

Direito digital: Uma análise da Responsabilidade Civil e das implicações da proteção de dados pessoais à luz da Lei 13.709/2018

Digital Law: An analysis of Civil Liability and the implications of personal data protection in light of Law 13.709/2018

DOI:10.34117/bjdv7n11-411

Recebimento dos originais: 12/10/2021

Aceitação para publicação: 23/11/2021

Tamis Nunes Magalhães

Bacharela em Direito pela Faculdade Kennedy de Minas Gerais
Rua Andrelândia, número 710, Xangrilá, Contagem/ MG, CEP: 32187-070,
E-mail: tamismicamagalhaes@yahoo.com.br

Eduardo Gonçalves Santos

Bacharel em Direito pela Faculdade Kennedy de Minas Gerais
Rua Minas Novas, 125, Sevilha B, Ribeirão das Neves/ MG, CEP: 33840-630,
E-mail: eduardogoncalvesgq@outlook.com

Silvia A. Andrade Portilho

Professora orientadora - Mestre em Direito Civil pela Universidade Federal de Minas Gerais,
Professora de Direito Civil e Hermenêutica da Faculdade Kennedy de Minas Gerais.
Rua José Dias Viêira, 46, Rio Branco, Belo Horizonte /MG, 31535-040,
E-mail: silvia.portilho@somoskennedy.com.br

RESUMO

A utilização de cadastros de dados para o acesso a diversos recursos disponibilizados na rede mundial de computadores é cada vez mais crescente na sociedade atual. Juntamente a esta expansão do acesso à tecnologia, surgiram também problemas relacionados à proteção de dados pessoais de usuários da internet. Neste contexto, no mês de agosto do ano de 2018, foi publicada a Lei 13.709/2018, que trata justamente da proteção a estes dados pessoais. Assim, o presente artigo pretende fazer uma análise das mudanças trazidas por essa recente legislação no âmbito da Responsabilidade Civil e do Direito Digital, especialmente no que diz respeito à responsabilidade civil dos agentes responsáveis pelo tratamento de dados dos usuários.

Palavras-chave: Direito Digital, Responsabilidade Civil, Proteção de dados.

ABSTRACT

The use of data registers to access various resources available on the world wide web is increasing in today's society. Along with this expansion of access to technology have also arisen problems related to the protection of personal data of internet users. In this context, in August 2018, Law 13.709 / 2018 was published, which deals precisely with the protection of this personal data. Thus, this article intends to analyze the changes brought about by this recent legislation in the field of Responsibility. Civil Law and Digital Law, especially as regards the civil liability of agents responsible for processing user data.

Keywords: Digital Law, Liability, Protection of personal data.

1 INTRODUÇÃO

Tendo em vista a crescente expansão tecnológica, utilização de aplicativos, redes sociais e a solicitação de diversos cadastramentos em lojas para se auferir descontos, surgem também as consequências que acompanham essa nova realidade tecnológica.

Diante dessa problemática, o Brasil, acompanhando tendência da União Europeia¹, aprovou no mês de agosto de 2018, a Lei n.º 13709/2018- Lei Geral de Proteção de Dados Pessoais (LGPD), na busca de uma efetiva proteção de dados pessoais de usuários.

Nesse contexto o presente artigo buscará responder aos seguintes questionamentos: o que mudou com a aprovação da lei 13.709/2018, na perspectiva do instituto da responsabilidade civil e do Direito Digital? Quais as sanções civis a serem aplicadas em caso de violação da proteção dos dados dos usuários?

Tem-se como objetivo geral a análise da lei 13.709/2018, legislação esta que foi aprovada recentemente, e ainda está em período de *Vacatio Legis*, devendo de fato produzir seus efeitos após 18 (dezoito) meses de sua publicação. Como objetivo específico, buscou-se a produção bibliográfica concernente ao tema e a análise e caracterização da forma como ocorrerá a responsabilização civil dos sujeitos que realizam o tratamento de dados pessoais, além da realização de um breve estudo de caso, sobre a temática da proteção de dados pessoais.

Neste trabalho, é realizada, primeiramente, uma breve exposição cronológica de legislações anteriores à Lei 13.709/2018, que tratavam da proteção de dados pessoais. Observa-se ainda como o instituto da responsabilidade civil foi tratado na Lei 12.965/2014, haja vista ter sido esta a legislação que antecedeu à Lei 13.709/2018. Importante ainda para o entendimento do tema, o conhecimento dos fundamentos, princípios e conceitos presentes na nova lei de proteção de dados pessoais.

Como cerne deste trabalho, destaca-se a análise da responsabilidade civil no âmbito da Lei 13.709/2018, seguida de um estudo de caso que envolveu uma rede de

¹SILVA, Letícia Brum; SILVA, Roseane Leal. A Proteção Jurídica de Dados Pessoais na *Internet*: análise comparada do tratamento jurídico do tema na União Europeia e no Brasil. Disponível em: <<http://www.publicadireito.com.br/artigos/?cod=e4d8163c7a068b65>>. Acesso em: 30 set.2019.

drogarias, multada por solicitar dados pessoais de seus clientes sem demonstrar de forma clara a finalidade que se tinha com esta solicitação.

Desta forma, incumbe analisar a espécie de responsabilidade civil prevista na Lei 13.709/2018 – Lei Geral de Proteção de Dados, já que este diploma legal aborda tanto a responsabilização do controlador quanto também a do operador de dados, conceitos estes que também serão expostos ao longo do trabalho.

2 A PROTEÇÃO DE DADOS PESSOAIS NO BRASIL – BREVE HISTÓRICO

A proteção de dados pessoais já vem há algum tempo sendo uma demanda da sociedade. Com a expansão da internet, a necessidade de proteção de dados pessoais se potencializou, pois, o procedimento de coleta e transferência de dados se intensificou tornando-se mais rápido, efetivo e barato. Neste aspecto, convém demonstrar como legislações esparsas que, de alguma forma, traziam um fio condutor para a proteção de dados pessoais deram origem, no Brasil, a uma lei específica que tem por objetivo a efetiva proteção de dados pessoais.

Através de uma disposição cronológica das legislações que apresentam, ainda que de forma tímida, a proteção de dados pessoais, destacam-se o Código Brasileiro de Telecomunicações (Lei 4.117/1962), a Política Nacional de Informática (Lei 7.232/1984), a Constituição da República Federativa do Brasil (1988), o Código de Defesa do Consumidor (Lei 8.078/1990), a Lei do Cadastro Positivo (Lei 12.414/2011), a Lei de Acesso à Informação (Lei 12.527/2011) e o Marco Civil da Internet (Lei 12.965/2014), dentre outras.

O Código Brasileiro de Telecomunicações, mesmo sem aprofundar na temática da proteção de dados, trouxe em seu artigo 56 a previsão do crime de violação de telecomunicações para aquele que divulgasse determinado tipo de informação. Transcorrido algum lapso temporal, adveio a Política Nacional de Informática que tratou em seu artigo 2º, incisos VIII e IX, sobre a proteção do sigilo de dados armazenados e a possibilidade de retificação de dados em bases públicas ou privadas.

A Constituição da República Federativa do Brasil de 1988 trouxe em seu texto a proteção dos direitos fundamentais à intimidade e à privacidade (artigo 5º, inciso X) e ainda consagrou o direito à inviolabilidade do sigilo de comunicações, de dados e de comunicações telefônicas (art. 5º, inciso XII). Após passados cerca de dois anos, entrou em vigor o Código de Defesa do Consumidor (lei n.º 8.078/90), que destinou a seção VI

- *Dos Bancos de Dados e Cadastros de Consumidores*, constituída pelos artigos 43, 44 e 45 da lei, para tratar dos bancos de dados que contém informações dos consumidores.

A Lei do Cadastro Positivo – Lei n.º 12.414/2011 - regulamenta a formação de bancos de dados com informações de adimplemento de pessoas naturais ou jurídicas, e por tratar da administração de dados pessoais, traz em vários de seus artigos normatizações que visam proteger os dados pessoais que formam esse específico banco de dados, tais como demonstram os artigos 7º, 9º, 15 e 16 da mencionada legislação. Destaca-se ainda a Lei de Acesso à Informação - Lei 12.527/2011, que em seu artigo 31 trata exclusivamente da proteção às informações pessoais.

De todas as legislações apresentadas, a que mais se aproximou de uma efetiva proteção de dados foi o Marco Civil da Internet – Lei n.º 12.965/14. Esta lei trouxe como princípio norteador a proteção de dados pessoais (art. 3º, inciso III). Além desse princípio, a lei passou a exigir a necessidade do consentimento do usuário para a utilização de seus dados pessoais na internet, dentre outras exigências que também se repetem na atual Lei Geral de Proteção de Dados Pessoais – Lei n.º 13.709/2018, que entrará em vigor em 14 de agosto de 2020.

Porém, embora seja uma legislação mais abrangente, a Lei n.º 12.965/14, assim como as demais legislações que trazem de alguma forma a temática da proteção de dados, não conseguiu suprir as necessidades e centralizar uma efetiva proteção dos dados pessoais. Neste sentido, ao se aprovar a lei 13.709/2018, o legislador buscou estabelecer um marco regulador da proteção de dados pessoais, seguindo uma tendência mundial.

3 A RESPONSABILIDADE CIVIL E A PROTEÇÃO DE DADOS PESSOAIS À LUZ DA LEI Nº 12.695/2014 – MARCO CIVIL DA INTERNET

Primeiramente, far-se-á uma análise da Lei n.º 12.695 de 23 de abril de 2014, popularmente conhecida como o Marco Civil da internet no Brasil, especificamente em seus artigos voltados para a proteção de dados pessoais e para o instituto da responsabilidade civil. A referida legislação, em seu artigo terceiro, disciplinou os princípios que regem o uso da internet no Brasil, dentre eles, em seu inciso III, o princípio da proteção de dados pessoais. Dito isso, Pinheiro (2018, ‘n.p’), define dados pessoais no seguinte sentido:

Toda informação relacionada a uma pessoa identificada ou identificável, não se limitando, portanto, a nome, sobrenome, apelido, idade, endereço residencial ou eletrônico, podendo incluir dados de localização, placas de automóvel, perfis de compras, número de *Internet Protocol* (IP), dados acadêmicos, histórico de compras, entre outros. Sempre relacionados a pessoa natural viva.

O capítulo II da legislação trata dos direitos e garantias dos usuários. Em seu art. 7º, *caput* a lei dispõe que o acesso à internet é essencial ao exercício da cidadania. No mesmo dispositivo, o inciso VII “assegura o não fornecimento a terceiros dos dados pessoais dos usuários, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado, ou nas hipóteses previstas em lei”.

Porquanto, o consentimento é definido por Pinheiro (2018), como sendo:

Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada. Não é o único motivo que autoriza o tratamento de dados, mas apenas uma das hipóteses.

Diante disso, a própria lei define em seu art. 7º, IX a necessidade do “consentimento **expresso** sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais”. Sob o mesmo ponto de vista, Bioni (2019, “n.p”) explica que:

Aquele que exerce tal atividade de tratamento de dados pessoais deve prestar informações claras e completas, utilizando-se de cláusulas contratuais destacadas e dando publicidade às suas políticas de uso para o preenchimento dos adjetivos em questão.

Do mesmo modo, a Lei do Marco Civil da Internet –Lei n.º 12.965/14 dispôs a respeito da forma de exclusão definitiva de dados pessoais em seu art.7º,X relatado *in verbis*:

Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
X -exclusão definitiva dos dados pessoais que tiver fornecido determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas em lei.

Sob o ponto de vista da proteção aos registros, aos dados pessoais e às comunicações privadas, Bioni (2019) define que:

Todas as normas desembocam na figura do cidadão-usuário para que ele, uma vez cientificado a respeito do fluxo de seus dados pessoais, possa controlá-lo por meio do consentimento. Essa perspectiva de controle perpassa desde a fase de coleta e compartilhamento dos dados em terceiros até o direito de deletá-los junto ao prestador de serviços e produtos de internet ao término da relação.

Em sua seção III, a legislação em estudo deste capítulo – lei n.º 12.695 de 23 de abril de 2014, trata da responsabilidade por danos decorrentes de conteúdo gerado por terceiros. Neste aspecto, a responsabilidade civil pelos danos causados aos usuários, na legislação do Marco Civil da Internet, deve ser analisada em dois momentos.

Primeiramente, a lei menciona a responsabilidade civil do denominado provedor de conexão à internet. Este provedor, Leonardi (2012) define como sendo:

A pessoa jurídica fornecedora de serviços que consistem em possibilitar o acesso de seus consumidores à internet. Para sua caracterização, basta que ele possibilite a conexão dos terminais de seus clientes à internet. Em nosso país os mais conhecidos são: Net Virtua, Brasil Telecom, GVT e operadoras de telefonia celular como TIM, Claro e Vivo, estas últimas que fornecem o serviço 3G e 4G.

O artigo 18 do diploma legal aqui mencionado dispõe que “o provedor de conexão à internet não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros”. Entende-se que o provedor de conexão não será responsabilizado por conteúdos gerados por terceiros, ou seja, não há que se falar em nenhum tipo de responsabilização do provedor de conexão neste contexto.

Em segundo momento, cabe mencionar a responsabilidade civil prevista no art. 19, que assim dispõe, *in verbis*:

Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário.

Após análise do artigo supramencionado, pode-se dizer que o legislador definiu como sendo subjetiva a responsabilidade civil do provedor de aplicações de internet² (CEROY, 2012), uma vez que este provedor só poderá ser responsabilizado caso

² Um termo que descreve qualquer empresa, organização ou pessoa natural que, de forma profissional ou amadora, forneça um conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet, não importando se os objetivos são econômicos.

descumpra uma ordem judicial específica. Neste contexto, Gagliano e Filho (2019), definem responsabilidade civil subjetiva sendo aquela decorrente de um dano causado em função de ato culposo ou doloso. A culpa, portanto, se caracterizará quando o agente causador do dano agir com negligência, imprudência ou imperícia.

Dessa forma, conclui-se que o provedor de conexão à internet não será responsabilizado em fatos de terceiros, ou seja, a própria legislação o isentou de qualquer responsabilização em fatos de terceiros. Já o provedor de aplicações de internet terá uma responsabilidade subjetiva caso não se adeque dentro das recomendações e prazos previsto na legislação.

Cumpra destacar ainda a responsabilidade civil do provedor de aplicações de internet que advém do artigo 21 da Lei n° 12.695/2014, transcrito *in verbis*:

Art. 21. O provedor de aplicações de internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo.

Assim, em se tratando de violação de intimidade decorrente da divulgação de imagens, vídeos ou outros materiais contendo cenas de nudez ou atos sexuais, nota-se que o provedor de aplicações de internet será responsabilizado caso após ser notificado – extrajudicialmente ou judicialmente - não retire do ar esta suposta violação da intimidade. Para os demais casos, no entanto, exige-se que a notificação seja judicial. No entanto, de qualquer forma, a responsabilidade civil do provedor de aplicações será subjetiva, e somente incide em caráter subsidiário, ou seja, caso o conteúdo não seja por ele retirado.

4 FUNDAMENTOS, PRINCÍPIOS E CONCEITOS DA LEI 13.709/2018 – LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

A Lei Geral de Proteção de Dados Pessoais – Lei n.º 13.709/2018, possui fundamentos, princípios e conceitos que facilitam no melhor entendimento de sua aplicabilidade.

Considerando os fundamentos previstos na lei, estão os mesmos elencados no artigo 2º sendo eles: respeito à privacidade; autodeterminação informativa; liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade,

da honra e da imagem; o desenvolvimento econômico, tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Dentre todos esses fundamentos percebe-se a intensa preocupação com a proteção do titular dos dados, haja vista que dos 7 (sete) fundamentos dispostos, 5 (cinco) deles são diretamente ligados a direitos do titular de dados, de forma que este não seja apenas um espectador da utilização de seus dados pessoais, mas que possa ser um sujeito ativo que toma decisões com relação ao uso de suas informações.

Um dos fundamentos que demonstra essa ideia da participação ativa do titular é a autodeterminação informativa, que está intimamente ligada ao conceito de consentimento e que também é vista como de crucial importância no Marco Civil da Internet - MCI, conforme bem destaca Bioni (2019):

Pela combinatória de tais dispositivos, verifica-se ser a autodeterminação informacional o parâmetro normativo eleito pelo MCI para a proteção de dados pessoais. Todas as normas desembocam na figura do cidadão-usuário para que ele, uma vez cientificado a respeito do fluxo de seus dados pessoais, possa controlá-lo por meio do consentimento.

No que concerne aos princípios elencados na Lei 13.709/2018, o legislador aponta os seguintes: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas. Todos esses princípios devem ser respeitados quando do tratamento de dados e nesse sentido percebe-se que o uso de dados deve ser feito de forma consciente e limitando-se a um fim específico, não sendo, portanto, permitido a partir da entrada em vigor da referida legislação que o uso exacerbado e irrestrito de dados pessoais permaneça. Vejamos o que explanam Neto e Fenili (2018, pág.4):

No âmbito da proteção de dados pessoais a preocupação está em como esses dados serão utilizados, tendo em vista que a utilização indevida pode acarretar em discriminações, bem como em violação do direito à privacidade.

Em relação aos conceitos que a lei trouxe em seu artigo 5º, tem-se como essenciais para a compreensão da discussão aqui tratada as seguintes definições: dado pessoal, dado pessoal sensível, dado anonimizado, banco de dados, controlador, operador, encarregado, tratamento de dados, consentimento, transferência internacional de dados e autoridade nacional de proteção de dados.

Pinheiro (2018) traz em sua obra a definição dos conceitos presentes na lei de uma forma mais simplificada e esclarecedora. O dado pessoal é definido como informação relacionada a uma pessoa natural viva que permita identificá-la, podendo ser por exemplo, uma placa de automóvel.

Souza (2018, pág.5) neste mesmo alinhamento, define dados pessoais como:

Os dados pessoais são cumulações de fatos e acontecimentos que formam a personalidade de cada indivíduo, os dados pessoais podem contar de forma precisa a história de vida de cada cidadão. Com o passar dos anos, essas informações tiveram diversos meios de existirem, desde diários, cartas, telegramas e fotos chegando finalmente a internet, por meio de email, blogs, redes sociais.

Bioni (2019) destaca o conceito de dado pessoal demonstrando sua importância como sendo um direito da personalidade:

Sob essa perspectiva, um dado, atrelado à esfera de uma pessoa, pode se inserir dentre os direitos da personalidade. Para tanto, ele deve ser adjetivado como pessoal, caracterizando-se como uma projeção, extensão ou dimensão do seu titular.

Embora os autores descrevam a importância de um dado pessoal, não se observa atualmente que os titulares de dados estejam dando a devida importância à manipulação de seus dados, haja vista que muitos preenchem formulários sem sequer ler os termos de uso, e dessa forma coadunam para que ocorra o desrespeito ao direito de proteção dos dados e da personalidade do indivíduo.

Já o dado pessoal sensível é tratado como uma informação que demanda maior proteção, haja vista que tem relação com características das preferências pessoais e da personalidade do indivíduo, como por exemplo sua orientação sexual e suas opiniões políticas. Tem-se ainda, o dado anonimizado que é aquele em que não se pode conhecer seu titular, por ter sido este desvinculado daquele.

Com relação ao banco de dados, trata-se de conjunto de dados de diversos titulares que são armazenados de forma física ou digital. Portanto convém destacar que não se trata apenas de uma proteção no que concerne ao ambiente digital, considerando que a proteção se estende a arquivos físicos em que há a observância de dados pessoais.

Ainda em se tratando de conceitos primordiais para o entendimento deste trabalho destacam-se os agentes do tratamento dos dados, ou seja, as pessoas que poderão ser responsabilizadas diante da inobservância das normas previstas na Lei nº 13.709/2018, sendo eles: o controlador, que é aquele que recebe os dados pessoais dos titulares

mediante seu consentimento, e o operador, que é aquele que realiza algum tratamento dos dados mediante ordem do controlador.

A lei menciona ainda as pessoas do encarregado e da autoridade nacional. Como encarregado, entende-se a pessoa que é indicada pelo controlador e que serve como interlocutor entre controlador e titulares de dados.

A Autoridade Nacional de Proteção de Dados trata-se de um órgão da Administração Pública Federal e conforme destaca Monteiro (2019, pág. 11) sua função é

O segundo mecanismo é a criação de uma Autoridade Nacional de Proteção de Dados (ANPD), com a função principal de zelar pela proteção de dados pessoais por meio do exercício de competências normativa, deliberativa, fiscalizadora e sancionatória.

No que diz respeito ao tratamento de dados, entende-se que é considerada qualquer operação que seja feita com o dado pessoal, como por exemplo, a coleta, classificação e arquivamento. E para que ocorra o tratamento de dados deve-se obter o consentimento de seu titular, ou seja, a autorização manifestada de forma livre, informada e inequívoca.

E por fim, mas não menos importante, conceitua-se a transferência internacional de dados como a disponibilização de dados pessoais do Brasil para países estrangeiros ou organismos internacionais.

Diante de todos esses fundamentos e conceitos tem-se uma noção preliminar dos objetivos buscados pela Lei 13.709/ 2018, conforme destaca Monteiro (2018, pg. 9):

Regular o uso e o tratamento de dados pessoais é o principal objetivo das leis de proteção de dados. Estas visam não somente proteger a privacidade, mas também outros direitos fundamentais e liberdades individuais, que somente podem ser exercidos na sua completude caso seja garantido o uso adequado dos dados pessoais que, muitas vezes, funcionam como representação do indivíduo. Desta forma, as leis de proteção de dados são como “guarda-chuvas” regulatórios que protegem outros direitos.

Trata-se de Lei que vem seguindo tendência mundial³ no que tange a uma legislação específica que trate da proteção de dados pessoais. Assim, ao analisar seus fundamentos, princípios e conceitos, percebe-se a busca de uma proteção abrangente e eficaz no que tange aos dados pessoais e também a seu titular.

³ Argentina - Personal Data Protection Act (2000)

México – Ley Federal de Protección de Datos Personales em Posesión de los Particulares (2010)

União Europeia – General Data Protection Regulation (GDPR – 2016)

5 A RESPONSABILIDADE CIVIL À LUZ DA LEI Nº 13.709/2018 – LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Em primeiro lugar, cumpre esclarecer que nos tempos atuais vive-se a era da sociedade da informação, devido ao avanço da tecnologia, o acesso à informação e o uso da internet. Por consequência, foi criada a lei nº 13.709/18, conhecida como Lei Geral de Proteção de Dados Pessoais. Devido a era informacional em que se vive, dados pessoais são considerados como um novo direito da personalidade. Nesse viés, Costa (2018, pág. 44) discorre:

Nesse contexto, faz-se necessária, além da articulação de diversas medidas de controle social, a definição de proteção de dados pessoais como novo direito da personalidade, no sentido de não subordinar este direito a nenhum outro, tendo em vista sua enorme relevância no atual contexto. Nesse sentido, não devemos nos ater a classificações que consideram o indivíduo como dono dos dados a seu respeito, visto que o direito à proteção de dados está estritamente vinculado à proteção da personalidade, e não a mero direito de propriedade.

Inclusive, a lei nº 13.709 de 2018, em seu texto, define os agentes de tratamento como responsáveis pela coleta, tratamento, armazenamento e exclusão dos dados pessoais. Neste contexto, os agentes de tratamento, caso não realizem o tratamento de dados pessoais de acordo com a legislação citada, poderão responder na esfera cível. Neste contexto, está presente o instituto da responsabilidade civil. Nos dizeres de Cavalieri Filho, em sua obra Programa de Responsabilidade Civil (2018, p. 2):

O principal objetivo da ordem jurídica, afirmou o grande San Tiago Dantas, é proteger o lícito e reprimir o ilícito. Vale dizer: ao mesmo tempo em que ela se empenha em tutelar a atividade do homem que se comporta de acordo com o direito, reprime a conduta daquele que o contraria (Programa de Direito Civil, v.I, Ed.Rio). Para atingir esse desiderato, a ordem jurídica estabelece deveres que, conforme a natureza do direito a que correspondem, podem ser positivos, de dar ou fazer, como negativos, de não fazer ou tolerar alguma coisa. Fala-se, até, em um dever geral de não prejudicar a ninguém, expresso pelo Direito Romano através da máxima *neminem laedere*. Alguns desses deveres atingem a todos indistintamente, como no caso dos direitos absolutos; outros, nos direitos relativos, atingem a pessoa ou pessoas determinadas.

Acrescenta-se que a proteção de dados pessoais tem grande relevância no contexto social da atualidade. Sendo assim, a própria lei nº 13.709/18 trata em sua Seção III acerca da responsabilidade e do ressarcimento de danos, em seus artigos 42 a 45.

Assim sendo, dispõe o artigo 42, ao tratar da responsabilização dos agentes de tratamento, *in verbis*:

Art. 42. 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.

§ 1º A fim de assegurar a efetiva indenização ao titular dos dados:

I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;

II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.

§ 2º 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.

§ 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente.

§ 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.

Assim, o referido artigo traz, em seu texto, o controlador ou o operador como responsáveis em razão do exercício do tratamento de dados, caso causem danos aos usuários, que são, em sua maior parte, também consumidores. Dito isso, pode-se concluir, que está presente o instituto da responsabilidade civil solidária. Nesse viés, segue o entendimento trazido por Pinheiro (2018), “assim como no GDPR, artigos 24, 25 e 26, a lei brasileira traz em sua previsão o caráter solidário da responsabilização do controlador e operador”

Além disso, o art. 42, § 2º; retrata que o juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados, considerando o titular dos dados como parte hipossuficiente. Nesse viés, nota-se ser aplicável o mesmo tratamento já previsto na lei nº 8.078/90 (Código de Defesa do Consumidor) – a inversão do ônus probatório a favor do consumidor.

Diante do exposto, verifica-se que a análise da responsabilidade civil pelos danos causados aos usuários deverá ser efetuada à luz da denominada “Teoria do Diálogo das Fontes”, conforme Marques (2002, pag.52) define:

Nesta realidade, o aplicador do Direito tem como primeiro desafio a multiplicidade de leis. Com este o amplo campo de aplicação legislativa, seja em aspectos subjetivos ou materiais, logicamente surgem dúvidas quanto à colisão ou derrogação de leis, bem como conflitos normativos que sintetiza esta ideia de aplicação coerente e coordenada de fontes legislativas plúrimas convergentes, seja de maneira complementar, subsidiária, ou por opção das partes. Busca-se então nesta teoria, uma eficiência do sistema múltiplo e

complexo do Direito como um todo, de modo a evitar antinomias, incompatibilidades ou incoerências.

Logo, ocorre o presente fenômeno da teoria do diálogo das fontes quando uma legislação faz referência à outra legislação para que ambas complementem uma a outra. Também discorre Tartuce (2018) no que tange à Teoria do Diálogo das Fontes:

A teoria do diálogo das fontes surge para substituir e superar os critérios clássicos de solução das antinomias jurídicas (hierárquico, especialidade e cronológico). Realmente, esse será o seu papel no futuro.

Da mesma forma, segue-se o alinhamento com o pensamento de Pinheiro (2018) que aduz:

Dependendo do tipo de violação de direitos do titular serão aplicadas penalidades conforme já previsto na legislação consumerista (Código de Defesa do Consumidor) e/ou pela regra geral do Código Civil Brasileiro (arts.186,187 e 927).

Dito isso, principalmente em casos envolvendo relação de consumo – que são a imensa maioria - tem-se presente o instituto da responsabilidade civil objetiva. Conforme assinala Sá Junior (2019, pag.27):

Em maior medida, nenhum tipo de segurança será capaz de cobrir absolutamente todos os riscos da atividade. Porém, com base nos preceitos do CDC, o Poder Judiciário considerará a teoria do risco da atividade para concluir pela responsabilidade objetiva do fornecedor.

Logo, a aplicação do diálogo das fontes torna-se imprescindível para que a LGPD não seja aplicada de forma isolada, devendo buscar uma coexistência ou convivência entre as demais normas, tais como a Constituição da República Federativa de 1988, o Código de Defesa do Consumidor (lei nº 8.078/90), o Código Civil (lei nº 10406/02) e o Marco Civil da Internet (lei n.º 12.965/14). Neste viés, as leis se completam, aplicando assim a premissa de uma visão unitária do ordenamento jurídico.

6 UM BREVE ESTUDO DE CASO

Para ilustrar a responsabilidade civil que decorre da utilização indevida dos dados pessoais, será mencionado, brevemente, um estudo de caso envolvendo uma conhecida

rede de drogarias⁴, que foi multada em quase 8 milhões de reais, por descumprimento de um Termo de Ajustamento de Conduta –TAC, firmado com o Ministério Público de Minas Gerais.

No dia 26 de junho de 2018, o Instituto de Referência em Internet e Sociedade – IRIS⁵, representou junto ao Ministério Público do Estado de Minas Gerais buscando providências, haja vista que uma rede de Drogarias no Estado de Minas Gerais estaria solicitando informações como o número do CPF de seus clientes, e com isso ofertavam descontos em produtos vendidos na drogaria. Ocorre que tal prática não era feita de forma clara e transparente e não havia nenhum regulamento que trouxesse de maneira explícita o que seria feito a partir da coleta dos dados desses clientes.

A representação feita pelo IRIS foi fundamentada em direitos e garantias previstos na Constituição da República Federativa do Brasil de 1988 em seu artigo 5º, incisos X e XXXII e do Código de Defesa do Consumidor em seus artigos 6º, incisos III e IV, 8º, 12º e 43º, sendo em tais dispositivos verificados direitos inerentes à intimidade, privacidade e informação.

Após a representação ter sido processada pelo Ministério Público de Minas Gerais - MPMG, a rede de Drogarias se comprometeu firmando Termo de Ajustamento de Conduta – TAC, a adequar suas práticas às exigências impostas pelo MPMG no prazo de 30 (trinta) dias. Porém isso não ocorreu, e em virtude do não cumprimento do TAC, a rede de drogarias foi multada em um valor que chegou a quase 8 milhões de reais⁶.

Em análise do caso, denota-se percebe-se que tal situação ocorreu no ano de 2018 e o procedimento ainda continua tramitando perante o Ministério Público de Minas Gerais, na 14ª Promotoria de Justiça de Defesa do Consumidor de Minas Gerais tendo como últimas movimentações a remessa dos autos à junta recursal em 11/01/19 e a sua distribuição em 02/05/2019⁷.

⁴Ministério Público de Minas Gerais. Drogaria Araújo deverá pagar multa de R\$ 7 milhões por capturar CPF dos consumidores. Minas Gerais. Disponível em: <<https://www.mpmg.mp.br/comunicacao/noticias/drogaria-araujo-devera-pagar-multa-de-r-7-milhoes-por-capturar-cpf-dos-consumidores.htm>>. Acesso em 14 mar. 2019

⁵DAVI, Teofilo. MPMG propõe medidas de adequação da prática de coleta do CPF em drogarias. Instituto de Referência em Internet e Sociedade. Minas Gerais, 2018. Disponível em: <<http://irisbh.com.br/>>. Acesso em: 15 out. 2019.

⁶ERNESTO, Marcelo. Drogaria Araujo é multada em quase R\$ 8 milhões por pedir CPF de clientes. Jornal Estado de Minas Gerais. Minas Gerais, 2018. Disponível em: <https://www.em.com.br/app/noticia/economia/2018/12/06/internas_economia,1011120/drogaria-araujo-e-multada-em-quase-r-8-milhoes-por-pedir-cpf-de-clien.shtml>. Acesso em 20 mai. 2019.

⁷Informação retirada de: <<https://www.mpmg.mp.br/aceso-a-informacao/pesquisa-de-processos-e-procedimentos/>>. Acesso em: 15 out. 2019.

A Lei Geral de Proteção de Dados foi aprovada em agosto de 2018, porém só produzirá seus efeitos em agosto de 2020, estando em período de *Vacatio Legis*.

Na análise do caso em epígrafe, infere-se que a conduta da rede de drogarias viola os fundamentos previstos no art. 2º, incisos II e VI da Lei 13.709/2018, sendo eles a autodeterminação informativa e os direitos do consumidor, haja vista que a rede de drogarias não deixava claro para os clientes o que seria feito com o número de CPF, violando o dever de informar e a transparência nas relações negociais.

Verifica-se ainda a violação aos princípios da finalidade, adequação, necessidade, transparência, segurança, responsabilização e prestação de contas, considerando que a prática de solicitar o número de CPF para a oferta de descontos não demonstrava de forma clara o fim esperado. Considerando que tal prática permitiria o acesso a várias outras informações do titular, desta maneira a conduta adotada pela drogaria não se mostra um meio adequado e necessário para a oferta de descontos. Além disso, demonstra a falta de transparência e segurança ao usuário, pois não há prestação de contas ou qualquer informação pormenorizada da utilização dessa prática.

A conduta ainda descumpre o requisito para tratamento de dados previsto no artigo 7º inciso I da Lei 13.709/2018, haja vista que não há o consentimento livre, informado e inequívoco do titular dos dados. A maioria dos consumidores apenas informava o número de seu CPF para obter o desconto, porém o Ministério Público de Minas Gerais verificou que a rede de drogarias não tinha sequer um regulamento da promoção disponível para consulta nas lojas ou no site da rede de drogarias.

Sendo assim, verifica-se que se a legislação estivesse produzindo plenos efeitos, esta situação provavelmente não ocorreria, haja vista que empresas que realizam tratamento de dados pessoais já teriam feito as adequações necessárias em acordo com a legislação, até porque, deu-se o prazo de 24 (vinte e quatro) meses após a publicação da Lei nº 13.709/2018 para essa adequação. Não tendo a rede de drogarias feito as adequações necessárias, a autoridade nacional, ao verificar as violações, poderia solicitar de imediato medidas cabíveis para cessar as violações conforme previsto no artigo 31 da LGPD.

No caso de não haver a cessação das violações e ocorrer algum dano, seja de cunho patrimonial ou moral, poderiam os titulares pleitear junto ao Poder Judiciário, na modalidade individual ou coletiva, a obrigação de reparação dos prejuízos causados. Nesse sentido, os agentes de tratamento de dados (controlador e operador) previstos na legislação, poderiam ser responsabilizados na esfera cível na forma objetiva, não

excluindo ainda a responsabilização que poderiam sofrer na esfera administrativa, como dispõe o artigo 52 da Lei 13.709/2018.

7 CONCLUSÃO

Retomando o problema de pesquisa e os objetivos deste trabalho, pretendeu-se analisar as mudanças relativas à forma de responsabilização civil dos agentes de tratamento dos dados pessoais dos usuários após a aprovação da Lei 13.709/2018, bem como as sanções aplicadas em caso de violação ao que dispõe a legislação já referenciada.

Nesse viés foi possível concluir que a Lei nº 13.709/2018 trouxe uma mudança no que tange à responsabilização civil daqueles que de alguma forma violarem os dispositivos contidos no texto da Lei Geral de Proteção de Dados Pessoais, apresentando de forma explícita a responsabilidade civil solidária aos agentes de tratamento de dados. Ainda é possível firmar o entendimento de que, caso se trate de relação que possa ser reconhecida como relação de consumo, a responsabilidade civil pode ser na forma objetiva, tendo sido verificado que a Lei Geral de Proteção de Dados, poderá reconhecer, assim como já acontece no Código de Defesa do Consumidor – Lei nº 8.078/1990 a condição do titular de dados pessoais como um sujeito hipossuficiente. Desta maneira, é possível verificar um avanço em relação a Lei nº 12.965/2014 – Marco Civil da Internet, que tinha como forma de responsabilização civil a forma subjetiva, e nesta modalidade não se vislumbrava essa ideia de titular de dados como sujeito hipossuficiente.

Verifica-se ainda a necessidade de aplicação da denominada Teoria do Dialogo das Fontes a fim de interpretar a nova legislação aqui tratada, considerando que a Lei 13.709/2018 surge para promover um diálogo com as demais legislações que buscam a proteção de dados pessoais. É o que se observa, por exemplo, em relação ao Código de Defesa do Consumidor, conforme já exposto acima, sendo esta a principal legislação que subsidia a aplicabilidade da Lei 13.709/2018.

Importante demonstrar que o Brasil não somente procedeu à criação desta legislação com o intuito de proteger dados pessoais; mais do que isso, é possível verificar que a tendência mundial de grandes potências econômicas como a União Europeia é a criação de legislações que visem a proteção de dados pessoais, e para não perder espaço na economia mundial, o Brasil sentiu a necessidade de se adequar às mudanças mundiais para não perder espaço no mercado econômico.

Considerando as dificuldades encontradas em relação ao tema, percebe-se que, apesar de se constituir uma novidade no cenário legislativo, trata-se de temática que está

em voga no cenário mundial, e portanto a importância de discutir, tanto no âmbito acadêmico quanto nos Tribunais, a aplicabilidade que será conferida à responsabilização dos agentes de tratamento dos dados pessoais, sempre no intuito de efetivar a concretização dos princípios basilares previstos na LGPD, em prol de maior segurança, transparência e privacidade a favor dos usuários.

REFERÊNCIAS

ARGENTINA, Argentina Personal Data Protection Act, 30 October 2000. Argentina, 2000. Disponível em: <<http://unpan1.un.org/intradoc/groups/public/documents/undpadm/unpan044147.pdf>> Acesso em: 23 de set. 2019.

BIONI, Bruno Ricardo. Proteção de Dados Pessoais a função e os limites do consentimento. Rio de Janeiro. Forense, 2019.

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). Brasil, 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em 14 mar.2019.

BRASIL. Lei nº 4.117, de 27 de agosto de 1962. Institui o Código Brasileiro de Telecomunicações. Brasil, 1962. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l4117.htm>. Acesso em 15 jul.2019.

BRASIL. Lei nº 7.232, de 29 de outubro de 1984. Dispõe sobre a Política Nacional de Informática, e dá outras providências. Brasil, 1984. Disponível em: <http://www.planalto.gov.br/ccivil_03/LEIS/L7232.htm>. Acesso em 15 jul.2019.

BRASIL. Constituição da República Federativa do Brasil de 1988. Brasil, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em 15 jul.2019.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Brasil, 1990. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8078.htm>. Acesso em 15 jul.2019.

BRASIL. Lei nº 12.414, de 9 de junho de 2011. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Brasil, 2011. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/112414.htm>. Acesso em 15 jul.2019.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do §3º do art. 37 e no §2º do art. 216 da Constituição Federal; altera a Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Brasil, 2011. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/112527.htm>. Acesso em 15 jul.2019.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Brasil, 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm>. Acesso em 15 jul.2019.

CAVALIERI, Sergio Filho. Programa de Responsabilidade Civil. São Paulo. 13ª Ed. Editora Atlas, 2018.

CEROY, Frederico Meinberg. Os conceitos de Provedores no Marco Civil da Internet. 2014. Disponível em: <<https://www.migalhas.com.br/dePeso/16,MI211753,51045>>. Acesso em 27 out.2019.

COSTA, Mariana Monteiro da. A Era da Vigilância no Ciberespaço e os Impactos da Nova Lei Geral de Proteção de Dados Pessoais no Brasil: Reflexos no direito à privacidade. Rio de Janeiro, 2018. Disponível em: <<https://pantheon.ufrj.br/handle/11422/8252>>. Acesso em: 20 out.2019.

DAVI, Teofilo. MPMG propõe medidas de adequação da prática de coleta do CPF em drogarias. Instituto de Referência em Internet e Sociedade. Minas Gerais, 2018. Disponível em: <<http://irisbh.com.br/>>. Acesso em: 15 out. 2019.

ERNESTO, Marcelo. Drogaria Araujo é multada em quase R\$ 8 milhões por pedir CPF de clientes. Jornal Estado de Minas Gerais. Minas Gerais, 2018. Disponível em: <https://www.em.com.br/app/noticia/economia/2018/12/06/internas_economia,1011120/drogaria-araujo-e-multada-em-quase-r-8-milhoes-por-pedir-cpf-de-clien.shtml>. Acesso em 20 mai. 2019.

GAGLIANO, Pablo Stolze; FILHO, Rodolfo Pamplona. Novo Curso de Direito Civil - Responsabilidade Civil. Editora Saraiva. São Paulo, 2019.

LEONARDI, Marcel. Internet: elementos fundamentais. In Responsabilidade Civil na Internet e nos demais meios de comunicação, coordenado por Regina Beatriz Tavares da Silva e Manoel J. Pereira dos Santos. 2. Ed. São Paulo: Saraiva, 2012.

MARQUES, Claudia Lima. Diálogo entre o Código de Defesa do Consumidor e o novo Código Civil: do “diálogo das fontes” no combate às cláusulas abusivas. Revista Direito do Consumidor, nº 45. São Paulo, 2003.

MARTINS, Ana Paula Pereira. Vazamento e Mercantilização de Dados Pessoais e a fragilidade da Segurança Digital do Consumidor: Um Estudo dos Casos Netshoes e Uber. São Paulo, 2018. Disponível em: <<https://www.researchgate.net/publication/327416131>>. Acesso em: 20 out.2019.

MÉXICO, Ley Federal de Protección de Datos Personales em Posesión de los Particulares, 5 de julio de 2010. México, 2010. Disponível em: <<http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf>> Acesso em: 23 de set. 2019.

MINISTÉRIO PÚBLICO DE MINAS GERAIS. Drogaria Araújo deverá pagar multa de R\$ 7 milhões por capturar CPF dos consumidores. Minas Gerais. Disponível em: <<https://www.mpmg.mp.br/comunicacao/noticias/drogaria-araujo-devera-pagar-multa-de-r-7-milhoes-por-capturar-cpf-dos-consumidores.htm>>. Acesso em 14 mar. 2019.

MONTEIRO, Renato Leite. Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil. Instituto Igarapé – Artigo Estratégico 39. São Paulo, 2018. Disponível em: <<https://igarape.org.br/wp-content/uploads/2018/12/Existe-um-direito-a-explicacao-na-Lei-Geral-de-Protecao-de-Dados-no-Brasil.pdf>>. Acesso em: 30 set.2019.

MONTEIRO, Yasmin Sousa. A efetividade dos mecanismos de proteção de dados pessoais na lei 13.709/2018. Brasília, 2019. Disponível em:

<https://repositorio.uniceub.br/jspui/bitstream/prefix/13383/1/21486829.pdf>>. Acesso em: 15 out. 2019.

NETO, Pery Saraiva; FENILI, Maiara Bonetti. Novos marcos legais sobre a proteção de dados pessoais e seus impactos na utilização e tratamento de dados para fins comerciais. Revista de Estudos Jurídicos e Sociais. Santa Catarina, 2018. Disponível em: <<https://www.univel.br/ojs-3.0.2/index.php/revista/article/view/46>>. Acesso em: 30 set.2019.

PINHEIRO, Patricia Peck. Proteção de Dados Pessoais, Comentários à Lei nº 13709/2018 (LGPD). São Paulo. Saraiva, 2018.

Portal do Ministério Público de Minas Gerais (Pesquisa de Processos e Procedimentos). Minas Gerais. Disponível em: <<https://www.mpmg.mp.br/aceso-a-informacao/pesquisa-de-processos-e-procedimentos/>>. Acesso em: 15 out. 2019

SÁ JUNIOR, Sergio Ricardo C. A regulação jurídica da proteção de dados pessoais no Brasil. 2019. Monografia de especialização – Pontífca Universidade Católica do Rio de Janeiro, Rio de Janeiro.

SILVA, Letícia Brum; SILVA, Roseane Leal. A Proteção Jurídica de Dados Pessoais na Internet: análise comparada do tratamento jurídico do tema na União Européia e no Brasil. Disponível em: <<http://www.publicadireito.com.br/artigos/?cod=e4d8163c7a068b65>>. Acesso em: 30 set.2019.

SOUZA, Luíza Ribeiro de Menezes. Proteção de dados pessoais: estudo comparado do regulamento 2016/679 do Parlamento Europeu e Conselho e o Projeto de Lei Brasileiro n. 5276/2016. Brasília, 2018. Disponível em: <<https://www.portaldeperiodicos.idp.edu.br/cadernovirtual/article/view/3153/1484>>. Acesso em: 28 agost.2019.

TARTUCE, Flávio. Manual de Direito Civil: volume único. 2ª Ed. Rio de Janeiro: Forense, 2012.

TAVARES, Letícia Antunes; ALVAREZ, Bruna Acosta. Da proteção dos dados pessoais: uma análise comparada dos modelos de regulação da Europa, dos Estados Unidos da América e do Brasil. São Paulo, 2016 Disponível em: <<http://www.tjsp.jus.br/download/EPM/Publicacoes/ObrasJuridicas/ii%204.pdf?d=636680444556135606>>. Acesso em: 17 jul.2019.

UNIÃO EUROPEIA, General Data Protection Regulation (GDPR), 04 of may de 2016. União Europeia, 2016. Disponível em: < <https://gdpr-info.eu>> Acesso em: 23 de set. 2019.

VALENTE, Jonas. Legislação de proteção de dados já é realidade em outros países. Política-Agência Brasil. Brasília, 2018. Disponível em: <<http://agenciabrasil.ebc.com.br/politica/noticia/2018-05/legislacao-de-protecao-de-dados-ja-e-realidade-em-outros-paises>>. Acesso em 15 set. 2019.