estados-membros também foi permitida a previsão de medidas específicas e sanções para o combate ao *spam* (artigo 13, item 6, da Diretiva 2002/58/CE).

A necessidade de implementar uma proteção uniforme dos dados pessoais nos Estados-membros incentivaram a reforma das normas de privacidade e proteção de dados da União Europeia (SAFARI, 2017). Originou-se dessa reforma o Regulamento Geral sobre a Proteção de Dados (RGPD), que entrou em vigor no dia 25 de maio de 2018.

O RGPD aplica-se ao tratamento de dados: de estabelecimento situado na União Europeia, mesmo que o tratamento ocorra em outro local (artigo 3º, item 1, do RGPD); e quando o titular dos dados reside na União Europeia e o responsável pelo tratamento não se encontra na União, desde que o processamento tenha relação com oferta de bens e serviço ao titular ou monitoramento do seu comportamento (art. 3º, item 2, do RGPD).

Para esclarecer a importância de um regulamento, observa-se que as diretivas, embora vinculem o Estado-membro da União Europeia ao resultado que se pretende alcançar, deixa a cargo das autoridades nacionais de cada Estado a escolha da forma para executar seus preceitos. Por sua vez, o regulamento é "obrigatório em todos os seus elementos e diretamente aplicável em todos os Estados-membros" (artigo 288 do Tratado sobre o funcionamento da União Europeia – versão consolidada).

Assim, para assegurar a coerência com as previsões já vigentes, na seção de considerações, o RGPD dispôs que a Diretiva 2002/58/CE deveria ser revista e, eventualmente, alterada em conformidade com o novo regulamento. Não obstante, ao RGPD não cabe impor obrigações adicionais a pessoas sujeitas a obrigações específicas com o mesmo objetivo estabelecidas na *ePrivacy Directive* (artigo 95 do RGPD).

Em 2015, quando o regulamento ainda era um esboço, já havia sido realizado relatório, a pedido da Comissão Europeia, para analisar a efetividade da Diretiva 2002/58/CE. Como resultado, verificou-se que Estados-membros introduziam em seus territórios os preceitos da Diretiva na forma de leis de privacidade eletrônica ou de comércio eletrônico, ou em uma mistura de ambas as leis (TIME.LEX e SPARK, 2015).

Porém, havia grande diversidade nas partes que cabiam a discricionariedade de cada Estado, como no caso do tratamento de outras formas de *marketing* direto não abrangidas pela Diretiva, em que poderia haver a escolha pelo sistema *opt-in* ou *opt-out* (TIME.LEX e SPARK, 2015). A recomendação final do relatório foi a transformação da Diretiva em um regulamento, a fim de facilitar a sua harmonização com o RGPD (TIME.LEX e SPARK, 2015).

Posteriormente, em 2016, foi realizada uma consulta pública sobre a *ePrivacy Directive*, que contou com a participação da sociedade civil, setor industrial e autoridades públicas. No que concerne às comunicações comerciais, a maioria da sociedade civil e das autoridades públicas defenderam a manutenção do sistema *opt-in*, ao contrário da maioria do setor industrial que preferiu o sistema *opt-out*, ante a existência de ferramentas que bloqueiam o *marketing* direto, como os filtros de *spam* nas plataformas de *e-mails* (EUROPEAN COMMISSION, 2016).

O *Article* 29 *Working Party* também realizou análise da *ePrivacy Directive*, na *Opinion* 3/2016, a fim de harmonizá-la com o RGPD. As principais recomendações foram as seguintes: consentimento prévio para todos os tipos de comunicações; meios simples e gratuitos para o indivíduo revogar o seu consentimento; consentimento específico, ou seja, um mesmo consentimento não pode ser utilizado para mais de uma finalidade (ARTICLE 29 WORKING PARTY, 2016).

A Comissão Europeia, após todos esses estudos, ao invés de somente revisar e alterar pontos específicos da Diretiva 2002/58/CE, resolveu revogá-la e criar um regulamento chamado *ePrivacy Regulation*, para dispor sobre a privacidade e proteção de dados nas comunicações eletrônicas e nos serviços prestados para esse fim (VOSS, 2017).

Em relação às comunicações comerciais, o atual esboço do regulamento manteve a necessidade de consentimento prévio para o seu envio (o sistema *opt-in*) e a exceção que permite o envio em caso de relação comercial anterior, desde que seja garantido o direito de oposição (*opt-out*) ao cliente e o direito de retirada do consentimento nas mensagens encaminhadas (artigo 16 do *ePrivacy Regulation*).

As inovações significativas do regulamento em relação a Diretiva 2002/58/CE, são a inserção do mesmo âmbito de aplicação do RGPD para o tratamento de dados, já mencionado

anteriormente, e a ampliação dos objetos de incidência que, além das comunicações eletrônicas anteriores, passará a englobar os novos serviços de comunicação fornecidos pela *internet*, como as redes sociais, aplicativos de conversas instantâneas e os *over-the-top* (OTT) *services*, que são os serviços de áudio e vídeo (VOSS, 2017).

1.3.3 A regulamentação brasileira do *e-mail marketing* ilustrada a partir de um anúncio enviado pela empresa Saraiva

A regulamentação do uso da *internet* no Brasil ocorreu a partir da entrada em vigor, em 2014, do Marco Civil da *Internet*. Ainda mais recente foi a sanção da Lei Geral de Proteção de Dados (LGPD), que é a primeira lei nacional que regulamenta o tratamento de dados no país. Com a vigência da LGPD, em fevereiro de 2020, espera-se que os brasileiros passem a ter maiores garantias de privacidade e controle sobre seus dados.

No que diz respeito ao tema do presente trabalho, o reconhecimento nacional do endereço eletrônico como um dado pessoal, que merece proteção diferenciada, torna ainda mais eficaz o combate ao *spam* e a necessidade de legitimar o *e-mail marketing*. Porém, as comunicações comerciais não solicitadas nesse meio já eram um problema muito antes da edição dessas normas, como se observa com a elaboração do CAN-SPAM nos Estados Unidos em 2003 e, no ano anterior, da Diretiva 2002/58/CE na União Europeia.

No Brasil, foram elaborados projetos de lei para regulamentar o *spam*, como o PL 2423/2003, posteriormente apensado ao PL 2186/2003, ao qual foram agregados mais quatro projetos de lei com o mesmo objetivo (PL 3731/2004, PL 3872/2004, PL 1227/2007 e PL 4187/2008). O PL 2186/2003 foi desarquivado em fevereiro de 2015 e, desde então, não houve mais atualizações na sua tramitação na Câmara dos Deputados.

Enquanto o Projeto de Lei não tramitava, o setor privado com anuência do Comitê Gestor da *Internet* no Brasil (CGI.br) elaborou o Código de Autorregulamentação para a Prática de *E-mail Marketing* (CAPEM), de 2010, para tratar especificamente da prática de *e-mail marketing* e, assim, evitar que essa forma de publicidade seja limitada ou vedada ao ser confundida com o *spam*.

As entidades do setor privado que elaboraram o Código foram: Associação Brasileira de Anunciantes (ABA); Associação Brasileira de Marketing Direto (ABEMD); Associação Brasileira das Agências Digitais (ABRADi); Associação Brasileira dos Provedores de Internet (ABRANET); Associação Brasileira das Relações Empresa Cliente (ABRAREC); Associação

Gaúcha das Agências Digitais (AGADI), atual Associação Brasileira dos Agentes Digitais – Regional Rio Grande do Sul (ABRADi-RS); Associação Paulista das Agências Digitais (APADI), atual Associação Brasileira dos Agentes Digitais – Regional São Paulo (ABRADi-SP); Federação do Comércio do Estado do Rio Grande do Sul (FECOMÉRCIO-RS); Federação do Comércio do Estado de São Paulo (FECOMÉRCIO-SP); Federação das Associações Comerciais e de Serviços do Rio Grande do Sul (FEDERASUL); *Interactive Advertising* Bureau do Brasil (IAB); Associação dos Provedores de Acesso, Serviços e Informações da Rede *Internet* (INTERNETSUL); Associação Brasileira de Defesa do Consumidor (PRO TESTE); e Sindicato das Empresas de Informática do Rio Grande do Sul (SEPRORGS).

O CAPEM, no capítulo três, intitulado "*e-mail marketing* eticamente correto", apresenta as regras para que essa comunicação comercial não seja considerada um *spam*. Essas regras seguem o sistema europeu de *opt-in* e *soft opt-in*, com a necessidade de recurso *opt-out* em todas as mensagens enviadas (artigo 3º, *caput* e inciso IV, do CAPEM).

O Código especifica que o recurso *opt-out* deve estar no corpo da mensagem em forma de *link*, além de haver mais uma alternativa, pelo menos, como telefone ou *e-mail*, para entrar em contato e solicitar o descadastramento (artigo 6º do CAPEM). Além disso, o remetente deve disponibilizar a sua política de *opt-out*, com o prazo para remoção do endereço eletrônico do destinatário de até dois dias úteis, quando utilizado o *link* para descadastramento, ou cinco dias úteis, quando o cancelamento da inscrição for solicitado por outro meio (artigo 4º, inciso VI, do CAPEM).

Há uma exceção à necessidade de disponibilizar o descadastramento (*opt-out*), quando os *e-mails* enviados têm a finalidade de garantir a execução contratual (artigo 4º, inciso VIII, do CAPEM). Essa hipótese, porém, não se enquadra no conceito aqui adotado de *e-mail marketing*, é, na verdade, uma mensagem de cunho relacional entre consumidor e vendedor. Nesse mesmo sentido é o entendimento adotado pelo CAN-SPAM, que exclui esse tipo de mensagem do contexto de comunicação comercial eletrônica.

O Código esclarece, também, que precisa haver identificação do remetente e endereço eletrônico válido (artigo 3º, inciso I, do CAPEM), que esteja vinculado ao seu nome de domínio próprio (artigo 3º, inciso II, do CAPEM). Além de não ser permitida "a prática do primeiro envio para se obter a permissão do Destinatário para envios posteriores" (artigo 4º, inciso I, do CAPEM) e o envio de arquivo anexo depende de autorização específica prévia e comprovável do destinatário (artigo 4º, inciso II, do CAPEM).

Há regras próprias para empresas parceiras, definidas como aquelas que contratam uma ação de *e-mail marketing* com uma pessoa física ou jurídica que detém uma lista de endereços

eletrônicos (base de destinatários), com os quais mantém relacionamento (artigo 2º, incisos III e XII, do CAPEM).

Os principais requisitos para a parceira enviar seu *e-mail marketing* são: o consentimento prévio específico (*opt-in*) da base de destinatários para o envio de campanhas da parceira; recurso de descadastramento para o *e-mail* de parceira; e recurso de descadastramento para o envio de *marketing* de todas as parceiras daquele que detém a base de destinatários (artigo 7º, incisos I e III, do CAPEM).

Ademais, o Código dispõe que não há relação comercial entre o responsável por um *site* e o destinatário de *e-mail* enviado por um visitante que utilizou ferramenta de compartilhamento de conteúdo do *site* por *e-mail* (artigo 8º, inciso V, do CAPEM). Por não estar configurada hipótese de *soft opt-in*, não é autorizado o envio subsequente de *e-mail marketing* ao destinatário. Nesse caso, o Código deveria ter incluído o remetente na vedação, para evitar que o visitante da página seja importunado com futuros *e-mails*.

No capítulo cinco do Código, há previsão de formação de um Conselho Superior e um Conselho de Ética, esse último é responsável por apreciar e julgar as denúncias de infrações às normas do Código (artigo 10, *caput* e inciso II, do CAPEM). O Conselho Superior é composto por um representante titular e um suplente de cada entidade signatária, com mandato de três anos (artigo 10, §2º, do CAPEM). Já o Conselho de Ética é formado por um Coordenador e mais quatro membros, indicados pelo Conselho Superior (artigo 10, §4º, do CAPEM), com mandato de dois anos (artigo 10, §5º, do CAPEM).

As medidas que o Conselho de Ética pode aplicar, após pronunciamento do investigado, são: advertência (artigo 11, inciso I, do CAPEM); recomendação para bloquear o domínio do remetente (artigo 11, inciso II, do CAPEM); divulgação da posição do Conselho, caso não haja a adoção das medidas sugeridas (artigo 11, inciso III, do CAPEM); e "sugestão de ação judicial inibitória cumulada com pedido de cancelamento de domínio" (artigo 11, inciso IV, do CAPEM).

O CAPEM representou um avanço na proteção à privacidade do usuário da *internet*, pois sequer existiam o Marco Civil da *Internet* e a Lei Geral de Proteção de Dados quando o Código foi elaborado. No entanto, não se pode dizer que o Código é plenamente efetivo, pois, em oito anos de vigência, não há publicação de decisões do Conselho de Ética no seu site oficial,

conforme requisitado pelo Regimento Interno do Conselho de Ética (RICE) como local para publicação da resolução dos processos consultivos e contenciosos[28].

Por outro lado, para ilustrar a adoção parcial das medidas do CAPEM para um *e-mail marketing* eticamente correto, observa-se, a seguir, o *e-mail marketing* da Saraiva (Saraiva e Siciliano S.A.)[29], companhia brasileira consolidada na área de livraria e edição de livros desde 1914.

[28] "Artigo 14 – Ao Relator para o qual for distribuído o Processo Consultivo caberá analisá-lo e apresentar seu parecer no prazo máximo de 15 (quinze) dias, sendo, ato imediatamente contínuo, remetido dito parecer aos demais julgadores, simultaneamente, para que, no prazo máximo de 15 (quinze) dias, profiram seus votos.

[...]

§6º. As decisões serão publicadas no website www.capem.org.br."

"Artigo 15 – O Processo Contencioso será realizado mediante Reclamação de pessoas físicas – devidamente inscritas no Cadastro de Pessoas Físicas (CPF) – ou de uma das entidades signatárias quanto à suposta inadequação de determinado email às recomendações do CAPEM.

§ 1º. – O Processo Contencioso será público, gratuito e se dará integralmente em meios eletrônicos, sem autos físicos, por intermédio do website www.capem.org.br."

"Artigo 17. Esgotado o prazo para oferecimento de defesa, caberá ao Relator apreciar o mérito da Reclamação e apresentar seu parecer no prazo máximo de 15 (quinze) dias, o qual será remetido aos demais julgadores, simultaneamente, para que profiram seus votos, no prazo máximo de 15 (quinze) dias.

[...]

§4º. As decisões serão publicadas no website www.capem.org.br."

[29] O *e-mail marketing* da Saraiva tem como objetivo, tão somente, ilustrar a aplicação parcial das regras do CAPEM. Não há a pretensão de servir como estudo empírico que evidencie o grau de observância do referido Código pelas empresas e indivíduos que realizam *e-mail marketing* no Brasil.

Figura 2: *E-mail marketing* da Saraiva.[30]

Na parte superior da imagem, verifica-se que a identificação do remetente, no caso, a Saraiva, está correta e o endereço eletrônico "saraiva@envios.saraiva.com.br" está vinculado ao seu nome de domínio próprio, qual seja "saraiva.com.br".

Há, também, a adoção do recurso *opt-out* ao lado do endereço eletrônico da Saraiva e no final do corpo da mensagem na forma do *link* "cancelar inscrição" e "remova aqui", respectivamente, conforme se verifica na figura 2. Ao clicar em um desses *links*, o destinatário do *e-mail marketing* é direcionado a uma página para o descadastramento, ilustrada a seguir, onde deverá selecionar o motivo pelo qual não deseja mais receber *e-mails* comerciais da empresa.

[30] Por não se relacionarem aos propósitos deste trabalho, foram suprimidos os trechos do *e-mail marketing* da Saraiva indicados pelas reticencias em colchetes.

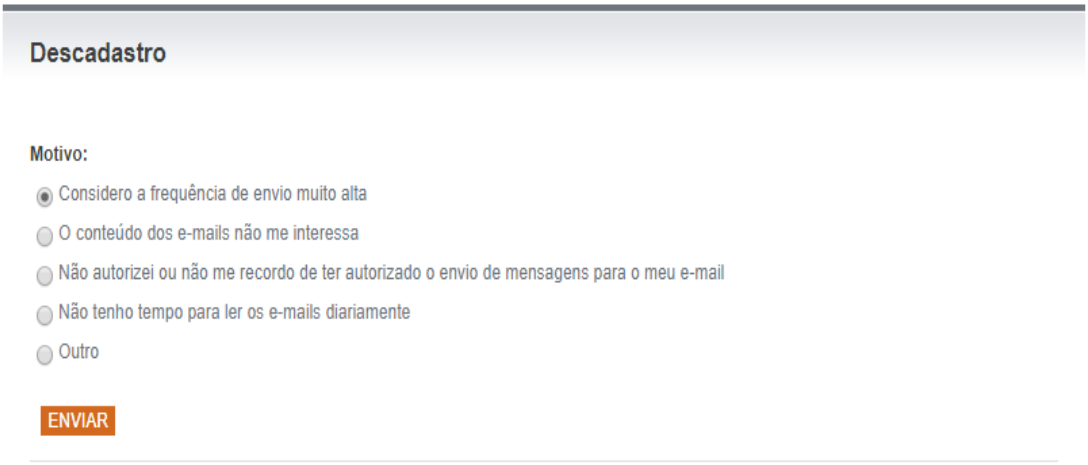

Figura 3: Página de descadastramento do *e-mail marketing* da Saraiva, exibida ao se clicar em um dos *links* de descadastramento presentes na mensagem ilustrada na Figura 2.

Por outro lado, a mensagem não indica outro meio para o cancelamento da inscrição, além dos *links* já mencionados, e não disponibiliza a sua política de *opt-out* com o prazo de até dois dias para remoção do endereço eletrônico do destinatário da base. Outrossim, conforme se observa no topo da Figura 2, o assunto do *e-mail* "Abre aê, abre aê, olha o e-mail aÊ! 🎵🎵" não traz informações sobre o conteúdo da correspondência, o que dificulta a sua imediata identificação como comunicação meramente comercial pelo destinatário.

Em relação ao requisito *opt-in*, no momento da realização do cadastro no *site* da Saraiva, que é obrigatório para realizar compras na sua loja virtual, há uma caixa pré-selecionada para o recebimento de *e-mails* com ofertas promocionais da companhia, observada a seguir.

Figura 4: Caixa pré-selecionada para recebimento de *e-mail marketing* da Saraiva.

Por fim, destaca-se que, de acordo com as regras do CAPEM, o requisito *opt-in* estaria preenchido com o oferecimento desse espaço para o consumidor recusar, especificamente, o recebimento de *e-mail marketing*. No entanto, verifica-se, nesse caso, o consentimento por inércia do titular do dado pessoal, que é considerado inválido pela Diretiva europeia

2002/58/CE e pelo RGPD. Com a entrada em vigor da LGPD, essa forma de consentimento terá que ser vedada pelo CAPEM, pois não atende os requisitos da manifestação livre e inequívoca do titular, que exigem um agir explícito do indivíduo para permitir a utilização de seu dado pessoal.

Ainda assim, de um modo geral, o CAPEM possui regras atuais e em consonância com a LGPD, ao prever a necessidade de consentimento prévio para utilização de endereços eletrônicos e o direito dos titulares desse dado pessoal de revogação do consentimento, exercido a partir do recurso de descadastramento.

No entanto, é preciso dar efetividade plena às suas disposições, especialmente na atual conjuntura de desenvolvimento dos comércios eletrônicos, em que muitas lojas virtuais utilizam *e-mail marketing* para se comunicar com os consumidores. Para aperfeiçoar a regulação dessa prática, evitando que se torne *spam* e garantido privacidade dos indivíduos, no capítulo seguinte elabora-se uma proposta de aplicação da teoria da regulação responsiva.

2 PROPOSTA DE REGULAÇÃO RESPONSIVA DA PRÁTICA DE *E-MAIL MARKETING* NO BRASIL

A primeira seção deste capítulo aborda a essência da teoria da regulação responsiva para sua compreensão. Ao final, apresentam-se nove princípios, elaborados pelo coautor da teoria, John Braithwaite (2011), que devem guiar a atuação do regulador responsivo.

Para aplicar tais princípios, é necessário definir quem será o regulador responsivo dessa prática, o que será discutido na segunda seção, com base nos atributos das autoridades de proteção de dados estrangeiras e a recente sanção da LGPD que, antes do veto presidencial, previa uma Autoridade de Proteção de Dados Pessoais (ANPD).

Definido o regulador responsivo, a última seção apresenta uma proposta de regulação responsiva da prática de *e-mail marketing* no Brasil, para tornar efetiva a proteção do endereço eletrônico dos indivíduos de *e-mails* comerciais abusivos, a partir do estímulo à cooperação e ao diálogo entre regulador e regulados.

2.1 A essência da teoria da regulação responsiva

A existência de uma regulamentação para determinada atividade não impede que os regulados a desrespeitem e gerem prejuízos para a comunidade, como pode ocorrer com um *e-mail marketing* que descumpre o CAPEM ao não inserir o recurso *opt-out*, tornando-se um *spam*.

Nesse ambiente digital, em que a tecnologia frequentemente modifica-se, podendo coibir práticas lesivas ou, até mesmo, facilitá-las, uma abordagem regulatória tradicional de comando e controle poderia sufocar a inovação benéfica. Por outro lado, uma regulação que se coloca entre o livre mercado (desregulação) e a regulação estatal forte, como a regulação responsiva, adequa-se mais a esse ambiente e ao seu contexto de privacidade (MCGEVERAN, 2016).

Na regulação responsiva, o regulador busca, em primeiro lugar, a cooperação com o regulado, ao invés de proceder diretamente às sanções em caso de violação das normas (AYRES e BRAITHWAITE, 1992). Muitos dos problemas do setor regulado podem ser resolvidos pelos próprios atores regulados, por isso, o regulador deve interagir com eles para capacitá-los e estimulá-los positivamente a cumprir a norma (BRAITHWAITE, 2011).

Se, ainda assim, a persuasão para o cumprimento da norma não for eficaz, o regulador poderá aplicar sanções com diferentes níveis de rigor, a fim de que cada infração tenha uma penalização que lhe seja proporcional. Ian Ayres e John Braithwaite (1992) propõem que as possíveis respostas do regulador a uma infração sejam visualizadas em uma pirâmide, na sua base se encontra a persuasão e nos demais segmentos as sanções em ordem crescente de rigor.

O regulador irá subir a pirâmide à medida que o regulado não cooperar. Caso ele volte a cooperar, a regulação responsiva permite a reconciliação, assim, o regulador restabelece o diálogo com o regulado e, se houver nova infração, a pirâmide será aplicada a partir da base (BRAITHWAITE, 2011).

Ao contrário do que se pode imaginar, o regulado não ficará sempre subindo e descendo a pirâmide, pois, ao escalá-la uma vez, ele verificará que é mais benéfico cooperar com o regulador, tendo em vista que se manter na base da pirâmide, onde há apenas diálogo, gera menos ônus (BRAITHWAITE, 2011). Essa possibilidade cooperação entre regulador e regulado é vislumbrada, também, pelo professor Othon de Azevedo Lopes no seguinte trecho.

> [...] Embora assimétrica a relação regulatória, ela se fundamenta numa mútua observação que pode ser conduzida para que *enforcement* [constrangimento legal] e *compliance* [conformidade] sejam coordenados de forma a instaurar um jogo de cooperação entre reguladores e regulados, como forma de potencializar a eficiência regulatória. (LOPES, 2018, p. 200)

Assim, somente se o agente regulado não tiver competência para cooperar ou agir de forma irracional, insistindo em não cooperar, deverá ser aplicada a sanção mais grave de incapacitação.

Destaca-se que o regulador deve ser transparente, para tanto, deve revelar a existência da pirâmide, notificar o regulado quando for subi-la, para que ele tenha possibilidade de ajustar sua conduta e evitar a escalada. Essa característica, que também incentiva o diálogo em primeiro lugar, faz com que a regulação seja vista de forma legítima e justa pelo regulado, o que aumenta a possibilidade de sua cooperação (BRAITHWAITE, 2011).

Essa é a base para compreensão da teoria da regulação responsiva, que foi utilizada em diversas pesquisas que ampliaram seu âmbito inicial de aplicação na regulação de empresas, para abranger investigações sobre crime, construção da paz, entre outros. Tendo isso em vista, para sintetizar a essência da teoria, o seu coautor, John Braithwaite, propôs nove princípios da regulação responsiva, apresentados a seguir.

1. Pense em contexto, não imponha uma teoria pré-concebida;
2. Ouça ativamente; estruture um diálogo que:

- Dê voz aos principais envolvidos;
- Estabeleça resultados em acordo e como monitorá-los;
- Construa compromisso ajudando os atores a encontrar as suas próprias motivações para melhorar;
- Comunique a decisão de trabalhar em um problema até que ele seja resolvido.

3. Envolva aqueles que resistem com imparcialidade; mostre a eles respeito interpretando a resistência deles como uma oportunidade para aprender como melhorar o desenho regulatório;
4. Elogie aqueles que demonstram compromisso:
   - Apoie a sua inovação;
   - Promova motivação para o aprimoramento contínuo;
   - Ajude líderes a mover os retardatários para novos níveis de excelência.
5. Sinalize a preferência por alcançar resultados pelo apoio e auxílio para construir habilidades;
6. Sinalize, mas não ameace, um rol de sanções que você pode escalar; sinalize que as sanções extremas podem ser usadas quando necessário, mas somente como último recurso;
7. Crie governança da pirâmide em rede com o engajamento de uma ampla rede de parceiros conforme é subida a pirâmide;
8. Extraia responsabilidade ativa (responsabilidade por alcançar resultados melhores no futuro), recorrendo à responsabilidade passiva (tornar os atores responsáveis pelas ações passadas) quando a responsabilidade ativa falhar;
9. Aprenda; avalie o quão bem e a que custo os resultados foram alcançados; comunique as lições aprendidas. (BRAITHWAITE, 2011, p. 476, tradução da autora).

Pela leitura desses princípios, verifica-se que eles versam sobre a atuação que deve ter um regulador responsivo. Por isso, antes propor a aplicação dos referidos princípios para regulação responsiva da prática de *e-mail marketing* no Brasil, é necessário estabelecer quem exercerá o papel de agente regulador dessa prática, o que será discutido na próxima seção.

2.2 Futura Autoridade Nacional de Proteção de Dados como reguladora responsiva da prática de *e-mail marketing*

A Lei Geral de Proteção de Dados previa, nos seus artigos 55 a 57, a criação da Autoridade Nacional de Proteção de Dados, que seria integrante da administração pública federal indireta, sob regime autárquico especial e vinculada ao Ministério da Justiça, mas com independência administrativa e ausência de subordinação hierárquica. A função desse órgão, que seria regido pela Lei 9.986, de 2000 (Lei das Agências Reguladoras), seria de fiscalização e expedição de normas complementares para proteção de dados.

No entanto, esses artigos foram vetados pelo Presidente da República, sob a justificativa de ter havido vício de iniciativa para a criação da autoridade, que deveria ter partido do Poder

Executivo. Não obstante, o Presidente manifestou-se pela necessidade de criação da ANPD, mas por meio de novo projeto de lei (AGÊNCIA SENADO, 2018).

Autoridades de proteção de dados, comuns em países da União Europeia[31], são órgãos essenciais para garantia da privacidade, proteção de dados, resolução de conflitos e cooperação sobre temas relativos à *internet* com outros órgãos do país de origem e com outras autoridades internacionais[32]. Na América Latina, há autoridades na Argentina (*Dirección Nacional de Protección de Datos Personales*), Colômbia (*Superintendencia de Industria y Comercio*), Costa Rica (*Agencia de Protección de Datos de los Habitantes*), México (*Instituto Federal de Acceso a la Información y Protección de Datos*), Peru (*Autoridad Nacional de Protección de Datos Personales*) e Uruguai (*Unidad Reguladora y de Control de Datos Personales*).

Órgãos que possuem área de atuação além do âmbito digital podem desempenhar o papel de autoridades de proteção de dados, como ocorre na Colômbia e nos Estados Unidos. Nesse último, a já mencionada Comissão Federal de Comércio (*Federal Trade Commission*), embora seja uma agência reguladora de comércio responsável pela defesa do consumidor, também realiza o *enforcement* (constrangimento legal) nacional das leis relativas à privacidade e proteção de dados.

A *internet*, ambiente de natureza compartilhada e dispersa mundialmente, onde os atores envolvidos são diversos, como o governo, empresas e indivíduos, torna ainda mais propícia a existência de conflitos internacionais. É com existência dessas autoridades, que cooperam entre si, que há a resolução desses conflitos, além da troca de experiências entre elas para implementação de melhores práticas, o que ocorre na Conferência Internacional dos Comissários de Proteção de Dados e Privacidade, fórum mundial que reúne esses órgãos (LEMOS, 2018).

Além disso, o RGPD, no artigo 45, parágrafo 1º, dispõe que a transferência internacional de dados pessoais entre os Estados-membros da União Europeia e um país terceiro ou organização internacional somente será possível se os últimos assegurarem um nível de proteção adequado. Entre os requisitos para se averiguar essa adequação, há a necessidade de existência e efetivo funcionamento de uma ou mais autoridades de proteção de dados, que sejam independentes e dotadas de poderes coercitivos suficientes para garantir os direitos dos titulares de dados (artigo 45, parágrafo 2º, item b, do RGPD).

---

[31] A Diretiva 95/46/CE já previa a obrigatoriedade de cada Estado-membro criar uma ou mais autoridades, conforme artigo 28, parágrafo 1º, da referida Diretiva. No RGPD, a previsão encontra-se no artigo 51, parágrafo 1º.

[32] No mundo, setenta e seis países possuem autoridade de proteção de dados, segundo a *Commission Nationale de l'Informatique et des Libertés*, autoridade francesa de proteção de dados (CNIL, 2018).

A centralidade que a autoridade assume para a proteção de dados, sua existência em diversos países, possibilitando a cooperação internacional, e sua imprescindibilidade para que haja relações comerciais e públicas com a União Europeia, que envolvam fluxo de dados, são alguns dos principais argumentos que demonstram a necessidade e urgência de criação da ANPD.

O Brasil avançou tanto com a sanção da LGPD, que o veto à criação da ANPD, como bem observou Laura Schertel Mendes e Danilo Doneda (2018), é algo como "morrer na praia". Por outro lado, observa-se que o veto decorreu de questões procedimentais, não tendo sido questionada a necessidade de criação da ANPD, pelo contrário, o Presidente da República esclareceu que ela será concretizada por meio de nova lei.

No contexto da regulação responsiva, entende-se que as autoridades de proteção de dados, em geral, assumem uma postura que se adequa à referida teoria. Esse entendimento decorre de análise dos principais atributos dessas autoridades apresentados no relatório intitulado "*Seeking Solutions: Attributes of Effective Data Protection Authorities*", elaborado pela Câmara de Comércio dos Estados Unidos (*U.S. Chamber of Commerce*) e pela firma de advocacia *Hunton & Williams*.

Segundo o relatório, esses órgãos possuem os atributos de educar e conscientizar a comunidade sobre práticas de proteção de dados, além de oferecer orientações e assistência para esclarecer previsões legais ou regulamentos e compartilhar sua opinião a respeito de questões nebulosas da *internet*, novas práticas e tecnologias (U.S. CHAMBER OF COMMERCE e HUNTON & WILLIAMS LLP., 2017).

Esses atributos, que se concretizam a partir de palestras, artigos, relatórios, manuais e auditorias realizadas pela própria autoridade, são importantes, porque a ausência de comprometimento pode decorrer da falta de conhecimento ou compreensão do setor regulado acerca das normas de privacidade e proteção de dados.

Antes do veto presidencial, a LGPD previa atribuição semelhante à ANPD no artigo 56, inciso VI, qual seja a promoção de conhecimento na população sobre as normas e políticas públicas de proteção de dados e medidas de segurança. Já no inciso XVI, do mesmo artigo da LGPD, havia a atribuição de realizar ou determinar auditorias no âmbito de sua competência de fiscalização.

Para efetivar essas características, é fundamental que a autoridade compreenda o mercado e as tecnologias, a fim de evitar o sufocamento das inovações benéficas. As tecnologias devem ser utilizadas a seu favor para garantir sua eficiência e transparência, um exemplo é a utilização do *YouTube* para divulgação de suas ações e entendimentos.

A transparência, como a fundamentação das decisões e publicação de relatórios das atividades desempenhadas, também é atributo essencial, pois propicia o reconhecimento das autoridades como confiáveis pelo setor regulado. Essa característica estava igualmente presente na ANPD, no artigo vetado 56, incisos XII, XIV (parte final) e XV, da LGPD, que tinha como atribuição elaborar relatórios anuais sobre as suas atividades, receitas e despesas, além de prestar contas das suas atividades e planejamentos.

Outro atributo é o poder decisório utilizado a partir de uma abordagem baseada em risco, em que se pondera o benefício de uma eventual intervenção com o seu custo. Assim, o órgão atua de acordo com a situação concreta e sua gravidade, para decidir se inicia uma investigação ou se aplica multa ou outras sanções. Esse *enforcenment* sob medida da autoridade privilegia entidades que cooperam, por outro lado, é mais rígido com aqueles que frequentemente descumprem as regras, o que incentiva a cooperação com o regulador (U.S. CHAMBER OF COMMERCE e HUNTON & WILLIAMS LLP., 2017).

Ademais, a autoridade deve buscar retorno do setor regulado, por meio de comentários públicos ou encontros com os diversos atores públicos e privados, por exemplo, a fim de saber se a regulação está sendo efetiva e o que pode ser aprimorado. “Esse processo colaborativo geralmente resulta em um consenso sobre as melhores práticas de privacidade e códigos de conduta, que influencia a interpretação das leis de privacidade pelo Estado e regulador” (U.S. CHAMBER OF COMMERCE e HUNTON & WILLIAMS LLP., 2017, p. 6, tradução da autora).

A LGPD preocupou-se com a atualização da ANPD em relação às melhores práticas ao prever originalmente no artigo 56, inciso VII, a promoção de estudos sobre prática locais e estrangeiras de proteção de dados pessoais e privacidade. Além disso, segundo o inciso VIII, do referido artigo, a ANPD deveria estimular a adoção de padrões em serviços e produtos que facilitassem a autodeterminação informativa do titular, ou seja, o controle sobre seus dados pessoais.

O diálogo com o setor regulado também estava previsto no artigo 56, incisos XIV e parágrafo 2º, da LGPD, que estabelecia à ANPD a atribuição de ouvir a sociedade e os responsáveis pelo tratamento de dados quando a matéria era de interesse relevante e de realizar consultas e audiências públicas para edição de regulamentos e normas sobre proteção de dados pessoais e privacidade.

A última característica é a já mencionada cooperação entre as autoridades internacionais, para aumento de sua eficiência e consistência regulatória mundial, a partir da troca de conhecimento e informações relevantes. Além disso, a cooperação diminui os custos

das autoridades, que evitam o trabalho duplicado quando há uma questão que necessita de atuação conjunta para o *enforcement* (U.S. CHAMBER OF COMMERCE e HUNTON & WILLIAMS LLP., 2017). A LGPD, no artigo 56, inciso IX, também previa a promoção de ações de cooperação internacional com as autoridades estrangeiras de proteção de dados.

Neste tópico, por meio dos atributos expostos e as disposições originárias da LGPD, demonstrou-se a importância da existência de um órgão tecnicamente especializado, tal como a ANPD, para se garantir a proteção de dados na prática de *e-mail marketing* de forma cooperativa entre o regulador e o regulado, potencializando o ganho de todos, inclusive, da sociedade.

Resta enfrentar a questão de como regular o *e-mail marketing* de acordo com os princípios da regulação responsiva enumerados na seção anterior. Tal empreendimento será realizado a seguir, com a proposta de aplicação dos referidos princípios.

2.3 Proposta de regulação responsiva da prática de *e-mail marketing* no Brasil a partir da aplicação dos princípios responsivos

Estabelecida a futura ANPD como reguladora responsiva da prática de *e-mail marketing*, propõe-se a aplicação dos princípios da regulação responsiva a essa prática, a fim de orientar os agentes regulados na preservação da privacidade dos indivíduos em observância às disposições da Lei Geral de Proteções de Dados.

O primeiro princípio, “pense em contexto, não imponha uma teoria pré-concebida” (BRAITHWAITE, 2011, p. 476, tradução da autora), aborda a necessidade de flexibilidade do regulador responsivo, que deve entender que a teoria da regulação responsiva e qualquer outra teoria não é um dogma que não pode ser questionado. Para tanto, é preciso que o regulador “pense em contexto”, ou seja, observe e entenda a realidade em que se insere o agente regulado, a fim de fornecer a melhor resposta regulatória possível (BRAITHWAITE, 2011).

Esse princípio é relevante em um ambiente computacional ante as frequentes alterações e aperfeiçoamentos das tecnologias, que demandam uma atuação flexível do regulador para entender quando é necessário mudar sua abordagem diante de determinada questão. No cenário brasileiro de *e-mail marketing*, verifica-se que o país seguiu caminho diverso dos Estados Unidos e da União Europeia, pois, mesmo sem existir regulamentação e autoridade de proteção de dados, foi elaborado o CAPEM.

A própria existência desse Código de autorregulamentação demonstra uma atenção ao contexto pelo Estado brasileiro em legitimar os *e-mails* comerciais que se adequam ao Código, ao invés de considerá-los *spams*. Essa atuação estatal ocorreu indiretamente através do CGI.br, entidade privada, que adota modelo multissetorial composto por vinte e um membros[33], dos quais nove são representantes do governo. Ressalta-se, igualmente, a atenção ao contexto pelo CGI.br no desenvolvimento de soluções tecnológicas, como o já mencionado projeto Gerência da Porta 25 para o combate ao *spam*.

Além disso, o CAPEM no seu preâmbulo transparece flexibilidade e adequação diante da conjuntura e suas frequentes alterações ao aduzir que as suas disposições "poderão ser utilizadas como fonte subsidiária no contexto da legislação que direta ou indiretamente trate ou venha a tratar da matéria". Essa previsão mostrou-se útil com a sanção da Lei Geral de Proteção de Dados, que aborda indiretamente a matéria ao estipular regras para que o tratamento de dados não ocorra de forma abusiva, violando os direitos fundamentais de liberdade e privacidade dos indivíduos (artigo 1º da LGPD).

Para entender o contexto em que o agente regulado se insere e incentivar as mudanças necessárias, é preciso que o regulador "ouça ativamente; estruture um diálogo que dê voz aos principais envolvidos" (BRAITHWAITE, 2011, p. 476, tradução da autora). Essa é a primeira parte do segundo princípio da regulação responsiva que também está presente na criação do Código de autorregulamentação e sua anuência pelo CGI.br, tendo em vista que entidades privadas envolvidas com *e-mail marketing* elaboraram as regras para melhorar, legitimar e fiscalizar essa prática.

Por outro lado, a segunda parte do segundo princípio, "estabeleça resultados em acordo e como monitorá-los" (BRAITHWAITE, 2011, p. 476, tradução da autora), restou parcialmente atendida, pois, apesar de constar no Código as diretrizes que devem ser seguidas para um *e-mail marketing* eticamente correto e as sanções a que estariam sujeitos os infratores, verificou-se a inatividade dos Conselhos Superiores para efetivar as suas disposições. Conforme visto no

[33] O Decreto nº 4.829 de 2003, que criou o CGI.br, no artigo 2º, inciso I, prevê que o Comitê será composto por um representante dos seguintes órgãos e entidades: Ministério da Ciência, Tecnologia e Inovação; Casa Civil da Presidência da República; Ministério das Comunicações; Ministério da Defesa; Ministério do Desenvolvimento, Indústria e Comércio Exterior; Ministério do Planejamento, Orçamento e Gestão; Agência Nacional de Telecomunicações; Conselho Nacional de Desenvolvimento Científico e Tecnológico; e Conselho Nacional de Secretários para Assuntos de Ciência, Tecnologia e Inovação (antigo Fórum Nacional de Secretários Estaduais para Assuntos de Ciência e Tecnologia). Os demais membros, estipulados no artigo 2º, incisos III a VI, do referido Decreto, são um representante de notório saber em assuntos de *internet*, quatro do setor empresarial, quatro do terceiro setor e quatro da comunidade científica e tecnológica.

capítulo anterior, não há publicação de demandas em análise ou já julgadas pelo Conselho de Ética.

Entende-se que essa falha decorre da limitação da regulação do *e-mail marketing* no Brasil à criação do CAPEM. Como visto na primeira seção deste capítulo, para efetivação da regulação responsiva é preciso haver outros meios de compelir os entes regulados a cumprirem as regras. Assim, se a autorregulação não funciona, deve ser possível ao regulador escalar uma pirâmide de estratégias regulatórias e de sanções até que os agentes voltem a cooperar.

Para que os demais princípios sejam aplicados, é preciso aperfeiçoar o desenho regulatório, o que se propõe, no presente trabalho, que seja feito pela futura ANPD, a partir da elaboração da pirâmide de estratégias regulatórias juntamente com a pirâmide de sanções. A elaboração das pirâmides atende a segunda parte do segundo princípio, "estabeleça resultados em acordo e como monitorá-los" (BRAITHWAITE, 2011, p. 476, tradução da autora), pois fixa a forma de monitoramento da cooperação dos entes regulados pelo agente regulador, além das sanções que podem ser empregadas para desestimular infrações.

A própria existência das pirâmides comunica a decisão da ANPD de "trabalhar em um problema até que ele seja resolvido" (BRAITHWAITE, 2011, p. 476, tradução da autora), pois a autoridade irá primeiro escutar e dialogar com os regulados, mas, se eles não cooperarem, ela irá escalar a pirâmide até que voltem a cooperar. Em primeiro lugar, o monitoramento será feito pela autorregulação com a manutenção do CAPEM e depois, caso os resultados não sejam satisfatórios, escalam-se as pirâmides.

A utilização do CAPEM na base da pirâmide de estratégias regulatórias mantém o diálogo já estabelecido com o setor regulado e constrói "compromisso ajudando os atores a encontrar as suas próprias motivações para melhorar" (BRAITHWAITE, 2011, p. 476, tradução da autora). Os atores regulados serão estimulados a mudar seu comportamento desinteressado no funcionamento do Código e dos seus órgãos, a fim de não terem que se submeter à regulação estatal, que se encontra no segundo nível da pirâmide de estratégias regulatórias, e à escalada da pirâmide de sanções.

Nesse ponto, observa-se que o terceiro princípio da regulação responsiva de envolver os que resistem com imparcialidade não se aplica ao caso, tendo em vista que não há resistência do setor regulado, mas sim ausência de interesse das entidades signatárias do CAPEM na sua efetivação. Não obstante, acredita-se que o desinteresse pode vir a se transformar em comprometimento com a regulação, tendo em vista a recente sanção da lei de proteção de dados, que demonstra uma maior preocupação da sociedade brasileira atual com a privacidade e autodeterminação informativa dos indivíduos.

Por isso, entende-se que o CAPEM ainda é útil para a adequação da prática de *e-mail marketing* no Brasil aos parâmetros estabelecidos pela LGPD, que, inclusive, autoriza a formulação de regras de boas práticas e de governança em privacidade por associações, conforme o artigo 50, *caput*, da referida Lei[34]. Ademais, como visto na seção anterior, uma das atribuições da ANPD era estimular a adoção de padrões em serviços e produtos que facilitassem a autodeterminação informativa do titular, o que pode ser vislumbrado no CAPEM.

No *e-mail* comercial da Saraiva, analisado no primeiro capítulo, verificou-se a observância de alguns dispositivos do Código. Algumas empresas, inclusive, em suas políticas de privacidade, dizem realizar sua prática de envio de *e-mail* comercial em conformidade com os padrões estabelecidos no CAPEM[35]. Além disso, empresas que comercializam o serviço de *e-mail marketing* têm se preocupado em estar em consonância com a LGPD, mencionando o CAPEM como o manual de boas práticas para o envio de *e-mails* comerciais (PADRON, 2018; PASCOAL, 2018).

É pressuposto da regulação responsiva o regulador sempre dialogar para persuadir os regulados a cooperarem antes de escalar a pirâmide. Por isso, o regulador deve primeiro persuadir as entidades signatárias para que elas aperfeiçoem o funcionamento do CAPEM, considerando as novidades legislativas da LGPD, e executem as atividades dos Conselhos.

Ademais, propõe-se a criação de um canal de fácil acesso para os cidadãos enviarem suas denúncias de empresas e indivíduos que realizam *e-mail marketing* em desconformidade com os dispositivos do Código. Esse canal continuará funcionando nas demais estratégias regulatórias, uma vez que as entidades privadas subscritoras do CAPEM também estarão presentes nesses níveis como parceiras.

Explica-se, a construção da pirâmide de estratégias regulatórias atende, principalmente, o sétimo princípio, segundo o qual o regulador deve engajar uma ampla rede de parceiros à medida em que sobe a pirâmide. Para a regulação responsiva da prática de *e-mail marketing* no Brasil, propõe-se a pirâmide ilustrada a seguir.

---

[34] "Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais."

[35] As políticas de privacidade verificadas foram: da marca Melissa, da empresa Grandene S.A. (https://www.melissa.com.br/sobre/politica-de-privacidade); da marca Ingresso Rápido, da Empresa Brasileira de Comercialização de Ingressos S.A. (https://www.ingressorapido.com.br/privacy); da Wok Grill, nome fantasia da empresa Nobre Pari Comercial LTDA (https://www.wokgrill.com.br/Politica-de-privacidade?&utmi_p=_&utmi_pc=Html&utmi_cp=menu). Todos os sítios eletrônicos foram acessados no dia 07 de outubro de 2018.

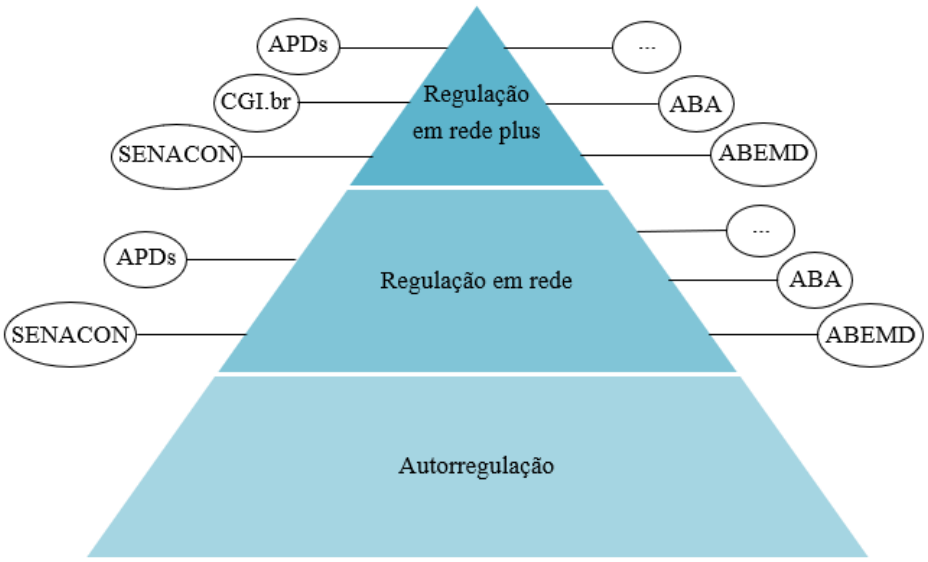

Figura 5: Pirâmide de estratégias regulatórias da prática de *e-mail marketing* no Brasil.

Na figura acima, as reticências representam as demais entidades privadas signatárias do CAPEM, já mencionadas na subseção 1.3.3 do primeiro capítulo. Ademais, APDs é o acrônimo utilizado para se referir às autoridades de proteção de dados estrangeiras, que auxiliarão em casos de cooperação internacional, e Senacon significa Secretaria Nacional do Consumidor. A rede de parceiros tem como objetivo garantir a eficácia da regulação e diminuir os custos do agente regulador, já que outros agentes atuarão na fiscalização do setor regulado (BRAITHWAITE, 2006).

Juntamente com a pirâmide de estratégias regulatórias aplica-se a pirâmide de sanções, ilustrada a seguir.

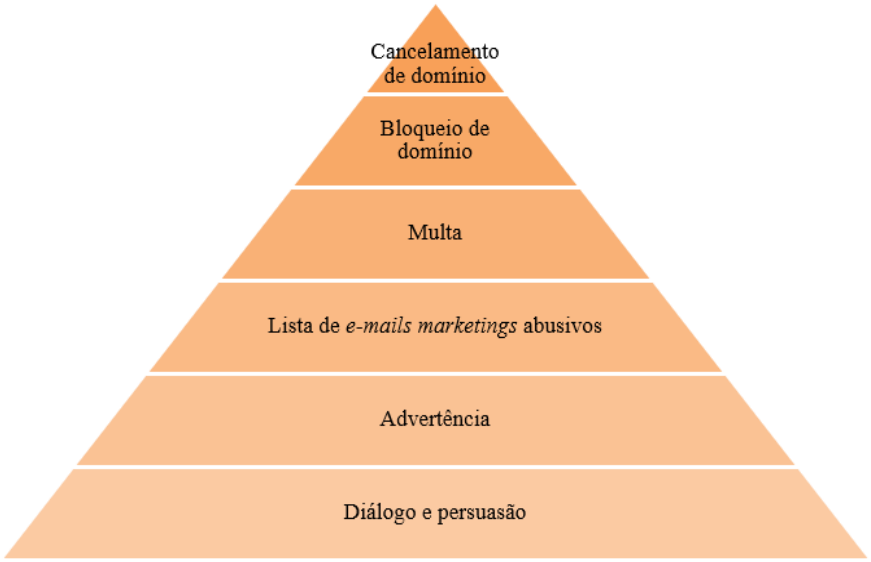

Figura 6: Pirâmide de sanções da prática de *e-mail marketing* no Brasil.

Enquanto a regulação estiver na base da pirâmide de estratégias regulatórias, com o funcionamento da autorregulação, o regulador permanecerá na base da pirâmide de sanções, onde sua atuação limita-se ao diálogo e persuasão dos entes regulados. Dentro da autorregulação aplicam-se as ações do Conselho de Ética estipuladas no CAPEM, apresentadas no primeiro capítulo.

Caso o modelo autorregulatório continue a não funcionar, a ANPD poderá subir para o segundo nível da pirâmide de estratégias regulatórias, denominada regulação em rede[36]. Observa-se que mesmo com a escalada da pirâmide para adoção da regulação em rede, os preceitos do CAPEM para um *e-mail marketing* eticamente correto, em consonância com a LGPD, continuarão a servir como parâmetro para fiscalização dos *e-mails* comerciais dos entes regulados.

Na regulação em rede, poderão ser aplicados o primeiro, segundo e terceiro níveis da pirâmide de sanções, observada essa ordem, pois sempre deverá haver primeiro o diálogo, exceto em circunstâncias excepcionais, que demandam maior repreensão. Somente se o diálogo não funcionar, o regulador subirá para o segundo nível, para advertir os regulados que não estão cumprindo as regras do CAPEM para um *e-mail* comercial eticamente correto. A advertência

[36] Observa-se que, na base da pirâmide de estratégias regulatórias, há o modelo de autorregulação, em que as empresas do setor privado elaboram suas próprias regras e fiscalizam-se sem a presença do Estado, tal como é proposto no CAPEM. Caso esse modelo não funcione, propõe-se a escalada para o segundo nível da pirâmide, substituindo a autorregulação pela regulação em rede, em que há a interferência do Estado para fiscalizar, dialogar e aplicar as sanções ao setor.

está prevista no artigo 52, inciso I, da LGPD, que inclui a indicação de um prazo para o infrator adotar as medidas corretivas.

Persistindo a conduta errônea, sobe-se para o terceiro nível, em que a empresa ou indivíduo terão seu endereço eletrônico registrado em uma lista de *e-mails marketings* abusivos pela Senacon, que será a responsável por administrar a lista. As entidades privadas subscritoras do CAPEM, ao receber a denúncia, irão verificar se o *e-mail marketing* é realmente abusivo e, caso seja, a ANPD tentará primeiro o diálogo e depois a advertência. Se as tentativas forem frustradas, os dados da empresa ou do indivíduo infrator serão enviados para a Senacon[37].

A criação dessa lista tem como base o cadastro de reclamações dos consumidores contra fornecedores de produtos e serviços previsto no artigo 44 do Código de Defesa do Consumidor[38], que possibilita a criação de um *ranking* de empresas que tiveram o maior número de reclamações, a fim de informar a sociedade sobre quais empresas mais violaram o CDC e direcionar políticas públicas para a solução desses conflitos[39]. Atualmente, o *ranking* das empresas mais demandadas nos órgãos de defesa do consumidor encontra-se no *site* do Sistema Nacional de Informações de Defesa do Consumidor[40].

A lista de *e-mails marketings* abusivos servirá para informar a sociedade sobre as empresas e indivíduos que violam a privacidade dos cidadãos com *e-mails* comerciais em desconformidade com as regras do CAPEM. Haverá, também, a viabilização do registro de outros dados sobre esses abusos, que, ao serem devidamente analisados pelo Senacon, poderá informar se os maiores infratores são empresas de grande porte ou indivíduos, por exemplo. Os dados coletados também serão úteis para o aperfeiçoamento do desenho regulatório pela ANPD.

---

[37] Observa-se que o Procon de Santa Catarina (Procon-SC) implementou, por meio do Decreto nº 638 de 2016, a opção de bloquear *telemarketing*, nos moldes da lista do "não perturbe" do Procon-SP, e a opção de bloquear mensagens ou *spam*, equiparando-as ao *telemarketing* (artigo 2º, inciso II, do referido Decreto). Assim, o indivíduo também pode inserir na lista, além do seu número de telefone, o seu endereço eletrônico, a fim de proibir o encaminhamento de qualquer *e-mail marketing* e *spam*, conforme verificado no seguinte sítio eletrônico que disponibiliza o serviço: <https://bloqueiotelemarketing.procon.sc.gov.br/>. Acessado no dia 13 de outubro de 2018.

[38] "Art. 44. Os órgãos públicos de defesa do consumidor manterão cadastros atualizados de reclamações fundamentadas contra fornecedores de produtos e serviços, devendo divulgá-lo pública e anualmente. A divulgação indicará se a reclamação foi atendida ou não pelo fornecedor.

§ 1° É facultado o acesso às informações lá constantes para orientação e consulta por qualquer interessado."

[39] Um exemplo de política pública implementada pela Senacon, em junho de 2014, foi a plataforma "consumidor.com.br". Trata-se de um serviço público que possibilita a conciliação direta entre consumidor, que faz a reclamação na plataforma *online*, e a empresa registrada voluntariamente no programa. Em outubro de 2018, 471 empresas e 1.103.025 consumidores estavam cadastrados na plataforma, já tendo sido finalizadas 1.460.210 reclamações. O índice médio de solução das empresas, de junho de 2014 a dezembro de 2017, foi de 80,6% e o prazo médio de respostas foi de 6,3 dias (SENACON, 2018, p. 3).

[40] Confira o site: <https://sindecnacional.mj.gov.br/pentaho/api/repos/%3Apublic%3ASindec%3AFornecedor%3ASINDEC_Fornecedor.wcdf/generatedContent?>. Acessado em: 10 de outubro de 2018.

Além disso, os usuários poderão bloquear os endereços eletrônicos presentes na lista por meio das ferramentas disponibilizadas pelos seus servidores de *e-mail*. Na versão gratuita do *Gmail* é possível importar filtros e optar por excluir os *e-mails* inseridos nele. Para ser importada como um filtro, a lista de *e-mails marketings* abusivos deverá ser disponibilizada pela Senacon em um arquivo no formato ".xml"[41].

No primeiro capítulo, verificou-se a existência de filtragem dos correios eletrônicos pelo próprio servidor de *e-mail*, a fim de identificar *spams*, excluí-los ou colocá-los em quarentena. Assim, a disponibilização da lista de *e-mails marketings* abusivos também poderá ser utilizada para alimentar o banco de dados do mecanismo de filtragem dos servidores de *e-mail* e, com isso, a mensagem comercial abusiva será encaminhada diretamente para caixa de *spam*, por exemplo.

Portanto, a lista servirá como uma forma de incentivar o comprometimento das empresas e indivíduos que se preocupam com a sua imagem perante a sociedade e que não desejam ter seus *e-mails* comerciais bloqueados. A Senacon também ficará responsável por atender os recursos eventualmente encaminhados contra a inserção do endereço eletrônico na lista e por retirar dela as empresas e indivíduos que adequarem sua prática de *e-mail marketing* aos parâmetros do CAPEM.

É importante destacar o papel essencial dos cidadãos na fiscalização dos *e-mails* comercias e envio das denúncias, para que o desenho regulatório proposto seja efetivo. O cidadão não precisa compor a pirâmide de estratégias regulatórias como um parceiro, pois, no paradigma do Estado Regulador, ele já é visto como "uma engrenagem essencial e uma força motriz necessária à implementação do interesse público, mediante co-participação na prestação de atividades socialmente relevantes" (ARANHA, 2018, p. 1023 do livro digital).

Se o regulado insistir em não regularizar seu *e-mail* comercial, a autoridade nacional poderá subir para o último nível da pirâmide de estratégias regulatórias, denominado regulação em rede *plus*, onde o CGI.br ingressa como parceiro. Essa escalada concede acesso ao quarto, quinto e sexto níveis da pirâmide de sanções, para eventual aplicação de multa pela ANPD, bloqueio e cancelamento de domínio pelo CGI.br, respectivamente. Ressalta-se que, mesmo estando no último nível da pirâmide de estratégias regulatórias, a pirâmide de sanções será aplicada a partir da base.

---

[41] O passo a passo para importar um filtro no *Gmail* pode ser conferido no seguinte *site*: <https://support.google.com/mail/answer/6579?hl=pt-BR>. Acessado em: 10 de outubro de 2018.

A multa está prevista no artigo 52, incisos II e III, da LGPD, na forma de: multa simples de até 2% do faturamento da pessoa jurídica no último exercício, com o limite de R$ 50.000.000,00 (cinquenta milhões de reais); e multa diária, observado o limite total da multa simples. Embora constitua uma violação ao CAPEM, nem todas as empresas e indivíduos que realizam *e-mail marketing* possuem um *site* para anunciar ou vender seus produtos e serviços. Por isso, considera-se que, nesses casos, a multa é a sanção extrema, que possibilitaria a dissuasão do regulado para que ele retorne a cooperar.

As duas últimas sanções constituem no bloqueio e cancelamento do domínio (endereço do sítio eletrônico) pelo CGI.br, que possui órgão específico, o Registro.br, para cuidar da administração dos domínios. Atualmente, no contrato firmado entre o Registro.br e o interessado em ter um *site*, constam como hipóteses de cancelamento do domínio: a expressa solicitação do requerente; a falta de pagamento da manutenção do domínio; a inserção no registro de dado pessoal falso, inválido, incorreto ou desatualizado; a não apresentação de documentos perante o Registro.br em tempo hábil; e a ordem judicial (REGISTRO.BR, 2011).

Não obstante, com a criação da ANPD, propõe-se a inserção das hipóteses de bloqueio e cancelamento de domínio a requerimento da autoridade, após o devido processo administrativo. Essas hipóteses não prejudicariam o ingresso do interessado no Judiciário para reverter a medida, ante a independência das instâncias administrativa e judicial e a previsão constitucional, no artigo 5º, inciso XXXV, de não exclusão de apreciação pelo Poder Judiciário de lesão ou ameaça a direito.

O bloqueio de domínio servirá para indisponibilizar temporariamente o sítio eletrônico, enquanto o regulado não regularizar sua prática de *e-mail marketing*, já o cancelamento de domínio indisponibiliza definitivamente o acesso ao sítio eletrônico. No caso de empresas de comércio eletrônico, que dependem de suas lojas virtuais para venderem seus produtos e serviços, o cancelamento de domínio significa a incapacitação da atividade exercida pelo regulado.

Ressalta-se a importância do regulador analisar o contexto do regulado, por isso, o sexto princípio que prevê a pirâmide de sanções dispõe que o regulador deve assinalar que “as sanções extremas podem ser usadas quando necessário, mas somente como último recurso” (BRAITHWAITE, 2011, p. 476, tradução da autora). Ou seja, a postura que autoridade deve adotar é a de persuadir o regulado a manter-se na base de ambas as pirâmides, evitando a utilização da sanção extrema.

A sanção extrema de cancelamento de domínio poderia ser aplicada, por exemplo, em uma empresa que vende, no seu sítio eletrônico, serviço de *e-mail marketing* abusivo, pois não

inclui a opção de descadastramento, e, mesmo após ter sido multada, se recusa a regularizar seu serviço. Assim, para evitar que essa violação à privacidade dos destinatários se dissemine, uma vez que outras pessoas podem comprar esse serviço, e se perpetue, a ANPD solicitaria o cancelamento do domínio dessa empresa pelo CGI.br.

O regulador responsivo também deve reconhecer o desempenho positivo dos regulados, elogiando aqueles que demonstram compromisso, apoiando as suas inovações e motivando-os ao aprimoramento contínuo de suas práticas. Essas ações correspondem à primeira e segunda parte do quarto princípio, que tem como objetivo incentivar os regulados a buscar o aperfeiçoamento da regulação como um todo (BRAITHWAITE, 2011).

Na experiência internacional, observa-se a autoridade de proteção de dados do México, que concede o *Premio de Innovación y Buenas Prácticas en la Protección de Datos Personales* aos trabalhos que desenvolvem melhores práticas e inovações para o tratamento de dados (INAI, 2018). Por sua vez, a autoridade da França e da Espanha realizam concurso para conceder prêmios monetários para organizações que empregam as melhores práticas no campo da proteção de dados (U.S. CHAMBER OF COMMERCE e HUNTON & WILLIAMS LLP., 2017).

Para o objeto de estudo do presente trabalho, propõe-se a criação de uma lista de *e-mails marketings* idôneos, a fim de reconhecer e promover as empresas que estão em conformidade com as regras estabelecida pelo CAPEM e pela LGPD. Essa espécie de *whitelist* é uma forma da ANPD ajudar "líderes a mover os retardatários para novos níveis de excelência" (BRAITHWAITE, 2011, p. 476, tradução da autora), ou seja, os regulados, no caso os retardatários, além de evitarem entrar na lista de *e-mails marketings* abusivos, desejarão compor a lista de *e-mails marketings* idôneos, para estar em igualdade com as outras empresas e indivíduos, que são os líderes por já comporem essa lista.

A lista de *e-mails marketings* idôneos também é uma forma da ANPD atender o quinto princípio responsivo de alcançar resultados pelo apoio e auxílio para construir a habilidade dos regulados atuarem em conformidade com a regulação. Para tanto, a autoridade deverá promover o conhecimento das regras do CAPEM para um *e-mail* comercial idôneo e auxiliar as empresas e indivíduos que desejam adequar sua prática para que possam integrar a lista de *e-mails marketings* idôneos. Esses são alguns dos atributos já vistos na seção anterior essenciais para autoridades de proteção de dados.

O oitavo princípio da regulação responsiva, de extrair a responsabilidade ativa dos regulados, ou seja, a responsabilidade por alcançar melhores resultados no futuro, sintetiza a ideia principal da teoria de promover a cooperação entre regulador e regulados. Recorre-se à

responsabilidade passiva, a responsabilização dos atores pelas ações passadas, tão somente se a responsabilidade ativa falhar (BRAITHWAITE, 2011).

A primeira manifestação de extração de responsabilidade ativa pela ANPD seria a manutenção da autorregulação pelas entidades privadas signatárias do CAPEM. E ainda se for escalada a pirâmide de estratégias regulatórias, para a regulação em rede e a regulação em rede *plus*, será possível extrair responsabilidade ativa dos regulados através do diálogo e persuasão até a advertência para correção da prática abusiva, que correspondem ao primeiro e segundo nível da pirâmide de sanções, respectivamente.

O último princípio da regulação responsiva aborda a necessidade do regulador avaliar quão bem e a que custos os resultados foram alcançados, para descobrir como aperfeiçoar o desenho regulatório (BRAITHWAITE, 2011). Afinal, pode ocorrer do desenho planejado e executado não se revelar eficaz ou ser muito oneroso, o que demandaria a investigação de outras formas de atuação.

No caso da regulação de práticas desenvolvidas na *internet*, é fundamental estar sempre atento, pois, a qualquer momento, podem ser criadas tecnologias que possibilitem a violação da regulação ou o seu aprimoramento. A necessidade de buscar retorno do setor regulado é, inclusive, um dos atributos de autoridades de proteção de dados eficazes visto na seção anterior, o que incentiva o processo colaborativo entre regulador e regulados para implementação das melhores práticas de privacidade e proteção de dados pessoais.

A ANPD deverá observar, por exemplo, se a escalada da pirâmide de sanções foi eficaz ou se teria sido mais benéfico permanecer em determinado nível. Ou, ainda, se seria necessário retirar determinada sanção para aplicar, em seu lugar, uma nova ferramenta tecnológica, que impeça, de forma efetiva e com menor custo, as violações à privacidade dos indivíduos.

Portanto, esclarece-se que a presente proposta de aplicação da teoria responsiva não pretende ser a única solução regulatória ou, até mesmo, a solução completa e final de regulação responsiva da prática de *e-mail marketing*. Ao contrário, objetiva-se conhecer e compreender uma forma de o agente regulador atuar para obter o comprometimento dos regulados no ambiente digital, que incentive o diálogo e cooperação entre ambos, indo além da mera aplicação de multas.

CONCLUSÃO

Este trabalho analisa o *e-mail marketing* como a forma legítima de *e-mail* comercial, mas que pode se tornar *spam*, se realizada de forma abusiva, violando a privacidade dos indivíduos.

Tendo em vista que o objeto de estudo do presente trabalho está inserido no ambiente digital, abordou-se, inicialmente, a importância da garantia da privacidade e proteção de dados na sociedade conectada à *internet*. Nesse ponto, destacou-se a necessidade de os cidadãos terem controle sobre seus dados pessoais, o que é feito a partir do consentimento e da possibilidade de revogação do consentimento para o uso desses dados por terceiros.

Em seguida, a partir do conhecimento da arquitetura computacional envolvida no funcionamento do *e-mail*, observou-se que o protocolo SMTP utilizado para envio de correios eletrônicos não verifica a autenticidade do endereço eletrônico do remetente das mensagens, por isso, mesmo que o remente seja falso, é possível enviar *e-mails* para qualquer endereço eletrônico.

Assim, surgiram os *spams* enviados por computadores infectados, com o objetivo de coletar dados pessoais dos destinatários, como contas bancárias, e os *spams* que possuem conteúdo exclusivamente comercial, conhecidos como *e-mail* comercial não solicitado. Para combater essa violação à privacidade dos destinatários, foram desenvolvidas soluções tecnológicas, como a Gerência da Porta 25 e os filtros de mensagens dos servidores de *e-mail*.

Por outro lado, ressaltou-se que o *e-mail marketing*, mesmo sendo um *e-mail* comercial, não viola a privacidade do destinatário, pois seu endereço eletrônico não é coletado de forma indevida e, caso ele não queira continuar recebendo novas mensagens comerciais, é possível recusar o recebimento. Verificou-se, então, que os Estados Unidos e a União Europeia se preocuparam em legitimar essa prática e delimitar os seus contornos para que não se torna-se *spam*.

As regras dos Estados Unidos para envio de *e-mail* comercial podem ser encontradas no CAN-SPAM Act, de 2003, que adota o sistema *opt-out*, que possibilita ao destinatário descadastrar o seu endereço eletrônico para deixar de receber novas correspondências. Por sua vez, a União Europeia, adotou, na Diretiva 2002/58/EC, o sistema *opt-in* com recurso *opt-out*, que requer o consentimento prévio do destinatário, mas permite o seu descadastramento.

A partir da análise desses dois sistemas, observou-se que o Brasil adotou o sistema europeu, no entanto, na forma de uma autorregulamentação, com o Código de

Autorregulamentação para a Prática de *E-mail Marketing*, de 2010, elaborado por entidades do setor privado com anuência do CGI.br. Constatou-se que as regras do Código para um *e-mail* comercial eticamente correto, de um modo geral, são compatíveis com a recém sancionada Lei Geral de Proteção de Dados.

No entanto, constatou-se, também, a inatividade dos órgãos que deveriam realizar a fiscalização do CAPEM, o que inviabiliza a proteção à privacidade dos indivíduos, que continuam sendo importunados por *e-mails* comerciais abusivos. Assim, para aperfeiçoar e tornar efetiva essa regulação, elaborou-se uma proposta de regulação responsiva da prática de *e-mail marketing* no Brasil, a partir da aplicação dos princípios responsivos, que orientam a atuação do regulador.

A LGPD previa a Autoridade Nacional de Proteção de Dados como responsável pela fiscalização e expedição de normas complementares para proteção de dados, que, eventualmente, será criada por projeto de lei de iniciativa do Poder Executivo. Com isso, a partir da análise dos atributos das autoridades de proteção de dados estrangeiras e dos artigos vetados que previam as suas atribuições, observou-se que a futura ANPD deverá assumir uma postura que se adequa à teoria da regulação responsiva.

Definiu-se, pois, a futura ANPD como reguladora da proposta de regulação responsiva de *e-mail marketing* no Brasil. Após, com a aplicação dos princípios responsivos, recomendou-se a utilização de uma pirâmide de estratégias regulatórias com uma rede de parceiros para auxiliar na fiscalização e efetivação do desenho regulatório. Além disso, aconselhou-se a utilização de uma pirâmide de sanções, a serem aplicadas de forma proporcional à infração do regulado, mas sempre iniciando com diálogo.

Concluiu-se que a teoria da regulação responsiva, ao incentivar a cooperação entre o regulador e os regulados, pode fazer com que as empresas e indivíduos que realizam *e-mail marketing* no Brasil tornem-se responsáveis ativos pela execução dessa prática em conformidade com o CAPEM e a LGPD.

Este trabalho também deverá servir de estímulo à construção de uma ANPD que regule de forma cooperativa para garantir a privacidade e proteção de dados dos cidadãos brasileiros, seguindo os atributos das autoridades de proteção de dados estrangeiras eficazes, que procuram tratar seus regulados como parceiros, ao invés de adversários.

REFERÊNCIAS

AGÊNCIA SENADO. **Sancionada com vetos lei geral de proteção de dados pessoais**, 15 ago. 2018. Disponível em: <https://www12.senado.leg.br/noticias/materias/2018/08/15/sancionada-com-vetos-lei-geral-de-protecao-de-dados-pessoais/#conteudoPrincipal>. Acesso em: 20 ago. 2018.

AKERLOF, G. A.; SHILLER, R. J. **Pescando tolos:** a economia da manipulação e fraude. Rio de Janeiro: Alta Books, 2016. 320 p.

ALLEN, A.. Protecting One's Own Privacy in a Big Data Economy. **Harvard Law Review Forum**, 130, 2016. pp. 71-78.

ARANHA, M. I. **Manual de Direito Regulatório:** Fundamentos de Direito Regulatório. 4ª. ed. Laccademia Publishing, 2018. 190 p.

ARTICLE 29 WORKING PARTY. **Opinion 5/2004 on unsolicited communications for marketing purposes under Article 13 of Directive 2002/58/EC**, 2004. Disponível em: <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp90_en.pdf>. Acesso em: 11 jun. 2018.

ARTICLE 29 WORKING PARTY. **Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC)**, 2016. Disponível em: <https://iapp.org/resources/article/all-of-the-article-29-working-party-guidelines-opinions-and-documents/>. Acesso em: 20 jun. 2018.

ARTICLE 29 WORKING PARTY. **Guidelines on consent under Regulation 2016/679**, 2018. Disponível em: <http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051>. Acesso em: 06 maio 2018.

AYRES, I.; BRAITHWAITE, J. **Responsive Regulation:** transcending the deregulation debate. 1ª. ed. New York: Oxford University Press, 1992.

BRAITHWAITE, J. Responsive Regulation and Developing Economies. **World Development**, v. 34, n. 5, mai. 2006. pp. 884-898.

BRAITHWAITE, J. The essence of responsive regulation. **UBC Law Review**, 44, 2011. pp. 475-520.

BRASIL. **A proteção de dados pessoais na relação de consumo:** para além da informação creditícia. Brasília: SDE/DPDC, 2010.

CASTELLANO, A. C. H. C. **Privacidade e proteção de dados eletrônicos**: uma análise jurídico-regulatória do marco civil da internet sob a perspectiva das teorias da regulação do ciberespaço de Lessig e Murray. Trabalho de Conclusão de Curso (graduação em Direito) - Faculdade de Direito, Universidade de Brasília, Brasília, 2016.

CERT.BR. **Cartilha de Segurança para Internet, versão 4.0**. 2ª. ed. São Paulo: Comitê Gestor da Internet no Brasil, 2012.

CNIL. **Data protection around the world**, 18 mai. 2018. Disponível em: <https://www.cnil.fr/en/data-protection-around-the-world>. Acesso em: 22 set. 2018.

DATTA, A.; TSCHANTZ, M. C.; DATTA, A. Automated experiments on ad privacy settings: a tale of opacity, choice, and discrimination. **Proceedings on Privacy Enhancing Technologies**, v. 1, p. 92-112, 2015.

DONEDA, D. **Da Privacidade à Proteção de Dados Pessoais**. Rio de Janeiro: Renovar, 2006.

DONOVAN, C. Implementation of the e-Privacy Directive in the UK: understanding the new rules. **Computer Law & Security Report**, 20, n. 2, 2004. 127-132.

EUROPEAN COMMISSION. **Synopsis report of the public consultation on the evaluation and review of the ePrivacy Directive**, European Union, 2016. Disponível em:

<https://ec.europa.eu/digital-single-market/en/news/full-report-public-consultation-eprivacy-directive>. Acesso em: 20 jun. 2018.

FEDERAL TRADE COMMISSION. **FTC Publishes Inflation-Adjusted Civil Penalty Amounts**, 23 jan. 2018. Disponível em: <https://www.ftc.gov/news-events/press-releases/2018/01/ftc-publishes-inflation-adjusted-civil-penalty-amounts>. Acesso em: 20 mai. 2018.

FORD, A. **CAN-SPAM Rule Review, 16 C.F.R. Part 316, Project No. R711010**. University of New Hampshire. p. 14. 2017.

FRAZÃO, A. Big data e concorrência: principais impactos sobre a análise concorrencial (Parte 1). **Jota**, 2017. Disponivel em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/big-data-e-impactos-sobre-a-analise-concorrencial-29112017>. Acesso em: 28 abr. 2018.

HOEPERS, C.; STEDING-JESSEN, K. **Gerência de Porta 25: motivação, importância da adoção para o combate ao spam e discussões no Brasil e no mundo**. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) e Núcleo de Informação e Coordenação do Ponto BR (NIC.br). pp. 1-7. 2009.

HOEPERS, C.; STEDING-JESSEN, K.; KUHL JR, R. **Proposta da Comissão de Trabalho Anti-Spam do Comitê Gestor da Internet no Brasil: Tecnologias e Políticas para Combate ao Spam**. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) e Núcleo de Informação e Coordenação do Ponto BR (NIC.br). pp. 1-9. 2008.

HOFF, P. M. G. **Tratado de Oncologia**. São Paulo: Editora Atheneu, 2013.

INAI. **Premio de Innovación y Buenas Prácticas en la Protección de Datos Personales**, 2018. Disponível em: <https://premioinnovacionpdp.inai.org.mx/Pages/Bienvenida.aspx>. Acesso em: 16 out. 2018.

KUBOTA, T. Deep learning algorithm does as well as dermatologists in identifying skin cancer. **Stanford News**, Janeiro 2017. Disponível em:

<https://news.stanford.edu/2017/01/25/artificial-intelligence-used-identify-skin-cancer/>. Acesso em: 15 maio 2018.

KUMAR, V.; ZHANG, X.; LUO, A. Modeling Customer Opt-In and Opt-Out in a Permission-Based Marketing Context. **Journal of Marketing Research**, vol. LI, Agosto 2014. pp. 403-419.

LEMOS, A. N. L. E. O Judiciário como Ator Regulador da Internet: seu papel no esquema de forças do Estado moderno. **Revista de Direito Setorial e Regulatório**, Brasília, v. 4, n. 1, mai. 2018. pp. 169-188.

LOPES, O. D. A. **Fundamentos da Regulação**. Rio de Janeiro: Editora Processo, 2018. 345 p.

LORENTZ, D. The Effectiveness of Litigation under the CAN-SPAM Act. **The Review of Litigation**, Vol. 30, n. 3, Primavera 2011. pp. 559-605.

MAGGS, P. B. Abusive Advertising on the Internet (SPAM) Under United States Law. **The American Journal of Comparative Law**, Vol. 54, Outono 2006. pp. 385-394.

MCGEVERAN, W. Friending the Privacy Regulators. **Arizona Law Review**, Vol. 58, 2016. pp. 959-1025.

MENDES, L. S. **Privacidade, proteção de dados e defesa do consumidor:** linhas gerais de um novo direito fundamental. Brasília: Saraiva, 2014.

MENDES, L. S. A vulnerabilidade do consumidor quanto ao tratamento de dados pessoais. **Revista de Direito do Consumidor**, v. 102, Novembro-Dezembro 2015. pp. 19-43.

MENDES, L. S.; DONEDA, D. Marco jurídico para a cidadania digital: uma análise do Projeto de Lei 5.276/2016. **Revista de Direito Civil Contemporâneo**, v. 9, Outubro-Dezembro 2016. 35-48.

MENDES, L. S.; DONEDA, D. Lei de proteção de dados não pode morrer na praia. **Folha de S. Paulo**, 20 jul. 2018. Disponível em: <https://www1.folha.uol.com.br/opiniao/2018/07/laura-schertel-mendes-e-danilo-doneda-lei-de-protecao-de-dados-nao-pode-morrer-na-praia.shtml>. Acesso em: 25 ago. 2018.

MUTCHLER, A. CAN-SPAM versus the European Union E-Privacy Directive: Does Either Provide a Solution to the Problem of Spam. **Suffolk University Law Review**, Vol. 43, 2010. pp. 957-981.

NISSENBAUM, H. A Contextual Approach to Privacy Online. **Dædalus, Journal of the American Academy of Arts & Sciences**, v. 140, n. 4, Fall 2011. pp. 32-48.

NORWEGIAN CONSUMER COUNCIL. **Toyfail**: an analysis of consumer and privacy issues in three internet-connected toys, Dezembro 2016. Disponível em: <https://fil.forbrukerradet.no/wp-content/uploads/2016/12/toyfail-report-desember2016.pdf>. Acesso em: 03 mai. 2018.

O'NEIL, C. **Weapons of math destruction:** how big data increases inequality and threatens democracy. 1ª. ed. New York: Crown Publishers, 2016.

PADRON, J. **O PL 53/2018 de proteção de dados pessoais e seu impacto sobre o email marketing**, 2018. Disponivel em: <https://templateria.com/blog/boas-praticas/pl-53-2018-e-email-marketing/>. Acesso em: 10 out. 2018.

PANIGRAHI, A. E-Marketing: leading edge for booming business world wide. **Journal of Management Research and Analysis**, v. 3, n. 3, Julho-Setembro 2016. pp. 131-135.

PASCOAL, H. **Regulamentação de e-mail marketing:** o que você precisa saber!, 05 out. 2018. Disponível em: <https://blog.e-goi.com.br/regulamentacao-email-marketing-o-que-precisa-saber/#Lei_sobre_protecao_de_dados_pessoais>. Acesso em: 10 out. 2018.

RAO, J. M.; REILEY, D. H. The Economics of Spam. **The Journal of Economic Perspectives**, vol. 26, n. 3, Summer 2012. pp. 87-110.

REGISTRO.BR. **Contrato para registro de nome de domínio sob o ".br"**, 16 set. 2011. Disponível em: <https://registro.br/dominio/contrato.html>. Acesso em: 17 ago. 2018.

RIZZARDO, A. **Contratos**. 15. ed. Rio de Janeiro: Forense, 2015.

RODOTÀ, S. **A vida na sociedade da vigilância:** a privacidade hoje. Rio de Janeiro: Renovar, 2008.

SAFARI, B. A. Intangible privacy rights: how europe's GDPR will set a new global standart for personal data protection. **Seton Hall Law Review**, Vol. 47, 2017. pp. 809-848.

SENACON. **Balanço Consumidor.gov.br 2017**, 2018. Disponível em: <https://www.consumidor.gov.br/pages/publicacao/externo/>. Acesso em: 12 out. 2018.

SOLOVE, D. J. Privacy self-management and the consent dilema. **Harvard Law Review**, v. 126, 2013. pp. 1880-1903.

SYMANTEC. **Internet Security Threat Report**. v. 23, 2018.

TANENBAUM, A. S.; WETHERALL, D. **Rede de Computadores**. Tradução de Daniel Vieira. São Paulo: Pearson Prentice Hall, 2011. p. 583 p.

TIME.LEX; SPARK. ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation. **European Union**, 2015.

U.S. CHAMBER OF COMMERCE; HUNTON & WILLIAMS LLP. **Seeking Solutions: Attributes of Effective Data Protection Authorities**. U.S. Chamber of Commerce. p. 1 - 40. 2017.

VOSS, W. G. First the GDPR, now the proposed ePrivacy Regulation. **Journal of Internet Law**, Vol. 21, n. 1, jul. 2017. pp. 03-11.