Coleta e tratamento de dados pessoais: pontos de equilíbrio e coexistência de direitos e de deveres fundamentais (*)

Collection and processing of personal data: points of balance and coexistence of fundamental rights and duties

Recolección y tratamiento de datos personales: puntos de equilibrio y coexistencia de derechos y deberes fundamentales

Lucas Marques Assad[1]

Gabriel Tristão Mazzoli Coutinho[2]

Bruna Lyra Duque[3]

Sumário: Introdução. **1.** Breve relato dos interesses que permeiam a coleta e o tratamento de dados pessoais. **2.**

(*) Recibido: 30 junio 2019 | Aceptado: 10 agosto 2019 | Publicación en línea: 1ro. octubre 2019.

[1] Graduando do curso de Direito da Faculdade de Direito de Vitória – FDV. lucassad.marques@gmail.com

[2] Graduando do curso de Direito da Faculdade de Direito de Vitória – FDV. gabrieltrista@hotmail.com

[3] Doutora e Mestre pelo Programa de Pós-Graduação *stricto sensu* em Direitos e Garantias Fundamentais da Faculdade de Direito de Vitória (FDV). Especialista em Direito Empresarial pela FDV. Coordenadora do curso de pós-graduação *lato sensu* em Direito de Família e Sucessões da FDV. Professora de Direito Civil da graduação e pós-graduação *lato sensu* da FDV. Advogada. bruna@lyraduque.com.br

Legitimidade das finalidades e das ações dos controladores de dados pessoais: criação do banco de dados ao tratamento. **3.** Limites do direito à privacidade em uma sociedade conectada e seus paradoxos. **4.** Responsabilidade civil dos controladores de dados e deveres fundamentais nas relações privadas. – Considerações finais. – Referências.

Resumo: Este artigo trata sobre a legitimidade e os limites da coleta e do tratamento de dados pessoais pelos controladores frente ao direito à privacidade dos titulares, tendo como foco de análise a Lei Geral de Proteção de Dados brasileira, que sucedeu ao Marco Civil da Internet. Objetiva-se averiguar em que circunstâncias é possível a conciliação entre liberdade e privacidade. Para isso, serão analisadas, de início, as ações dos controladores para obter informações pessoais e quando estas se tornam abusivas. Em seguida, analisar-se-á a redefinição do direito à privacidade. Por fim, será abordado a figura da responsabilidade civil dos controladores com intuito de pontuar, criticamente, a Lei Geral de Proteção de Dados. O cerne deste trabalho é elucidar como alcançar pontos de equilíbrio que permitam a coexistência de direitos e de deveres fundamentais, diante da regulamentação proposta nesta nova estrutura normativa de dados.

Palavras-chave: Lei Geral de Proteção de Dados, controladores de dados, liberdade, direito à privacidade.

Abstract: This article is about the legitimacy and the limits of the collection and treatment of personal data by controllers in contrast to its holders' right to privacy, using as an analysis focus the brazilian General Data Protection Law, which succeeded the Civil Internet Landmark. The objective is to ascertain in which circumstances the conciliation between liberty and privacy is possible. Therefore, the controllers actions to obtain personal data and when those become abusive will be analysed at first. Subsequently, the analysis will be transported to the redefinition of the right to privacy. At last, the civil responsability of data controllers will be analysed in order to evaluate, critically, the General Data Protection Law. The main goal of this project is to elucidate how to reach balance points that allow the coexistence of fundamental rights and fundamental duties, to the eyes of the regulation proposed in this current normative structure of data.

Key-words: General Data Protection Law, data controllers, liberty, right to privacy.

Resumen: Este artículo trata sobre la legitimidad y los límites de la recolección y el tratamiento de datos personales por parte de los responsables del tratamiento en relación con el derecho a la privacidad de los titulares, centrándose en la Ley General de Protección de Datos de Brasil, que sucedió dentro del Marco Civil de Internet. El objetivo es determinar en qué circunstancias es posible conciliar la libertad y la vida privada. Para ello, se analizarán en primer lugar las acciones de los responsables del tratamiento para obtener información personal y cuándo se convierten en abusivos. A continuación, se analizará la redefinición del derecho a la privacidad. Finalmente, se abordará la figura de la responsabilidad civil de los responsables del tratamiento con el fin de puntualizar críticamente la Ley General de Protección de Datos. El núcleo de este trabajo es dilucidar cómo alcanzar puntos de equilibrio que permitan la coexistencia de derechos y deberes fundamentales, dada la regulación propuesta en este nuevo marco regulador de datos.

Palabras clave: Ley General de Protección de Datos, responsables del tratamiento, libertad, derecho a la intimidad.

INTRODUÇÃO

A rápida evolução tecnológica, que teve início a partir da metade do século XX, culminou na chamada era da informação. A informação em si passou a ter um valor comercial (MATOS, 2005, p. 5) cuja principal característica é o acesso fácil com a dispersão e a obtenção de dados que podem atingir diretamente a privacidade das pessoas.

O atual cenário trouxe uma situação como nunca antes vista, principalmente, com a evolução e massificação da internet, que passou a fazer a interligação de um quantitativo expressivo de dados e equipamentos por todo o mundo, e mais, um novo conceito de ambiente, o denominado virtual.

Sob este aspecto, chegou-se a um embate entre a necessidade e a liberdade de comunicação**,** consubstanciado no avanço tecnológico e um ordenamento jurídico, cujo processo revisional é mais lento, obrigando inclusive aos legisladores e profissionais do direito a passarem a compreender os meandros tecnológicos presentes em tais relações, tendo em vista que tais avanços representam um impacto direto na questão da personalidade e da responsabilidade civil.

Neste cenário, entrou em vigor a Lei 12.965/14, que passou a ser conhecida como Marco Civil da Internet (ARNAUDO, 2017, p. 6). O objetivo do Marco é a regulamentação dos direitos e deveres dos usuários da internet, instituindo uma regulamentação para o uso, a proteção e a transferência de dados pessoais no Brasil, nos âmbitos privado e público, definindo as figuras envolvidas, as suas atribuições e as responsabilidades com fundamento na liberdade.

Outro fato que também influenciou essa iniciativa foi o implemento do comércio eletrônico nos últimos anos - tanto de bens e serviços privados como também da disponibilização de serviços públicos pela internet e redes sociais -, proporcionando aos fornecedores uma base de informações, contendo dados pessoais e preferências de milhares de pessoas ávidas pelo consumo, agregando valor de mercado aos bancos de dados.

Com intuito ainda de regular de forma mais detalhada a matéria, foi publicada a Lei 13.709/2018, que introduziu delimitações conceituais importantes, tais como: quem é o titular de dados ("a quem se referem os dados"); quem é o controlador ("compete as decisões sobre o tratamento dos dados, seja pessoa natural ou jurídica, bem como pública ou privada*"*); quem é o operador ("realiza o tratamento em nome do controlador").

Ademais, por meio da MP 869, foi introduzida também a figura do encarregado e da Agência Nacional de Proteção de Dados (ANPD), sendo que o encarregado, indicado pelo controlador, será o responsável pelo canal de comunicação entre o Titular, o Controlador e a Agência Nacional de Proteção de Dados. Já a função básica da ANPD é a fiscalização das empresas e órgãos públicos ou privados para garantir o cumprimento da Lei Geral de Proteção de Dados. Isto inclui garantir as devidas punições para casos de vazamento de dados pessoais e o uso indevido das informações dos usuários.

A regulamentação define, ainda, o dado pessoal como toda e qualquer informação que permita identificar ou torne identificável o seu titular (artigo 5°, I, Lei nº 13.709/18). Já o tratamento dos dados é o processo de coleta, utilização, acesso, transmissão, processamento, arquivamento, armazenamento e transferência (artigo 5°, X, Lei nº 13.709/18).

Uma das preocupações da lei foi a questão do armazenamento destes dados, dos *logs* de acessos e outros, que devem ser guardados com segurança e sigilo por parte também dos provedores de acesso à internet.

Este artigo, portanto, busca explanar como alcançar os pontos de equilíbrio que permitam a coexistência de direitos e de deveres, diante do progresso tecnológico e das regras impostas pela LGPD.

1. BREVE RELATO DOS INTERESSES QUE PERMEIAM A COLETA E O TRATAMENTO DE DADOS PESSOAIS

Destaca-se, inicialmente, a participação ativa dos usuários brasileiros nas redes sociais e como as postagens diárias são feitas com divulgações das suas vidas.

Muito embora a LGPD esteja alicerçada na liberdade de expressão dos usuários da rede, é crucial que as empresas operadoras, ao coletarem as informações desses indivíduos, solicitem permissão para a utilização dos seus dados pessoais, havendo a necessidade do detalhamento específico sobre como serão utilizados, inclusive, de forma destacada das demais cláusulas contratuais.

A expressa autorização, ante um processo transparente, por parte do titular acerca de como serão utilizados os seus dados, acarretará na negativa de utilização indevida dos dados por ele fornecidos, uma vez que houve uma prévia disponibilização dessas informações por parte do usuário, considerando-se também o cumprimento de todas as vertentes para a formalização do negócio jurídico, conforme disposto no artigo 104 do Código Civil brasileiro[4].

E, nesse contexto, o controlador torna-se responsável, pois cabe ao mesmo as decisões sobre o tratamento dos dados na forma da lei, sendo relevante a transparência na utilização dos dados e a restrição de seu uso às finalidades previamente informadas aos seus titulares, bem como a obtenção da devida autorização.

Desse modo, ater-se-á ao chamado "princípio da necessidade" (LIMA, 2016, p.134), um princípio do direito penal que pode ser aplicada de forma análoga ao tratamento de dados, no sentido de usar o mínimo necessário para se atingir o objetivo informado quando da captação, bem como restringir-se também ao prazo necessário.

Assim, o aparente conflito de interesses entre o titular dos dados em manter a sua privacidade e o controlador que pode dispor dessas informações conforme estabelecido em um contrato previamente estipulado, não merece ser considerado, em abstrato, como uma regra. Isto será factível, é claro,

[4] Artigo 104. A validade do negócio jurídico requer: I - agente capaz; II - objeto lícito, possível, determinado ou determinável; III - forma prescrita ou não defesa em lei (BRASIL, 2019).

quando existir um ambiente legítimo e equilibrado, de tal forma que o titular possa compreender e se manifestar de forma livre e inequívoca sobre o uso que será dado às informações por ele fornecidas.

A observância e adequação, por parte das instituições públicas ou privadas, com as responsabilidades na figura de seus controladores, quando do tratamento dos dados pessoais - principalmente os considerados como "dados pessoais sensíveis", que são os relativos à origem racial, política, fé religiosa, saúde e outros (artigo 5º, inciso II, Lei nº 13.709/18), captados para determinadas finalidades -, deverá observar premissas e restrições previstas na lei, como forma de evitar possíveis conflitos.

No entanto, o dano causado por terceiro ao usuário de rede é indenizável, desde que seja devidamente comprovado o descumprimento contratual e a violação à LGPD (artigo 42, Lei nº 13.709/18).

Diante deste cenário, existe uma linha tênue entre a utilização necessária e a desnecessária referente aos dados pessoais coletados para a consecução da finalidade contratada, de forma que a responsabilidade do controlador estará no cerne dos embates e dos balanceamentos da conjugação dos direitos e dos deveres fundamentados aí envolvidos.

2. LEGITIMIDADE DAS FINALIDADES E DAS AÇÕES DOS CONTROLADORES DE DADOS PESSOAIS: CRIAÇÃO DO BANCO DE DADOS AO TRATAMENTO

Vistos os interesses que permeiam a discussão do tratamento de dados pessoais, faz-se importante compreender a problemática em questão sob a ótica dos controladores de dados, estabelecendo-se as seguintes premissas: se as suas ações são legítimas ou abusivas em relação à privacidade dos titulares; qual será o limite da privacidade na Era Digital; e como se dará a figura da responsabilidade civil em relação aos controladores em caso de violação da privacidade.

A informação sempre foi um bem valioso, porém tornou-se ainda mais relevante com os avanços tecnológicos e com o advento da internet, já que nunca foi tão fácil obter e gerenciar informações, atribuindo-as um novo "valor de mercado" (MATOS, 2005, p. 5).

Com isso, é possível apontar duas transformações econômicas: a primeira é uma transição para uma economia centrada na informação e a segunda é a migração para uma comunicação globalmente integrada por meio da internet, o que Blenker (apud CASTELLANO, 2005, p. 5) denomina de "economia da informação em rede".

Não é difícil compreender o interesse dos controladores no tratamento de dados pessoais. A partir desse tratamento, torna-se concebível a criação de bancos de dados e de perfis de consumo, o que permite direcionar investimentos e personalizar a venda de produtos e serviços, mas, também, permite um maior um controle sobre a pessoa, anulando a autonomia e a voz do indivíduo sobre seu "patrimônio informativo" (TEFFÉ; MORAES, 2017, p. 121).

Existem requisitos legais para criação de bancos de dados e cadastros dos consumidores a fim de que a esfera individual seja preservada, como já regulamenta o Código de Defesa do Consumidor, especificamente nos artigos 43 ao 45. Dessa maneira, são garantidos os direitos básicos do consumidor, em especial, os direitos de comunicação, de acesso e de correção de dados (SCHERAIBER, 2002, p. 157).

Destaca-se que criação de banco de dados e de perfis de consumo pelos controladores em si não é uma violação *a priori*, pelo contrário, é um interesse legítimo que possui previsão legal, o que possibilita a sua conciliação com a autonomia e a privacidade dos titulares. Para tanto é necessário saber de qual forma os controladores de dados adquirem informações pessoais para, assim, averiguar em quais situações essa possibilidade é passível de ser concretizada.

Os bancos de dados podem ser formados por meio de formulários nos quais os consumidores têm consciência de que estão fornecendo dados pessoais, ficando a seu critério fornecer ou não (MATOS, 2005, p. 9). Por outro lado, sites da internet, no momento do acesso do consumidor, podem implantar um programa "espião", no disco rígido do computador do internauta, que capta informações para o depósito no banco de dados do site sem que haja solicitação ou permissão de seu titular, sendo este programa denominado *cookie* (SCHERAIBER, 2002, p. 152).

Entretanto, o *cookie* não transmite vírus e só tem seu acesso aqueles que o colocaram no *hard disk* do usuário, podendo ser muito útil ao criar carrinhos de compra, que, em caso do consumidor perder a sua conexão, possibilita que este não perca também suas compras em potencial, mas também abre a possibilidade da venda de dados para empresas interessadas em *mailing lists*[5] (ZANELLATO, 2002, p. 186).

[5] Ciro Scheraiber (2002, p. 154) afirma que *as mailing lists* "passam a remeter, em massa, milhares ou milhões de propagandas comerciais que ao chegarem ao destinatário entopem o seu endereço eletrônico ou e-mail de forma até a causar-lhe problemas técnicos, além de lhe proporcionar importante dispêndio de tempo para examinar tais mensagens, a fim de selecionar aquilo que é proveitoso e o que não é, fazendo com que o seu computador deixe de lhe ser útil."

A captação de dados particulares possibilita a conduta do "Tratamento Personalizado", como descreve Roberto Pompeu de Toledo (apud SCHERAIBER, 2002, p. 153), na qual pessoas desconhecidas se dirigem umas às outras pelo nome como se fossem íntimas, reagindo ao anonimato de massificação, o que faz com que o consumidor seja levado a investir e a comprar serviços e produtos não solicitados. Consoante a isso, Marco Antonio Zanellato (2002, p. 177) adverte:

> Estaríamos, assim, sob o domínio do mal na World Wide Web? Nada mais absolutamente falso. Essas tecnologias, ao tomar conta das informações pessoais na Web, melhoram incrivelmente a nossa vida, com sites personalizados, banners que parecem feitos sob medida para nós, ofertas de comércio eletrônico irresistíveis etc. O desafio, a esta altura, é traçar os limites entre o que é aceitável e o que é abuso de privacidade na Internet.

Dessa maneira, o tratamento de dados pessoais representa um campo fértil para o desenvolvimento da livre iniciativa (artigo 1°, inciso IV, da CR/88) e da livre concorrência (artigo 170, inciso IV, da CR/88), princípios gerais da Ordem Econômica brasileira, ambos também reconhecidos pela Lei 13.709/18 em seu artigo 2° (inciso VI), o que é benéfico não só para as empresas, mas também para os próprios consumidores.

Além disso, as tecnologias empregadas para propiciar o tratamento personalizado é um retrato do desenvolvimento econômico, do avanço tecnológico e da real inovação presente nas relações jurídicas atuais, fundamentos, igualmente, protegidos pela Lei Geral de Proteção de Dados.

Tais direitos, todavia, não são absolutos e devem estar em consonância com outras regras trazidas pela Lei Geral de Proteção de Dados, como o respeito a privacidade (artigo 2°, I), a inviolabilidade da intimidade, honra e imagem (artigo 2°, inciso IV) e o livre desenvolvimento da personalidade (artigo 2°, inciso VII).

Assim, é necessário estabelecer um critério delimitativo entre a ação dos controladores e a forma pela qual ocorre o uso dos dados pessoais dos titulares.

Defende-se que o *cookie* não é um meio legítimo para a obtenção de dados pessoais, mesmo que seus interesses o sejam, enquadrando-se como uma espécie de ilícito informático, uma vez que é um meio não-explícito de coleta (ZANELLATO, 2002, p. 181). Diante disso, Jason Catlett (apud ZANELLATO, 2002, p. 184) "considera que os cookies só devem ser usados com autorização explícita dos usuários".

Chega-se, pois, ao ponto crucial para revestir de legitimidade a obtenção de dados pessoais pelos controladores: o consentimento.

Nota-se que o consentimento deve ser caracterizado como a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada", segundo o artigo, 5°, inciso VII, da Lei Geral de Proteção de Dados, possibilitando-se a coexistência entre o tratamento de dados pessoais e a privacidade de seu titular.

O consentimento do titular é o maior álibi dos controladores. Reforça-se que tal consentimento deve ser provado pelo controlador e pode ser revogado a qualquer momento pelo titular, conforme dispõe o artigo 8° da LGPD.

Porém, há uma exceção à regra, uma vez que o controlador pode usar dados pessoais sem o consentimento do titular para análise de risco de crédito (sistema de *credit scoring*) segundo o julgado do STJ, desde que não se utilize dados sensíveis (CORRÊA, 2017, p. 264) e que garanta o direito de acesso às fontes dos dados e o direito de explicação da lógica do seu tratamento (MONTEIRO, 2018, p. 8), o que culminou na criação da Súmula 550[6].

Mesmo com tal exceção, a regra é que para haver o tratamento de dados por parte do controlador deve haver o consentimento expresso do titular, o que reporta as discussões para as políticas de privacidade dos sites. Tais políticas são contratos de adesão, ou seja, contratos que possuem suas cláusulas estabelecidas unilateralmente pelo fornecedor de produtos ou serviços, sem que o consumidor modifique ou discuta seu conteúdo, conforme regulamentado pelo artigo 54 do Código de Defesa do Consumidor (MATOS, 2005, p. 25)

Os contratos de adesão designam um sistema de *opt-out* ("pegue ou deixe") (CASTELLANO, 2016, p. 40). Logo, ao aceitar a política de privacidade, os consumidores estão concordando com o tratamento de dados proposto, consumando uma permuta entre sites e usuários de produtos e serviços, em troca de dados pessoais (MATOS, 2005, p. 25 e 26).

Para tanto, as políticas de privacidade devem ser claras no sentido de informar os titulares sobre o propósito e a forma de tratamento dos dados pessoais, respeitando, assim, o princípio da finalidade (artigo 6°, inciso I, Lei

[6] "A utilização de escore de crédito, método estatístico de avaliação de risco que não constitui banco de dados, dispensa o consentimento do consumidor, que terá o direito de solicitar esclarecimentos sobre as informações pessoais valoradas e as fontes dos dados considerados no respectivo cálculo" (BRASIL, 2015).

n° 13.709/18) de tal modo que a coleta e o tratamento de dados não sejam como uma "rede jogada ao mar para pescar qualquer peixe" (MULHOLLAND, 2018, p. 164). Consoante a isso, destacamos o trecho inicial da política de privacidade do Google (2019, p.1):

> Quando você usa nossos serviços, está confiando a nós suas informações. Entendemos que isso é uma grande responsabilidade e trabalhamos duro para proteger essas informações e colocar você no controle.
>
> Esta Política de Privacidade destina-se a ajudar você a entender quais informações coletamos, porque as coletamos e como você pode atualizar, gerenciar, exportar e excluir essas informações.

Nota-se que o Google não apenas elucida quais informações são coletadas e porque são coletadas, mas permite que o próprio titular atualize, gerencie, exporte e exclua informações. Essa medida protetiva é conhecida como privacidade por design (*privacy by design*) na qual são incorporados à própria arquitetura do sistema desenvolvido mecanismos protetores que criam condições para que o usuário preserve e gerencie sua privacidade e a coleta e tratamento de seus dados (CASTELLANO, 2016, p. 47), o que é um reflexo da redefinição de privacidade à autodeterminação informativa.

Assim, o contrato de adesão, que é a política de privacidade, torna-se ainda mais legítimo, quando se pautar na transparência (artigo 6°, inciso I, Lei n° 13.709/18) e observar as regras de boa prática e governança (artigo 50, Lei n° 13.709/18), garantindo maior segurança e proteção aos dados pessoais por meio da criptografia[7], da anonizimação[8] de dados e de uma autorregulação dos próprios agentes de mercado, o que permite a criação de selos de qualidade utilizados como diferenciais competitivos (REIS; SPALER, 2018, p. 297).

Por conseguinte, faz-se importante a atitude proativa dos controladores para adequarem-se à Lei Geral de Proteção de Dados Pessoais. Sendo legítimo o interesse na coleta e no tratamento de dados, desde que observados os meios legais para tanto, como o formulário e o consentimento dos titulares.

Com efeito, propõe-se um equilíbrio entre os direitos dos titulares, com amplo respeito ao núcleo privado dos mesmos, e a preservação da autonomia dos controladores no exercício das suas atividades econômicas, desde que

[7] Tiago Matos (2005, p. 28) define criptografia "como a arte de cifrar a escrita, de modo a torná-la ilegível para quem não possuir o respectivo código."

[8] Artigo 5°, inciso III, da Lei 13.709/18 - 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 (BRASIL, 2019).

observados os deveres fundamentais correspectivos aos direitos fundamentais dos titulares.

3. LIMITES DO DIREITO À PRIVACIDADE EM UMA SOCIEDADE CONECTADA E SEUS PARADOXOS

O ordenamento jurídico fundamenta a proteção da esfera privada do indivíduo tanto no artigo 5°, inciso X, da Constituição da República como no artigo 21, do Código Civil (MULHOLLAND, 2018, p. 171).

O termo "direito à privacidade", por sua vez, trata-se de um conceito genérico e amplo de tal modo que a privacidade corresponderia ao gênero do qual são espécies os direitos à intimidade, honra e imagem, conforme a doutrina clássica (REIS; SPALER, 2018, p. 283).

O direito à honra compreende a reputação (honra objetiva) e autoestima da pessoa (honra subjetiva); o direito à imagem diz respeito à não reprodução da representação fotográfica de uma pessoa (imagem-retrato) e à forma pela qual o indivíduo é visto no meio social onde vive (imagem-atributo) (MATOS, 2005, p. 15); e, por fim, o direito à intimidade alude à proteção do núcleo mais interno e secreto da privacidade (REIS; SPALER, 2018, p. 283).

Tradicionalmente, o conceito mais essencial de privacidade advém da ideia do "direito de estar só" (*the right to be let alone*), proposta por Warren e Brandais, em 1890, sob uma perspectiva liberal individualista. Posteriormente, no século XX, a teoria clássica italiana já dividia a privacidade em *diritto ala sagratezza* (impedimento a ingerências alheias na vida privada) e *diritto ala riservatezza* (direito de defender-se da divulgação de notícias particulares por terceiros), extraindo daí a inviolabilidade pessoal que refere-se ao poder legal de evitar os demais, a qual é o elemento central da "Teoria das Esferas" de Henkel (CÔRREA, 2017, pp. 258 e 259).

Entretanto, com o advento da internet e o desenvolvimento da biotecnologia, o acesso a dados pessoais por terceiros e sua consequente divulgação foram facilitados, expandindo as formas potenciais de violação da esfera privada, o que levou ao surgimento um novo conceito de privacidade (*privacy*) referente ao direito de ter controle sobre seus próprios dados (MULHOLLAND, 2018, p. 173), a chamada autodeterminação informativa que atua como uma ferramenta de consolidação da personalidade (CÔRREA, 2017, p. 262). Nesse sentido, Rodotà (apud MULHOLLAND, 2018, p. 172) apregoa que a privacidade pode ser definida como:

> o direito de manter o controle sobre as próprias informações sendo a esfera privada aquele conjunto de ações, comportamentos, opiniões, preferências,

> informações pessoais, sobre os quais o interessado pretende manter um controle exclusivo.

Diversamente disso, na prática, as redes sociais virtuais impactaram diretamente na expectativa de privacidade das pessoas, uma vez que dificilmente o indivíduo conseguirá obter um alto grau de controle de suas informações, de modo que a velocidade da circulação de informação é inversamente proporcional à sua capacidade de controle (TEFFÉ; DE MORAES, 2017, p. 122).

Portanto, o direito à privacidade, mesmo sendo um direito fundamental inviolável, irrenunciável, imprescritível e intransmissível, hoje encontra limites práticos em uma sociedade conectada na qual a rigidez de seus atributos já não é mais sustentável, uma vez que os indivíduos flexibilizam o uso dos seus dados ao aceitarem os termos e as condições das políticas de privacidade (REIS; SPALER, 2018, p. 289).

Por outro lado, é possível evidenciar o paradoxo da proteção de dados pessoais a partir da lógica do "queremos tudo": os consumidores querem as conveniências do desenvolvimento tecnológico, porém não estão dispostos a negociar sua privacidade para obtê-los, como apontado pelo Índice EMC de Privacidade. Segundo o levantamento, 91% dos entrevistados valorizam o acesso mais fácil à informação, enquanto apenas 27% trocariam parte de sua privacidade por maior conveniência e facilidade online (CASTELLANO, 2005, p. 51).

Então, quanto ao novo conceito de privacidade ligado à autodeterminação informativa que este encontra limites na sociedade conectada, o que torna sua atuação plena como um direito fundamental inviolável e irrenunciável impossível. Paradoxalmente, nota-se que a tutela da privacidade está sendo regida através da lógica do "queremos tudo", na qual os usuários querem os benefícios tecnológicos, mas não estão dispostos a abdicar parte de sua privacidade para tanto.

A responsabilidade civil dos controladores frente à violação de privacidade dos usuários é uma forma de estabelecer limites neste jogo de interesses. Mas, pretende-se, fazendo uso de uma abordagem dialética, criticar a noção de reciprocidade da Lei Geral de Proteção de Dados Pessoais para abarcar a visão dicotômica entre direitos e deveres presente no referido conteúdo normativo.

4 RESPONSABILIDADE CIVIL DOS CONTROLADORES DE DADOS E DEVERES FUNDAMENTAIS NAS RELAÇÕES PRIVADAS

A celeridade no processo de informação não só pode ser verificada na tutela da personalidade, como também na incidência da responsabilidade civil nesse cenário (CÔRREA, 2017, p. 255). Vale destacar, inicialmente, um dos Princípios para a Governança e Uso da Internet – o princípio da inimputabilidade da rede, presente no Marco Civil da Internet em seu artigo 18, o qual restringe o combate a ilícitos virtuais aos responsáveis finais e não os meios de acesso e transporte a fim de impedir a censura e promover a liberdade de expressão (BEZERRA; WALTZ, 2014, p.168).

Porém, isso não significa que os controladores de dados estão completamente isentos de responsabilidade civil em casos de abuso da privacidade. Pelo contrário, há uma seção apenas para delegar as responsabilidades do controlador na Lei Geral de Proteção de dados – a Seção III, do Capítulo VI, identificada como "Da Responsabilidade e do ressarcimento de danos".

Na referida seção, o controlador tem a obrigação de reparar os danos ocasionados aos titulares dos dados nas esferas patrimonial, moral, individual ou coletiva (artigo 42, Lei n° 13.709/18).

Ao reverso, os agentes de tratamento não serão responsabilizados quando realizaram o tratamento que lhes é atribuído (artigo 43, I Lei n° 13.709/18); quando não houver violação à legislação de proteção de dados (artigo 43, II Lei n° 13.709/18); e quando o dano for proveniente de culpa exclusiva do titular de dados ou de terceiros (artigo 43, inciso III Lei n° 13.709/18).

Assim, a responsabilidade civil é uma consequência dos atos praticados pelos agentes de tratamento, quando não cumprido o dever atribuído ao controlador de dados, mesmo frente ao princípio da inimputabilidade da rede.

Na verdade, a Lei Geral de Proteção de Dados Pessoais é uma cartilha de deveres para os controladores, mas que precisa delimitações quanto à necessária autorresponsabilidade dos usuários, no exercício das suas atividades nas redes, o que resultará no desejável equilíbrio entre as obrigações recíprocas assumidas nas relações jurídicas estabelecidas entre partes, como bem elucidado por Bruna Lyra Duque e Adriano Sant'Ana Pedra (2013, p. 153):

> Assim, na tentativa de relacionar a autonomia com os deveres, no que diz respeito à horizontalidade dos deveres fundamentais, pode-se identificar no

> constitucionalismo uma ideia simples, a saber: quem possui direitos deve também possuir deveres (DIMOULIS & MARTINS, 2011, p. 339). Tal contraprestação ocorre, por exemplo, no caso do indivíduo que tem a sua intimidade preservada, nas redes sociais, e igualmente respeita a intimidade de outrem no mesmo universo virtual.

Com isso, critica-se a interpretação *in abstrato* da tutela absoluta da privacidade, pois isto colocaria, em todos os casos, a tutela do direito do usuário numa situação jurídica de vantagem (ganho), enquanto o dever do controlador se colocaria numa posição de desvantagem (sem ganho) gerando, assim, uma relação desequilibrada.

Pinheiro e Haikal (apud COSTA; PENDIUK, 2018, p. 31) apontam que, frente à responsabilização atribuída aos invasores de dispositivos alheios para obtenção ilícita de informações, o usuário também é responsável pela proteção de seus dispositivos. Assim, é imperioso mencionar os deveres dos titulares no uso e na proteção de dados pessoais, assim como foi feito com os controladores de dados.

Para tanto, o usuário deve tomar as seguintes precauções: utilizar senhas, códigos e dados biométricos, evitando o acesso desautorizado; deixar o sistema de *firewall* e de detecção de intrusos sempre ativo; e comunicar a autoridade policial quando perceber alguma atividade suspeita, buscando imediatamente a ajuda de um especialista, enquanto isso deve-se evitar o uso do dispositivo (COSTA; PENDIUK, 2018, p. 33).

O uso consciente e a proteção de dados devem ser incentivados, por meio de uma educação em ética e segurança, principalmente dentro dos ambientes familiares onde, muitas vezes, a tecnologia é fornecida à crianças e adolescentes indiscriminadamente, ou seja, os pais e responsáveis também têm que cumprir com os seus deveres (COSTA; PENDIUK, 2018, p. 28).

Nesse sentido, destaca-se a "Teoria das quatro modalidades de regulação" proposta por Lessig, na qual sustenta que os indivíduos têm o seu comportamento limitado por diferentes elementos independentes e complementares: a lei, as normas sociais, o mercado e a arquitetura (CASTELLANO, 2005, p. 15).

Assim, não é possível a plena proteção e segurança dos usos de dados mediante a mera legislação e arquitetura desenvolvida pelos controladores para tal, é necessário que as normas sociais influenciem a opinião pública, criando uma conscientização coletiva. Com isso, faz-se necessário evidenciar os deveres que os próprios titulares têm com o uso responsável e a proteção de dados pessoais.

CONSIDERAÇÕES FINAIS

A relação fomentada entre o titular de dados e o controlador é uma troca legítima e pautada em interesses recíprocos. Defende-se que não há violação na privacidade do indivíduo, quando os deveres dos controladores são cumpridos. A premissa de violação da privacidade não pode ser uma regra.

O controlador torna-se responsável, pois cabe ao mesmo as decisões sobre o tratamento dos dados na forma da lei (princípio da necessidade), sendo relevante a transparência na utilização dos dados e a restrição de seu uso às finalidades previamente informadas aos seus titulares, bem como a obtenção da devida autorização.

No ambiente contratual, portanto, as cláusulas presentes nos termos eletrônicos têm que ser explícitas a ponto de esclarecer ao usuário a forma que os seus dados serão utilizados, assim o titular não poderá alegar desconhecimento ou um parcial entendimento acerca do acordo.

A relação entre os sujeitos envolvidos deve ser marcada pela reciprocidade e pela correspectividade de direitos e deveres, nas quais os efeitos jurídicos são comumente de interesses para ambos os lados, quanto aplicada nas obrigações contraídas.

Assim, há o entendimento que hoje a privacidade, apesar de se tratar de um direito fundamental inviolável, encontra limites em uma sociedade conectada, visto que o indivíduo utiliza essas informações, que tem um certo valor para os controladores, como "moeda de troca" para ter acesso a outros serviços do seu interesse, sendo claro que se trata de uma escolha na qual o indivíduo exerce a liberdade, delineada pela autonomia privada nas relações jurídicas.

Não haverá direito violado do titular de dados pelo controlador, caso o balanceamento aos direitos do sujeito de direitos e da sua personalidade sejam atendidos, bem como se os deveres impostos ao controlador forem respeitados, garantindo-se, assim, os três pilares sancionados pelo Marco Civil da Internet: privacidade dos usuários, neutralidade da rede e liberdade de expressão.

REFERÊNCIAS

AMORIM, Jocelino Soares de; CORRÊA, Edson Simões; CARNEIRO, Rogério de Queiroz Trabuco. **Marco Civil da Internet Não Foi Regulamentado Análise do Nó Crítico**: Falta de Consenso Sobre Neutralidade e Proteção de Dados. 2016. 47 f. Primeiro Passo do Trabalho de Conclusão de Curso (Pós-Graduação Lato Sensu em

"Estado, Políticas Públicas e Gestão de entidades da sociedade civil") – Fundação Santo André e Fundação Abramo, Santo André, 2016. Disponível em: <https://bibliotecadigital.fpabramo.org.br/xmlui/bitstream/handle/123456789/161/Marco%20Civil%20da%20Internet%20N%C3%A3o%20Foi%20Regulamentado.pdf?sequence=1>. Acesso em: 7 mar. 2019.

ARNAUDO, Daniel. O Brasil e o Marco Civil da Internet: O Estado de Governança Digital Brasileira. **Instituto Ingarapé**, Rio de Janeiro, artigo estratégico 25, abr. 2017. Disponível em: <https://igarape.org.br/marcocivil/pt/>. Acess7o em: 9 mar. 2019.

BEZERRA, Arthur Coelho; WALTS, Igor. Privacidade, neutralidade e inimputabilidade da internet no Brasil: Avanços e Deficiências no Projeto do Marco Civil. **Revista Eptic Online**, Sergipe, v..16 n.2, p.161-175, mai./ago. 2014. Disponível em: <http://repositorio.ibict.br/bitstream/123456789/858/2/Arthur.pdf>. Acesso em: 7 mar. 2019.

BRASIL. Constituição (1988). **Constituição [da] República Federativa do Brasil.** São Paulo: Saraiva, 2007. Disponível em: <http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm >. Acesso em: 7 mar. 2019.

BRASIL**.** Código Civil, Lei 10.406, de 10 de janeiro de 2002. 1a edição. São Paulo: **Revista dos Tribunais**, 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L8078.htm >. Acesso em: 8 mar. 2019.

BRASIL. Lei nº. 8.078, de 11 de setembro de 1990. **Código de Defesa do Consumidor**. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/L8078.htm>. Acesso em: 7 mar. 2019.

BRASIL. Lei n°. 12.965, de 23 de abril de 2014. **Diário Oficial [da] República Federativa do Brasil,** Brasília, DF, 10 jan. 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 7 mar. 2019.

BRASIL. Lei n°. 13.709 de 14 de agosto de 2018. **Diário Oficial [da] República Federativa do Brasil,** 15 ago. 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 7 mar. 2019.

CASTELLANO, Ana Carolina Costa. **Privacidade e proteção de dados eletrônicos:** uma análise jurídico-regulatória do Marco Civil da Internet sob perspectiva das teorias de regulação do ciberespaço de Lessig e Murray. 2016. 106 f. Monografia (Bacharelado em Direito) – Faculdade de Direito da Universidade de Brasília, Brasília, 2016. Disponível em: <http://bdm.unb.br/bitstream/10483/15882/1/2016_AnaCarolinaHeringerCostaCastellano_tcc.pdf>. Acesso em: 7 mar. 2019.

CORRÊA, Rafael. Os plúrimos sentidos da privacidade e sua tutela: a questão da proteção de dados pessoais e sua violação na atual construção jurisprudencial brasileira. In: FACHIN, Luiz Edson; CORTIANO JUNIOR, Eroulths; RUZYK, Carlos Eduardo; KROETZ, Maria Cândida Pires Vieira do Amaral (Coord.). **Jurisprudência Civil Brasileira**: Métodos e Problemas. Belo Horizonte: Fórum, 2017.

COSTA, Roberto Renato da; PENDIUK, Fábio. Direito digital: o Marco Civil da Internet e as inovações jurídicas no ciberespaço. **FESPPR Publica**, Curitiba, v. 2, n., 2018. Disponível em: <http://publica.fesppr.br/index.php/publica/article/view/129/38>. Acesso em: 8 mar. 2019.

DUQUE, Bruna Lyra. **A causa do contrato**: entre direitos e deveres. Belo Horizonte: Conhecimento, 2018.

DUQUE, Bruna Lyra; PEDRA, Adriano Sant'ana. Os deveres fundamentais e a solidariedade nas relações privadas. **Revista de Direitos Fundamentais e Democracia,** Curitiba, v. 14, n. 14, p. 147-161, jul./dez. 2013. Disponível em:<http://revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/article/viewFile/345/335>. Acesso em: 9 mar. 2019.

LIMA, Renato. Manual de Processo Penal. São Paulo: 7. Ed. Juspodivm, 2019

MATOS, Tiago Farina. Comércio de dados pessoais, privacidade e Internet. **Revista de Doutrina da 4ª Região**, Rio Grande do Sul, n. 7, 18 jul. 2005. Disponível em: <https://core.ac.uk/download/pdf/16049789.pdf>. Acesso em: 7 mar. 2019.

MONTEIRO, Renato Leite. Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil?. **Instituto Ingarapé**, Rio de Janeiro, artigo estratégico 39, dez. 2018. Disponível em: <https://www.sanderecella.com.br/wp-

content/uploads/2018/12/Sander-Cella-Direito-Empresarial-Digital-lgpd-gdpr-Existe-um-direito-a-explicacao-na-Lei-Geral-de-Protecao-de-Dados-no-Brasil.pdf>. Acesso em: 9 mar. 2019.

MORAES, Maria Celina Bodin de; TEFFÉ, Chiara Spadaccini de. Redes sociais virtuais: privacidade e responsabilidade civil: análise a partir do Marco Civil da Internet. **Pensar**, Fortaleza, v. 22, n.1, p. 108-146, jan./abr. 2017. Disponível em: <https://periodicos.unifor.br/rpen/article/view/6272 >. Acesso em: 6 mar. 2019.

MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da Lei Geral de Proteção de Dados (Lei 13.709/18). **Revista de Direitos e Garantias Fundamentais**, Vitória, v. 19, n. 3, p. 159-180, set./dez. 2018. Disponível em: <http://sisbib.emnuvens.com.br/direitosegarantias/article/view/1603/pdf>. Acesos em: 9 mar. 2019.

REIS, Rafael Almeida de Oliveira; SPALER, Mayara Guibor. Limites do direito fundamental à privacidade frente a uma sociedade conectada. **Revista Jurídica da Escola Superior de Advocacia da OAB-PR**, Curitiba, ano 3, n. 3, p. 280-302, dez. 2018. Dsiponível em: <http://revistajuridica.esa.oabpr.org.br/wp-content/uploads/2018/12/revista-esa-8.pdf>. Acesso em: 7 mar. 2019.

SCHERAIBER, Ciro Expedito. “Mailing Lists” e o Direito do Consumidor. **Caderno Jurídico da Escola Superior do Ministério Público do Estado de São Paulo**, São Paulo, ano 2, v. 1, n. 4, p. 147-166, jul. 2002. Disponível em: <http://www.mpsp.mp.br/portal/page/portal/Escola_Superior/Biblioteca/Cadernos_Tematicos/direito_e_internet.pdf>. Acesso em: 7 mar. 2019.

ZANELLATO, Marco Antonio. Condutas Ilícitas na Sociedade Digital. **Caderno Jurídico da Escola Superior do Ministério Público do Estado de São Paulo**, São Paulo, ano 2, v. 1, n. 4, p. 167-227, jul. 2002. Disponível em: <http://www.mpsp.mp.br/portal/page/portal/Escola_Superior/Biblioteca/Cadernos_Tematicos/direito_e_internet.pdf>. Acesso em: 8 mar. 2019.