A RESPONSABILIDADE DOS APLICATIVOS MEDIANTE A DIVULGAÇÃO DE DADOS

OLIVEIRA, BRUNA[1]
OLIVEIRA, Lucas Paulo Orlando de[2]

RESUMO: O presente artigo apresenta de forma clara e objetiva a responsabilidade dos aplicativos mediante à divulgação de dados de seus usuários, bem como aborda se a o vínculo existente entre os aplicativos e os usuários se enquadra em uma relação de consumo. Para tanto, serão apresentados o posicionamento dos tribunais, da doutrina jurídica, de estudiosos acerca do assunto e da legislação vigente. A relevância do assunto abordado encontra-se na segurança jurídica, uma vez que, com o crescente aumento da utilização de aplicativos, o indivíduo torna-se cada vez mais dependente do meio digital, ocasionando uma vulnerabilidade de seus dados, bem como a forma como são tratados e o destino ao qual se dará.

PALAVRAS-CHAVE: Proteção de dados. Responsabilidade civil. Vulnerabilidade.

APPLICATIONS 'RESPONSIBILITY THROUGH DATA DISSEMINATION

ABSTRACT: This work presents in a clear and objective way the responsibility of the applications through the disclosure of data from their users, as well as addresses whether the existing link between the applications and users fits into a consumption relationship. For this purpose, the positioning of the courts, legal doctrine, scholars on the subject and current legislation will be presented. The relevance of the subject approached lies in legal security, since, with the increasing use of applications, the individual becomes increasingly dependent on the digital environment, causing a vulnerability of their data, as well as the way in which they are treated and the destination to which they will be given.

KEYWORDS: Data Protection. Civil Responsability. Vulnerability.

1 INTRODUÇÃO

Este artigo versa sobre o direito à proteção de dados, em virtude da responsabilidade civil dos desenvolvedores de aplicativos mediante à divulgação dos dados de seus usuários.

A era digital ou a era da informação, como também é denominada, teve o seu marco histórico em meados do século XX, e com o seu surgimento houve uma mudança no cotidiano dos indivíduos, pois, com o crescente uso da internet, houve também um impulso na criação e no desenvolvimento de aplicativos para múltiplos fins.

Diante dessa nova fase, os aplicativos foram ganhando cada vez mais espaço, ocasionando uma busca maior para inovar nas interações virtuais. Apesar dos benefícios advindos da tecnologia, ocorre que o uso demasiado de aplicativos pode ocasionar uma dependência do indivíduo para com esse meio.

[1]Acadêmica do curso de Direito do Centro Universitário Fag, e-mail: bruna.denovo@hotmail.com.
[2] Docente orientador do curso de Direito do Centro Universitário Fag, e-mail: lucasoliveira@fag.edu.br.

Nesse sentido, com a grande criação e desenvolvimento desenfreado de novos meios que facilitem a comunicação entre pessoas, há também uma necessidade de proteger o cidadão em face daquilo ao qual ele não conhece, ou seja, protegê-lo no que concerne ao meio digital. É certo que os aplicativos surgiram para facilitar o dia a dia, por exemplo, atualmente não é mais necessário ir até um estabelecimento para efetuar a compra de uma mercadoria, bem como não é mais preciso se deslocar até um restaurante para realizar a compra de uma refeição. Entretanto, para que alguém utilize um aplicativo, ele deve concordar com os termos de uso nele previstos; caso a pessoa não o aceite, será impedida de utilizar a ferramenta digital, já que o termo está condicionado ao uso.

Após a inserção dos dados necessários para a utilização de determinado aplicativo, gratuito ou pago, dá-se início a interação nas plataformas digitais. As informações fornecidas pelo usuário vão para um local denominado como banco de dados; a partir desse momento o titular dos dados fornecidos não tem qualquer informação sobre o que feitos é ou será feito com os seus dados.

Diante disso, ocorrem inúmeras dúvidas com relação à informação fornecida, se esses dados estarão realmente protegidos, se em caso de uma eventual violação de segurança desses aplicativos os dados fornecidos serão afetados, bem como se o titular dos dados estará vulnerável perante a uma falha no sistema, já que, a cada interação com o meio digital, são colhidas informações a fim de se traçar um perfil. Por exemplo, as interações feitas nos ambientes digitais, como o compartilhamento de uma localização, as perguntas realizadas no navegador do aplicativo, as compras em determinados sites da internet, os *likes* nas redes sociais, são utilizadas para criar um perfil capaz de identificar o usuário na internet, com o escopo de encaminhar-lhe certo tipo de material que possa ser interessante.

Com a demasiada dependência do meio digital, o usuário passa a ter o seu direito à privacidade violado com a criação de perfis para o encaminhamento de ofertas ou conteúdos apenas com base em pesquisas realizadas em momentos distintos. É importante ressaltar que a privacidade do indivíduo é um dos direitos tutelados pela Constituição Federal em seu artigo 5º, incisos X e XII, e uma vez violada a privacidade do usuário tem-se a sua vulnerabilidade.

A partir dessa violação é que se encontra a grande questão que o presente artigo passa a discutir, isto é, a possibilidade dos aplicativos franquear os dados de seus usuários a outros aplicativos ou até mesmo a outras empresas que fazem o uso do meio digital, sem o devido consentimento efetivo, bem como a forma como os dados devem ser tratados por seus servidores. Dessa forma, o problema levantado por esta pesquisa é: se o aplicativo expuser os dados de seus usuários de forma indevida, a empresa que é responsável pelo seu desenvolvimento e uso poderá ser responsabilizada?

Esse tema assume elevada relevância, não somente por estar relacionado ao atual contexto de grande utilização de ferramentas digitais, mas principalmente porque trata da proteção do usuário em face da divulgação e circulação de seus dados a outros provedores, da forma que a Lei Geral de Proteção de Dados posiciona-se com relação ao assunto, bem como a importância e a relevância do consentimento do titular das informações para os aplicativos.

Neste estudo, objetiva-se esclarecer e fazer uma análise criteriosa da responsabilidade dos aplicativos no que concerne à divulgação, à comercialização dos dados de seus usuários que porventura podem violar o direito à privacidade e à extensão de sua responsabilidade, além de identificar em que espécie de responsabilidade civil se enquadra o vazamento de dados e estabelecer se a prestação de serviços de um aplicativo pode se enquadrada em uma relação de consumo.

Dessa forma, busca-se promover o maior esclarecimento relacionado à divulgação de dados que ocorrem no meio digital, bem como estimular o indivíduo a ampliar seu conhecimento sobre a utilização de aplicativos gratuitos e pagos, que se utilizam de dados pessoais para fins econômicos. Em acréscimo, espera-se promover uma maior conscientização do indivíduo para com a segurança de seus dados que são inseridos em plataformas digitais.

Os objetivos específicos relacionados à relação de vulnerabilidade dos usuários dos aplicativos são: demonstrar os dispositivos legais que versam acerca do direito à proteção de dados; identificar a responsabilidade civil dos aplicativos e redes sociais pelo vazamento de dados dos seus usuários; e expor o pensamento de renomados doutrinadores, ministros e estudiosos acerca do assunto e ainda identificar a possibilidade de soluções para o quadro em questão.

Para apresentar os dados da pesquisa, o texto encontra-se assim organizado: inicialmente, discute-se sobre os elementos que contribuem para a caracterização da responsabilidade civil no direito brasileiro; posteriormente, discorre-se sobre a lei de proteção de dados e gestão de dados por usuários de aplicativos; na sequência, são analisados casos concretos sobre a gestão de dados dos consumidores pelos aplicativos; por fim, são apresentadas as considerações finais, seguidas das referências bibliográficas.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 ELEMENTOS PARA A CARACTERIZAÇÃO DA RESPONSABILIDADE CIVIL NO DIREITO BRASILEIRO

O ordenamento jurídico estabelece alguns deveres que podem ser positivos ou negativos. A primeira categoria reúne os deveres de dar ou de fazer algo; a segunda, por sua vez, se refere aos efeitos de não fazer, deixar de fazer ou tolerar algo. Esses deveres podem atingir tanto a coletividade quanto uma determinada pessoa, o indivíduo por si só. Quando violado o dever jurídico originário (obrigação), dá-se origem ao dever jurídico sucessivo, no qual compete ao indivíduo que violou o seu dever para com o outro lhe indenizar o prejuízo, reparando o dano. A responsabilidade civil, desse modo, torna-se o dever jurídico sucessivo, pois a ela compete reparar o dano causado por meio da violação do dever jurídico originário (CAVALIERI FILHO, 2012).

Nesse sentido, Gagliano e Pamplona Filho (2018) fazem uma análise acerca das espécies de responsabilidade civil, que pode ser a subjetiva, em que "se caracterizará quando o agente causador do dano atuar com negligência ou imprudência" (GAGLIANO; PAMPLONA FILHO, 2018, p. 14), ou seja, somente aquele que gerar o dano se tornará culpado.

A responsabilidade civil subjetiva tem alguns elementos essências a serem observados, sendo o primeiro deles a conduta culposa do agente, que está calcada na ação ou na omissão voluntária do indivíduo que atua com negligencia ou com imprudência. O segundo elemento é o nexo causal, que é o vínculo que liga o fato à causa, isto é, a comprovação do fato. O último elemento, por sua vez, é o dano; refere-se a o prejuízo que o agente tem por ser afetado pela ação ou pela omissão de outrem. Vale ressaltar que a conduta do agente nasce de forma licita, uma vez que ele quer praticar o ato, mas não tem o intuito de produzir o resultado. Se o indivíduo age de forma culposa, violando um direito de terceiro e, por meio dessa violação, ocorre um dano, a partir desses três elementos tem-se uma conduta ilícita, que ocasiona o dever de indenizar (CAVALIERI FILHO, 2012).

Sendo assim, a ação é uma conduta positiva, é a abstenção, a violação de um dever jurídico e um fazer de forma livre e voluntária; já a omissão é uma conduta negativa, pois o indivíduo se abstém de um comportamento devido, quer dizer, é a inatividade do indivíduo. Ambas as condutas são pressupostos necessários para que se configure a responsabilidade civil do agente. Portanto, a omissão gera um dever jurídico, principalmente quando o dever de agir do indivíduo pode impedir que determinado resultado se consume, um deixar de agir faz com que o agente coopere, porém, ele só se tornará responsável se tiver o dever jurídico de agir (CAVALIERI FILHO, 2012).

Gonçalves (2017) se refere também à culpa presumida. Nesse caso, a culpa presumida incumbe ao autor do dano provar que a vítima não sofreu com determinada conduta. Para a vítima; porém, bastará apenas provar que existe um nexo causal entre o ato e o dano sofrido.

Além da culpa, poderá haver o dolo, que consiste na violação de forma consciente do agente. Nesse caso, o indivíduo, ao praticar determinado fato, prevê as suas consequências e mesmo

assim o faz. Logo, a conduta já nasce ilícita, pois, com a sua ação, visa a atingir determinado resultado, sendo assim, o agente age de forma premeditada, voluntária e intencional (GONÇALVES, 2017).

O dolo tem dois elementos para a sua caracterização: a representação do resultado, que nada mais é do que a previsão do resultado, e a consciência do agente, isto é, ele tem pleno discernimento de que a conduta não é licita, mas, mesmo assim, age com o fim de atingir o resultado esperado (CAVALIERI FILHO, 2012).

Já a espécie objetiva é aquela baseada no risco, conforme defende Pinheiro (2016):

> Para o Direito Digital, a teoria do risco tem maior aplicabilidade, uma vez que, nascida na era da industrialização, vem resolver os problemas de reparação do dano em que a culpa é um elemento dispensável, ou seja, onde há responsabilidade mesmo que sem culpa em determinadas situações, em virtude do princípio de equilíbrio interesses e genérica equidade (PINHEIRO, 2016, p. 503).

Nessa perspectiva, a responsabilidade objetiva é baseada na relação de causalidade entre a conduta e o dano dela decorrente. Não é preciso, nesse caso, que seja comprovada a culpa, apenas a relação do autor com a vítima, uma vez que não há como acusar um terceiro de ter gerado o dano se ele não concorreu para que o dano se consumasse. A teoria do risco mencionada acerca da responsabilidade objetiva é aquela desenvolvida por meio de algumas atividades que o indivíduo exerce, as quais posteriormente podem gerar algum dano a terceiros (GONÇALVES, 2017).

Gagliano e Pamplona Filho (2018) compreendem que a responsabilidade civil pode ser atribuída não somente aos atos calcados em ilicitude, mas também àqueles que são considerados lícitos, pois o agente atua conforme o direito, sendo assim, deverá haver uma previsão legal referente à conduta lícita causadora do eventual dano.

Além da responsabilidade civil objetiva e subjetiva, tem-se a responsabilidade contratual, que advém de um vínculo obrigacional, de uma relação preexistente na qual a indenização torna-se uma consequência que provém do inadimplemento previsto em contrato, como o descumprimento de determinada cláusula. Se houver a lesão do direito subjetivo e essa não tiver qualquer vínculo de relação jurídica preexistente, mas somente estiver prevista em lei, trata-se então da responsabilidade extracontratual, também denominada como aquiliana, a qual não foi pactuada entre as partes (CAVALIERI FILHO, 2012).

Segundo Gonçalves (2017), a responsabilidade extracontratual, ou aquiliana, está atrelada à violação de deveres ou à omissão para com eles. Além disso, se enquadram como os direitos da personalidade e os direitos reais, que estão previstos a partir do artigo 186 do Código Civil (GONÇALVES, 2017).

Após analisar o que significa o termo responsabilidade civil, deve-se conceituar a noção de dano. Esse pode ser causado pela conduta lícita ou ilícita do agente. Gagliano e Pamplona Filho (2018) definem "dano ou prejuízo como sendo a lesão a um interesse jurídico tutelado — patrimonial ou não —, causado por ação ou omissão do sujeito infrator" (GAGLIANO; PAMPLONA FILHO, 2018, p. 40). Se não houver um dano, não há o que reparar. Os autores ressaltam que o dano não está baseado apenas com relação ao patrimônio, mas também pode ser o dano extrapatrimonial, como o dano moral. Todo o dano causado ao indivíduo pode vir a gerar um dano à coletividade

Nesse tocante, o dano pode se manifestar em diferentes modalidades, como o dano patrimonial que "traduz lesão aos bens e direitos economicamente apreciáveis do seu titular. Assim ocorre quando sofremos um dano em nossa casa ou em nosso veículo" (GAGLIANO; PAMPLONA FILHO, 2018, p. 45), ou seja, é o dano que causa a redução do acervo de bens de outrem.

Além do dano patrimonial, tem-se o dano moral que transcende o direito ao patrimônio, pois está diretamente ligado ao direito da personalidade e ao direito da dignidade da pessoa humana, algo que fere a honra, o nome, a imagem ou até a reputação do indivíduo, algo que não consiga ser mensurado (CAVALIERI FILHO, 2012).

Destarte, deve-se provar que houve o dano, e, para que isso ocorra, deve haver alguns requisitos mínimos, tais como: "a violação de um interesse jurídico patrimonial ou extrapatrimonial de uma pessoa física ou jurídica [...] certeza do dano [...] subsistência do dano" (GAGLIANO; PAMPLONA FILHO, 2018, p. 42). Posto isso, os autores supracitados mencionam que a certeza do dano pode ser flexibilizada.

A flexibilização mencionada está diretamente ligada ao dano moral, pois não se pode utilizar dos mesmos meios para a comprovação do dano material, já que não há como comprovar a dor ou a humilhação que o indivíduo está sentindo em seu íntimo. Nesse sentido, o dano moral pode ser atestado com o próprio ato danoso, desde que demonstrado que esse ato gerou algum dano. É o que ocorre com o dano presumido, em que não há como comprovar o dano da mesma forma como quando há dano material, porém, baseado no ato e nas consequências, considera-se de que houve o dano (CAVALIERI FILHO, 2012).

Uma vez provado o dano, há que se mencionar a sua reparação, denominada pela doutrina de indenização. De acordo com Venosa (2013), o correto é que a indenização seja condizente com o dano sofrido, contudo, ocorre que em alguns casos torna-se impossível de acontecer. Vale ressaltar que a indenização não deverá causar o enriquecimento indevido da vítima.

Sendo assim, a reparação civil deverá compensar o dano, fazendo com que as coisas retornem ao *status quo ante;* quando isso não é possível, o agente causador do dano pagará uma

quantia equivalente a estimativa do dano. Há também a reparação civil na forma de punir o agente que gerou alguma lesão a outrem, uma forma de fazer com que o agente tenha uma percepção de que a sua falta de cautela gerou um dano a um terceiro. A última pretensão da reparação civil consiste em desmotivar eventuais condutas semelhantes, que, quando tomadas novamente, serão punidas de igual forma (GAGLIANO; PAMPLONA FILHO, 2018).

2.2 LEI GERAL DE PROTEÇÃO DE DADOS E A GESTÃO DOS DADOS DOS USUÁRIOS PELOS APLICATIVOS

Primeiramente, antes de se discutir sobre a Lei Geral de Proteção de Dados (LGPD), é mister se esclarecer os conceitos de "dados" e "informações". Essas palavras, ao contrário do que se pensa, não são sinônimas. Como destaca Bioni (2019), "dado é o estado primitivo da informação [...] são simplesmente fatos brutos, que quando processados e organizados se convertem em algo inteligível, podendo ser deles extraída uma informação" (BIONI, 2019, p. 56).

A informação é algo intangível; está sujeita a diversos tipos de ameaças. Quando se trata do direito digital, essas ameaças vêm por meio da fraude eletrônica e acesso indevido de informações, as quais, posteriormente, podem ser furtadas, como o uso indevido de uma marca, a violação de algum direito autoral, entre outros elementos. Vale ressaltar que o principal responsável por todo esse meio de divulgação é o próprio usuário que age de forma não intencional, por não possuir conhecimento técnico acerca do assunto (PINHEIRO, 2016).

Discorrendo acerca do assunto, Maciel (2019) destaca que há alguns tipos de dados, como os pessoais, que são aqueles que são capazes de identificar o usuário de forma direta, quando há um maior número de informações sobre o indivíduo (informações sobre raça, religião, opinião política, saúde ou até mesmo os dados genéticos), ou ainda, de forma indireta, quando as informações são mais escassas. Com o cruzamento dessas informações é possível criar um perfil que identifica o usuário; um claro exemplo disso é o compartilhamento de uma localização.

Conforme a Lei nº 13.709/2018, o artigo 5º e seus incisos versam sobre os tipos de dados: i) os pessoais, que são informações que demonstram como identificar o indivíduo; ii) os dados pessoais sensíveis, que são os supracitados; iii) os dados anonimizados, que são aqueles que não identificam de forma fácil, direta e rápida o usuário, pois, para que isso ocorra, é necessário um tipo de tratamento. Todo esse material coletado necessita de um local de armazenamento, conforme disciplina o referido artigo, o denominado banco de dados, que nada mais é do que um conjunto de dados que é estruturado para ser armazenado em um ou vários locais (BRASIL, 2018).

Nesse sentido, segundo Venosa (2013), a criação desse banco comporta três fazes: a primeira é quando são inseridos os dados, que é chamada de *input;* a segunda é quando ocorre a divulgação ou a comercialização desses dados, a qual é denominada de *output;* e a terceira e última fase se efetiva quando os dados fornecidos pelos usuários são armazenados e posteriormente ficam à disposição de quem os armazenou para que decida livremente como utilizá-los.

Atualmente, os bancos de dados mantêm as informações de seus usuários sem o seu consentimento, sendo coletados a partir das redes sociais. Nesse caso, tem-se o termo denominado como *data brokers*, que se refere ao armazenamento do maior número de dados possíveis para o fornecimento de diversos tipos de serviços, que engloba o conceito de cadastro de consumo, uma vez que são utilizados dados fornecidos pelo seu próprio arquivo ou por terceiros com o intuito de direcionar determinado conteúdo (BIONI, 2019).

Com o crescente aumento da publicidade direcionada, criou-se um novo método de negócio, denominado como *zero-price advertisement business model*. Nesse método, o consumidor deixa de realizar o pagamento por um bem de consumo de forma pecuniária e passa a efetuá-lo com o fornecimento de seus dados cadastrados no sistema, acarretando a divulgação e a sua comercialização. Assim, a prestação de serviço que tinha o objetivo de ser gratuita torna-se matéria-prima, pois ocorre uma transação de dados por diversos servidores que cooperam uns com os outros (BIONI, 2019).

A Lei nº 8.078, de 11 de setembro de 1990, mais conhecida como Código de Defesa do Consumidor, traz em seu artigo 2º, caput e parágrafo único o conceito de consumidor como "toda pessoa física ou jurídica que adquire ou utiliza produto ou serviço como destinatário final. Parágrafo único. Equipara-se a consumidor a coletividade de pessoas, ainda que indetermináveis, que haja intervindo nas relações de consumo" (BRASIL, 1990, s/p).

De acordo com Tartuce e Neves (2016), o fornecedor ou prestador de serviço pode ser qualquer pessoa física ou jurídica, nacional ou estrangeira, que desempenhe determinada função de forma habitual, visando a uma remuneração pelo exercício da atividade.

O Código de Defesa do Consumidor assim se posiciona, no artigo 43, sobre o cadastro de banco de dados:

> Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes. § 1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos. § 2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele. § 3° O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção,

> devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas. (BRASIL, 1990, s/p).

Segundo Tartuce (2018), os bancos de dados cadastrais, que contemplam o nome, elencado como um direito da personalidade cuja finalidade é representar o ser humano perante o meio de convívio social, não devem ser utilizados para fins difamatórios ou que denigram a imagem do usuário.

Soma-se a isso o que Schreiber (2013) aduz acerca dos bancos de dados. Para o autor, os bancos de dados são criados para facilitar o enquadramento do usuário em um tipo de perfil, que visa a objetivar o encaminhamento de assuntos que se enquadrem nos moldes do perfil do usuário, facilitando, dessa forma, o envio de e-mail com publicidade que se limita às suas características.

Nesse contexto, o direito digital surge para regulamentar as ações dos usuários da rede de internet, pois, com a sua utilização, crimes que aconteciam somente fisicamente passaram a acontecer na esfera digital, como os crimes de calúnia, injúria e difamação, tipificados pelo Código Penal brasileiro. Quando esses crimes ocorrem no meio digital, as proporções que podem assumir são imensas, pois o alcance desses crimes é muito maior em um meio que leva apenas segundos para se propagar todo e qualquer tipo de informação (NOVO, 2019).

No ano de 2014, entrou em vigor a Lei Federal n.º 12.965/2014, denominada como Marco Civil da Internet. A referida lei tem como base a regulamentação da utilização da internet, sendo pautada em princípios, como garantias e deveres que os seus usuários têm ao utilizarem a rede de internet (GARCIA, 2016).

A implementação do Marco Civil da Internet dá ênfase à privacidade do ser humano perante a inclusão de informações na rede de internet. Ressalta-se ainda que a lei visa a assegurar a ampla informação que os aplicativos devem fornecer aos seus usuários. Essas informações devem ser claras e precisas, devem explicar a forma como serão coletados os dados, a forma em que se dará o tratamento, bem como a sua destinação final e o seu armazenamento (GARCIA, 2016). Portanto, a LGPD proporciona ao usuário maior segurança jurídica para as relações ocorridas no meio digital.

2.3 ANÁLISE DE CASOS CONCRETOS SOBRE A GESTÃO DE DADOS DOS CONSUMIDORES PELOS APLICATIVOS

Recentemente, uma empresa russa criou um aplicativo denominado como "*FaceApp*", cujo escopo é demonstrar como os usuários das redes sociais ficariam se tivessem uma idade mais

avançada. Não obstante, o aplicativo violou uma vasta gama de direitos dos usuários, compartilhando os seus dados (MARTINES, 2019).

No caso supracitado, a empresa que desenvolveu o aplicativo somente disponibilizava os termos de uso em língua estrangeira, e as duas empresas autorizadas a fazer a utilização desse aplicativo - o *Google* e a *Apple*, sendo as únicas fornecedoras autorizadas do aplicativo - estabeleceram políticas de privacidade com condições abusivas. Dentre essas políticas está a possibilidade do compartilhamento de dados, com todos aqueles que integram o grupo, transcendendo a área territorial brasileira, infringindo o disposto na Lei 12.965/14, em seu artigo 7º. Diante do ocorrido, ambas as empresas autorizadas de fornecerem o serviço prestado pelo aplicativo foram multadas pelo Procon do estado de São Paulo (MARTINES, 2019).

Ainda nesse tocante, no ano de 2018, a empresa conhecida como *Netshoes* teve os dados de seus usuários expostos, tais como nome, histórico de compras, endereço eletrônico e data de nascimento. Após o ocorrido, o Ministério Público do Distrito Federal e Territórios (MPDFT) determinou que a empresa entrasse em contato com os seus clientes e os informasse do ocorrido. Ademais, foi firmado acordo entre o MPDFT e a empresa por meio de um termo de ajustamento de conduta, definindo-se que ela pagaria o valor de R$500.000,00 (quinhentos mil reais) a título de indenização ao Fundo de Defesa de Direitos Difusos (FDD), por meio de depósito. Além do montante, a empresa deverá fornecer informações sobre os riscos obtidos no meio cibernético, bem como divulgar medidas de proteção de dados. Caso ocorra o descumprimento do que foi determinado, o MPDFT ajuizará ação de reparação pelos danos morais coletivos (MPDFT, 2018).

Nesse âmbito, a empresa *Yahoo!*, atualmente conhecida como *Altaba*, também foi alvo da divulgação de dados dos seus usuários no ano de 2014, deixando de fornecer as informações acerca do ocorrido aos usuários no momento oportuno, algo que fez somente em 2016. Em decorrência disso, a empresa a princípio firmou um acordo judicial equivalente a US$47.000.000,00 (quarenta e sete milhões de dólares), para encerrar três processos judiciais. Segundo a Altaba, os dados que foram vazados consistiam em nomes, endereços eletrônicos, números de telefones, datas de aniversários, senhas, dentre outras informações (COELHO, 2018).

Outra situação aconteceu no final do ano de 2016. O aplicativo da *Uber*, empresa que atua como intermediadora de transporte, teve o seu banco de dados invadido, o que gerou acesso a informações pessoais de cerca de 57 milhões de motoristas que utilizam a ferramenta como meio de subsistência. A empresa havia emitido notificações somente para alguns de seus usuários no Canadá, porém, após realizar acordo com a Comissão de Proteção dos Dados Pessoais do Ministério Público do Distrito Federal e Territórios (MPDFT), os usuários brasileiros que foram afetados com essa divulgação de dados também passaram a ser notificados sobre o ocorrido. Estima-se que 196

mil usuários brasileiros foram notificados por meio de mensagens enviadas por e-mail. De acordo com o MPDFT, os dados aos quais hackers obtiveram acesso não foram divulgados na internet; além disso, o site da Uber disponibilizou informações sobre do ocorrido, fornecendo ainda algumas recomendações. (MPDFT, 2019).

No ano de 2019, registrou-se nova ocorrência. Dessa vez, o *Facebook* foi alvo de uma ação civil pública ajuizada pelo Instituto Defesa Coletiva (IDC), que tinha por objetivo questionar a violação dos dados dos seus usuários, já que a rede social havia pago funcionários terceirizados para transcrever áudios que foram enviados no aplicativo *Messenge*r. O próprio aplicativo admitiu que foi realizada tal conduta e que o seu sistema tinha algumas vulnerabilidades que abriam brechas para que hackers instalassem alguns tipos de *software* que fornecem acesso a dados dos aparelhos, aos microfones e as câmeras de maneira imperceptível. A ação civil pública requeria indenização por danos morais coletivos em paralelo à obrigação da empresa em notificar os seus usuários das falhas ocorridas. É importante enfatizar que não é a primeira vez que o *Facebook* é alvo de uma ação pública ajuizada pelo IDC (COELHO, 2019).

Em consonância, segundo o site do IDC, a Secretaria Nacional do Consumidor do Ministério da Justiça e Segurança Pública (Senacon) emitiu uma notificação para a referida empresa prestar informações a respeito de sua conduta, bem como abriu um procedimento para a investigação acerca do tratamento dos dados dos usuários do *Facebook* no Brasil (IDC, 2019).

Acerca do assunto, a advogada Lillian Jorge Salgado, atualmente presidente do IDC, afirma que, como o *Facebook* é uma rede social que atua no ramo de compartilhamento de dados dos seus usuários, uma vez ocorrida uma falha no armazenamento desses dados, constitui-se sim um vício na prestação de serviços pela parte da empresa, posto que o usuário torna-se o consumidor e o *Facebook* torna-se o fornecedor, caracterizando-se uma relação de consumo (COELHO, 2019).

Conforme reportagem de Clara Fabro para o site Techtudo, recentemente Athul Jayaram, pesquisador e especialista em segurança digital, identificou uma falha no sistema de segurança do aplicativo WhatsApp. A falha consiste na divulgação dos números de no mínimo 29 mil usuários, podendo chegar até a 300 mil números privados que podem ser encontrados em buscas no Google, e, além do número, existe a possibilidade da exposição da imagem do usuário por meio de sua foto de perfil. Conforme a reportagem, o número do resultado das buscas pelo número privado do usuário pode variar, a depender do domínio do explorador. A respeito do assunto, a empresa se pronunciou por meio de um porta-voz, dizendo que o recurso que permite a criação de URL a fim de facilitar a comunicação é demasiadamente utilizado por empresas que visam a uma maior interação com os seus clientes. Ele ressaltou ainda que a divulgação dessa URL parte do usuário,

que optou por tal recurso; o porta-voz afirmou que, caso o usuário não queira receber certa mensagem, e poderá bloqueá-la (FABRO, 2020).

Outra empresa que também foi alvo de uma ação judicial pelo vazamento de dados de um usuário foi a *OLX*, condenada a pagar uma indenização por danos morais no valor de R$20.000,00 (vinte mil reais) e também deverá se retratar do ocorrido. Os dados vazados eram de um advogado da Paraíba, os quais foram usados em anúncios sem o devido conhecimento e consentimento; além do mais, as informações divulgadas no site colocavam em risco a sua reputação (SANTOS, 2020).

A seguir, tem-se mais um exemplo de uma ação relacionada ao uso indevido de informações de usuários. O caso foi julgado pelo Tribunal de Justiça do Distrito Federal e dos Territórios sob o acórdão 971.472:

> DIREITO DO CONSUMIDOR. FALHA NA PRESTAÇÃO DE SERVIÇOS. SEGURANÇA DA INFORMAÇÃO. ANÚNCIO EM SITE DE CLASSIFICADOS ONLINE. PÁGINA DE ACOMPANHANTES. DANOS MORAIS. VALOR DA INDENIZAÇÃO. […] **3. Responsabilidade civil. Dano Moral. O dano causado à autora é evidente, considerando que seu nome, sobrenomes e telefones, inclusive profissional, de atividade completamente distinta, foram disponibilizados em site de classificados online, como anúncio de acompanhante. A autora demonstra que seus dados pessoais foram expostos e que foi atingida em seus atributos da personalidade, de modo que é cabível indenização por danos morais** (DISTRITO FEDERAL, 2016, s/p, grifos nossos).

Como se nota no acórdão, constata-se como o uso indevido de informações divulgadas a terceiros sem o consentimento do usuário pode acarretar em uma situação humilhante e vexatória, difamando a reputação do indivíduo. No caso a seguir, julgado pelo Tribunal de Justiça do Estado do Paraná, o dano ficou comprovado com a veiculação de informações, ocorrendo uma falha na prestação do serviço:

> AÇÃO DE INDENIZAÇÃO POR DANOS MORAIS EM RAZÃO DA DISPONIBILIZAÇÃO DE DADOS PARA APLICATIVO. OFENSA À HONRA. SENTENÇA DE PROCEDÊNCIA. INDENIZAÇÃO POR DANOS MORAIS FIXADA EM R$ 2.000,00. [...]**AINDA QUE OS SERVIÇOS SEJAM PRESTADOS PELO RECORRENTE A TÍTULO GRATUITO, ELE AUFERE LUCRO COM A REDE SOCIAL, SE ENQUADRANDO NA PREVISÃO DO ART. 3º, § 2º DO CDC**, ALÉM DO QUE A PLATAFORMA DO APLICATIVO LULU FUNCIONAVA DE FORMA INTEGRADA COM A PLATAFORMA DO FACEBOOK, TANTO É ASSIM QUE OCORREU ALTERAÇÃO NA POLÍTICA DE USO, DE MODO QUE A CESSÃO DE IMAGEM E DADOS PÚBLICOS NÃO AFASTA O DEVER DE INDENIZAR, TAMPOUCO A LEGITIMIDADE, MORMENTE QUANDO EMPREGADO EM APLICATIVO QUE OBTÉM TAIS DADOS DA REDE SOCIAL SEM NENHUMA AUTORIZAÇÃO EXPRESSA. A CESSÃO DE INFORMAÇÕES PESSOAIS PÚBLICAS PELO SAITE DE RELACIONAMENTOS FACEBOOK DEVE RESPEITAR OS DIREITOS DA PERSONALIDADE DO USUÁRIO, RELATIVAMENTE IRRENUNCIÁVEIS E DISPONÍVEIS. NO CASO DO APLICATIVO LULU, A MIGRAÇÃO DOS DADOS PERMITE AVALIAÇÃO DE CUNHO SEXUAL DO USUÁRIO, ATRIBUINDO-LHE NOTAS, SEM O PRÉVIO

> CONSENTIMENTO EXPRESSO, EXTRAPOLA E MUITO A MERA CESSÃO DAS INFORMAÇÕES PÚBLICAS CONSTANTES DO TERMO DE ADESÃO. LIMITES DA CESSÃO EXTRAPOLADOS. UTILIZAÇÃO DA IMAGEM. (PARANÁ, 2014, s/p, grifos nossos).

Não é a primeira vez que o aplicativo do *Facebook* em conjunto com o aplicativo *LULU* são alvos de ações pelo vazamento de dados dos seus usuários. Outro caso em que ambos figuraram no polo passivo ocorreu no Rio Grande do Sul; um perfil criado pelo aplicativo *LULU*, sem a devida autorização do titular dos dados, resultou em diversas avaliações de mulheres a respeito de seu desempenho sexual. O usuário somente tomou conhecimento do perfil criado no aplicativo após uma colega de trabalho alertá-lo. Após o ajuizamento da ação, teve julgado improcedente o pedido de danos morais, porém, o autor interpôs o recurso de apelação, que posteriormente revogou de forma integral a sentença atribuída anteriormente, pois, para o Desembargador Carlos Eduardo Richinitti, não houve o consentimento do autor para a inserção de seu perfil na plataforma, bem como houve falha no fornecimento da prestação de serviço por parte de ambas as empresas (artigo 14 da Lei n.º 8.078/1990). Dessa forma, conforme o disposto no artigo 47 da Lei n.º 8.078/1990, as cláusulas contratuais deverão ser interpretadas de forma mais favorável ao consumidor (MARTINS, 2018).

Segundo a Ministra Nancy Andrighi (Recurso Especial 1.758.799), as informações sobre os indivíduos que são inseridos em bancos de dados passam a ter cunho econômico, e a partir do momento em que um banco de dados decide comercializá-las, deverá informar isso ao usuário, haja vista que quando usuário fornece seus dados a um aplicativo, está apenas cumprindo os requisitos necessários para se utilizar do serviço. Com isso, a não informação do usuário acerca do tratamento dos seus dados pode gerar dano moral. A decisão da ministra foi esta:

> RECURSO ESPECIAL. FUNDAMENTO NÃO IMPUGNADO. SÚM. 283/STF. AÇÃO DE COMPENSAÇÃO DE DANO MORAL. BANCO DE DADOS. COMPARTILHAMENTO DE INFORMAÇÕES PESSOAIS. DEVER DE INFORMAÇÃO. VIOLAÇÃO. DANO MORAL IN RE IPSA. JULGAMENTO: CPC/15. [..]6. O consumidor tem o direito de tomar conhecimento de que informações a seu respeito estão sendo arquivadas/comercializadas por terceiro, sem a sua autorização, porque desse direito decorrem outros dois que lhe são assegurados pelo ordenamento jurídico: o direito de acesso aos dados armazenados e o direito à retificação das informações incorretas. 7. A inobservância dos deveres associados ao tratamento (que inclui a coleta, o armazenamento e a transferência a terceiros) dos dados do consumidor - dentre os quais se inclui o dever de informar - faz nascer para este a pretensão de indenização pelos danos causados e a de fazer cessar, imediatamente, a ofensa aos direitos da personalidade. [..]Do mesmo modo, o fato de alguém publicar em rede social uma informação de caráter pessoal não implica o consentimento, aos usuários que acessam o conteúdo, de utilização de seus dados para qualquer outra finalidade, ainda mais com fins lucrativos. 11. Hipótese em que se configura o dano moral in re ipsa. 12. Em virtude do exame do mérito, por meio do qual foram rejeitadas as teses sustentada

> pela recorrente, fica prejudicada a análise da divergência jurisprudencial. 13. Recurso especial conhecido em parte e, nessa extensão, desprovido. (BRASIL, 2019, s/p).

Com relação à decisão mencionada, segundo a Terceira Turma do STJ, toda e qualquer informação fornecida por uma empresa que atua no ramo de gestão de dados torna-se de sua ampla responsabilidade, pois, para que ocorra qualquer tipo de divulgação de dados, deve haver a prévia comunicação de seu compartilhamento ao seu titular. Para a ministra Nancy Andrighi, o dano moral é presumido, não sendo necessária à sua comprovação (BRASIL, 2019).

O vazamento de dados conforme ocorreu nos casos supracitados violam a boa-fé, o princípio da transparência, a finalidade, a segurança, dentre outros elementos dispostos no artigo 6º da Lei nº 13.709 de 14 de agosto de 2018. Já o 7º artigo da lei salienta a necessidade do consentimento do titular de maneira inequívoca para o tratamento dos seus dados. O 9º artigo, por sua vez, destaca que o titular dos dados deverá ter livre acesso às informações referentes à sua forma de tratamento, disponibilizadas de forma clara, tornando-se de fácil compreensão. Ademais, se houver algum tipo de mudança de finalidade para com o tratamento que não condiz com as quais o titular anuiu, esse deverá ser informado de imediato, para que, em casos de discordância, possa fazer-lhe a revogação do seu consentimento (BRASIL, 2018).

Nesse sentido, conforme explana o artigo 42 da Lei nº 13.709/2018, o mero dano em si já é plausível de reparação, seja esse dano moral, patrimonial, coletivo ou individual. Tal dispositivo, porém, não menciona o quesito culpa como elemento primordial, estando previsto somente no artigo 43 como uma excludente. O entendimento jurisprudencial acerca do assunto prevê a comprovação do dano sofrido pela vítima, para que possa ser mensurado o dano moral, independente de culpa (SILVA, 2019).

De acordo com o a Lei nº 8.078, de 11 de setembro de 1990, em seu 3º artigo, define-se fornecedor como qualquer pessoa física ou jurídica, de natureza pública ou privada, nacional ou ainda estrangeira que exerça a atividade de produção, de transformação, de distribuição de comercialização seja de produtos ou serviços, desde que mediante remuneração (BRASIL, 1990).

Conforme menciona Tartuce (2018), a remuneração tratada no artigo 3º da Lei não se refere apenas à remuneração direta, mas também a de cunho indireto. Isso significa que, mesmo que o aplicativo seja oferecido gratuitamente, ele aufere lucro de alguma forma.

Em um meio como a internet, em que ocorre a constante divulgação de dados, o direito à privacidade deve ser respeitado, a fim de proteger o indivíduo de situações que causem constrangimento à sua vida particular. O usuário deve ter o controle ou ao menos ter conhecimento de como serão utilizados seus dados, que foram coletados de maneira habitual e inofensiva para o

preenchimento de um cadastro para a realização de eventual compra. Uma vez utilizados tais dados de forma irregular, pode-se gerar um extenso dano a quem os forneceu (SCHREIBER, 2013).

3 CONSIDERAÇÕES FINAIS

Com base nas informações obtidas por meio do estudo para este artigo, constatou-se que a facilidade de acesso ao meio digital acabou por tornar os indivíduos dependentes da tecnologia. Esse fato também deu margem para o grande avanço tecnológico, uma vez que vem ocasionando o crescente aumento na criação de novos aplicativos para facilitar a interação social.

Todavia, com uma maior oferta de aplicativos, aumentou também a inserção de informações disponibilizadas pelas pessoas, dados que são armazenados em bancos digitais e que devem manter em sigilo todas as informações que lhe são conferidas.

Diante do cenário atual, vem sendo cada vez mais recorrente o anúncio pelas mídias de eventuais vazamentos de dados, de todo os meios, desde sistemas de aplicativos pagos aos aplicativos que fornecem material de entretenimento de forma gratuita. Mesmo que um aplicativo seja gratuito, vale ressaltar que recebem outro tipo de remuneração que passa a ser mais valiosa, tornando o dado, ou seja, as informações de usuários como um tipo de moeda de troca em seu meio.

Por meio dessa nova moeda, o indivíduo torna-se um elemento essencial para esse novo mercado, que vem enfrentando problemas cada vez maiores com relação à proteção de dados. Esses problemas foram devidamente demonstrados nos casos apresentados, indicando diversas situações nas quais os usuários tiveram seus dados divulgados sem consentimento, reforçando a vulnerabilidade da proteção dos sistemas presentes nos aplicativos.

Após a apresentação dos dispositivos legais e análise de casos, é possível responder à problematização levantada: Se o aplicativo expuser os dados de seus usuários de forma indevida, a empresa que é responsável pelo seu desenvolvimento e uso poderá ser responsabilizada? A resposta é afirmativa, sim, o vazamento e o compartilhamento de dados violam o previsto na Constituição Federal, em seu artigo 5º, incisos X e XII, que reforçam que o indivíduo tem direito à privacidade.

Alguns aplicativos recorrentemente têm sofrido ações judiciárias por transmitir os dados dos seus usuários. Essa situação fez com que houvesse a implementação de normas que regulamentam como os dados serão processados por esses aplicativos, a sua forma de inserção, o seu tratamento, a sua destinação e o seu armazenamento. Tudo isso deverá se dar com o consentimento do seu titular, que deverá ser informado de eventuais divergências aos termos pelo qual anuiu para a utilização do serviço vinculado ao aplicativo.

Ressalta-se, ainda, a incidência da relação de consumo entre o aplicativo e o usuário, uma vez que o aplicativo se enquadra na categoria de fornecedor que presta serviços e aufere lucro com a utilização dos seus serviços e com o armazenamento/comercialização de dados dos seus usuários. Assim, o aplicativo tem ampla responsabilidade pela forma como recebe, trata, transmite e armazena os dados dos seus usuários. Nesse sentido, caso seja alvo de falhas em seu sistema, ou, ainda, quando divulgadas, comercializadas ou vazadas informações sobre os seus usuários sem que a esse lhe tome o consentimento, a empresa pode pagar indenização.

Ainda sobre a responsabilidade do aplicativo, essa se torna objetiva, visto que é pautada no dever e na segurança, pois, quando o usuário insere as suas informações para poder utilizar o aplicativo, confia e espera que as suas informações sejam mantidas em segurança e sejam utilizadas apenas para os fins que autorizou. Todavia, quando as informações fornecidas passam a transacionar entre provedores, o dever de segurança ao qual o aplicativo deveria foi claramente violado, pois agiu de forma diversa da qual se esperava.

Acerca da indenização por dano moral, essa se torna relativa, pois, para alguns, o entendimento é que o dano é presumido, sendo assim, com o simples vazamento dos dados já é possível pleitear a indenização, sem a comprovação efetiva do dano por parte da vítima. Entretanto, para outros, o dano deverá ser comprovado, demonstrando que o vazamento de dados definitivamente causou prejuízo ao titular, como ocorreu em um dos casos citados no presente artigo.

Vale ressaltar que a relação entre o usuário e o aplicativo se enquadra em uma relação de consumo, já que o aplicativo enquadra-se como um fornecedor, ou seja, um prestador de serviço, conforme o disposto no artigo 3º de Lei nº 8.078, de 11 de setembro de 1990, que dispõe sobre a proteção do consumidor, informando o conceito de fornecedor, bem como sobre produto e ainda sobre a prestação de serviço. De acordo com a lei, para se enquadrar em uma relação de consume, deve haver uma forma de remuneração; nos casos dos aplicativos, eles auferem lucro com a sua utilização, por isso, o usuário se equipara ao consumidor e o aplicativo ao fornecedor.

Salienta-se que a criação da Lei Geral de Proteção de Dados, que está prevista para entrar em vigência em agosto de 2020, é de suma importância, visto que traz maior segurança jurídica para as relações do meio digital, bem como traz maiores informações e obrigações para os bancos de dados, possibilitando que o titular revogue a utilização dos seus dados perante os aplicativos.

Diante do exposto, verifica-se que uma má gestão de dados no meio digital pode desencadear diversos tipos de prejuízos quando utilizados de forma diversa a esperada. Em decorrência disso, faz-se necessária uma atuação do Poder Judiciário de forma mais efetiva e com

cautela, a fim de se realizar uma forma de uniformização jurisdicional que garanta uma maior segurança jurídica, regulando a relação entre o usuário e o aplicativo.

REFERÊNCIAS

BIONI, B. R. **Proteção de dados pessoais**: a função e os limites do consentimento. 1.ed. Rio de Janeiro: Forense, 2019.

BRASIL. Senado Federal. **Lei n.º 8.078**, 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8078.htm>. Acesso em: 27 out. 2019.

_____. _____. **Lei n.º13.709**, 14 de agosto de 2018. Dispõe sobre a lei geral de proteção de dados pessoais. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 25 mai. 2020.

_____. Superior Tribunal de Justiça. **Recurso Especial 1758799.** Relator: Min. NANCY ANDRIGHI. 3º Turma, Data de Julgamento: 12/11/2019. Publicado no DJe: 19/11/2019. Disponível em < http://www.stj.jus.br/SCON>. Acesso em: 31 mai. 2020.

CAVALIERI FILHO, Sérgio. **Programa de responsabilidade civil.** 10. ed. São Paulo: Atlas, 2012.

COELHO, G. **Yahoo! poderá pagar 47 milhões de dólares por vazamento de dados**. 2018. Disponível em: <https://www.conjur.com.br/2018-set-19/yahoo-pagar-us-47-milhoes-vazamento-dados-2014>. Acesso em: 11 mai. 2020.

COELHO, G. IDC pede punição do Facebook por violação de dados pessoais. **Revista Consultor Jurídico,** 2019. Disponível em: <https://www.conjur.com.br/2019-ago-31/idc-punicao-facebook-violacao-dados-pessoais>. Acesso em: 12 abr. 2020.

COELHO, G. Não informar comercialização de dados pessoais gera dano moral, diz STJ. **Revista Consultor** Jurídico, 2019. Disponível em: <https://www.conjur.com.br/2019-dez-17/nao-informar-comercializacao-dados-pessoais-gera-dano-moral> Acesso em: 21 mai. 2020.

DISTRITO FEDERAL. Tribunal de Justiça do Distrito Federal e dos Territórios**. Acórdão 971.472**. Relator Juiz Aiston Henrique de Sousa, 2ª Turma, Data de Julgamento: 5/10/2016. Publicado no DJe: 13/10/2016. Disponível em <https://www.tjdft.jus.br/consultas/jurisprudencia/jurisprudencia-em-temas/cdc-na-visao-do-tjdft-1/o-consumidor-na-internet/divulgacao-de-informacoes-pessoais-na-internet>. Acesso em: 25 out. 2019

FABRO, C**. WhatsApp:** números de celular privados são expostos no Google. 2020. Disponível em: <https://www.techtudo.com.br/noticias/2020/06/whatsapp-numeros-de-celular-privados-sao-expostos-no-google.ghtml >. Acesso em: 09 jun. 2020.

GARCIA, R. Marco civil da internet no Brasil: repercussões e perspectivas. **Revista dos Tribunais Online**, 04 abr. 2016. Disponível em <http://www.rtonline.com.br/2016/04/marco-civil-da-internet-no-brasil-repercussoes-e-perspectivas/>. Acesso em: 04 nov. 2019.

GAGLIANO, S. P.; PAMPLONA FILHO, R. **Novo curso de direito civil 3:** responsabilidade civil. 17. ed. Saraiva, 2018.

GONÇALVES, C. R**. Direito civil brasileiro, volume 4**: responsabilidade civil. 12. ed. São Paulo: Saraiva, 2017.

MACIEL, R. F. **Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais** (Lei nº 13.709/18). 1. ed. Goiânia: RM Digital Education. 2019.

MARTINES. F. Procon multa Google e Apple por aplicativo que dita imagens de rostos. **Revista Consultor Jurídico**, 30 de agosto de 2019. Disponível em <https://www.conjur.com.br/2019-ago-30/procon-multa-google-apple-aplicativo-edita-imagens-rosto>. Acesso em: 13 abr. 2020.

MARTINS, J. Homem será indenizado por ter perfil criado sem autorização no aplicativo Lulu. **Revista Consultor Jurídico.** Disponível em: <https://www.conjur.com.br/2018-dez-01/homem-indenizado-perfil-criado-autorizacao-lulu>. Acesso em: 27 mai. 2020.

MPDFT. **Uber termina de notificar usuários brasileiros afetados por vazamento de dados.** 2018. Disponível em: <https://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2018/10012-uber-termina-de-notificar-usuarios-brasileiros-afetados-por-vazamento-de-dados>. Acesso em: 18 mai. 2020.

MPDFT. **MPDFT e Netshoes firmam acordo para pagamento de danos morais após vazamento de dados.** 2019. Disponível em: <https://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2019/10570-mpdft-e-netshoes-firmam-acordo-para-pagamento-de-danos-morais-coletivos-apos-vazamento-de-dados>. Acesso em: 11 mai. 2020.

NOVO, B. N. Direito digital. **Revista Jus Navigandi**, v. 24, n. 5843, jul. 2019. Disponível em: <https://jus.com.br/artigos/74019>. Acesso em: 27 out. 2019.

PARANÁ. Tribunal de Justiça do Estado do Paraná. **RI nº 0028512-61.2013.8.16.0019**. Relator Juiz Vitor Toffoli, 1ª Turma, Data de Julgamento: 21/10/2014. Publicado no DJe: 24/10/2014. Disponível em < https://portal.tjpr.jus.br/jurisprudencia/j/2100000001476861/Ac%C3%B3rd%C3%A3o-0028512-61.2013.8.16.0019 >. Acesso em: 31 mai. 2020.

PINHEIRO, P. P. **Direito digital**. 6. ed. São Paulo: Saraiva, 2016.

RAMOS, G.; NAVARRO, L. A LGPD no Brasil e o direito à autodeterminação informativa na era digital. **Revista Consultor Jurídico.** Disponível em: <https://www.conjur.com.br/2020-abr-07/entrada-vigor-lgpd-brasil-direito-autodeterminacao-informativa-digital>. Acesso em: 21 mai. 2020.

SANTOS, R. OLX irá indenizar advogado que teve dados usados em fraudes na Paraíba**. Revista Consultor Jurídico**. 2020. Disponível em: < https://www.conjur.com.br/2020-mar-05/juiza-condena-olx-indenizar-advogado-teve-dados-sequestrados>>. Acesso em: 21 mai. 2020.

SCHREIBER, A. **Direitos da personalidade**. 2. ed. São Paulo: Atlas, 2013.

SILVA, M. C. O vazamento de dados de consumidores gera dano moral indenizável? **Revista Consultor Jurídico**. 2019. Disponível em: <https://www.conjur.com.br/2019-dez-03/muriel-silva-vazamento-dados-consumidores-gera-dano-moral>. Acesso em: 12 abr. 2020.

TARTUCE, F. **Manual de responsabilidade civil**. Volume único. Rio de Janeiro: Forense, São Paulo, 2018.

TARTUCE, F.; NEVES, A. A. D. **Manual do direito do consumidor: direito material e processual**. 5. ed. Rio de Janeiro: Forense: São Paulo: Método, 2016

VENOSA, S. S. **Direito civil**: responsabilidade civil. 13. ed. São Paulo: Atlas, 2013.