DOI: http://dx.doi.org/10.14295/revistadaesmesc.v26i32.p363

DIREITO À PRIVACIDADE NA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

RIGHT TO PRIVACY IN THE GENERAL LAW ON THE PROTECTION OF PERSONAL DATA

Gisele Primo Carvalho [1]

Tainá Fernanda Pedrini [2]

Resumo: O direito à privacidade, previsto no art. 5°, inciso X, da Constituição da República Federativa do Brasil de 1988 (CRFB/88) é constitucionalmente assegurado a todos, em decorrência da universalidade dos direitos fundamentais, a qual assegura, sob a perspectiva informacional, ao indivíduo o controle de suas próprias informações pessoais. Nesse sentido, pesquisa-se o núcleo essencial desse direito para, posteriormente, compreender as implicações jurídicas advindas a partir da promulgação de legislações infraconstitucionais, em especial, a Lei n. 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD) e o Marco Civil da Internet, Lei n. 12.737/14. Por conseguinte, explanam-se as disposições legais da LGPD, as quais têm por finalidade a proteção do usuário nas relações que envolvem a disponibilização de dados pessoais, inclusive, os dados considerados sensíveis. Por fim, averiguam-se pontos vulneráveis da LGPD, notadamente, no que diz respeito aos vetos presidenciais. Nesse viés, conclui-se que, com a promulgação da referida lei, o direito à privacidade, principalmente, no que se refere à proteção de dados pessoais, recebeu amparo jurídico específico, entretanto, ainda assim, vislumbra-se necessidade de complementá-la, na medida em que, são identificados alguns impasses jurídicos na implementação efetiva das disposições legais, em especial, a previsibilidade da Autoridade Nacional de Proteção de Dados Pessoais, bem como a tipificação de penalidades mais severas. O método utilizado foi o indutivo.

1 Acadêmica do Curso de Direito da Universidade do Vale do Itajaí (Univali), atualmente é estagiária no Tribunal de Justiça de Santa Catarina, comarca de Camboriú. E-mail: giisele_carvalho@hotmail.com

2 Assessora Jurídica. Mestranda em Ciência Jurídica pela Widener University, Delaware Law School e pela Univali. Pós-graduanda em Direito Tributário pelo Instituto Brasileiro de Estudos Tributários (IBET) e em Direito Registral de Notarial pela Faculdade Damásio. Membro da Rede para o Constitucionalismo Democrático Latino-Americano. Advogada licenciada. E-mail: tainapedrini@live.com

Palavras-chave: Direito à privacidade. Proteção de dados pessoais. Banco de dados.

Abstract: The right to privacy provided in article 5, X, of the Constitution of the Federative Republic of Brazil is constitutionally guaranteed to all, as a result of the universality of fundamental rights, which ensures, from the information perspective, the individual's control of their own personal information. In this sense, the essential nucleus of this right is investigated in order to later understand the legal implications arising from the promulgation of infraconstitutional legislations, especially ACT n. 13.709/2018, known as the general law on Data Protection (LGPD) and the Internet Civil Law, ACT n. 12.737/14. Therefore, the legal provisions of the LGPD are explained, whose purpose is to protect the user in the relationships that involve the provision of personal data, including data considered sensitive. Lastly, LGPD vulnerabilities are being investigated, notably with regard to presidential vetoes. In this bias, it is possible concluded that, with the promulgation of said law, the right to privacy, especially regarding the protection of personal data, received specific legal protection, however, there is still a need to complement it, insofar as some legal impasses are identified in the effective implementation of legal provisions, in particular, the predictability of the national authority for the Protection of Personal Data, as well as the definition of more hard penalties. To the elaborate this work the method inductive was used.

Keywords: Right to Privacy. Protection of Personal Data. Database.

1. INTRODUÇÃO

Vive-se, atualmente, a influência das tecnologias nas relações jurídicas entre empresa e consumidor/usuário. Como consequência dela, eles são cercadosde mecanismos de armazenamento do conteúdo produzido ou fornecido, denominado Banco de Dados, que pode ser definido como"uma coleção de dados inter-relacionados, representando informações sobre um domínio específico" (KORTH; SILBERSCHATZ, 1994).

Aliado a isso, também, vislumbra-se a desproteção dessas informações repassadas, na medida em que, anteriormente ao ano de 2018, não havia promulgação de legislação protecionista específica.

Sob a influência internacional europeia, do Regulamento Geral de Banco de Dados Pessoais (GDPR), foi promulgada, no Brasil, a Lei n. 13.709/18, conhecida como Lei Geral de

Proteção de Dados (LGPD). Trata-se do marco regulatório da proteção de dados pessoais no país, nas relações entre usuário e o setor público e/ou privado, consubstanciada em princípios fundamentais de liberdade, livre desenvolvimento da personalidade e privacidade (BRASIL, 2018).

Na mesma linha, assegurava-se, abstratamente, no art. 5º, inciso X, da Constituição da República Federativa do Brasil de 1988 (CRFB/88), o direito constitucional à privacidade que, para a presente pesquisa, pode ser compreendido como a "pretensão do indivíduo de não ser foco da observação por terceiros, de não ter os seus assuntos, informações pessoais e características particulares expostas a terceiros ou ao público em geral" (MENDES, 2012, p. 321).

A par disso, analisa-se a vulnerabilidade da privacidade dos indivíduos, ante a globalização e os avanços dos meios comunicacionais, como a *internet* e, por conseguinte, estuda-se a legislação específica sobre a proteção de dados pessoais no Ordenamento Jurídico Brasileiro.

Outrossim, destaca-se a relevância da pesquisa em razão das mudanças tecnológicas e globalizadas, que ocasionam a desproteção de direitos fundamentais, de tal forma que é relevante ao público em geral a busca incessante pelo conhecimento e pela proteção dos direitos constitucionais e infraconstitucionais, inclusive, em ambientes virtuais

Quanto à metodologia empregada na fase de investigação, utilizou-se o método indutivo. Acionou-se as técnicas do referente, que é a "explicitação prévia do(s) motivo(s), do(s) objetivo(s) e do produto desejado, delimitando o alcance temático e de abordagem para a atividade intelectual, especialmente para uma pesquisa" (PASOLD, 2008, p. 54); da categoria, considerando como sendo a "palavra ou expressão estratégica à elaboração e/ou à expressão de uma ideia." (PASOLD, 2008,

p. 25); do conceito operacional, que pode ser descrito como "uma definição para uma palavra ou expressão, com o desejo de que tal definição seja aceita para os efeitos das ideias que expomos" (PASOLD, 2008, p. 37) e da pesquisa bibliográfica.

2. IMPLICAÇÕES JURÍDICAS DO DIREITO À PRIVACIDADE NO AMBIENTE TECNOLÓGICO E INFORMACIONAL DE COMUNICAÇÕES

São indiscutíveis as facilidades surgidas e aperfeiçoadas por meio da "Era Tecnológica". Constata-se tal observação com a mudança cotidiana da vida em Sociedade. A exemplo, o uso celulares, "*notebooks*", *"tabletes*" e outros "*hardwares*" e a agilidade trazida com a utilização desses bens, bem como a fluidez com que os dados se dissipam em larga escala.

Nessa celeuma, há dupla perspectiva no tocante à multiplicidade de instrumentos tecnológicos: a primeira se refere aos anseios por notícias e, portanto, vive-se em uma era de muitas vias comunicacionais – como, também, viabiliza-se a formação do conhecimento, razão pela qual a tecnologia minimiza as barreiras temporais e espaciais, colaborando para que o conteúdo chegue de modo imediato e expansivo aos usuários.

Em contrapartida, em segunda perspectiva, observa-se grande volume de informações a que se têm acesso pelas mídias – "*smartphones*", *internet*, televisão, redes sociais – o que, muitas vezes, não permite análises críticas e apuradas de seu teor, não sendo incomum, por exemplo, a divulgação de "*fake-news*", notícias falsas, em tradução livre.

Para além disso, nas novas mídias, forma-se espaço aberto e democrático, já que a divulgação de conteúdo não é prerrogativa de uns, mas é possibilitada a todos os seus usuários. Ou seja, somos destinatários e, ao mesmo tempo, formadores e

veiculadores de opiniões. Assim, apesar dos benefícios surgidos e aperfeiçoados por meio do ambiente tecnológico, está-se, também, constantemente, exposto à possibilidade de ferir direitos constitucionais.

No que se refere ao direito à privacidade, observa-se que, este pertence ao gênero denominado direitos fundamentais e encontra-se respaldado juridicamente na CRFB/88, no art. 5°, inciso X, "*in verbis*": "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" (BRASIL, 2018). À luz da sistemática constitucional, garante-se não apenas o direito material à intimidade, à vida privada e à honra, colorados do direito à privacidade, mas também à devida proteção em decorrência de eventuais violações morais ou materiais.

Destaca-se, segundo Moraes (2002, p. 60), que "o direito à vida privada, à intimidade, à honra, à imagem dentre outros, aparecem como consequência imediata da consagração da dignidade da pessoa humana como fundamento da República Federativa do Brasil". Isso porque, é princípio estruturante, consagrado no art. 1º, inciso III, da CRFB/88, que envolve a tutela protecionista dos direitos fundamentais, principalmente, por irradiar seus efeitos a todas as cláusulas constitucionais, incluindo, o direito à privacidade, inerente à individualidade do ser humano.

Nessa celeuma, cabe mencionar o conceito trazido por José Afonso da Silva (2009, p. 206) que compreende o direto à privacidade como "conjunto de informações acerca do indivíduo que ele pode decidir manter sob seu exclusivo controle, ou comunicar, decidindo a quem, quando, onde e em que condições, sem a isso poder ser legalmente sujeito".

Nesse viés, percebe-se que o direito à privacidade protege os dados pessoais pertinentes ao seu detentor, o qual possui

discricionariedade em mantê-los sob seu domínio ou, se preferir, expô-los, podendo impor limites e condições, em todo caso, observados os ditames do Ordenamento Jurídico a que se submete. Nesse relatório de pesquisa, pretende-se, na verdade, analisar os moldes dados pela Fontes Jurídicas brasileiras, segundo o qual pode ser compreendido como sendo "os Textos Normativos elaborados pela autoridade competente (legislação e precedentes, conforme a vinculação ao *civil law* ou ao *commomlaw*), salvo autorização normativa expressa para o acesso a outros elementos (como os princípios gerais do Direito, a doutrina e aos costumes), visando à heterointegração" (ZANON JÚNIOR, 2016, p. 3).

Entende Branco e Mendes (2012, p. 320) que *"*no âmago do direito à privacidade está o controle de informações sobre si mesmo". Assim, o núcleo básico do direito à privacidade consiste em um controle de informações a respeito de seu próprio ser. Sabe-se que, segundo Silva (2009, p. 206), a inviolabilidade desse direito, não está restrita, apenas, ao aspecto íntimo do indivíduo, mas, também, a outros segmentos da vida do ser humano, tais como as esferas sociais, profissionais, comerciais.

Importante pôr em destaque que, atualmente, o direito à privacidade vem ganhando novos contornos e significados, correspondendo ao, consoante as palavras de Paesani (2014, p. 43), "direito reconhecido ao indivíduo de exercer o controle sobre o uso dos próprios dados pessoais inseridos num arquivo eletrônico".

Assim, segundo esse pensamento, é possível realizar o corte epistemológico da pesquisa na inviolabilidade do direito à privacidade, que é comumente utilizada nos dias atuais, qual seja, o ambiente virtual. Isso porque, conforme ensina Diniz (2008, p. 157) o "direito à privacidade da pessoa (CF, art. 5º, X; CC, art. 21) contém interesses jurídicos, de sorte que o sujeito de direito pode impedir intromissões em sua esfera privada ou íntima (CF, art. 5º, XI), inclusive via *internet*".

Nesse diapasão, frisam-se aspectos referentes à publicidade, sob o ponto de vista jurídico, os quais se encontram positivados na CRFB/88, em vários momentos, notadamente, vinculado ao Poder Público, como forma de garantir a transparência dos atos governamentais (art. 37, *caput e* art.37,§ 1º), bem como, aos processos judiciais (art. 5°, inciso LX). Conquanto, para a presente pesquisa, realiza-se o corte epistemológico na violação gerada por meio da publicização de dados de caráter pessoal.

À evidência disso, passa-se à análise de exemplos mencionados por Diniz (2008, p. 158), em que se mostra explicitamente presente a violação à privacidade nos meios virtuais e informáticos:

> [...] coleta de informações pelos inadmissíveis *cookies*; uso de [...] meios eletrônicos para obrigar alguém a revelar fatos de sua vida particular ou segredo profissional; utilização de *software* para espionar quem transmite na *web* [...] invasão não autorizada a um sistema de computadores (*hacking*); espionagem em *site* ou *e-mail* por *crakers* para violar a intimidade ou descobrir segredo [...] com ânimo de prejudica ou causar dano; intrusão informática, por meio de programa-espião *trojan horse*, que, criando um *backdoor*, se instala, furtivamente, no computador do usuário, abrindo portas em seu micro, possibilitando roubo de arquivos, senhas etc. e utilização de *spywares*, programas espiões que enviam informações do computador do usuário da rede para desconhecidos [...]; instalação de *sniffers*, programas que, escondidos no *sites*, rastreiam informações sobre internautas como o endereço e o programa de navegação por eles empregado, visando, p. ex., pesquisar hábitos dos consumidores [...] (3º T. do TST da 3º R. – AIRR 1926/2003-044-03.40.6) [...]

Infere-se do exposto que são diversos os modos de transgressão à privacidade de dados em plataformas de comunicação, como a *internet* ou semelhantes, principalmente, quando são capturadas e/ou vendidas por outrem, sem a comunicação e autorização prévia, ocasionando, com isso, a violação à liberdade de autodeterminação do indivíduo acerca de seus próprios dados.

Forçoso perceber que a informação disponibilizada em banco de dados está migrando para outro patamar, qual seja, "*status* de mercadoria", e não, tão somente, ao uso restritivo daquele que a possui para fins comerciais ou não, pois em muitos casos a inviolabilidade consiste na comercialização desse conteúdo a terceiros, tema que será debatido posteriormente (FIORILLO, 2013, p. 45).

2.1. Vulnerabilidade do direito à privacidade no ambiente digital

Desde muito tempo, o ser humano percebeu a necessidade de armazenar informações em um suporte. Em primeiro momento, utilizou-se de estruturas físicas como papiro, papel e similares. Com a evolução científica e tecnológica, tornou-se viável a criação de materiais lógicos, tais como "*softwares*", incluindo, nesse gênero, a espécie Banco de Dados "*online*".

Essa criação, aliada à utilização de "*hardwares*", a exemplo, o uso de computadores, possibilitou a implementação de programas específicos de Banco de Dados em empresas públicas e privadas com a finalidade de agrupar de informações que dizem respeito ao mesmo assunto, a exemplo, dados comerciais, colaborando, por conseguinte, com a diminuição de armazéns e depósitos físicos (DEVMEDIA, 2018).

Trata-se, certamente, de melhora significativa em diversos sentidos: econômico, financeiro, tecnológico, logístico, entre outros, no entanto, do ponto de vista jurídico, tal realização pode implicar na possibilidade de violação a direitos fundamentais, mediante várias formas, dentre as quais se destacam, a comercialização e o repasse clandestino de informações pessoais dispostas nesses Bancos de Dados.

Observa-se, ademais, que esses instrumentos estão cada vez mais evoluídos e sofisticados, o que contribui para a vulnerabi-

lidade do direito à privacidade, já que esse pode ser violado, até mesmo, por longas distâncias, mediante o uso de aparelhos e instrumentos altamente tecnológicos (PAESANI, 2014, p. 37).

Além do mais, o próprio ato de ter acesso a informações sigilosas e pessoais e usá-las para fins diversos, sem o prévio consentimento, já caracterizaria o risco à violabilidade da privacidade e a configuração de prática abusiva, pois, consoante a autodeterminação informativa, ao detentor da informação é dado o direito de ter a ciência de quais os locais, sejam estes físicos ou não, tramitam seus dados.

Outrossim, considera-se comportamento agravante na segurança da informação a utilização de dados de outrem com a pretensão de divulgá-los na *internet*, sem a prévia anuência, isso porque, ao concretizar essa conduta, torna-se pública a intimidade e a privacidade, garantidos como direitos fundamentais individuais na CRFB/88.

Em face disso, sabe-se que a *internet,* como meio de comunicação, alcança um público infinitamente maior do que outros meios de transmissão de conteúdo (televisão, rádio, jornal, revista, por exemplo), podendo, com isso, gerar maiores e imensuráveis danos àqueles que têm seus dados pessoais vazados, capturados, transmitidos ou acessados por terceiros não autorizados.

Há de se observar que é comum o ato de um usuário disponibilizar suas informações, a saber, perante a contratação de determinados serviços. Todavia, não se deve confundir esse comportamento com o repasse clandestino, o que é defeso, pois, além de ferir disposições constitucionais, torna o usuário plenamente vulnerável a ações de pessoas físicas ou jurídicas más intencionadas a diversos propósitos.

Nessa oportunidade, para ilustrar os pontos expostos até o presente momento, apresenta-se um caso notório, ocorrido

em 2014, em que a empresa de telefonia OI (TNL PCS S/A OI), por meio do serviço de banda larga Velox, violava direitos fundamentais, em especial, a privacidade, a informação, a neutralidade de rede (BRASIL, 2014).

A ação da empresa consistia em monitorar o tráfego de dados dos usuários da *internet*, criando seu perfil de navegação. Além disso, para este feito foi desenvolvido um software específico em parceria com a empresa britânica "*Phorm*" e, então, essas informações eram repassadas e comercializadas com anunciantes, agências de publicidades e outros portais da *internet* (BRASIL, 2014).

Quanto à fundamentação jurídica atrelada à condenação, observa-se que a Empresa OI violava direitos relativos à informação, à proteção contra a publicidade enganosa, à privacidade e à intimidade do consumidor, mediante práticas abusivas e violações aos princípios de boa-fé e princípios fundamentais do Comitê Gestor da Internet no Brasil, bem como, do Marco Civil da Internet, tais como, neutralidade de rede, padronização e outros. (MAIN, 2015). Por consequência disso, foi autua pelo Departamento de Proteção e Defesa do Consumidor (DPDC), que a multou em um montante de 3,5 milhões (BRASIL, 2014).

2.2. Legislação especial sobre a proteção de dados pessoais no Brasil

A Lei n. 12.737, conhecida como Marco Civil da Internet, promulgada pela Presidência da República em 23 de abril de 2014, de modo geral, regulamenta o uso da *internet* no Brasil e estabelece princípios, garantias, direitos e deveres, bem como, determina diretrizes para a atuação dos entes federativos no país em relação à matéria (BRASIL, 2014).

Observa-se que, a partir desse marco, houve significativo avanço legislativo, no tocante à edição de leis específicas sobre

a regulamentação do ambiente virtual no Brasil, uma vez que o tema foi alvo de reclamações da Sociedade no ano de 2009, que repudiava as iniciativas de criminalização, sem a prévia positivação de direitos garantidos aos internautas na plataforma virtual, ou seja, defendiam que para que houvesse a punição criminal dos agentes que cometiam algum ato contrário à privacidade, à vida privada e à intimidade no ambiente digital era necessário a previsão legal para tanto.

Todavia, ainda, encontram-se muitos percalços na regulamentação e na solução de problemas decorrentes do ambiente digital, inclusive, na proteção de dados pessoais. Isso porque comportamentos informáticos mediante o uso de *"drive"* ou *"driver"*, assim considerados respectivamente a parte física "*hardware*" e lógica "*software*" deveriam ser considerados condutas ensejadoras de análise da legislação penal e não meramente as técnicas ou instrumentos utilizados no comportamento criminoso, como comumente é tipificado nas normas penais (JESUS; MILAGRE, 2016, p. 168-169).

Deve-se, portanto, fazer análise com a finalidade de averiguar se "as técnicas empregadas estão ou não contidas no comportamento". Assim, conforme os referidos autores, a tipificação de condutas criminosas seria mais ampla. Entretanto, mais importante do que tipificar e punir, é, sem dúvidas, criar mecanismos preventivos, principalmente quando violados direitos e garantias fundamentais (JESUS; MILAGRE, 2016, p. 168-169).

Isso porque, o ambiente digital está ganhando novos contornos e melhorias contínuas, o que leva a pensar na dificuldade legislativa de acompanhar esse movimento, a saber, o processo legislativo é mais demorado do que os avanços tecnológicos. Por essa perspectiva, os princípios são fundamentais para acompanhar e abranger a maior possibilidade de casos possíveis, a fim de determinadas situações serem abrangidas pela proteção legislativa e jurídica.

Nesse sentido, no que se refere à proteção dos usuários nesse ambiente, é imprescindível a observância conjunta e sistemática dos princípios fundamentais contidos no Marco Civil da Internet para analisá-los sob a égide da Lei n. 13.709/18 – Lei de Proteção de Dados (LGPD). Pode-se, à vista disso, mencionar três princípios fundamentais voltados à proteção do usuário na *internet*, a saber, neutralidade de rede, liberdade de expressão e privacidade.

Em primeiro lugar, tem-se o princípio da neutralidade da rede, que pode ser compreendido como um reforço às diretrizes do direito do consumidor, pois suas bases estão contidas na proibição de cobrança diferenciada em razão dos serviços e páginas acessadas pelo usuário, devendo o provedor de conexão de rede cobrar apenas pela velocidade da *internet*, colaborando para se ter uma rede neutra, os seja, todos os sites possuem a mesma velocidade e, por isso, o usuário que delimita por quais deseja navegar (CRUZ, 2018).

O segundo princípio é liberdade de expressão, que garante o direito de difusão de informações e opiniões na rede, garantido que conteúdos publicados sejam apenas retirados por expressa anuência do autor ou, a depender do caso, mediante ordem judicial. Além disso, em decorrência desse princípio, assegura-se que provedores e serviços não sejam responsabilizados pelas publicações dos usuários (CRUZ, 2018).

O terceiro, e igualmente importante, é o princípio da privacidade, razão pela qual é proibido aos provedores e *"sites"* o uso dos dados dos usuários com finalidade comercial, devendo manter sob guarda essas informações pelo prazo mínimo de 06 (seis) meses, inclusive, esse comando deve ser cumprido, quando empresas estrangeiras se submetem às leis brasileiras (CRUZ, 2018).

Evidencia-se que, no viés de proteção do usuário perante

o ambiente virtual, deve-se considerar os preceitos principiológicos e diretrizes do Marco Civil da Internet, uma vez que são verdadeiras conquistas dos internautas frente ao mundo tecnológico. Entretanto, há, ainda, outro comando legislativo que deve ser igualmente observado, trata-se, pois, da LGPD, que trata detalhadamente e especificamente da proteção dos usuários, quando suas informações estão dispostas em banco de dados públicos ou privados.

Adverte-se, no entanto, consoante descreve Pinheiro (2018, p. 19), que antes LGPD havia a presença de algumas leis esparsas no Brasil, em especial, a Lei n. 12.737/12 (BRASIL, 2012), anteriormente já mencionada, e a Lei n. 12.414/11 (BRASIL, 2011). Porém, a questão da proteção de dados pessoais era confusa, quanto aos critérios de averiguação do atendimento de padrões de segurança condizentes.

Com efeito, outro ponto a ser analisado, é que a LGPD regulamenta o uso, a proteção e a transferência de informações pessoais e dados sensíveis, que conforme o art. 5º, inciso II, da LGPD, estes correspondem a elementos como "origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural", garantido, com isso, maior controle dos cidadãos acerca de suas próprias informações (BRASIL, 2018).

Para tanto é exigido, segundo os termos desse instrumento normativo, o consentimento expresso para fins de coleta e de uso dos dados, bem como possibilita, caso necessário, a visualização, a correção e a exclusão por parte do legítimo proprietário do conteúdo (BRASIL, 2018).

Ocorre que, a referida lei brasileira de proteção de dados pessoais passou por influências do Regulamento Geral de

Proteção de Dados Pessoais Europeu n. 679 (GDPR), que foi aprovado em 27 de abril de 2016, mas que somente entrou em vigor, inclusive, com aplicações das penalidades, a partir de 25 de maio de 2018 (PINHEIRO, 2018, p. 18).

Em âmbito nacional, o projeto de lei n. 53/2018 tramitava no Congresso Nacional para, posteriormente, ser submetido à sanção presidencial, o qual na visão do Instituto Brasileiro de Defesa do Consumidor (IDEC) poderia ser ratificado integralmente por estar em conformidade com os direitos de proteção ao consumidor, fortalecendo o sistema de proteção de direitos coletivos (IDEC, 2018).

É de se considerar que, com a promulgação, em agosto de 2018, da Lei n. 13.709/18 houve, sem dúvidas, o preenchimento de uma das lacunas existentes na proteção dos usuários no ambiente tecnológico e informatizado, especialmente, na definição objetiva de padrões e normatizações acerca, por exemplo, de atributos quantitativos da proteção dos dados pessoais (PINHEIRO, 2018, p. 19).

Outrossim, a LGPD, em comparação com a GDPR, é menos extensiva, quanto ao conteúdo, o que contribuiu para a maior margem de interpretação, uma vez que existem "alguns pontos de insegurança jurídica por permitir espaço para a subjetividade onde deveria ter sido mais assertiva". Exemplificando disso, é que enquanto a GDPR prevê prazos exatos, a LGPD dispõe de "prazo razoável" (PINHEIRO, 2018, p. 22).

Vale observar que a LGPD passou por alguns vetos presidenciais, e, um dos pontos mais questionáveis, quanto aos mecanismos de efetividade, foi a retirada da criação da Autoridade Nacional de Proteção de Dados Pessoais (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, os quais seriam órgãos independentes, com a dotação de orçamentos próprios, cuja competência seria a fiscalização

do cumprimento dos termos da LGPD.

O motivo do veto dos órgãos fiscalizadores foi mencionado pelo Presidente da República, durante a cerimônia de sanção da Lei de Proteção de Dados Pessoais, em 14 de outubro de 2018, segundo o qual mencionou que havia vício de iniciativa, já que a competência para instituir autoridade deveria ter sido realizada pelo Poder Executivo e não do Poder Legislativo, conforme previa o projeto de lei (IDEC, 2018).

Nesse viés, sob a análise do IDEC, a referida lei encontra-se fragilizada em razão dos vetos presidenciais sofridos em suas cláusulas, em especial, na supressão da Autoridade de Proteção de Dados, tendo em vista a perda substancial, quanto ao conteúdo da LGPD, inviabilizando a previsão de regulamentadores com expertise e técnica, bem como a existência de estrutura administrativa capacitada para o monitoramento, a qual previa inicialmente o PL.

Assim, pode-se gerar, num primeiro momento, insegurança jurídica à aplicabilidade dos dispositivos da LGPD, posto que não há a previsão, de imediato, da fiscalização independente e específica de um órgão central com a capacidade técnica referente à nova matéria.

Nessa vereda, descreve Pinheiro (PINHEIRO, 2018, p. 22):

> O veto à criação da ANPD gera uma lacuna inicial estruturante no projeto se implementação da nova regulamentação no país, além de não permitir que o Brasil receba o reconhecimento por parte da União Europeia de legislação de mesmo nível do GDPR, pois um dos requisitos é a existência de uma autoridade nacional de fiscalização independente, o que pode não apenas dificultar a aplicação e fiscalização das medidas propostas, mas também criar um entrave nas relações comerciais para o Brasil.

Com efeito, acertadamente, foi editada, em 28 de dezembro de 2018, a Medida Provisória nº 869/2018 (BRASIL, 2019),

que instituiu a criação da Autoridade Nacional de Proteção de Dados, uma vez que, de acordo com Lemos, caso não houvesse a devida edição poderia acarretar juridicamente a insegurança, quanto aos meios de fiscalização do cumprimento das disposições da LGPD, como também, futuramente, o questionamento de sua constitucionalidade perante o Supremo Tribunal Federal (LEMOS, 2019).

Além disso, vetou-se, o art. 28 da referida lei, que previa a necessidade de publicidade de práticas de compartilhamento de informações pessoais aos cidadãos por parte do Poder Público, quando se utiliza a Lei de Acesso à Informação.

Sobre isso, aponta Rafael Zanatta (IDEC, 2018):

> […] O veto faz com que o Poder Público deixe de dar publicidade ao uso compartilhado de dados pessoais dentro do Estado (por exemplo, o repasse de informações do Ministério da Saúde para o Ministério do Planejamento). Na prática, torna o compartilhamento mais opaco e menos conhecido pela população […]

Ademais, quanto à previsibilidade de punições, observa-se um sistema sancionatório fragilizado, após a supressão de alguns trechos, ao momento do veto presidencial, isso porque, em comparação com a GDPR, há constante na LGPD, penas mais atenuadas, dentre as quais são se destacam a penalidade de advertência, multa, publicização da infração, bloqueio dos dados pessoais, entretanto, não consta mais a possibilidade de aplicação da pena de suspensão, por exemplo (IDEC, 2018).

Outro ponto a ser observado é que se impõe às instituições públicas ou privadas o dever de, após conclusão da relação jurídica, apagarem os registros dos usuários contidos nas plataformas de armazenamento de dados e, caso haja a continuidade do vínculo, deve-se manter a responsabilidade quanto à transparência e o controle do usuário às suas informações, ocasião em que, pode-se, a qualquer momento, acessá-las, conferi-las

ou modificá-las (BRASIL, 2018).

Por fim, constata-se que, com a edição de legislações infraconstitucionais com a finalidade de tutelar juridicamente a proteção de dados pessoais nas plataformas informatizadas e tecnológicas, houve ampliação na segurança jurídica, principalmente, por respaldar direitos como: à liberdade, à privacidade, ao livre desenvolvimento da personalidade da pessoa natural, à honra, à imagem.

Colabora-se, dessa maneira, com a previsibilidade de mais garantias específicas no tratamento e disponibilização de informações, momento em que, geram-se mais obrigações às empresas, que devem aderir aos comandos legislativos e respeitar princípios norteadores na relação empresa e usuário, sob pena de aplicação de multa.

3. CONCLUSÃO

Com a evolução tecnológica, a proteção jurídica dos dados pessoais, incluído, os dados sensíveis, tornou-se deveras relevante, na medida em que a desproteção dessas informações pode acarretar a vulnerabilidade de direitos e princípios constitucionais, perante, por exemplo, práticas como a apropriação e o repasse no ambiente digital, sem autorização do usuário.

No presente artigo científico, observou-se que as cláusulas da Lei n. 12.737/14, conhecida como Marco Civil da Internet, bem como da Lei Geral de Proteção de Dados Pessoais (LGPD) de n. 13.709/18 são promulgadas com o objetivo de proteger os internautas no ambiente digital, tendo por base as premissas do livre desenvolvido da personalidade da pessoa natural, boa-fé nas relações de tratamento de dados pessoais e cumprimento de princípios da segurança da informação.

Nesse viés, o direito à privacidade ganhou novo amparo jurídico específico, na medida em que a reunião desses instrumen-

tos normativos colaborou para tutelar os direitos e garantias de forma mais efetiva no ambiente digital e "online", posto que anteriormente não era regulamentado de forma satisfatória.

Entretanto, vislumbra-se que, mesmo após a edição da Medida Provisória nº 869/2018, que instituiu a criação da Autoridade Nacional de Proteção de Dados, a necessidade de complementação da legislação infraconstitucional, pois as disposições nacionais à proteção de dados deixam lacunas na efetividade da segurança informacional do internauta perante seus próprios dados, a exemplo, a previsibilidade de penalidades mais severas quando se descumpre os comandos dispostos na LGPD.

Enfatiza-se que o tema acerca da proteção de dados é um assunto imprescindível a ser estudado, analisado e entendido, face a Sociedade globalizada, que, constantemente, utiliza, tem acesso e usa informações pessoais nas relações, especialmente, jurídicas, deve-se, dessa forma, garantir relações traçadas na confiabilidade, integridade, com o viés de proporcionar maior segurança jurídica e respeito à autodeterminação informativa, incluindo o dever se proteger o direito à privacidade.

E, por fim, sabe-se que, quando se trata de meios para se garantir a segurança da informação e a proteção de dados pessoais, é necessário o aperfeiçoamento constante das legislações, dos instrumentos para torná-la aplicável efetivamente, bem como dos modos de conscientização dos usuários/proprietários dos seus próprios dados, sendo, portanto, um trabalho constante, tanto do Poder Público, quanto da Sociedade.

REFERÊNCIAS

BRASIL. **Constituição da República Federativa do Brasil (1988).** Brasília: Senado Federal, 1988. Disponível em: http://www.planalto.gov.br. Acesso em: 19 nov. 2018.

BRASIL. **Formação e consulta a banco de dados (lei 12.414/2011).** Brasília: Senado Federal, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 19 nov. 2018.

BRASIL. **Lei de acesso à informação (lei 12.527/2011).** Brasília: Senado Federal, 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 28 dez. 2018.

BRASIL. **Marco civil da internet (lei 12.965/2014).** Brasília: Senado Federal, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato20 11-2014/2014/lei/l12965.htm. Acesso em: 28 dez. 2018.

BRASIL. **Medida provisória nº 869/2018.** Brasília, 28 dez. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Mpv/mpv869.htm. Acesso em: 06 jan. 2019. Acesso em: 01 nov. 2018.

BRASIL. Ministério Da Justiça E Segurança Pública. **Ministério da justiça multa Oi por monitorar navegação de consumidores na internet**. Brasília, DF: Governo Federal, 2014. Disponível em: http://www.justica.gov.br/news/ministerio-da-justica-multa-oi-por-monitorar-navegacao-de-consumidores-na-internet. Acesso em: 07 maio de 2019.

BRASIL. **Proteção de dados pessoais (lei 13.709/2018).** Brasília: Senado Federal, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 21 dez. 2018.

BRASIL. **Tipificação criminal de delitos informáticos (lei 12.737/2012)**. Brasília: Senado Federal, 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 08 maio 2019.

CETIC.BR. **"Panorama setorial da internet".** Disponível em https://cetic.br/media/docs/publicacoes/6/Panorama_Setorial_11.pdf. Acesso em: 01 ago. 2018.

CORRÊA, Gustavo Testa. **Aspectos jurídicos da internet.** São Paulo: Saraiva, 2000.

CRUZ, Fundação Oswaldo. **Princípios fundamentais do marco civil da internet.** Disponível em: https://portal.fiocruz.br/documento/principios-fundamentais-do-marco-civil-da-internet. Acesso em: 17 nov. 2018.

DINIZ, Maria Helena. **Curso de direito civil brasileiro:** responsabilidade civil. 22. ed. rev. amp. atual. São Paulo: Saraiva, 2008.

FIORILLO, Celso Antonio Pacheco; CONTE, ChristianyPegorari. **Crimes no meio ambiente digital.** São Paulo: Saraiva, 2013.

IDEC.Governo sanciona lei de proteção de dados pessoais: para Idec, vetos a pontos centrais da legislação, como o de criação de uma autoridade fiscalizadora, fragiliza a norma. 2018. Disponível em: https://idec.org.br/noticia/governo-sanciona-lei-de-protecao-de-dados-pessoais. Acesso em: 28 dez. 2018.

IDEC. Posicionamento – projeto de lei de proteção de dados pessoais. 2018. Disponível em: https://idec.org.br/release/posicionamento-projeto-de-lei-de-protecao-de-dados-pessoais. Acesso em: 24 dez. 2018.

JESUS, Damásio de; MILAGRE, José Antonio. **Manual de crimes informáticos.** São Paulo: Saraiva, 2016.

KORTH, Henry F.; SILBERSCHATZ, Abraham. **Sistemas de banco de dados.** ed. 2. Makron Books, 1994.

LEMOS, Ronaldo. **A criação da autoridade nacional de proteção de dados pela MP n.**

869/2018. 2018. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/a-criacao-da-autoridade-nacional-de-protecao-de-dados-pela-mp-no-869-2018-29122018/amp. Acesso em: 06 jan. 2019.

MAIN, Lucimara Aparecida; BORGES, Camila Aparecida. Direito à privacidade e a coleta de dados pessoais palas empresas de telefonia: um desafio para a sociedade da informação. **Conpedi,** São Paulo, v. 4, n. 15, p.142-151, out. 2015. Disponível em: https://www.conpedi.org.br/publicacoes/z307l234/ep7692ah/M3N8QN2M90mF196K.pdf. Acesso em: 17 nov. 2018.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de direito constitucional.** 7. ed. rev. e atual. São Paulo: Saraiva, 2012.

MORAES, Alexandre de. **Direitos humanos fundamentais.** 4. ed. São Paulo: Jurídico, 2002.

MORGADO, Laerte Ferreira. **O cenário internacional de proteção de dados pessoais. Necessitamos de um código brasileiro?** Disponível em: http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=6336. Acesso em: 14 out. 2018.

Paesani, Liliana Minardi. **Direito e internet:** liberdade de informação, privacidade e responsabilidade civil. 7. ed. São Paulo: Atlas. 2014.

PASOLD, Cesar Luiz. **Metodologia da pesquisa jurídica:** teoria e prática. 11. ed. Florianópolis: Conceito editorial; Millennium Editora, 2018.

PINHEIRO, Patricia Peck. **Proteção de dados pessoais:** comentários à lei n. 13.709/2018 (LGPD). São Paulo: Saraiva Educação, 2018.

SANTOS, Bárbara Ferreira. **Apesar de expansão, acesso à internet no Brasil ainda é baixo.** Disponível em: https://exame.abril.com.br/brasil/apesar-de-expansao-acesso-a-internet-no-brasil-ainda-e-baixo/. Acesso em: 01 ago. 2018.

SILVA, José Afonso da. **Curso de direito constitucional positivo.** 32. ed. São Paulo: Malheiros, 2009.

ZANON JÚNIOR, Orlando Luiz. Formas jurígenas. **Revista de Estudos Constitucionais, Hermenêutica e Teoria do Direito (RECHTD),** v.8, n.3, p. 3, set./dez. 2016. Disponível em: http://revistas.unisinos.br/index.php/RECHTD/article/viewFile/rechtd.2016.83.04/5731. Acesso em: 29 out. 2018.

Recebido em: 28/04/2019
Aprovado em: 03/06/2019