UNIVERSIDADE DO SUL DE SANTA CATARINA

MURILO MENEGHEL PONTICELLI

O DIREITO FUNDAMENTAL À PRIVACIDADE NO ÂMBITO DA REDE MUNDIAL DE COMPUTADORES COM O ADVENTO DA LEI GERAL DE PROTEÇÃO DE DADOS

Tubarão, SC

2018

MURILO MENEGHEL PONTICELLI

O DIREITO FUNDAMENTAL À PRIVACIDADE NO ÂMBITO DA REDE MUNDIAL DE COMPUTADORES COM O ADVENTO DA LEI GERAL DE PROTEÇÃO DE DADOS

Monografia apresentada ao Curso de Direito da Universidade do Sul de Santa Catarina como requisito parcial à obtenção do título de Bacharel em Direito.

Linha de pesquisa: Justiça e Sociedade

Orientador: Prof. Ricardo Willemann, Esp

Tubarão

2018

MURILO MENEGHEL PONTICELLI

O DIREITO FUNDAMENTAL À PRIVACIDADE NO ÂMBITO DA REDE MUNDIAL DE COMPUTADORES COM O ADVENTO DA LEI GERAL DE PROTEÇÃO DE DADOS

Esta Monografia foi julgada adequada à obtenção do título de Bacharel em Direito e aprovada em sua forma final pelo Curso de Direito da Universidade do Sul de Santa Catarina.

Tubarão, 04 de dezembro de 2018.

Professor e orientador Ricardo Willemann, Esp.
Universidade do Sul de Santa Catarina

Prof. Klauss Correa de Souza, Dr.
Universidade do Sul de Santa Catarina

Prof. Débora Carla Melo e Pimenta, Esp.
Universidade do Sul de Santa Catarina

Dedico este trabalho ao meu filho(a).

AGRADECIMENTOS

Agradeço, primeiramente, ao meu orientador, Professor Ricardo Willemann, pela instrução, conselhos, apoio e suporte, que foram peças fundamentais para a elaboração deste trabalho monográfico. Agradeço aos meus colegas de curso que me auxiliaram durante toda a faculdade e tornaram o meu período na instituição acadêmica um dos mais felizes. Gostaria de demonstrar a minha gratidão ao colega Caio Gouveia Blazius, que demonstrou grande interesse neste trabalho de conclusão de curso e me auxiliou com novas ideias e perspectivas durante as nossas conversas. Por fim, agradeço à minha família, ao meu pai, Joares, à minha mãe, Patrícia, à minha avó, Cristina, ao meu afilhado, Luiz Augusto, à minha namorada, Roberta, e também a toda a sua família, amos a todos e, sem vocês, não chegaria até aqui.

“Se o produto é de graça, você é o produto” (Autor desconhecido).

RESUMO

O presente trabalho monográfico foi elaborado com o propósito de fornecer informações relativas ao Direito Fundamental à Privacidade nas relações tangentes à Rede Mundial de Computadores, principalmente com as questões advindas da Lei Geral de Proteção de Dados, de 14 de agosto de 2018. Portanto, é objetivo dessa pesquisa analisar o contexto evolutivo e atual do direito fundamental à privacidade na Rede Mundial de Computadores no Brasil, culminando com o advento da Lei Geral de Proteção de Dados e quais impactos ela trará aos usuários de internet e aos provedores de serviços. Tais questões derivam de características intrínsecas da internet, como a transnacionalidade da rede e a difusão de informações, motivo pelo qual se faz necessário um estudo acerca da prestação da tutela jurisdicional no âmbito da internet. Essa pesquisa tem um caráter dedutivo, visto que parte de uma proposição universal ou geral, qual seja o direito fundamental à privacidade na Rede Mundial de Computadores, para atingir uma conclusão específica ou particular, que diz respeito ao advento da Lei Geral de Proteção de Dados. Por outro lado, quanto ao nível de profundidade, temos a pesquisa exploratória, em que o objetivo é justamente proporcionar uma maior familiaridade com o tema. Verifica-se, também, uma pesquisa de abordagem qualitativa, visto o caráter interpretativo da Lei Geral de Proteção de Dados, no âmbito do direito fundamental à privacidade. Ademais, no que diz respeito ao procedimento utilizado para a coleta de dados, esta pesquisa se caracteriza como bibliográfica, discorrendo, mas não se limitando, sobre temas atinentes à Rede Mundial de Computadores, ao direito fundamental à privacidade e ao direito fundamental à privacidade no âmbito da Rede Mundial de Computadores.

Palavras-chave: Privacidade. Internet. Lei Geral de Proteção de Dados.

ABSTRACT

The present monographic work was elaborated with the purpose of providing information regarding the Fundamental Right to Privacy in the relations tangent to the World Wide Web, mainly with the issues arising from the General Law of Data Protection, of August 14, 2018. Therefore, it is The objective of this research is to analyze the evolutionary and current context of the fundamental right to privacy in the World Wide Web in Brazil, culminating with the advent of the General Law on Data Protection and what impacts it will bring to Internet users and service providers. These issues derive from the intrinsic characteristics of the Internet, such as the transnationality of the network and the dissemination of information, which is why a study is needed on the provision of judicial protection in the internet. This research has a deductive character, since part of a universal or general proposition, what is the fundamental right to privacy in the World Wide Web of Computers, to reach a specific or particular conclusion, that concerns the advent of the General Law of Protection of Data. On the other hand, regarding the level of depth, we have the exploratory research, in which the objective is exactly to provide a greater familiarity with the subject. It is also verified a qualitative approach, considering the interpretative character of the General Law of Data Protection, within the scope of the fundamental right to privacy. In addition, with regard to the procedure used for data collection, this research is characterized as bibliographical, discussing, but not limited to, issues related to the World Computer Network, the fundamental right to privacy and the fundamental right to privacy in the within the World Wide Web.

Keywords: Privacy. Internet. General Law of Data Protection.

SUMÁRIO

1 INTRODUÇÃO

O presente trabalho monográfico tem, como objetivo, o fornecimento de informações relativas ao Direito Fundamental à Privacidade nas relações atinentes à Rede Mundial de Computadores, principalmente com as questões advindas da Lei Geral de Proteção de Dados, de 14 de agosto de 2018.

1.1 DESCRIÇÃO DA SITUAÇÃO PROBLEMA

Quando a Rede Mundial de Computadores se tornou acessível aos civis ao redor do globo, foram, e ainda são, suscitadas diversas questões quanto à relação deste novo fenômeno com o ordenamento jurídico. Tais questões derivam de características intrínsecas da internet, como a transnacionalidade da rede e a difusão de informações, que posteriormente serão melhor elucidadas.

Por sua vez, o direito fundamental à privacidade sempre esteve em grande evidência por conta de sua conexão com o mundo digital, ao ponto em que o fluxo de informações atingiu parâmetros nunca antes vistos na história do mundo, fazendo com que a segurança do que era privado ao indivíduo ficasse ameaçada, pois seu computador poderia ser violado, seus dados poderiam ser tratados de maneira inadequada, e tudo isso em uma velocidade de difusão virtualmente instantânea, de forma que o dano causado por um leve equívoco poderia ser desastroso.

Nesse sentido, se o direito fundamental à privacidade era outrora conhecido como o “right to be alone” (direito de ser deixado só), e a internet quebrou barreiras, conectando e aproximando as pessoas, elas ficaram cada vez menos sós, e as vidas cada vez menos privadas.

Assim, o ordenamento jurídico começou a adotar medidas e foram criadas normas visando preservar e assegurar não apenas a privacidade do usuário de internet, mas também outros direitos, como o de liberdade.

As principais legislações advindas até então, que tratam sobre o direito fundamental à privacidade no âmbito da Rede Mundial de Computadores são a Lei Carolina Dieckmann (Lei n. 12.737, de 30 de novembro de 2012), o Marco Civil da Internet (Lei n. 12.965, de 23 de abril de 2014) e, recentemente, a Lei Geral de Proteção de Dados (Lei n. 13.709, de 14 de agosto de 2018).

1.2 FORMULAÇÃO DO PROBLEMA

Como o ordenamento jurídico brasileiro se comporta ante o direito fundamental à privacidade na internet e quais as modificações e as determinações legais que se originam com o advento da Lei Geral de Proteção de Dados?

1.3 HIPÓTESE

Apesar de terem sido verificados inúmeros avanços acerca do direito fundamental à privacidade no âmbito da Rede Mundial de Computadores ao longo dos últimos anos, sobretudo com aqueles advindos recentemente pela Lei Geral de Proteção de Dados, principalmente com relação à proteção de possíveis abusos comerciais feitos por empresas que realizam o tratamento de dados, como, por exemplo, a necessidade de fornecimento de um consentimento específico sobre uma cláusula destacada para as hipóteses de tratamento, a mesma legislação trouxe alguns institutos que podem vir a prejudicar o titular dos dados no contexto do tratamento realizado com finalidades como a "segurança pública" ou "defesa nacional", pois estes conceitos se traduzem em uma vasta amplitude hermenêutica e dão margem para uma arbitrariedade que pode ser prejudicial para a segurança jurídica e para a privacidade dos indivíduos.

1.4 DEFINIÇÃO DOS CONCEITOS OPERACIONAIS

Para garantir um melhor entendimento acerca do conteúdo que será exposto na presente monografia, faz-se necessária uma breve definição dos conceitos que serão utilizados no decorrer do trabalho.

Acerca das legislações que serão abordadas neste trabalho, entende-se a Lei Carolina Dieckmann como a Lei n. 12.737, de 30 de novembro de 2012, o Marco Civil da Internet, que também poderá ser chamado de marco regulatório ou simplesmente de Marco Civil como a Lei n. 12.965, de 23 de abril de 2014 e a Lei Geral de Proteção de Dados, também referida neste trabalho como LGPD como a Lei n. 13.709, de 14 de agosto de 2018.

Ademais, os termos "Rede Mundial de Computadores", "internet", "mundo digital" e simplesmente "rede" são utilizados nesta monografia como sinônimos.

O restante da terminologia empregada no decorrer deste trabalho monográfico terá sua conceituação em momento oportuno.

1.5 JUSTIFICATIVA

A importância deste trabalho encontra-se no fato de que a Rede Mundial de Computadores assume uma posição de extremo destaque no cenário global, sendo a “casa” de diversas das empresas mais valiosas do planeta, um elemento fundamental à rotina da maioria dos habitantes do país, impulsionadora de revoluções democráticas e maior responsável pela globalização e difusão de informações.

Entretanto, o ordenamento jurídico ainda demonstra dificuldades em lidar com as peculiaridades do mundo digital, principalmente porque o processo caótico, difundido e global da rede acarreta em transformações com muito mais velocidade do que o processo ordenado, concentrado e local da criação de normas.

Sendo assim, discorrer sobre o direito fundamental à privacidade na internet não é apenas pertinente, mas é essencial para que a tutela jurisdicional seja prestada da melhor forma possível.

A Lei Geral de Proteção de Dados, por sua vez, impõe normas que irão modificar as relações entre os provedores de aplicação de internet (como Facebook e Google) e o usuário destes serviços ou consumidores destes produtos, de forma que a análise desta legislação é de suma importância para qualquer pessoa que tenha acesso à rede.

Ademais, para os provedores de aplicação de internet, há a necessidade de adaptação com relação às novas regras, que diferem, em sua maioria, das práticas utilizadas no período anterior à vigência da Lei Geral de Proteção de Dados, de forma que o fato de estar em conformidade com os novos institutos é essencial para a manutenção da prestação de serviço ou fornecimento de produto no âmbito da Rede Mundial de Computadores.

1.6 OBJETIVOS

1.6.1 Geral

Analisar o contexto evolutivo e atual do direito fundamental à privacidade na Rede Mundial de Computadores no Brasil, culminando com o advento da Lei Geral de Proteção de Dados e quais impactos ela trará aos usuários de internet e aos provedores de serviços.

1.6.2 Específicos

Fornecer um contexto histórico-evolutivo da Rede Mundial de Computadores.

Diferenciar os provedores de serviços de internet em duas categorias principais: provedores de conexão e provedores de aplicações de internet, para fins de melhor entendimento acerca das normas aplicadas a cada um deles.

Tratar sobre a velocidade da difusão e o alcance da informação através da internet, assim como os impactos que estas características podem gerar na sociedade.

Analisar aspectos jurídicos da internet, como o fato de ser um direito fundamental, também o aspecto da neutralidade da rede e a sua transnacionalidade.

Elaborar um breve histórico acerca do direito fundamental à privacidade, assim como a sua conceituação.

Analisar o direito fundamental à privacidade no âmbito da Rede Mundial de Computadores, com o consequente estudo acerca da Lei Carolina Dieckmann, Marco Civil da Internet e, por último, da Lei Geral de Proteção de Dados.

Abordar as questões atinentes ao tratamento de dados, ao término do tratamento de dados, dos direitos do titular e da dicotomia entre interesse público versus direito fundamental à privacidade no âmbito da Lei Geral de Proteção de Dados.

1.7 DELINEAMENTO DA PESQUISA

Cervo e Bervian (1983, p. 23) afirmam que o método de abordagem de uma pesquisa “é a ordem que se deve impor aos diferentes processos necessários para atingir um fim dado ou um resultado desejado”. Nessa perspectiva, essa pesquisa tem um caráter dedutivo, visto que parte de uma proposição universal ou geral, qual seja o direito fundamental à privacidade na Rede Mundial de Computadores, para atingir uma conclusão específica ou particular, que diz respeito ao advento da Lei Geral de Proteção de Dados.

Por outro lado, quanto ao nível de profundidade, temos a pesquisa exploratória, em que o objetivo é justamente proporcionar uma maior familiaridade com o tema. É necessário “desencadear um processo de investigação que identifique a natureza do fenômeno e aponte as características essenciais das variáveis que se quer estudar” (KÖCHE, 1997, p. 126).

Dado o caráter flexível de uma pesquisa exploratória, quanto ao método de procedimento, temos um trabalho monográfico em que o objeto de estudo se centra na Lei Geral de Proteção de dados, sob a égide de uma análise jurídica.

Ainda, conforme Minayo (1994, p. 21), a pesquisa compreendida como qualitativa "[...] trabalha com o universo de significados, motivos, aspirações, crenças, valores e atitudes, o que corresponde a um espaço mais profundo das relações, dos processos e dos fenômenos que não podem ser reduzidos à operacionalização de variáveis". Em razão disso, verifica-se uma pesquisa de abordagem qualitativa, visto o caráter interpretativo da Lei Geral de Proteção de Dados, no âmbito do direito fundamental à privacidade.

1.7.1 Caracterização Básica

No que diz respeito ao procedimento utilizado para a coleta de dados, esta pesquisa se caracteriza como bibliográfica.

Koche (1997, p. 122) afirma que a pesquisa bibliográfica pode ser realizada com diferentes fins:

> a) para ampliar o grau de conhecimento em uma determinada área, capacitando o investigador a compreender ou delimitar melhor um problema de pesquisa; b) para dominar o conhecimento disponível e utilizá-lo como base ou fundamentação na construção de um modelo teórico explicativo de um problema, isto é, como instrumento auxiliar para a construção e fundamentação de hipóteses; c) para descrever ou sistematizar o estado da arte, daquele momento, pertinente a um determinado tema ou problema.

Esta pesquisa supera o âmbito da Rede Mundial de Computadores, com ênfase em aspectos jurídicos que a permeiam, tanto no que diz respeito ao direito fundamental da internet, como também no contexto da neutralidade garantida a partir do acesso do usuário sem qualquer tipo de interferência dos provedores e na ausência de fronteiras estatais (transnacionalidade).

Aborda, também, uma reflexão sobre o direito fundamental à privacidade, consagrado no art. 5º, inciso X, da Constituição Federal de 1988, que foi criado com o intuito de proteger a vida privada dos indivíduos contra a conduta invasiva de outros particulares ou do próprio Estado.

Assim, finalmente possível a análise do contexto da privacidade online, a partir das legislações nacionais criadas até o presente momento em uma tentativa de prestar a tutela jurisdicional de garantia de privacidade na rede, as quais merecem grande destaque a Lei Carolina Dieckmann (Lei n. 12.737, de 30 de novembro de 2012), o Marco Civil da Internet (Lei n. 12.965, de 23 de abril de 2014) e a Lei Geral de Proteção de Dados (Lei n. 13.709, de 14 de agosto de 2018).

1.8 ESTRUTURA BÁSICA DO RELATÓRIO FINAL

A estrutura da presente monografia possui 5 capítulos. No primeiro, será realizada a introdução do assunto, com o objetivo de familiarizar o leitor com os aspectos atinentes ao trabalho, tornando a compreensão do tema, do problema e das linhas que serão traçadas ficará mais acessível. Ademais, este primeiro capítulo também tem como objetivo apresentar os procedimentos metodológicos utilizados para a sua formação.

O segundo capítulo discorre acerca da Rede Mundial de Computadores, englobando a sua origem, os provedores de serviços que atuam na rede, a velocidade de difusão e o alcance da informação, assim como seus impactos e alguns aspectos jurídicos da internet, como a sua característica de direito fundamental, a neutralidade e a transnacionalidade da rede.

O terceiro capítulo, por sua vez, trata do direito fundamental à privacidade, fazendo um breve histórico e o conceituando, de forma que possam ser entendidos os elementos que caracterizam a violação de privacidade.

Já o quarto capítulo confronta a Rede Mundial de Computadores com o direito fundamental à privacidade, discorrendo sobre as formas de atuação governamental para a prestação da tutela jurisdicional no âmbito da internet e as dificuldades encontradas para garantir a eficácia desta tutela. Neste ponto, são trazidas as principais legislações sobre o tema, começando pela Lei Carolina Dieckmann, seguindo para o Marco Civil da Internet e culminando na Lei Geral de Proteção de Dados, de maneira que são expostas, no contexto desta última norma, as formas de tratamento de dados, o término do tratamento de dados, os direitos do titular e discutida a questão do interesse público versus o direito fundamental à privacidade.

O quinto e último capítulo irá expor as conclusões obtidas ao final do estudo.

2 A REDE MUNDIAL DE COMPUTADORES

Para que se possa iniciar a presente monografia, que possui como elemento central o direito fundamental à privacidade no âmbito da rede mundial de computadores, é necessário delinear alguns conceitos, serviços e até mesmo a origem da internet. Tal indispensabilidade decorre do fato de que apenas com uma compreensão acerca do funcionamento da World Wide Web (Rede Mundial de Computadores), ou internet, é possível realizar uma análise jurídica e acadêmica da Lei Geral de Proteção de Dados.

2.1 HISTÓRICO

Para Naughton (2000), a internet não surgiu em um momento claro e específico, sendo diversos os estágios e os agentes que impactaram a sua criação. Entretanto, "um ponto que marca o estopim certamente é aquele ocorrido em 4 de outubro de 1957, o dia em que a União Soviética lançou o primeiro satélite artificial da história da humanidade, o Sputnik" (NAUGHTON, 2000, p. 77), dando início à exploração espacial durante a Guerra Fria.

No contexto da Guerra Fria, que vigorou no mundo entre 1945 e 1991, envolvendo as duas superpotências político-econômicas da época, quais sejam Estados Unidos da América e União Soviética, a busca por inovações tecnológicas com potencial de uso militar era incessante, e desta forma foi criada a ARPA (Advanced Research Projects Agency), uma agência federal norte-americana focada no desenvolvimento de projetos militares.

Em 1962, Joseph Carl Robnett Licklider foi contratado pela ARPA, sendo o primeiro a utilizar o termo "Rede Intergaláctica de Computadores", significando uma "vasta comunidade interligada em tempo real". (NAUGHTON, 2000, p. 76), e o responsável por inúmeros avanços na pesquisa que resultaria na internet como conhecemos hoje.

A ameaça da Guerra Fria se tornar uma guerra de fato diminuiu após a década de 1970, fazendo com que a tecnologia criada tenha saído do âmbito militar e se alastrado rapidamente pelo mundo. Em sua tese, Joana Sierra (2018, p. 23) informa que "dos quatro computadores que deram início à rede, em 1972 passaram a ser ligados à web 40 computadores. Em 1981, chegavam a 200. Antes disso, em 1973, enfim, a rede foi oficialmente batizada como internet".

No final dos anos 1980, um homem chamado Tim Berners-Lee criou uma nova rede, transformando o foco praticamente exclusivo de envio de e-mails verificado à época para

uma “nova forma de estruturar, armazenar e acessar informação. Ele chamou esta rede de World Wide Web (Rede Mundial de Computadores)”. (NAUGHTON, 2000, p. 213).

Desta forma, a Rede Mundial de Computadores como conhecemos conectou todos os usuários em uma grande plataforma neutra, com espaços vazios praticamente ilimitados, prontos para serem preenchidos de informações que poderiam ser armazenadas, acessadas, modificadas ou alteradas, fornecidas por qualquer um que tivesse um ponto de acesso conectado à internet.

Conforme Joana Sierra (2018, p. 24), a internet chegou para o setor privado no Brasil apenas em 1995, e desde então o seu crescimento e disseminação de informação foi exponencial, sendo criados sites e serviços de pesquisa, redes sociais, inteligência artificial, enfim, tudo que o usuário quisesse criar.

2.2 PROVEDORES DE SERVIÇOS

O Marco Civil da Internet, apesar de subdividir os tipos de provedores de serviços em “provedores de conexão” e “provedores de aplicações de internet”, não os conceitua individualmente. Entretanto, em seu art. 5º, define aplicações de internet, in verbis “Art. 5o Para os efeitos desta Lei, considera-se: (...) VII - aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet” (BRASIL, 2014).

Considerando o conceito dado sobre aplicações de internet, é possível comparar esta caracterização com aquela verificada na obra de Ronaldo Lemos (2005, p. 40), que define Online Service Provider (OSP) como aquele que “[...] não fornece acesso à internet, mas sim utiliza-se desse acesso para a prestação de outros serviços. Como exemplo, um provedor de notícias como o Universo Online, ou ainda um sistema de busca como o Google [...]”. Logo, torna-se válida uma equiparação de Online Service Provider (OSP) com aquele destacado como “provedor de aplicações de internet” na redação do Marco Civil da Internet

Os provedores de conexão, por sua vez, seriam aqueles descritos na obra de Ronaldo Lemos (2005, p. 38) como os Internet Service Provider (ISP), sendo que os provedores de serviços de internet são “empresas ou outras entidades que fornecem acesso e tráfego de informações sobre a internet”.

Os provedores de aplicações de internet são o foco do presente trabalho, posto que é dentro do seu âmbito que são tratadas a maioria das informações. Existem outras subdivisões quanto aos provedores de aplicações de internet, mas não se faz necessária tal classificação

nesta monografia, uma vez que todas estas subdivisões podem ter acesso e realizar tratamento de dados pessoais.

Para citar alguns exemplos, existe, na classificação de Joana Sierra (2018, p. 51), os chamados "Provedores de Pesquisa", que seriam aqueles em que o usuário pode consultar uma gama de links, desde que indexados no site do provedor de pesquisa, relacionada com as palavras-chave pesquisadas. O provedor com maior visibilidade desta categoria seria o Google, e o tratamento de dados pessoais, neste caso, ocorre, de acordo com a Política de Privacidade da empresa, nos termos definidos a seguir por Google (2018)

> Quando você não está conectado a uma Conta do Google, armazenamos as informações que coletamos com identificadores exclusivos vinculados ao navegador, aplicativo ou dispositivo que você está usando. Isso nos ajuda a manter as preferências de idioma em todas as sessões de navegação, por exemplo. Quando você está conectado, também coletamos informações que armazenamos com sua Conta do Google e que tratamos como informações pessoais.

Sendo que os tipos de informações coletadas incluem, por exemplo, conforme Google (2018)

> Também coletamos o conteúdo que você cria, de que faz upload ou que recebe de outras pessoas ao usar nossos serviços. Isso inclui e-mails enviados e recebidos, fotos e vídeos salvos, documentos e planilhas criados e comentários feitos em vídeos do YouTube.

Outra subdivisão de provedores de aplicações de internet pode ser aquela, também definida por Joana Sierra (2018, p. 45), como os "Provedores de Conteúdo", que seriam os responsáveis pela disponibilização de conteúdo, criados de forma originária pelo provedor, a exemplo de sites de notícias, ou pelos próprios usuários, neste último caso destacando-se as redes sociais, a mais conhecida sendo o Facebook, que coleta os dados na forma definida em sua Política de Dados, conforme segue extraído de Facebook (2018)

> Coletamos o conteúdo, comunicações e outras informações que você fornece quando usa nossos Produtos, inclusive quando você se cadastra para criar uma conta, cria ou compartilha conteúdo, envia mensagens ou se comunica com outras pessoas. Isso pode incluir informações presentes ou sobre o conteúdo que você fornece (como metadados), como a localização de uma foto ou a data em que um arquivo foi criado.

Válido ressaltar que as políticas de privacidade de algumas empresas serão melhor exploradas em um momento posterior neste trabalho, sendo que agora foi utilizado como exemplo apenas para demonstrar que diferentes subcategorias de provedores de aplicações de internet podem realizar o tratamento de dados pessoais de formas diferentes e de origens distintas.

2.3 A VELOCIDADE E O ALCANCE DA DIFUSÃO DE INFORMAÇÕES E SEUS IMPACTOS

Na data de 18 de outubro de 2018, o jornal Folha de S. Paulo acusou empresas de estarem "comprando pacotes de disparos em massa de mensagens contra o PT no WhatsApp" (FOLHA DE S. PAULO, 2018) e informa que este fato pode afetar diretamente o resultado do segundo turno da eleição presidencial de 2018, caso confirmado.

O jornal The Guardian publicou, em 30 de outubro de 2017, uma reportagem afirmando que "conteúdo financiado pela Rússia pode ter atingido 126 milhões de americanos no Facebook durante e depois das eleições presidenciais de 2016" (THE GUARDIAN, 2017). O The Guardian também indica que, conforme o testemunho do Facebook submetido ao comitê de justiça do Senado norteamericano, "120 contas de perfis falsos, financiados pela Rússia, criaram 80.000 postagens que foram recebidas por 29 milhões de americanos diretamente, mas atingiram uma audiência maior pelo compartilhamento" (THE GUARDIAN, 2017).

Apesar de que em ambos os casos ainda restam dúvidas quanto a materialidade e a autoria dos fatos, torna-se claro que disseminação de informação na internet, principalmente após ocorrer um processo de viralização, qual seja aquele em que o compartilhamento de informações pelos usuários faz com que essas informações sejam espalhadas de forma exponencial, é um efeito que possui grande impacto em uma escala mundial, fazendo até mesmo com que a validade de eleições presidenciais sejam questionadas.

Uma pesquisa realizada pelo Cetic em 2017 apurou que, no Brasil, 74% das pessoas já acessaram a internet, sendo que 90% destas, ou 67% do total, tiveram acesso nos 3 meses anteriores à data da pesquisa. São mais de 140 milhões de indivíduos com acesso regular à internet. Para atingir 140 milhões de pessoas, em um efeito de viralização, basta que o indivíduo A envie uma informação para 520 pessoas distintas, que por sua vez enviarão, cada uma, para mais 520 indivíduos distintos, que farão o mesmo processo para mais 520 pessoas diferentes uma última vez, o resultado será mais de 140 milhões de pessoas atingidas.

Desta forma, como a transmissão de informação não ocorre de um único portal centralizado que tenta atingir o máximo de pessoas possíveis com as suas publicações, e sim através de um processo espontâneo e difuso de propagação de conteúdo realizado pelos próprios usuários, com base no relacionamento interpessoal proporcionado pelas redes sociais e aplicativos de troca de mensagens, o alcance e a velocidade de transmissão de informação dependem apenas da vontade dos indivíduos de compartilharem aquele conteúdo.

2.4 ASPECTOS JURÍDICOS DA INTERNET

Com o advento da internet, foram verificadas mudanças em todos os âmbitos da sociedade, não só brasileira, mas mundial. Provedores de pesquisa começaram a existir, facilitando a busca por sites de conteúdo educacional e modificando o processo de aprendizado daqueles que buscavam informação; não era mais preciso ir até uma biblioteca e ficar horas tentando localizar um trecho específico de um livro, bastavam apenas alguns minutos de pesquisa com as palavras-chave relacionadas ao tema. Houveram também mudanças nos sistemas bancários, com a possibilidade de pagamentos online e contas inteiramente digitais; o mercado de jogos eletrônicos, que já vinha em ascensão, não tardou em obter um faturamento maior do que a consolidada Hollywood; as redes sociais surgiram, trazendo um engajamento entre os usuários de forma a propagar diversos tipos de conteúdo e promovendo a socialização digital em um processo de globalização interno e externo.

O crescimento da internet aconteceu de forma exponencial e em um período muito curto de tempo. Seu aspecto neutro, caótico e desvinculado de qualquer regulação estatal assustou, de certa forma, o direito, não apenas brasileiro, mas mundial.

Neste mesmo teor, da globalização decorrente do surgimento da internet e das mudanças sociais trazidas por ela, o direito vem, incessantemente, se adaptando e encontrando as melhores formas de lidar com as novas demandas e fatos jurídicos advindos dessa revolução tecnológica.

2.4.1 A Internet como Direito Fundamental

Segundo o site especializado Internet World Stats, em pesquisa realizada em 30 de junho de 2018, mais de 4 bilhões de pessoas têm acesso a internet ao redor do mundo.

Com a finalidade de comunicação e principalmente sendo uma ferramenta de acesso a informação, a internet começou a se tornar cada vez mais essencial para a vida em sociedade, e, recentemente, sendo declarada pela ONU (2016) como um direito humano, advertindo as nações acerca da relevância do acesso universal a ela.

Quanto aos direitos fundamentais, nas palavras de Luiz Alberto David Araújo e Vidal Serrano Nunes Júnior (2005, p. 109-110)

> Os direitos fundamentais podem ser conceituados como a categoria jurídica instituída com a finalidade de proteger a dignidade humana em todas as dimensões. Por isso, tal qual o ser humano, tem natureza polifacética, buscando resguardar o homem na sua liberdade (direitos individuais), nas suas necessidades (direitos sociais, econômicos e culturais) e na sua preservação (direitos relacionados à fraternidade e à solidariedade).

Pela classificação supra, percebe-se que a rede mundial de computadores abrange diversos aspectos dos direitos fundamentais, superando as barreiras das diferentes gerações de direitos, quais sejam, por exemplo, a liberdade de expressão, o direito à privacidade e o direito à informação.

Nessa linha, atualmente está tramitando o Projeto de Emenda à Constituição 479/2010, proposta que "acrescenta o inciso LXXIX ao art. 5º da Constituição Federal, para incluir o acesso à internet em alta velocidade entre os direitos fundamentais do cidadão" (BRASIL, 2010).

Ademais, não obstante o prejuízo social que pode trazer a disseminação de informações falsas em uma eleição presidencial, como verificado no ano de 2018, é de suma importância que seja garantida a liberdade de expressão online não apenas como direito fundamental, mas como uma ferramenta democrática, pois é de fácil percepção que países que possuem um acesso restrito ao mundo digital seguem uma forma de governo ditatorial ou com poucos elementos democráticos, como Cuba, China, Coréia do Norte, entre outros.

2.4.2 Neutralidade da Rede

Outro assunto pertinente quanto ao uso da internet é a neutralidade de rede, que tem a finalidade de garantir o acesso do usuário à internet sem qualquer tipo de interferência dos provedores, assegurando o uso sem discriminação e restrição de acesso independente da razão ou local de utilização.

Pedro Henrique Soares Ramos (2015, p. 13) define, em sua dissertação, a neutralidade da rede

> Quando falamos que a neutralidade da rede deve ser um princípio de uso da internet, queremos dizer, essencialmente, que provedores de acesso têm o dever de entregar a velocidade e banda de rede contratadas, sem distinção de acordo com o uso que o usuário fará com seus dispositivos de acesso à internet – em outras palavras, o usuário tem liberdade e autonomia para utilizar a internet da maneira que lhe parecer mais adequada.

No Brasil, a neutralidade da rede é tida como princípio, positivado no artigo 3º, IV da Lei 12.965/2014, Marco Civil da Internet (BRASIL, 2014) na forma que segue

> Art. 3º. disciplina do uso da internet no Brasil tem os seguintes princípios:
>
> [...]
>
> IV - preservação e garantia da neutralidade de rede;

O conceito de neutralidade da rede vem no art. 9º da mesma norma, quando cita que "O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação". (BRASIL, 2014).

Desta forma, não há a possibilidade de determinados provedores de acesso favorecerem certos provedores de aplicações de internet através do aumento de velocidade de conexão do usuário quando utilizando essas aplicações, tampouco é praticável a redução de velocidade de conexão para embaraçar os provedores de aplicações de internet que eventualmente não tenham algum acordo com o provedor de acesso.

Portanto, a neutralidade da rede é medida que garante isonomia no ambiente virtual, evitando a formação de cartéis entre provedores de acesso e de aplicações de internet, possibilitando uma competição justa dentro da rede.

Como pôde ser visto, esse princípio dialoga diretamente com o tópico anterior, uma vez que ele tenta assegurar a liberdade de acesso ao usuário, reconhecendo a importância da internet como direito fundamental, ao ponto que funciona como um escudo para garantir outros direitos e princípios.

2.4.3 Transnacionalidade da Internet

O termo "transnacionalidade" aplicado à rede mundial de computadores significa dizer que não há fronteiras estatais que restrinjam a difusão de informação e a transferência de dados, a não ser pelos países que não possuem neutralidade da rede ou que possuam outro tipo de regulação dos provedores de acesso internamente.

Enquanto, por um lado, a característica da transnacionalidade traz evidentes benefícios ao mundo, que garantem e promovem, por exemplo, o livre exercício da democracia, por outro lado, impõe um largo obstáculo para o efetivo exercício da tutela jurisdicional, inicialmente pelo fato de que a própria identificação dos limites jurisdicionais dos Estados é confusa, geralmente sendo sinalizada dentro das legislações nacionais, como é o caso do Brasil, onde o artigo 11 da Lei n. 12.965, de 23 de abril de 2014 (Marco Civil da Internet) discorre

> Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.
> § 1o O disposto no caput aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.

> § 2o O disposto no caput aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil. (BRASIL, 2014).

Nesse sentido, restou delineada a fronteira jurisdicional brasileira no âmbito da Rede Mundial de Computadores, conforme explica Teixeira (2016, p. 100)

> Essa regra é aplicável quando pelo menos um desses atos ocorra em território brasileiro, isto é, ou a coleta, ou o armazenamento, a guarda ou o tratamento; para tanto, ao menos um dos terminais (computador ou dispositivo que se conecta à internet) deve estar localizado no Brasil.

Além disso, o maior problema decorrente da transnacionalidade da rede se dá pela alocação, por parte dos provedores de aplicações de internet, de servidores em países que possuem legislação díspar com a brasileira, sediando suas atividades ilícitas, de acordo com a nossa norma, em locais onde tal ilicitude é inexistente ou não é fiscalizada pelas autoridades locais, tornando penosa a tarefa de garantir a aplicação dos nossos institutos, restando como única saída a promoção de acordos bilaterais ou multilaterais de cooperação para a aplicação da lei nestes casos, solução esta que não demonstra tanta eficiência.

Dessa forma, verifica-se certa necessidade para que seja elaborada uma regulamentação internacional uniformizada sobre a internet, mas esta busca acaba esbarrando em diferenças culturais de um mundo ainda bastante heterogêneo. Francisco Victor Vasconcelos (2017, p. 60) explica, em sua dissertação que "não há organismo internacional, interestatal ou não, que promova uma proteção jurídica mínima à Internet".

Nessa linha, Francisco Victor Vasconcelos (2017, p. 60), segue o raciocínio

> É deveras difícil a criação de uma legislação mínima internacional (hard law) sobre a tônica da Internet, uma vez que a rede mundial de computadores, apesar da uniformidade de suas características, é utilizada diferentemente em cada Estado, com fundamento em suas peculiaridades.

Para o autor supracitado, é necessário que sejam criados entes, de caráter estatal ou não, para impor uma uniformização legal mínima, de modo que garanta aos usuários da internet uma observância de seus direitos fundamentais.

Portanto, uma vez que ainda não há nenhum órgão regulador transnacional das relações na internet, a proteção dos direitos conferidos internamente no Brasil, principalmente o direito à privacidade, encontra-se em xeque, pois está restrita a uma barreira física que não impõe os seus limites no âmbito digital, tornando a eficácia de qualquer legislação neste sentido limitada.

3 DIREITO FUNDAMENTAL À PRIVACIDADE

O direito à privacidade, previsto no art. 5º, inciso X, da Constituição Federal de 1988, tem o seguinte teor "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" (BRASIL, 1988), e pertence à gama de direitos relativos à personalidade. Foi criado com o intuito de proteger a vida privada dos indivíduos contra a conduta invasiva de outros particulares ou do próprio Estado.

Embora tenha suas origens na antiguidade clássica, o conceito de direito à privacidade utilizado nos dias atuais é uma construção recente.

3.1 HISTÓRICO

Quando se trata de direito à privacidade, a sua origem pode remeter a um tempo tão distante quanto a própria história da civilização ou quanto ao conceito de propriedade; uma vez que algo é meu, pertence ao meu íntimo, é privado. Nesse sentido, o site Global Internet Liberty Campaign informa que

> Privacidade tem raízes profundas na história. A Bíblia tem numerosas referências à privacidade. Também havia uma proteção real da privacidade nos primórdios das culturas hebraica, grega clássica e chinesa. A maioria destas proteções focavam no direito a ser deixado só

Conforme explica Cancelier (2017), na antiguidade clássica, a sociedade grega fazia a distinção entre a vida pública e a privada por meio da separação entre a vida familiar e a política, sendo que, ao adentrar nesta última, ao cidadão era dada uma "segunda vida", na qual se relacionava não mais com aquilo que lhe era próprio e particular, como a sua casa e sua família, mas sim com o que lhe era comum à sociedade.

Na idade média, os indivíduos mais abastados passaram a valorizar e buscar formas de isolamento, época em que as famílias nobres adquiriram o hábito de praticar certos atos em ambientes privados, a exemplo dos atos sexuais e das necessidades fisiológica (THIBES, 2014, p. 86, apud CANCELIER, 2017, p. 215). A evolução disto foi a valorização da esfera privada em que as casas e o ambiente familiar passaram a ser vistos como " centros de representação do poder político", sendo aquelas relacionadas futuramente a grandes dinastias (AGOSTINI, 2011, p. 120 apud CANCELIER, 2017, p. 215).

Segundo Cancelier (2017), com a ascensão da classe burguesa, potencializa-se a importância e consequentemente a busca pela individualidade como expressão da própria

personalidade dos indivíduos. A busca pelo direito à privacidade, uma vez que existia uma necessidade da confirmação de um local íntimo e particular para esta nova classe, que não estava sob as asas das monarquias ou do clero, acabou representando parte dos atos que, por fim, culminaram na destruição do absolutismo.

Em razão das transformações socioeconômicas trazidas pela revolução industrial, surgiu a necessidade de tutelar o direito à privacidade contra ingerências alheias, cujo marco se deu por meio da Declaração Universal dos Direitos Humanos da ONU em 1948 (que o reconheceu como um direito fundamental) e, posteriormente, tendo sido positivado em nosso ordenamento jurídico, no texto da Constituição Federal de 1988 e do Código Civil de 2002.

Segue o direito à privacidade consagrado nos incisos X, XI e XII do artigo 5º da Carta Magna brasileira (BRASIL, 1988)

> 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;
> XI - a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial;
> 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;

E o texto de ordem similar verificado no artigo 21 do Código Civil (BRASIL, 2002)

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

Apesar da positivação no ordenamento jurídico brasileiro, através deste breve histórico será possível perceber, no capítulo sobre privacidade online, que vivemos, de certa forma, em uma realidade paralela com o mundo antes de haver eficácia na defesa do direito à privacidade dos indivíduos. Quando estamos conectados ao mundo digital, as paredes não têm "ouvido" como em outrora, mas os microfones dos aparelhos estão ouvindo, as câmeras estão vendo e tudo pode estar sendo gravado.

3.2 CONCEITO

Antes de tentar definir o significado deste direito fundamental, cabe fazer um breve comentário acerca da distinção entre intimidade e privacidade, uma vez que a Constituição Federal de 1988 faz referência à "intimidade" e "vida privada". Alexandre de Moraes (2017, p. 97), esclarece que "os conceitos constitucionais de intimidade e vida privada apresentam grande

interligação, porém podem ser diferenciados por meio da menor amplitude do primeiro, que se encontra no âmbito de incidência do segundo". Para este autor, enquanto a intimidade diz respeito às relações subjetivas e de trato íntimo das pessoas como relações familiares e de amizades, a vida privada envolve todos os demais relacionamentos humanos, tais como relações comerciais, profissionais, acadêmicas, etc.

De difícil conceituação em razão da ampla abrangência que a palavra "privacidade" representa, este direito foi compreendido de diversas maneiras ao longo das décadas, especialmente porque a forma como a privacidade dos indivíduos pode ser violada também foi mudando com o tempo.

Assim, desde o "right to be let alone", do fim do século XIX, até os conceitos de privacidade que conhecemos hoje, muitas mudanças ocorreram (sociais, políticas, econômicas, tecnológicas), modificando e ampliando o conceito de privacidade.

Inerentes ao ser humano, conforme Bulos (2010) o direito à intimidade e privacidade funcionam como limites às intromissões abusivas e ilícitas de terceiros, possibilitando, inclusive, indenização por danos materiais e morais eventualmente causados.

A garantia à privacidade é o direito dos indivíduos de resguardarem-se dos sentidos alheios, em especial da vista e ouvidos (MIRANDA apud DONEDA, 2006). Assim, o direito à privacidade permite que o indivíduo mantenha o domínio daquilo que se relacione consigo mesmo, como o corpo, casa, propriedade, pensamentos, sentimentos, segredos e identidade, e tenha liberdade para escolher que parte deste domínio deseja permitir que outras pessoas tenham acesso. Ou seja, é uma garantia de que o indivíduo possa controlar a exposição e a disponibilidade de dados e informações sobre si mesmo que deseja tornar público.

René Ariel Dotti (apud AFONSO DA SILVA, 2004, p. 206) caracteriza a intimidade como "a esfera secreta da vida do indivíduo na qual este tem o poder legal de evitar os demais", reforçado por meio da garantia de inviabilidade de domicílio, de correspondências, do segredo profissional, sigilo bancário, entre outras.

No entanto, na sociedade contemporânea, em que os meios de comunicação em massa, as redes sociais, e os avanços tecnológicos são incessantes e cada vez mais rápidos, o conceito de privacidade vem sofrendo mutações constantes, extravasando a ideia de isolamento e tranquilidade antigamente aceita (DONEDA, 2006).

Dessa forma, o conceito inicial que caracterizava o direito à privacidade como o direito "de estar só", "ser deixado só" não representa a realidade atual. Como explica Alice Monteiro de Barros (2009), a utilização indevida das tecnologias que hoje estão ao alcance de

todos permite que a privacidade das pessoas seja invadida à distância, sem a presença física do infrator.

Considerando-se a infinidade de meios pelos quais as informações pessoais dos indivíduos podem ser divulgadas e compartilhadas em razão da internet, é seguro afirmar que o conceito de privacidade está em constante mutação. Percebe-se que, anteriormente ao surgimento da internet, as formas de violação da privacidade alheia eram significativamente menores. A divulgação indevida de informações a respeito de alguém alcançava um grupo limitado de pessoas e exigia, via de regra, a presença física do infrator, diferentemente dos dias atuais, em que o banco de dados de clientes de uma determinada empresa ou órgão público, por exemplo, pode ser compartilhado ou divulgado ilicitamente, com instituições e empresas localizadas em qualquer parte do mundo, muitas vezes não sendo possível sequer identificar o responsável pelo ato.

Inúmeros são os casos em que a privacidade de pessoas ou grupo de pessoas é violada. A gravidade dos casos varia entre a circulação de algum vídeo constrangedor de algum aluno pelos corredores da escola, e a venda não autorizada de banco de dados de clientes/usuários com informações privadas para empresas e instituições tirarem proveito político, econômico e financeiro.

4 PRIVACIDADE ONLINE

Com as questões atinentes ao funcionamento da internet e à disseminação de informação, combinadas com o direito fundamental à privacidade, tornam-se evidentes os obstáculos que o Estado enfrenta na tentativa de manter a sua tutela jurisdicional no âmbito digital, seja pela dificuldade no rastreamento dos indivíduos que violam o direito à privacidade, seja pelo caráter transnacional da internet, seja pela elevada velocidade de difusão da informação com a sua característica quase irreversível: uma vez incorporada na rede mundial de computadores, ela não "esquece".

Leonardi (2011, p. 39) comenta sobre o assunto

> A Internet não exige apenas novas soluções jurídicas para os novos problemas; ela também afeta a maneira como os problemas e as soluções jurídicas devem ser analisados. Ao romper com os paradigmas jurídicos tradicionais e desafiar os mecanismos convencionais de tutela, a Rede representa um dos principais objetos de estudo dos doutrinadores preocupados com essa nova realidade social.

Segundo Leonardi (2011), a busca pela solução para resolver os problemas inerentes das características da internet resultou em algumas correntes doutrinárias, quais sejam as de autorregulação, de "direito específico do ciberespaço", de analogia e de uma abordagem mista com sistema jurídico aliado à arquitetura da internet.

Nas definições de Leonardi (2011), a corrente de autorregulação enfatiza o ciberespaço como um ambiente anárquico, onde os conflitos seriam resolvidos pelos próprios usuários, sem nenhuma interferência governamental; a de "direito específico do ciberespaço" indica que, como a rede mundial de computadores não possui fronteiras no território físico mundial, seria impossível impor a tutela jurisdicional prestada por apenas um Estado, defendendo então a criação de um direito global específico, originado através de uma cooperação internacional para regular as interações no mundo virtual; a corrente de analogia defende que seria viável a regulação da internet apenas aplicando normas e princípios já existentes, de forma análoga nas situações cibernéticas; por último, a corrente de abordagem mista com sistema jurídico aliado à arquitetura da internet, que é a doutrina que prevalece, informa que é possível regular as interações digitais através do direito positivado, mas, além disso, é preciso utilizar-se da própria arquitetura da internet, ou seja, desenvolver tecnologia que opere dentro da rede para garantir a efetividade do direito, combater "fogo com fogo".

Dentre as legislações nacionais criadas até o presente momento em uma tentativa de prestar a tutela jurisdicional de garantia de privacidade na rede, merecem grande destaque a Lei Carolina Dieckmann (Lei n. 12.737, de 30 de novembro de 2012), o Marco Civil da Internet

(Lei n. 12.965, de 23 de abril de 2014) e a Lei Geral de Proteção de Dados (Lei n. 13.709, de 14 de agosto de 2018).

Entretanto, importante destacar que o direito à privacidade online não é absoluto, devendo ser analisado, principalmente, observando e respeitando o direito de liberdade de expressão dos indivíduos, de forma a encontrar harmonia para a coexistência dos dois institutos. Tal conflito se mostra bastante evidente, por exemplo, no campo de comentários do perfil de um usuário de alguma rede social, que pode acabar recebendo mensagens que o desagradem, ou até mesmo com empresas de telemarketing que conseguiram dados pessoais de indivíduos de alguma forma e realizam ligações.

Seguindo esta linha, conforme a 2ª Câmara de Coordenação e Revisão do MPF cita em seu Roteiro de Atuação Sobre Crimes Cibernéticos (2013, p. 336) "A intimidade não é um valor intangível como pregou a mídia no caso motriz da lei. A sua proteção impõe modelação com a liberdade de expressão, sempre para evitar abusos".

Portanto, é de suma importância reconhecer que existe uma linha tênue para alcançar a justiça ao pesar os direitos à privacidade e à liberdade de expressão no mundo virtual, de forma a garantir que não haja nada no mundo virtual que possa ser considerado invasivo em excesso, tampouco nada que caracterize qualquer forma de censura.

4.1 LEI CAROLINA DIECKMANN

A Lei n. 12.737, de 30 de novembro de 2012, também conhecida como Lei Carolina Dieckmann, complementa o Decreto-Lei n. 2.848, de 7 de dezembro de 1940 (Código Penal), e foi a primeira legislação brasileira a tratar sobre crimes informáticos.

O nome dado à lei tem sua origem devido a invasões cibernéticas (hacking) em um dispositivo de propriedade da atriz e apresentadora homônima, ocorrida em maio de 2012.

Conforme relatou o portal de notícias G1 (2012), a invasão adveio da execução de um programa malicioso (malware) recebido no e-mail da vítima, permitindo o acesso dos criminosos em seu dispositivo, que por sua vez efetuaram a cópia dos arquivos contendo fotos íntimas da atriz e posteriormente a extorquiram sob a ameaça de divulgação destes arquivos, fato que acabou se consumando.

Neste sentido, a Lei Carolina Dieckmann adicionou ao código penal o artigo 154-A, que determina, conforme Brasil (2012):

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim

> de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

E ainda frisa, nos § 3º e § 4º do mesmo artigo, a necessidade da proteção do direito à privacidade, quando informa, respectivamente:

> § 3o Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
> § 4o Na hipótese do § 3o, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos. (BRASIL, 2012).

Desta forma, a Lei n. 12.737, de 30 de novembro de 2012, foi a primeira a defender explicitamente a intimidade e a privacidade do usuário no âmbito da rede mundial de computadores.

Todavia, a referida lei apenas tratou da violação da privacidade em uma esfera criminal, abordando somente os hackings, termo utilizado para definir as invasões de dispositivos eletrônicos ou de registros contidos na internet, motivo pelo qual ainda existia a necessidade de uma legislação mais generalista acerca do uso da internet no Brasil, de forma a regular questões que o sistema jurídico possuía dificuldade em resolver. Nesse sentido, surgiu o Marco Civil da Internet.

4.2 MARCO CIVIL DA INTERNET

Em uma publicação feita no dia 24 de março de 2014, o site World Wide Web Foundation divulgou um pronunciamento de Sir Tim Berners-Lee, já apontado nesta monografia como inventor da internet na forma que conhecemos hoje, que demonstrou grande entusiasmo com a Lei n. 12.965, de 23 de abril de 2014 (Marco Civil da Internet), conforme segue a publicação de World Wide Web Foundation (2014)

> Se o Marco Civil for aprovado, sem maiores adiamentos ou modificações, este seria possivelmente o melhor presente de aniversário para os usuários de internet do Brasil e do mundo. Eu espero que, aprovando esta lei, o Brasil fixe sua orgulhosa reputação como um líder mundial em democracia e progresso social e ajude a inaugurar uma nova era, uma onde os direitos dos cidadãos em todos os países do mundo são protegidos por leis de direito digitais.

Além disso, para Sir Tim Berners-Lee, no mesmo pronunciamento, a legislação "reflete a internet como deveria ser: uma rede aberta, neutra e descentralizada, onde os usuários são o motor para a colaboração e inovação" (World Wide Web Foundation, 2014).

De fato, neste tópico ficará demonstrado como o Marco Civil da Internet se preocupou em abordar diversos direitos, garantias e deveres relativos à rede mundial de computadores, com foco a ser explorado, aqui, nas inovações com relação ao direito fundamental à privacidade online.

Nesse sentido, é o que informa Teixeira (2016, p. 84)

> Preocupado com a possibilidade de eventualmente haver alguma limitação à liberdade de expressão ou alguma violação da privacidade dos usuários da internet, o Marco Civil expressa que a garantia a esses dois direitos constitucionais é condição para o pleno exercício do direito à acesso à rede mundial de computador. Ou seja, a violação a esses direitos implica em quebra da própria finalidade do advento do Marco Civil enquanto uma lei federal que objetiva tutelar os usuários da internet.

Logo em seu artigo 3º, incisos II e III, o Marco Civil da Internet já estabelece, como princípios do uso da internet no Brasil, dentre outros, a "proteção da privacidade" e a "proteção dos dados pessoais, na forma da lei" (BRASIL, 2014), sendo que a proteção dos dados pessoais, conforme Teixeira (2016), não foi tratada de forma tão específica nesta norma, devendo ser disciplinado por uma lei posterior (no caso, a lei n. 13.709 de 14 de agosto de 2018, ou Lei de Proteção de Dados Pessoais, que será abordada em um tópico adiante).

Posteriormente, no artigo 7º, incisos I, II, III, VII, VIII, IX e X, é mais específica a legislação quanto aos direitos relativos à privacidade conferidos aos usuários de internet, garantindo, no primeiro inciso, a "inviolabilidade da intimidade e da vida privada", no segundo, a "inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei" e, no terceiro, a "inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial" (BRASIL, 2014).

É importante ressaltar que, neste ponto da lei, surge a expressão "salvo por ordem judicial", indicando que a inviolabilidade assegurada não é absoluta, podendo ser derrubada em alguns casos específicos, abrindo margem para uma discussão de suma importância acerca do interesse público do Estado para a prestação da tutela jurisdicional e garantia da segurança pública contra o direito de privacidade na rede, que será abordada nesta monografia em tempo oportuno.

Seguindo o raciocínio dos primeiros três incisos do art. 7º, segue o entendimento de Teixeira (2016, p. 69)

> Assim como nas questões fiscais, bancárias, etc. o fluxo das comunicações pela internet são sigilosas e invioláveis. Nestes casos, apenas por ordem judicial, conforme a legislação a ser editada, poderá decretar a quebra do sigilo das comunicações eletrônicas estabelecidas pela internet.

Ainda, é na mesma linha o texto publicado pela Academia Brasileira de Direito do Estado – ABDET (2015, p. 7)

> No mesmo sentido, a guarda de dados e informações dos usuários da internet prevista nessa lei deve ser realizada com a estrita observância das regras constitucionais de preservação da intimidade, sendo passíveis de serem reveladas somente através de ordem judicial.

Desta forma, evidente que a proteção ao sigilo das comunicações privadas no âmbito da internet é imprescindível, conforme a legislação citada, pois garante o direito à privacidade dos usuários, observando-se o dever de indenizar, moral ou materialmente, os danos causados por aquele que viola este direito.

Dando sequência, nos incisos VII, VIII, IX e X do artigo 7º do marco regulatório, são indicados alguns direitos relativos à proteção dos dados dos usuários, sendo que muitos destes incisos carecem de eficácia por conta da necessidade de uma lei que os regulamente, carência esta que será suprida quando entrar em vigência a Lei de Proteção de Dados Pessoais, conforme será abordado em um tópico posterior.

Seguem os enunciados do artigo e dos incisos referidos acima (BRASIL, 2014)

> Art. 7o O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
> (...)
> 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;

Percebe-se que todos estes incisos se referem aos dados pessoais dos usuários e traçam linhas gerais para o devido tratamento desses dados por parte dos provedores de acesso e de aplicações de internet. O inciso VII aponta a impossibilidade de fornecimento de dados a terceiros sem consentimento expresso, o VIII cita que há uma necessidade de transparência na relação de tratamento dos dados coletados com os usuários, o inciso IX, por sua vez, trata da exigência de consentimento expresso em cláusula contratual destacada e, por último, o inciso X informa, na descrição feita pela Academia Brasileira de Direito do Estado – ABDET (2015, p. 9), que “O usuário que deseje contratar com outra Prestadora poderá requisitar ao antigo provedor que não mantenha seus dados pessoais nos registros”.

Desta forma, já no Marco Civil da Internet foram estabelecidos diversos direitos no sentido da proteção de dados pessoais, demonstrando uma preocupação e a necessidade de uma legislação com a finalidade de proteger a vida privada dos usuários, assunto que será aprofundado posteriormente, quando a Lei de Proteção de Dados Pessoais for analisada.

No artigo 8º do marco regulatório, é positivado o entendimento que "a garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet" (BRASIL, 2014), concluindo-se, então, nas palavras da Academia Brasileira de Direito do Estado – ABDET (2015, p. 10) que

> Os provedores responsáveis deverão proteger os registros, dados pessoais e as comunicações privadas dos usuários, cuja finalidade é a preservação da intimidade, da privacidade, da honra e da imagem dos usuários, sendo que a divulgação de tais informações se dará apenas através de ordem judicial, ressalvada a possibilidade das autoridades administrativas obterem os dados cadastrais, na forma da lei.

Destarte, quanto ao supracitado, "qualquer pacto celebrado entre as partes, ou mesmo termos de uso, que viole o direito à privacidade e à liberdade de expressar-se do usuário é nulo de pleno direito". (TEIXEIRA, 2016, p. 84).

O Marco Civil também determinou, no parágrafo único, inciso I, do artigo 8º, que as cláusulas contratuais que impliquem "ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela internet" (BRASIL, 2014) são nulas de pleno direito, ou seja, expressamente indicou que tal sigilo tem tanta importância no ordenamento jurídico que deve ser um direito indisponível, isso porque ninguém deve ser constrangido a aceitar esta violação em troca de, por exemplo, a utilização de um serviço, salvaguardando o usuário de práticas comerciais abusivas que visem condicionar o uso de uma aplicação de internet a uma contraprestação desproporcional, qual seja a invasão de privacidade caracterizada pelo violação do sigilo das comunicações privadas dos usuários.

O Marco Civil da Internet segue, no artigo 10, discorrendo sobre a proteção dos registros de conexão, comunicações e dados dos usuários, ao citar que

> Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
> § 1o O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7o.
> § 2o O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7o.

> § 3o O disposto no caput não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.
> § 4o As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais. (BRASIL, 2014).

Válido destacar, neste artigo, que apesar de ser reforçada a custódia do direito à privacidade, são levantadas hipóteses mais concretas da não aplicação ou do rompimento destes direitos, seguindo o que já havia sido visualizado nos incisos II e III do artigo 7º. Dessa vez, o Marco Civil remete aos artigos 22 e 23 do seu texto, que exploram a possibilidade de requerimento ao juízo durante o curso de uma ação cível ou penal para que seja ordenado aos provedores o fornecimento dos registros relacionados a determinados indivíduos.

Nessa linha, conforme a Academia Brasileira de Direito do Estado – ABDET (2015), enquanto os §§ 1º e 2º tratam da necessidade de uma ordem judicial para a disponibilização de dados pessoais e de seu conteúdo, o § 3º classifica-se como uma exceção à regra, que seria a imprescindibilidade da ordem judicial, informando que os dados de qualificação pessoal contidos no dispositivo podem ser obtidos através de uma mera requisição feita pelas autoridades administrativas, levando em conta que, conforme o art. 11, § 3º, do Decreto n. 8.771, de 11 de maio de 2016, o qual regulamentou o Marco Civil da Internet, é vedado que os pedidos desse gênero sejam, quando coletivos, inespecíficos ou genéricos. Entretanto, a legislação não é clara quanto a especificação das autoridades administrativas competentes para fazer esta requisição.

Quanto ao artigo 11, já citado no tópico da transnacionalidade da rede, é importante destacar o § 3º, que indica que

> § 3o Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações. (BRASIL, 2014).

A regulamentação referida neste artigo chegou ao ordenamento jurídico brasileiro através do Decreto n. 8.771, de 11 de maio de 2016, o qual, entre outras questões, estabeleceu alguns padrões de segurança e sigilo dos registros, dados pessoais e comunicações privadas, como os elencados no artigo 13, incisos I a IV, do seu texto

> Art. 13. Os provedores de conexão e de aplicações devem, na guarda, armazenamento e tratamento de dados pessoais e comunicações privadas, observar as seguintes diretrizes sobre padrões de segurança:

> I - o estabelecimento de controle estrito sobre o acesso aos dados mediante a definição de responsabilidades das pessoas que terão possibilidade de acesso e de privilégios de acesso exclusivo para determinados usuários;
> II - a previsão de mecanismos de autenticação de acesso aos registros, usando, por exemplo, sistemas de autenticação dupla para assegurar a individualização do responsável pelo tratamento dos registros;
> III - a criação de inventário detalhado dos acessos aos registros de conexão e de acesso a aplicações, contendo o momento, a duração, a identidade do funcionário ou do responsável pelo acesso designado pela empresa e o arquivo acessado, inclusive para cumprimento do disposto no art. 11, § 3º, da Lei nº 12.965, de 2014; e
> IV - o uso de soluções de gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados, como encriptação ou medidas de proteção equivalentes. (BRASIL, 2016).

Desta maneira, restou claro que o tratamento dos dados pessoais, comunicações e registros dos usuários deve ter padrões de segurança internos no âmbito das entidades que detenham estes registros, como a definição de responsabilidades das pessoas que terão possibilidade de acesso aos dados, mecanismos de autenticação de acesso aos registros, criação de inventário dos acessos feitos pelos funcionários e uso de outras técnicas de gestão dos registros, tudo para assegurar a maior privacidade possível.

Ainda, foi fixado, no § 2º, incisos I e II, do artigo anterior, o seguinte

> § 2o Tendo em vista o disposto nos incisos VII a X do caput do art. 7º da Lei nº 12.965, de 2014, os provedores de conexão e aplicações devem reter a menor quantidade possível de dados pessoais, comunicações privadas e registros de conexão e acesso a aplicações, os quais deverão ser excluídos:
> I - tão logo atingida a finalidade de seu uso; ou
> II - se encerrado o prazo determinado por obrigação legal. (BRASIL, 2016)

Portanto, ao ponto em que encerrar o prazo determinado na legislação para a retenção dos dados e registros, ou quando a finalidade de seu uso for atingida, estes devem ser excluídos, indicando que o tratamento destes dados não tem caráter permanente e irrestrito, sendo o seu uso vinculado à finalidade para que foi captado, com aceite expresso do usuário, e com o tempo de duração do tratamento sendo aquele especificado em lei.

Dando sequência, o artigo 13 do Marco Civil da Internet informa que cabe ao provedor de conexão ou àqueles que possuam um sistema autônomo (como algumas universidades com endereço próprio de protocolo de internet) o dever de manter os registros de conexão em ambiente seguro e sob sigilo pelo prazo de 1 ano, sendo que tal responsabilidade não pode ser transferida para terceiros, e indica a possibilidade da autoridade administrativa, policial ou do Ministério Público requerer a guarda dos registros de conexão por tempo superior.

Para efeitos do artigo anterior, Teixeira (2016, p. 106), define registros de conexão como o “conjunto de informações referentes à data e hora de início e término de uma conexão

à internet, sua duração e o endereço IP utilizado pelo terminal para envio e recebimento de pacote de dados".

Desta forma, válido ressaltar, conforme Teixeira (2016), que o mero compartilhamento de rede Wi-Fi feita por estabelecimentos empresariais não significa que eles têm o dever de guardar os registros de conexão, uma vez que, geralmente, estas empresas não possuem um sistema autônomo, e sim uma rede considerada como uma única conexão identificada pelo mesmo protocolo de internet (IP) para o provedor de conexão.

Importante destacar, também, o artigo 14 do marco regulatório, que cita que "na provisão de conexão, onerosa ou gratuita, é vedado guardar os registros de acesso a aplicações de internet" (BRASIL, 2014). Nessa linha, a Academia Brasileira de Direito do Estado – ABDET (2015, p. 15), cita que

> O legislador vedou expressamente ao provedor de conexão guardar sob sigilo os registros de acesso a aplicações da internet, ficando tal obrigação a cargo do provedor de aplicações, que deverá constituir pessoa jurídica regular e manter os dados pelo prazo de 6 meses, conforme o artigo 15.

Já no artigo 15, conforme o Marco Civil

> Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.

É importante frisar aqui que os registros de acesso a aplicações de internet, no conceito de Teixeira (2016, p. 113) "tratam-se do conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço de IP".

Além disso, de acordo com o mesmo dispositivo, no § 1º, provedores de aplicações de internet que não estão sujeitos ao disposto no caput podem ser obrigados, mediante ordem judicial, a guardarem registros de acesso a aplicações de internet relativos a fatos específicos em um período determinado; no texto do § 2º, pode ser requerido por autoridade administrativa, policial ou pelo Ministério Público, cautelarmente, a qualquer provedor de aplicações de internet, que estes registros sejam guardados por prazo superior ao previsto. Ademais, no § 3º consta a informação que, em qualquer hipótese, no âmbito do artigo 15, deve haver uma autorização judicial que preceda qualquer disponibilização dos registros ao requerente

Portanto, restou estabelecido, para auxiliar na prestação da tutela jurisdicional na rede mundial de computadores, mesmo que implicando em uma limitação do direito fundamental à privacidade, que os provedores de conexão à internet devem guardar os registros

de conexão pelo prazo de um ano e que os provedores de aplicações de internet que exerçam atividade empresarial (ou até mesmo os que não exerçam, desde que seja determinado por ordem judicial), devem guardar os registros de acesso a aplicações de internet pelo prazo de 6 meses, como regra geral.

Essencial se faz a breve análise, também, do artigo 16, incisos I e II, do Marco Civil da Internet, que visa a proteção da privacidade em duas vertentes ao afirmar que

> Art. 16. Na provisão de aplicações de internet, onerosa ou gratuita, é vedada a guarda:
> I - dos registros de acesso a outras aplicações de internet sem que o titular dos dados tenha consentido previamente, respeitado o disposto no art. 7o; ou
> II - de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular. (BRASIL, 2014).

Com efeito, tais vedações reforçam os enunciados do artigo 7º, incisos VII e IX, do marco regulatório, já abordados neste trabalho. Conforme Teixeira (2016), esse reforço está ligado principalmente à ideia de proteção contra o marketing eletrônico, nos casos em que, por exemplo, sites de busca efetuem o armazenamento de informações dos usuários que utilizam a aplicação, visando vender essas informações para empresas que queiram divulgar seus produtos para estes próprios usuários, sem que tenha havido consentimento prévio para tal prática.

Em síntese, foram suscitados os principais institutos do marco regulatório com relação ao direito à privacidade, representando, como o próprio nome da lei sugere, um marco histórico na busca não só pela efetiva prestação da tutela jurisdicional no âmbito do mundo digital, mas também pela consolidação de direitos, deveres e conceitos importantes para definir juridicamente aspectos relacionados à internet, aos usuários, aos provedores e ao Estado.

Desta maneira, passaremos então à análise da Lei n. 13.709, de 14 de agosto de 2018, também conhecida como Lei Geral de Proteção de Dados – LGPD.

4.3 LEI GERAL DE PROTEÇÃO DE DADOS

A LGPD chegou ao ordenamento jurídico brasileiro, e entrará em vigor a partir de fevereiro de 2020, devido à necessidade de uma regulamentação acerca das questões relacionadas aos dados pessoais, principalmente com o crescente mercado publicitário nas redes, que movimenta uma quantia monetária titânica, sendo responsável pela consolidação de muitas das maiores empresas do mundo, como as chamadas “Big Four” da tecnologia, quais sejam o Facebook, Google, Amazon e Apple.

A relação entre os dados dos usuários captados pelos provedores de aplicação de internet e a ascensão de verdadeiros impérios que têm como comandantes os homens mais ricos do planeta está, principalmente, no fato de que, conforme Bioni (2018, l. 530),

> Com a inteligência gerada pela ciência mercadológica, especialmente quanto a segmentação dos bens de consumo (marketing) e a sua promoção (publicidade), os dados pessoais dos cidadãos converteram-se em um fator vital para a engrenagem da economia da informação.

Além disso, "com a possibilidade de organizar tais dados de maneira mais escalável (e.g., Big Data), criou-se um (novo) mercado cuja base de sustentação é a sua extração e comodificação" (BIONI, 2018, l. 530).

Tendo-se o termo "comodificação" empregado como a transformação dos dados coletados em produtos a serem vendidos, é possível visualizar que a publicidade na tecnologia, como uma publicidade direcionada, com o uso de algoritmos para maximizar a propagação e a identificação dos usuários com os produtos ofertados, tornou-se uma indústria multibilionária. Basta analisar, por exemplo, o valor de mercado do Facebook, que depende diretamente deste novo negócio, empresa que, conforme o site Statista (2018), possui o valor avaliado em quinhentos e quarenta e um bilhões e quinhentos milhões de dólares.

Através do tratamento de dados, combinado com a tecnologia atual, Bioni (2018) informa que são geradas classificações e segmentações das preferências, das tendências ideológicas e até mesmo do histórico de compras dos usuários, num processo conhecido como "profiling", no qual

> Os dados pessoais de um indivíduo formam um perfil a seu respeito para a tomada de inúmeras decisões. […]. Na famosa expressão de Eli Pariser, há uma bolha que, como um filtro invisível, direciona desde a própria interação do usuário com outras pessoas em uma rede social até o acesso e a busca por informação na rede. Doutrina-se a pessoa com um conteúdo e uma informação que giram em torno dos interesses inferidos por intermédio dos seus dados, formando-se uma bolha que impossibilita o contato com informações diferentes […]. (BIONI, 2018, l. 2.290).

Assim, por mais que não seja o objetivo deste trabalho monográfico discutir questões relativas ao direito de liberdade de informação na internet, percebe-se que a privacidade e a liberdade estão extremamente conectadas e até mesmo se confundem em diversos momentos nas relações do mundo digital. Paesani (2014, p. 5), explica que

> A liberdade de informação tem sido definida como a mãe de dois direitos: de informar e de ser informado. A informação deve ser observada sob o aspecto ativo e passivo. […] o aspecto passivo salvaguarda o direito de assimilar e receber as notícias e as opiniões expressas por alguém. Neste último caso, tem-se a liberdade de se informar, que Casavola define como atividade de indagação ou inspectio. É do equilíbrio entre esses dois perfis – ativo e passivo – da liberdade de informação que se garante a comunicação no interior de uma sociedade pluralista.

Ou seja, enquanto a coleta de dados, quando ilícita, gera uma invasão de privacidade frente ao titular, o tratamento destes dados com a formação de um profiling do titular, que toma diversas decisões acerca de, por exemplo, conteúdos que serão exibidos para este usuário, acaba por violar o direito de liberdade de informação, pois cerceia a possibilidade de exposição aos conteúdos que não estejam de acordo com o perfil criado para o titular, em outras palavras, cria uma bolha.

O problema é que, mesmo em um tratamento realizado licitamente, sendo inclusive com dados anonimizados, através da formação destes profilings, não apenas o titular é afetado pelas informações que recebe ou deixa de receber, interferindo em sua liberdade de acesso à informação e colocando-o em uma bolha, de forma que acaba por gerar um processo totalmente contrário à proposta inicial da internet, causando um isolamento social e uma ignorância daquilo que não está definido dentro dos parâmetros estabelecidos pelo algoritmo que decide o conteúdo ao qual o titular será exposto, como o titular também pode ser prejudicado de diversas outras formas ainda mais tangíveis na vida em sociedade.

Nesse sentido, uma vez que os dados são coletados e enviados para pacotes que possuem as mesmas características, são elaborados algoritmos que podem interpretar estes dados de inúmeras maneiras, dependendo do objetivo determinado pelo controlador, o qual pode ser, por exemplo, um levantamento de dados que correlaciona a prática de crimes à certa preferência de gênero musical, ou a prática de crimes à determinada inclinação política. O conteúdo destes estereótipos (preconceitos) poderia então ser vendido às empresas interessadas, de forma que o indivíduo “A”, ao procurar emprego na empresa “B”, pelo simples fato de gostar do gênero musical “C” e ter a inclinação política “D”, poderia ter seu pedido rejeitado por conta destas características estarem ligadas à pratica de crimes, fato que, por sua vez, geraria maior índice de desemprego para os indivíduos com as mesmas propensões de “A”, aumentando o coeficiente de criminalidade destas pessoas e perpetuando o estereótipo criado.

As novas tecnologias proporcionaram uma individualização das preferências pessoais daqueles que usam o serviço para um posterior agrupamento em um banco de dados onde todos possuem as mesmas tendências, criando grandes pacotes de estereótipos, tornando o processo publicitário mais simples, mais eficiente e relativamente mais barato.

A grande eficiência trazida por este novo mercado reside no fato de que uma propaganda ofertando uma churrasqueira em um canal aberto na televisão vai atingir toda sorte de pessoas, tem um caráter muito difuso, apenas uma minoria estará realmente interessada no produto, sendo assim muito pouco eficiente. Por outro lado, a propaganda desta mesma churrasqueira exibida dentro dos perfis de usuários de provedores de aplicação de internet que

gostem de churrasco ou culinária será extremamente mais eficiente, ainda que atingindo apenas uma parcela dos indivíduos que seriam impactados pela oferta publicitária no veículo de comunicação mais difuso, pois o interesse daqueles usuários é superior.

Conforme Bioni (2018), este modelo atual explica o fato de que a grande maioria dos conteúdos disponíveis na rede mundial de computadores são "gratuitos", fugindo do padrão tradicional de consumo onde uma prestação pecuniária é trocada por um serviço ou produto; aqui, o produto é o usuário, e a sua contraprestação pelos serviços disponibilizados é o fornecimento de seus dados.

Nesta recente modalidade de negócios, o principal instrumento de tratamento de dados é um contrato de adesão nomeado, geralmente, de Política de Privacidade, no qual o usuário é exposto aos termos do contrato, sendo condicionada a efetiva utilização da aplicação à concordância (consentimento) destes termos. Porém, tal instrumento apresenta grandes vícios "[...] seja porque ele reforça a aventada assimetria do mercado informacional, seja porque se trata de uma ferramenta que não capacita, efetivamente, o cidadão para exercer controle sobre suas informações pessoais". (BIONI, 2018, l. 4.603).

Entretanto, mesmo que superada a barreira da desinformação e atingido o objetivo de se possibilitar um verdadeiro esclarecimento dos termos do tratamento, de forma que o consentimento seja livre de qualquer vício, ainda há o revés de que, em muitos casos, o usuário é compelido ao aceite de qualquer imposição feita pelo agente de tratamento, uma vez que a conexão entre algumas aplicações, como o Facebook ou Google, e a vida em sociedade é muito próxima, fazendo com que o indivíduo que não participe dessas aplicações sofra com um constante isolamento social.

Nessa linha, informa Bioni (2018, l. 4.603)

> Essa dinâmica dos contratos de adesão assinala, sobretudo, a assimetria de forças das relações de consumo, na medida em que o seu elo mais forte fixa unilateralmente o programa contratual. Isso significa, em termos de proteção de dados pessoais, que será o fornecedor quem determinará os rumos do fluxo informacional dos seus usuários, eliminando, praticamente, qualquer faixa de controle a ser por eles operada.

Desta forma, com este novo mercado em evidência, verificou-se uma demanda expressiva para a regulamentação das questões relativas aos dados, como as hipóteses de tratamento de dados, os direitos do titular dos dados, as responsabilidades e a segurança, principalmente como forma de delimitar os requerimentos contidos nas Políticas de Privacidade das aplicações de internet.

4.3.1 Conceitos Preliminares

Partindo para a análise da Lei Geral de Proteção de Dados propriamente dita, já no segundo artigo da lei temos como primeiro fundamento elencado para a proteção de dados pessoais o "respeito à privacidade" e, no inciso IV, a "inviolabilidade da intimidade, da honra e da imagem", demonstrando prontamente a preocupação do legislador em evitar abusos no sentido das práticas utilizadas para a captação e tratamento de dados.

O artigo 5º da LGPD traz conceitos importantes acerca do tema, dentre os quais vale destacar os tipos de dados, contidos nos incisos I à IV, na forma que segue

> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> II - dado pessoal sensível: dado pessoal sobre 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;
> III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
> IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico; (BRASIL, 2018).

Destarte, quanto à diferença de dado pessoal e dado pessoal sensível, Bioni (2018, l. 2.200) informa que "os dados sensíveis são uma espécie de dados pessoais que compreendem uma tipologia diferente em razão de o seu conteúdo oferecer uma especial vulnerabilidade: discriminação". Por esse motivo, a LGPD protege ainda mais os dados pessoais sensíveis, conforme ainda será visto, pois o dano potencial de sua violação é, em regra, maior que apenas o de dados pessoais.

Enquanto nos dados pessoais sensíveis a proteção positivada é maior, nos dados anonimizados ocorre o contrário, isso porque, logicamente, o fato da impossibilidade de identificação da pessoa relacionada ao dado representa um baixo potencial de dano àquele indivíduo. Segundo o artigo 12 da Lei Geral de Proteção de Dados, os dados anonimizados somente serão considerados dados pessoais " [...] quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido". (BRASIL, 2018).

É relevante, também, analisar o conceito de "tratamento", o qual será utilizado com frequência nos artigos da LGPD, trazido pelo inciso X do artigo 5º desta lei

> X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração; (BRASIL, 2018).

Dessa forma, ao analisar-se a política de dados atual do Facebook, ficam evidenciadas diversas formas de tratamento de dados, como a coleta, quando cita, por exemplo, que "coletamos informações sobre como você usa nossos Produtos, como o tipo de conteúdo que você visualiza ou com o qual se envolve; os recursos que você usa", também a recepção, quando informa que "os anunciantes, desenvolvedores de aplicativos e publishers podem nos enviar informações [...]. Esses parceiros fornecem informações sobre suas atividades fora do Facebook [...]", a utilização, ao ponto em que discorre, em seus termos, que "usamos informações relacionadas à localização, como sua localização atual, onde você mora, os lugares que você gosta de frequentar, bem como as empresas e pessoas das quais você está próximo [...]" (FACEBOOK, 2018), entre outras formas de tratamento.

Ademais, a Lei Geral de Proteção de Dados traz as definições acerca das pessoas envolvidas em uma relação de dados, contidas nos incisos V à IX do artigo 5º

> V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
> VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
> VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
> VIII - encarregado: pessoa natural, indicada pelo controlador, que atua como canal de comunicação entre o controlador e os titulares e a autoridade nacional;
> IX - agentes de tratamento: o controlador e o operador; (BRASIL, 2018).

Nesse sentido, no exemplo utilizado anteriormente sobre o Facebook, os usuários da aplicação de internet são os titulares dos dados, enquanto a empresa se porta geralmente tanto como controlador, pois toma as decisões referentes ao tratamento de dados, quanto operador, pois realiza o tratamento destes dados, como acontece na maioria dos casos. Entretanto, nada impede que seja terceirizada a função de operador, sendo essa distinção importante pois acarreta em algumas diferenças de responsabilidades.

É de extrema importância frisar, também, o conceito de "consentimento", que, conforme Bioni (2018) é a definição central da LGPD, estando contido no artigo 5º, inciso XII, da LGPD, na forma que segue "XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada" (BRASIL, 2018).

Nessa linha, Bioni (2018, l. 3.736), informa, sobre o instituto do consentimento, que

> [...] grande parte dos princípios tem todo o seu centro gravitacional no indivíduo: a) de um lado, princípios clássicos, como a transparência, a especificação de propósitos, de acesso e qualidade de dados por meio do quais o titular do dado deve ser munido

> com informações claras e completas sobre o tratamento de seus dados e, ainda, ter acesso a eles para, eventualmente, corrigi-los; b) de outro lado, princípios mais "modernos", como adequação e necessidade, em que o tratamento dos dados deve corresponder às legítimas expectativas do seu titular. Isso deve ser perquerido de acordo com a finalidade especificada para o tratamento dos dados, assegurando-se que os dados sejam pertinentes, proporcionais e não excessivos (minimização de dados).

Bioni (2018), frisa que o termo "consentimento" é invocado 35 vezes na LGPD, demonstrando o quanto é fundamental para que possa haver uma efetiva proteção de dados e da privacidade, uma vez que, em diversos casos, o fato de ser verificado o devido consentimento transforma uma prática ilícita em lícita.

4.3.2 Tratamento de Dados Pessoais

A Lei Geral de Proteção de Dados traz diversos institutos acerca do tratamento de dados, sendo este a peça central da legislação. Enquanto o consentimento é o vetor principal para o tratamento de dados, este último é a matriz que deve ser observada nas relações que envolvam os dados.

O artigo 6º da LGPD indica que, no tratamento de dados pessoais, deve ser observada a boa-fé e outros princípios elencados, alguns já citados anteriormente, sendo importante destacar todas as definições trazidas pela lei, conforme seguem:

O princípio da finalidade, elencado no inciso I do artigo supra, tem sua definição como a "realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular" (BRASIL, 2018). Logo, deve ser respeitado o consentimento de finalidade cedido pelo titular, não podendo o tratamento dos dados superar os limites estabelecidos claramente pela manifestação da pessoa a quem se referem os dados. Quanto à legitimidade do interesse do controlador no tratamento de dados, o artigo 10 da LGPD traz duas hipóteses exemplificativas, sendo a principal o apoio e promoção de atividades do controlador.

O princípio da adequação, contido no inciso II do mesmo artigo, significa a "compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento" (BRASIL, 2018). O tratamento de dados não pode desviar seu curso daquele estabelecido, respeitando a finalidade para a qual foi concedido o consentimento, devendo ser aplicado o princípio da razoabilidade, uma vez que depende do contexto.

No inciso III verifica-se o princípio da necessidade, que é a "limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados" (BRASIL, 2018). Nessa linha, não deve o tratamento de dados superar o que baste para

cumprir a finalidade, mesmo que este poder tenha sido outorgado pelo titular. O artigo 10, § 1º, da LGPD traz uma confirmação deste instituto, ao ponto que afirma que "quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados". (BRASIL, 2018).

O inciso IV trata do princípio do livre acesso, sendo a "garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais" (BRASIL, 2018). Ou seja, deve ser fornecida a possibilidade para que o titular consulte facilmente e gratuitamente os aspectos do tratamento de seus dados, para que possa exercer certa fiscalização e controle. O artigo 9º da LGPD complementa este princípio, elencando algumas informações que devem ser disponibilizadas ao titular, como a finalidade, forma e duração do tratamento e informações de contato do controlador.

Já no inciso V, está positivado o princípio da qualidade dos dados, como a "garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento" (BRASL, 2018). Com efeito, o tratamento de dados deve corresponder à realidade daquilo que foi coletado, devendo manter-se atualizado.

O princípio da transparência, positivado no inciso VI, é a "garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial" (BRASIL, 2018). Nesse sentido, assemelha-se muito ao princípio do livre acesso; a diferença é que, enquanto o livre acesso busca a formação de uma estrutura de consulta de forma facilitada e gratuita, a transparência objetiva que o conteúdo dessa estrutura seja condizente à realidade, e que abrace os mais diversos campos do tratamento com informações claras.

No inciso VII, verifica-se o princípio da segurança, que trata da "utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão" (BRASIL, 2018). Com a grande quantidade de vazamento de dados e ataques cibernéticos, é essencial que sejam fornecidas garantias aos usuários para que não sofram prejuízos pelo tratamento de seus dados, motivo pelo qual este tratamento deve ser realizado da forma mais segura possível, utilizando-se as medidas técnicas e administrativas cabíveis. Ainda, a LGPD traz alguns institutos fundamentais relacionados à aplicação e efetividade deste princípio, contidos entre os artigos 46 e 49 da lei, de forma que é importante destacar a possibilidade da autoridade nacional dispor sobre medidas de segurança mínima que devem ser

observadas e também a responsabilidade de garantir a segurança dos dados por parte de todo agente de tratamento, e até mesmo por parte de qualquer pessoa que venha a intervir no tratamento, ainda que após o término deste.

Por sua vez, o inciso VIII trata do princípio da prevenção, sendo que deve haver a "adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais" (BRASIL, 2018). Diferentemente do princípio da segurança, o da prevenção não abrange hipóteses de proteção contra erro ou violação no âmbito do tratamento de dados, e sim determina que, caso verificadas as hipóteses de erro ou violação, o agente de tratamento tenha meios de prevenção da efetiva geração de danos, e também indica a utilização de medidas preventivas para que o ato de tratamento de dados não cause danos aos indivíduos.

O inciso IX traz o princípio da não discriminação com a definição de "impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos" (BRASIL, 2018). Assim, conforme Bioni (2018), a proteção de dados é, também, instrumento de contenção às práticas discriminatórias, e esta tutela permite ao usuário a possibilidade de se relacionar e se realizar na sociedade sem as barreiras discriminatórias, servindo assim até mesmo como uma ferramenta de isonomia.

Por último, o inciso X traz o princípio da responsabilização e prestação de contas, sendo, portanto, conforme indica a norma, a "demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas" (BRASIL, 2018). Dessa maneira, ficou estabelecido que é de responsabilidade dos agentes a adoção de medidas eficazes para o cumprimento das normas, sendo necessária a demonstração da adoção e de eficácia. Assim, o artigo 42 da LGPD definiu que

> O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo. (BRASIL, 2018).

Além disso, o artigo 42 também instituiu duas responsabilidades solidárias de grande impacto no ordenamento jurídico: a primeira é a do operador, que responde solidariamente junto do controlador quando "descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador" (BRASIL, 2018); a segunda se dá de forma horizontal entre todos os controladores que estiverem diretamente envolvidos no processo de tratamento que gerou danos ao titular.

Ademais, a LGPD também consagrou uma espécie de inversão de ônus da prova que muito se assemelha à consumerista, pois, conforme o artigo 42, § 2º, da Lei Geral de Proteção de Dados,

> o juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa. (BRASIL, 2018).

Logo, como o titular apresenta extrema vulnerabilidade com relação ao agente de tratamento, que geralmente é uma grande empresa, o legislador optou por garantir a possibilidade de inversão de ônus da prova através das alternativas supracitadas.

Os princípios citados serão, como o próprio nome indica, a base de toda a regulamentação acerca do tratamento de dados, que inicia de forma mais específica no artigo 7º da LGPD, quando cita as hipóteses em que o tratamento de dados será possível, de forma que qualquer violação a estas hipóteses implica em uma invasão de privacidade. O inciso I deste artigo aponta o primeiro (e principal) caso em que será permitido o tratamento de dados, que é "mediante o fornecimento de consentimento pelo titular", sendo que este consentimento deve ser, conforme o artigo 8º da mesma lei, "[...] fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular" e, caso seja escrito, "[...] esse deverá constar de cláusula destacada das demais cláusulas contratuais" (§ 1º) (BRASIL, 2018). Ainda, são nulas as autorizações genéricas para o tratamento de dados, devendo o consentimento referir-se a finalidades específicas (§ 4º), sendo que ele pode ser revogado a qualquer momento, caso manifeste de forma expressa o titular (§ 5º). Ademais, é importante frisar que o § 4º do artigo 7º deixou claro que não se exige consentimento quando o titular tornar públicos os dados, ou seja, ninguém pode alegar que teve sua privacidade invadida quando o próprio titular disponibiliza seus dados de forma pública na aplicação de internet utilizada.

É possível perceber que a grande maioria das aplicações de internet estão em desconformidade com as regras supracitadas. Certamente, a mera disponibilização de um texto escrito após o processo de cadastramento do Facebook (2018), na forma que segue "ao clicar em Inscreva-se, você concorda com nossos Termos, Política de Dados e Política de Cookies. Você pode receber notificações por SMS e pode cancelar isso quando quiser", assim como visualizado em diversos outros sites, não caracteriza um destaque sobre as formas de tratamento de dados, não sendo verificado então o consentimento por parte do titular em ter seus dados tratados pela aplicação, que desconhece, em parte ou totalmente, o que está sendo cedido.

Nessa mesma linha, também não está em conformidade com a LGPD a empresa Google, que é, em diversos momentos, na sua Política de Privacidade, genérica quanto aos dados coletados, ao citar, por exemplo, que "quando você não está conectado a uma Conta do Google, armazenamos as informações que coletamos com identificadores exclusivos vinculados ao navegador, aplicativo ou dispositivo que você está usando" (GOOGLE, 2018), e também "quando você está conectado, também coletamos informações que armazenamos com sua Conta do Google e que tratamos como informações pessoais" (GOOGLE, 2018). Nota-se que em nenhum momento a empresa expõe quais são as informações que estão sendo coletadas, violando claramente o já abordado § 4º do artigo 8º da Lei Geral de Proteção de Dados.

No âmbito do tratamento de dados pessoais sensíveis, uma vez que se referem a questões relacionadas à discriminação, de forma que possuem um potencial de dano maior caso não sejam tratados da maneira mais adequada, a LGPD optou por suprimir algumas das hipóteses de cabimento de tratamento de dados pessoais quando a relação se referir a dados pessoais sensíveis, determinando, por exemplo, a impossibilidade no caso de proteção de crédito, que é viável quando forem simplesmente dados pessoais.

Já no caso de tratamento de dados pessoais de crianças e adolescentes, é de suma importância destacar o § 4º do artigo 14 da LGPD, o qual dispõe sobre a impossibilidade de condicionar a entrega de produtos ou prestação de serviços, como jogos, aplicações de internet ou outras atividades, ao fornecimento de informações pessoais de crianças, além daquelas necessárias para que a atividade seja realizada. Nesse sentido, a legislação expõe uma grande preocupação com os infantes, que constituem um grupo de usuários da internet que possui alta vulnerabilidade a qualquer violação ou ameaça de violação aos seus direitos. Assim, atividades que possuem alto apelo infantil, como aplicativos de jogos, não podem se aproveitar desta situação para tratar os dados destes jovens.

4.3.3 Término do Tratamento de Dados Pessoais

O artigo 15 da LGPD elenca seis hipóteses de término do tratamento de dados, sendo relevante analisá-los pois qualquer tratamento que continue ocorrendo após constatado um destes cenários será tido como uma violação do direito fundamental à privacidade do titular, fazendo incidir uma responsabilidade dos agentes de tratamento.

Desta forma, observa-se o término do tratamento de dados quando houver algum dos casos a seguir

> I - verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;
> II - fim do período de tratamento;
> III - comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou
> IV - determinação da autoridade nacional, quando houver violação ao disposto nesta Lei. (BRASIL, 2018).

Apesar de existirem apenas quatro incisos, o primeiro se subdivide em três hipóteses: a primeira seria a análise de que a finalidade do tratamento foi atingida; já a segunda e a terceira, apesar de serem abordadas como duas hipóteses díspares, uma vez que o termo "pertinente" engloba o termo "necessário" (pois tudo aquilo que é necessário também é pertinente), é viável ignorar a condição da necessidade dos dados para o alcance da finalidade almejada, podendo apenas ser feita a indagação se é pertinente a continuidade deste tratamento.

É importante frisar, também, que a revogação do consentimento consiste em um direito titular, na forma do artigo 18, inciso IX, da LGPD, podendo ser feito a qualquer momento, o que não implica, logicamente, que a contraprestação do tratamento de dados deve ter continuidade com aquele que revogou o consentimento. Assim, há a possibilidade do titular não poder mais utilizar a aplicação ao ponto em que revogar o seu consentimento, dando término ao tratamento de seus dados.

Ainda, após o término do tratamento, conforme o artigo 16 da LGPD, devem ser eliminados os dados pessoais, de forma a garantir maior segurança ao titular, sendo possível a conservação apenas para:

> I - cumprimento de obrigação legal ou regulatória pelo controlador;
> II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou
> IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados. (BRASIL, 2018).

Nesse sentido, conforme o inciso IV, o término do tratamento não se dará em todos os seus termos na eventualidade de uso exclusivo pelo controlador, nos casos em que forem anonimizados, uma vez que a utilização de dados é uma espécie de tratamento. De certa forma, mesmo que haja o término do tratamento de dados por alguma das circunstâncias previstas no artigo 15, o inciso IV do artigo 16 abre margem para uma interpretação onde o tratamento não alcançará efetivamente o seu término, desde que preenchidos aqueles requisitos.

4.3.4 Direitos do Titular dos Dados

Os direitos do titular conferidos na Lei Geral de Proteção de Dados estão entre os artigos 17 e 22, e têm respaldo naqueles princípios já abordados nesta monografia. Dessa forma, é garantido ao titular o acesso, a correção e a portabilidade de seus dados, assim como a anonimização e a eliminação destes dados nas hipóteses cabíveis, tudo de forma gratuita, desde que haja o requerimento para tal ao controlador.

Outro direito de extrema importância é aquele elencado no § 3º do artigo 19 da LGPD, pois indica que

> Quando o tratamento tiver origem no consentimento do titular ou em contrato, o titular poderá solicitar cópia eletrônica integral de seus dados pessoais, observados os segredos comercial e industrial, nos termos de regulamentação da autoridade nacional, em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento. (BRASIL, 2018).

Assim, novamente é demonstrada a preocupação do legislador quando o tratamento se refere à hipótese de fornecimento de consentimento, conferindo ao titular o direito de obter uma cópia eletrônica integral de seus dados, de forma que possa exercer controle ainda maior acerca do tratamento.

4.3.5 Interesse Público versus Direito Fundamental à Privacidade Online

O contexto mundial atual é marcado por um confronto entre a privacidade na rede e os limites de atuação do Estado sob a justificativa de interesse público, que visa, ao menos em teoria, garantir os direitos dos usuários da internet.

Esta “guerra” tem algumas batalhas marcantes, de forma que os soldados nas trincheiras do mundo digital constantemente respondem, em retaliação, e de forma extremamente ágil, às investidas estatais. Por exemplo: quando instituições governamentais começaram a rastrear registros de conexão e de acesso dos usuários, e até mesmo a restringir certos acessos, a internet reagiu com a utilização de VPNs (Virtual Privator Network), que são redes privadas usadas para, entre outras funções, garantir maior privacidade e liberdade ao usuário em razão da dificuldade de rastreamento, caso extremamente comum em países mais fechados, como a China.

Além disso, outro caso relacionado que está bastante em evidência atualmente é o atinente às criptomoedas, como o Bitcoin, que são moedas geralmente desvinculadas de

qualquer instituição governamental e de difícil rastreamento, garantindo, novamente, maior liberdade e privacidade àqueles que as utilizam, enfraquecendo o poder estatal.

No Brasil, tivemos alguns casos de alta repercussão que evidenciam a dicotomia entre interesse público e privacidade, como os de bloqueio do aplicativo Whatsapp no país entre 2015 e 2016, nos quais a justiça determinava, conforme o jornal G1 (2016), o bloqueio do aplicativo em face da negativa de concessão das informações requisitadas, sob o argumento de que tais informações eram necessárias para investigações criminais.

No âmbito da Lei Geral de Proteção de Dados, existem alguns pontos que geram preocupação quanto ao futuro alcance da atuação do Poder Público em detrimento do sigilo dos dados dos titulares. O inciso III do artigo 4º da LGPD indica que ela não será aplicada no caso de tratamento de dados pessoais

> III - realizado para fins exclusivos de:
> a) segurança pública;
> b) defesa nacional;
> c) segurança do Estado; ou
> d) atividades de investigação e repressão de infrações penais; (BRASIL, 2018)

Por outro lado, o § 1º do mesmo artigo informa que o tratamento de dados nos casos do inciso III "será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei" (BRASIL, 2018). Sendo assim, é essencial que a referida legislação específica que venha a ser elaborada não só garanta, em seu texto, direitos aos titulares de forma que assegurem a sua privacidade, como também que preze pela eficácia destas normas, penalizando qualquer extrapolação do legítimo interesse público.

Válido ressaltar que o receio apresentado não é infundado, uma vez que foram institutos semelhantes a este do artigo 4º, inciso III, da LGPD que precederam a alta vigilância feita pela NSA (Agência de Segurança Nacional dos EUA), que teve sua criação após os atentados de 11 de setembro de 2001, nos Estados Unidos da América, através de uma lei denominada "Patriot Act" (Ato Patriota), a qual garantia à NSA, por exemplo, "autoridade para interceptar comunicações de via elétrica, oral ou de cabos, relacionadas ao terrorismo" (EUA, 2001), sendo que esta operação culminou com o vazamento de documentos feito por Edward Snowden, em 2013, os quais evidenciam, principalmente, "programas de vigilância que o país usa para espionar a população americana – utilizando servidores de empresas como Google, Apple e Facebook –" (G1, 2014), que manifestamente superavam os horizontes estabelecidos

na legislação, causando um escândalo mundial e fixando o debate sobre os limites da atuação governamental em nome da segurança nacional contra o direito fundamental à privacidade.

Por outro lado, fora da esfera abarcada pelo artigo 4º da LGPD, o artigo 23 da mesma legislação prevê outras hipóteses de tratamento pelo Poder Público, quais sejam elas:

> Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:
> I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos; e
> […]
> III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei. (BRASIL, 2018).

Logo, não se tratando de casos relativos à segurança pública, do Estado ou de defesa nacional, o Poder Público apenas poderá realizar o tratamento de dados no cenário acima exposto, sendo necessário o fornecimento de informações claras sobre a previsão legal deste tratamento, na qual, em tese, não pode ser arguida qualquer hipótese do artigo 4º, pois este engloba possibilidades de não aplicação da LGPD, e não de justificativa de tratamento de dados através dela. Em outras palavras, uma vez que a própria escusa da defesa nacional ou da segurança pública já exclui a aplicação da lei, invocar o artigo 23 para fundamentar o tratamento de dados nestes casos não é apenas ineficaz (já que existe outra previsão legal para atingir este objetivo), como também é impossível, afinal, se as hipóteses do artigo 4º excluem a aplicação da LGPD, o artigo 23 desta norma não pode ser invocado cumulativamente.

Assim, deve ser entendido que o artigo 23 indica que o Poder Público deve respeitar os pressupostos gerais estabelecidos na LGPD para o tratamento de dados, ou qualquer outra norma que tenha relação com tratamento de dados.

5 CONCLUSÃO

O estudo realizado para a elaboração da presente monografia, aqui englobando-se a análise legislativa, de doutrinas, de notícias e das políticas de privacidade de alguns fornecedores de aplicações de internet, acerca do direito fundamental à privacidade, principalmente com o advento da Lei Geral de Proteção de Dados, permite uma compreensão melhor da reação do ordenamento jurídico para com os fenômenos trazidos pela Rede Mundial de Computadores e, desta compreensão, é possível extrair-se algumas conclusões.

A primeira que, apesar de possuir um aspecto geral, é de suma importância, reside no fato de que a internet modificou as relações humanas no mundo moderno nos mais diversos aspectos: econômico-financeiro, social, educacional, etc. Assim, a criação de normas e soluções legais específicas para o mundo digital, de forma que superem ou tentem superar os obstáculos trazidos por ele, são necessárias para que a prestação da tutela jurisdicional seja efetiva na sociedade como um todo.

Ainda, conclui-se que o processo evolutivo das normas relacionadas à Rede Mundial de Computadores buscou constantemente a garantia do direito fundamental à privacidade, uma vez que a Lei Carolina Dieckmann define a invasão de dispositivo informático alheio como crime, que o Marco Civil da Internet discorre sobre diversas inviolabilidades de comunicações e informações privadas, e finalmente a Lei Geral de Proteção de Dados dispõe principalmente sobre as hipóteses e o cenário em que pode ocorrer o tratamento de dados pessoais, protegendo o titular de práticas comerciais abusivas.

Nesse sentido, provedores de aplicações de internet terão que se adaptar às regras trazidas pela Lei Geral de Proteção de Dados, que diferem em grande parte das práticas utilizadas por estes provedores atualmente, como a necessidade de uma cláusula destacada e específica acerca do que está sendo consentido ao registrar-se naquela aplicação, garantindo maior proteção aos titulares.

Ademais, com a exposição da dicotomia formada pelo interesse público na defesa nacional e segurança pública e pelo direito fundamental à privacidade, considerando que há a previsão de elaboração de uma norma para regulamentar este ponto, é necessário que ela busque o equilíbrio entre estes dois institutos, com a finalidade de garantir a proteção do indivíduo contra qualquer abuso que eventualmente possa vir a ser praticado pelas autoridades nacionais, como o ocorrido nos Estados Unidos da América através do Ato Patriota.

REFERÊNCIAS

ACADEMIA BRASILEIRA DE DIREITO DO ESTADO – ABDET. **Comentários ao Marco Civil da Internet.** Disponível em: <http://abdet.com.br/site/wp-content/uploads/2015/02/MCI-ABDET..pdf>. Acesso em: 15 de setembro 2018.

ARAUJO, Luiz Alberto David; NUNES JÚNIOR, Vidal Serrano. **Curso de Direito Constitucional**. 9. ed. São Paulo: Saraiva, 2005.

BARROS, Alice Monteiro de. **Proteção à intimidade do empregado**. 2.ed. São Paulo: LTr, 2009.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoas –** A Função e os Limites do Consentimento. São Paulo: Editora Forense, 2018.

BRASIL, DECRETO Nº 8.771, DE 11 DE MAIO DE 2016. **Regulamenta a Lei no 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações,** Brasília, DF, 2016. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8771.htm> Acesso em: 16 de setembro de 2018.

BRASIL. **Constituição da República Federativa do Brasil de 1988,** Brasília, DF, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm> Acesso em: 18 de outubro de 2018

BRASIL, LEI Nº 10.406, DE 10 DE JANEIRO DE 2002. **Institui o Código Civil**, Brasília, DF, 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/L10406compilada.htm>. Acesso em: 20 de outubro de 2018.

BRASIL. LEI Nº 12.965, DE 23 DE ABRIL DE 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil**, Brasília, DF, abril 2014. Disponivel em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm >. Acesso em: 5 out. 2018.

BRASIL, LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012. **Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências,** Brasília, DF, 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm>. Acesso em: 14 de setembro de 2018.

BRASIL, LEI Nº 13.709, DE 14 DE AGOSTO DE 2018. **Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet),** Brasília, DF, 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm> Acesso em: 4 de novembro de 2018.

BRASIL, PEC 479/2010. **Acrescenta o inciso LXXIX ao art. 5º da Constituição Federal, para Incluir o acesso à Internet em alta velocidade entre os direitos fundamentais do cidadão**, Brasília, DF, abril 2010. Disponível em: < https://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=473827#marcacao-conteudo-portal>. Acesso em: 15 de outubro de 2018.

BULOS, Uadi Lammêgo. **Curso de Direito Constitucional.** 5 ed. rev. e atual, São Paulo: Saraiva, 2010.

CANCELIER, Mikhail Vieira de Lorenzi. **O Direito à Privacidade hoje:** perspectiva histórica e o cenário brasileiro. Disponível em: <http://www.scielo.br/pdf/seq/n76/2177-7055-seq-76-00213.pdf>. Acesso em: 20 de outubro de 2018.

CETIC. **TIC Domicílios – 2017 Indivíduos: C1 – Indivíduos que já acessaram a internet.** Disponível em: < https://www.cetic.br/tics/domicilios/2017/individuos/C1/>. Acesso em: 12 de outubro de 2018.

CETIC. **TIC Domicílios – 2017 Indivíduos: C2 – Indivíduos, por último acesso à internet.** Disponível em: < https://www.cetic.br/tics/domicilios/2017/individuos/C2/>. Acesso em: 12 de outubro de 2018.

CERVO, Amado Luiz; BERVIAN, Pedro Alcino. Metodologia científica: para uso de estudantes universitários. 3. ed. São Paulo: McGraw-Hill do Brasil, 1983.

DA SILVA, José Afonso. **Curso de Direito Constitucional Positivo**. 23 ed. rev. e atual. São Paulo: Malheiros Editores Ltda, 2004.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** Rio de Janeiro: Renovar, 2006

ESTADOS UNIDOS DA AMÉRICA, PUBLIC LAW 107–56—OCT. 26, 2001. **Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001**. Disponível em: <https://grants.nih.gov/grants/policy/select_agent/Patriot_Act_2001.pdf>. Acesso em: 8 de novembro de 2018.

FACEBOOK. **Política de Dados.** Disponível em: <https://www.facebook.com/privacy/explanation>. Acesso em: 10 de outubro de 2018.

FOLHA DE S. PAULO. **Empresários bancam campanha contra o PT pelo WhatsApp.** Disponível em: <https://www1.folha.uol.com.br/poder/2018/10/empresarios-bancam-campanha-contra-o-pt-pelo-whatsapp.shtml>. Acesso em: 10 de outubro de 2018.

G1. **Entenda o caso de Edward Snowden, que revelou espionagem dos EUA.** Disponível em: <http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html>. Acesso em: 7 de novembro de 2018.

G1. **WhatsApp bloqueado:** Relembre todos os casos de suspensão do app. Disponível em: <http://g1.globo.com/tecnologia/noticia/2016/07/whatsapp-bloqueado-relembre-todos-os-casos-de-suspensao-do-app.html>. Acesso em: 6 de novembro de 2018.

GLOBAL INTERNET LIBERTY CAMPAIGN. **PRIVACY AND HUMAN RIGHTS:** An International Survey of Privacy Laws and Practice. Disponível em: <http://gilc.org/privacy/survey/intro.html>. Acesso em: 20 de outubro de 2018.

GOOGLE. **Privacidade & Termos.** Disponível em: <https://policies.google.com/privacy?hl=pt>. Acesso em: 10 de outubro de 2018.

INTERNET WORLD STATS. **Internet Users in the World by Regions – June 30, 2018.** Disponível em: <https://www.internetworldstats.com/stats.htm>. Acesso em: 15 de outubro de 2018.

KÖCHE, José Carlos. **Fundamentos de metodologia científica:** Teoria da ciência e iniciação à pesquisa. 20. ed. atualizada. Petrópolis, RJ: Vozes, 1997.

LEMOS, Ronaldo. **Direito, Tecnologia e Cultura.** São Paulo: FGV, 2005. Disponível em: <http://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/2190/Ronaldo%20Lemos%20-%20Direito%20Tecnologia%20e%20Cultura.pdf?sequence=1&isAllowed=y>. Acesso em: 7 de outubro de 2018.

MANN, Dillon. **Marco Civil:** Statement of Support from Sir Tim Berners-Lee. Disponível em: <https://webfoundation.org/2014/03/marco-civil-statement-of-support-from-sir-tim-berners-lee/>. Acesso em: 15 de setembro de 2018.

MARCEL, Leonardi. **Tutela e Privacidade na Internet**. Disponível em: <http://leonardi.adv.br/wp-content/uploads/2012/01/mltpi.pdf> . Acesso em: 12 de setembro de 2018.

MENEZES, Tyndaro; SOARES, Paulo Renato. **Polícia encontra hackers que roubaram fotos de Carolina Dieckmann.** Disponível em: <http://g1.globo.com/fantastico/noticia/2012/05/policia-encontra-hackers-que-roubaram-fotos-de-carolina-dieckmann.html/>. Acessado em: 14 de setembro de 2018.

MINAYO, M. C. de S. (Org.). **Pesquisa social:** teoria método e criatividade. 17ª ed. Petrópolis, RJ: Vozes, 1994.

MINISTÉRIO PÚBLICO FEDERAL – 2ª Câmara de Coordenação e Revisão. **Roteiro de Atuação sobre crimes cibernéticos**. Disponível em: <http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/roteiro-atuacoes/docs-cartilhas/crimes_ciberneticos_web.pdf>. Acesso em: 13 de setembro de 2018.

MORAES, Alexandre de. **Direito Constitucional.** 34. ed. São Paulo: Atlas, 2017. Disponível em: < https://forumdeconcursos.com/wp-content/uploads/wpforo/attachments/2/1722-Direito-Constitucional-Alexandre-de-Moraes-2018.pdf>. Acesso em: 20 de outubro de 2018.

NAUGHTON, John. **A Brief History of the Future: The Origins of the Internet.** 2. ed. Londres: Phoenix, 2000. Disponível em: <http://irishsecure.com/books/A_Brief_History_of_the_Future.pdf>. Acesso em: 2 de outubro de 2018.

PAESANI, Liliana Minardi. **Direito e Internet:** Liberdade de Informação, Privacidade e Responsabilidade Civil. 7. ed. São Paulo: Atlas, 2014.

RAMOS, Pedro Henrique Soares. **Arquitetura da rede e regulação:** A neutralidade da rede no Brasil**.** 2015. Dissertação – (Mestrado em Direito) – Escola de Direito de São Paulo, FGV, São Paulo, 2015. Disponível em: <https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/13673/Arquitetura%20da%20Rede%20e%20Regula%C3%A7%C3%A3o%20-%20a%20neutralidade%20da%20rede%20no%20Brasil%20%28PHSR%2C%20vers%C3%A3o%20final%29.pdf>. Acesso em: 17 de outubro de 2018.

SIERRA, Joana de Souza. **A não responsabilização dos provedores de aplicações de internet por conteúdos gerados por terceiros como ruptura dos sistemas tradicionais de responsabilidade civil:** notice and takedown e Marco Civil da Internet**.** 2018. Dissertação – (Mestrado em Direito) – Programa de Pós-Graduação em Direito, UFSC, Florianópolis, 2018. Disponível em: <https://repositorio.ufsc.br/xmlui/bitstream/handle/123456789/190087/PDPC1366-D.pdf?sequence=-1&isAllowed=y>. Acesso em: 3 de outubro de 2018.

STATISTA. **The 100 largest companies in the world by market value in 2018 (in billion U.S. dollars).** Disponível em: <https://www.statista.com/statistics/263264/top-companies-in-the-world-by-market-value/>. Acesso em: 2 de novembro de 2018.

TEIXEIRA, Tarcísio. **Marco Civil da Internet Comentado.** São Paulo: Almedina Brasil, 2016.

THE GUARDIAN. **Russia-backed Facebook posts 'reached 126m Americans' during US Election.** Disponível em: <https://www.theguardian.com/technology/2017/oct/30/facebook-russia-fake-accounts-126-million>. Acesso em: 10 de outubro de 2018.

UNITED NATIONS. **Human Rights Council: Thirty-second session.** Disponível em: <http://undocs.org/A/HRC/32/L.20>. Acesso em: 16 de outubro de 2018.

VASCONCELOS, Francisco Victor. **A segurança jurídica da computação em nuvem:** responsabilidade jurídica na proteção de dados digitais por parte dos provedores de aplicação de internet. Dissertação – (Mestrado em Direito) – Programa de Pós-Graduação em Direito, UFSC, Florianópolis, 2017. Disponível em: <https://repositorio.ufsc.br/bitstream/handle/123456789/186195/PDPC1347-D.pdf?sequence=-1&isAllowed=y>. Acesso em: 17 de outubro de 2018.