CENTRO UNIVERSITÁRIO ANTÔNIO EUFRÁSIO DE TOLEDO DE PRESIDENTE PRUDENTE

CURSO DE DIREITO

LEI GERAL DE PROTEÇÃO DE DADOS: Natureza da Responsabilização e Importância da ANPD

Tayline de Campos Garcia Silva

Presidente Prudente/SP

2021

CENTRO UNIVERSITÁRIO ANTÔNIO EUFRÁSIO DE TOLEDO DE PRESIDENTE PRUDENTE

CURSO DE DIREITO

LEI GERAL DE PROTEÇÃO DE DADOS: Natureza da Responsabilização e Importância da ANPD

Tayline de Campos Garcia Silva

Monografia apresentada como requisito parcial de Conclusão de Curso para obtenção do grau de Bacharel em Direito, sob orientação da Profa. Dra. Ana Laura Teixeira Martelli Theodoro.

Presidente Prudente/SP

2021

LEI GERAL DE PROTEÇÃO DE DADOS: Natureza da Responsabilização e Importância da ANPD

Monografia aprovada como requisito parcial para obtenção do Grau de Bacharel em Direito.

DRA. ANA LAURA TEIXEIRA MARTELLI THEODORO
Orientadora

MS. GISELE CAVERSAN BELTRAMI MARCATO
Examinadora

MS. PEDRO AUGUSTO DE SOUZA BRAMBILLA
Examinador

Presidente Prudente, ___de _____ de 2021

Dedico este trabalho a minha mãe, minha avó e meu avô (em memória) que são a minha base e que sempre moveram montanhas a fim de que eu trilhasse pelos melhores caminhos.

AGRADECIMENTOS

Agradeço primeiramente a Deus que, diante de algumas adversidades, sustentou-me até aqui.
Agradeço à professora Dra. Ana Laura Teixeira Martelli Theodoro pela oportunidade de me orientar na elaboração deste trabalho com muita atenção e paciência.
Agradeço especialmente a minha mãe que sempre acreditou em mim, aconselhou-me e impulsionou-me a alcançar altos voos.
Agradeço a minha avó e meu avô (em memória) que sempre cuidaram e incentivaram-me nos estudos.
A toda minha família, amigos, professores, Dr. Matheus Assad e Dra. Giovana Devito, que me ajudaram direta e indiretamente a produzir esse trabalho.

RESUMO

Busca-se, por meio deste trabalho, explorar as minúcias acerca do gerenciamento e fornecimento dos dados de seus usuários, focando na análise da natureza da responsabilidade no contexto de tratamento de dados, bem como comparando seu tratamento ao que ocorre em outros países para regular tal questão, haja vista a entrada em vigor da Lei Geral de Proteção de Dados (LGPD) em 18 de setembro de 2020 no Brasil, e a General Data Protection Regulation (GDPR), de maio de 2018, na União Europeia, grande inspiração para o modelo brasileiro. Faz-se uma análise sobre os princípios trazidos pela legislação brasileira de moda a entender o seu modus operandi, além estudar a Autoridade Nacional de Proteção de Dados, sua estruturação, fazendo uma breve comparação com entidades correspondentes nas legislações estrangeiras. Para isso, foram utilizados os métodos histórico, dedutivo, comparativo e doutrinário.

Palavras-chave: Responsabilidade civil. Lei Geral de Proteção de Dados. Dados pessoais. Princípios. Autoridade Nacional de Proteção de Dados.

ABSTRACT

It is sought, through this work, to explore the minutiae about the management and provision of its users' data, focusing on the analysis of the nature of responsibility in the context of data treatment, as well as comparing its treatment to what occurs in other countries to regulate such issue, given the entry into force of the General Data Protection Law (LGPD) on September 18, 2020 in Brazil, and the General Data Protection Regulation (GDPR) of May 2018 in the European Union, great inspiration for the Brazilian model. An analysis is made on the principles brought by the Brazilian legislation in order to understand its modus operandi, besides studying the National Data Protection Authority, its structuring, making a brief comparison with corresponding entities in foreign legislations. For this, the historical, deductive, comparative and doctrinal methods were used

Keywords: Liability. General Data Protection Law. Personal Data. Principles. National Data Protection Authority.

LISTA DE ABREVIATURAS E SIGLAS

LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018)

ANPD – Autoridade Nacional de Proteção de Dados

CC – Código Civil

CDC – Código de Defesa do Consumidor

EU – European Union - União Europeia

STJ – Superior Tribunal de Justiça

ITS – Instituto de Tecnologia e Sociedade do Rio

IDEC - Instituto Brasileiro de Defesa do Consumidor

PEC – Proposta de Emenda Constitucional

SUMÁRIO

1 INTRODUÇÃO

As informações sempre foram objeto de cobiça de governos e iniciativa privada que buscavam aperfeiçoar suas competências e, à vista disso, potencializar seus resultados, trazendo-lhes superiores rendimentos. Dessa forma, quanto mais tenham armazenamento de informações relevantes e uma aprimorada administração destas, superior é a probabilidade de estar apto a ter êxito frente a competições em âmbito econômico, social e político.

Com a progressão do capitalismo, a informação desempenha cada vez mais um papel principal na denominada “sociedade da informação”. Com ela, a concepção de tornar o acesso às informações efetivamente democrático tornou-se o legítimo princípio, que se valeu do avanço tecnológico para conseguir sua concretização.

Nesse novo panorama, a informação ascende à posição de objeto de maior cobiça, impulsionando em todas as esferas a utilização de tecnologias que propiciassem a coleta, processamento e armazenamento de dados.

Com a expectativa genuinamente otimista causada pelas vastas oportunidades prometidas pelo universo das novas tecnologias, houve um aumento ao acesso à tecnologia de informação pelos indivíduos, e a introdução dessas no seu cotidiano remodelou paradigmas e a forma de produção nas empresas, transformou as atividades nas esferas pública e privada, modificou o padrão cultural e a forma das pessoas se socializarem, em contrapartida, a maior imersão nesse novo contexto acabou por expor cada vez mais a intimidade e a vida privada dos usuários frente às modernas ferramentas computacionais.

Além do mais, com a crise gerada pela pandemia do COVID-19, que impôs o isolamento social e a utilização da tecnologia como alternativa para a manutenção das relações interpessoais, estudos e trabalhos, houve um aprofundamento da relação entre as pessoas e a tecnologia, e uma brutal imersão no mundo digital.

O desenvolvimento das inteligências artificiais e a presença cada vez mais assídua de objetos do cotidiano que possuem ligação contínua com a internet – acontecimento denominado “internet das coisas” – também contribuem para o estabelecimento dos dados pessoais como uma das mais recentes e relevantes *commodities* na atualidade sendo comparado com a indústria do petróleo.

A partir disso, grandes empresas de publicidades, indústrias, redes sociais e mídias digitais no geral traçam serviços e técnicas alicerçadas nesses dados, deleitando-se de um espaço que carecia de regulamentação até então.

Em que pese a utilização dos dados pelos agentes proporcione certo proveito aos titulares, principalmente quando se fala no meio digital onde revelam-se funções mais inteligentes e especificadas, que tornam a experiência na internet singular, a ausência, ou até mesmo a deficiência, da regulamentação possui enorme capacidade de gerar consequências adversas.

Episódios de vazamentos de dados pessoais de redes sociais, como o que ocorreu no caso Facebook - Cambridge Analytica suscitaram internacionalmente a intenção de se buscar uma proteção mínima aos dados pessoais visando a manutenção dos estados democráticos, bem como do próprio titular em si, que teve seu direito à privacidade e intimidade violados ao passo que seus dados pessoais foram manipulados sem seu devido consentimento e informação de finalidade. Assim, iniciou-se a busca por regulamentação que confira proteção aos dados pessoais sem que haja prejuízo à atividade comercial ou ao nascimento de novas tecnologias.

A União Europeia contava desde 1995 com a Diretiva nº 95/46/CE do Parlamento Europeu e do Conselho da União Europeia que tratava acerca da proteção de dados pessoais. No entanto, houve a necessidade amoldar seu regramento às demandas que surgiram, apontando assim a *General Data Protection Regulation* (GDPR).

O Brasil, por sua vez, não possuía uma legislação individual que tratasse de forma sistematizada a proteção de dados. A tutela consagrada à essa demanda era encontrada em legislações esparsas sem uma sistematização bem definida e estruturada.

Essa omissão foi suprida, quando em 2018 a Lei nº 13.709 foi aprovada Lei Geral de Proteção de Dados (LGPD), legislação genuinamente inspirada no modelo europeu, que proporcionou um respeitável rol de regramento para a proteção de dados pessoais, possuindo diretrizes que guiarão o tratamento de dados, além de prever a Autoridade Nacional de Proteção de Dados, que tem como objetivo dar efetividade à legislação.

Assim, a partir de análises histórica, comparativa, doutrinária e jurisprudência, devolverá essa construção cientifica buscando elucidar as indagações supramencionadas, destrinchando a Lei Geral de Proteção de Dados.

2 OS DADOS PESSOAIS

A Lei Geral de Proteção de Dados é considerada uma lei com natureza principiológica e conceitual. A primeira característica é atrelada a ela devido ao extenso rol exemplificativo de princípios contido em seu artigo sexto, que servirão como parâmetro para o desenvolvimento de atividade de tratamento de dados.

Já a segunda característica se justifica pelo modo com que se apresentou a definição de vários termos utilizados pela legislação localizados principalmente em seu artigo quinto. Este artigo buscou trazer a definição dado pessoal, fazendo uma importante decomposição em dois categorias de dados pessoais: os dados pessoais, no geral, e os dados pessoais sensíveis.

2.1 Conceito, Espécies e Natureza Jurídica dos Dados Pessoais

O conceito de dado pessoal é o componente essencial para que se aprimore a legislação em estudo ao passo que se estabelece limites para a própria tutela jurídica. Dessa forma, pode-se invocar a concepção de que qualquer dado que não possua essas determinadas caraterísticas não poderá ser considerado dado pessoal e, por conseguinte, não se valerá da regulamentação deste. Não seria qualquer dado que teria repercussão jurídica, mas, somente, aquele que atraísse o qualificador pessoal (BIONI, 2019, p. 68).

A LGPD trouxe a conceituação do dado pessoal como toda e qualquer informação relacionada a pessoa natural identificada ou identificável (BRASIL, 2018) e o dado pessoal sensível como

> dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. (BRASIL, 2018)

Nota-se que de acordo com a conceituação ampla trazida pela LGPD ao dado pessoal, entende-se que não será atribuída tal terminologia a este somente quando tiver aptidão de se referir diretamente a um indivíduo, como ocorre com o número de CPF, número de RG e título de eleitor, mas também as informações que se refiram indiretamente a um indivíduo contendo capacidade de identificá-lo, como

ocorre com os testemunhos de conexão (cookies), identificador de publicidade do celular, hábitos de consumo, preferências de lazer e dados de localização (por exemplo, a função de geolocalização de um celular). Esses dados também são conhecidos como metadados, denominação originada na ciência da computação.

Observa-se que diante das duas teorias existentes acerca do conceito de dados pessoais, reducionista e expansionista, a LGPD adotou a segunda, de modo que não apenas serão considerados pessoais os dados que inequivocadamente identificam uma pessoa mas também aqueles que têm potencial para identificá-la, já que:

> a expansionista aposta em uma lógica mais flexível que desconsidera a associação exata entre uma informação e uma pessoa. Dado pessoal pode ser qualquer tipo de informação que permita a sua identificação, ainda que o vínculo entre o dado e um indivíduo não seja estabelecido de prontidão, mas de forma mediata ou indireta. Um dado para ser pessoal deve ser, portanto, a projeção de uma pessoa identificável. (BIONI, 2015, p. 17)

Quando um dado pessoal passa pelo processo de anonimização, que consiste na utilização de meios técnicos razoáveis e disponíveis na ocasião do tratamento a fim de que não seja mais possível relacioná-lo ao seu titular, após o procedimento, perdendo a característica de identificação, o dado não será mais considerado um dado pessoal, e sim um dado anonimizado.

Atualmente, encontra-se disponível vários mecanismos para converter dados anônimos em identificáveis. Tem-se como exemplo o Caso Netflix Prize, em a plataforma de *streaming* de filmes e séries, Netflix, em que disponibilizou a sua base de dados com todas as avaliações dos filmes de seu catálogo do período de 1998 a 2005, suprimindo os nomes dos usuários avaliadores e deixando somente a data e a nota da avaliação (BIONI, 2019, p. 73), a fim de aprimorar seu algoritmo de sistema de sugestão de filmes.

Em que pese a anonimização dos dados ofertados pela plataforma, os pesquisadores cruzaram as informações com uma base de dados publicamente acessível conseguindo a reidentificação dos dados anonimizados.

> We have presented a de-anonymization methodology for sparse micro-data, and demonstrated its practical applicability by showing how to de-anonymize movie viewing records released in the Netflix Prize dataset. Our de-anonymization algorithm Scoreboard RH works under very general assumptions about the distribution from which the data are drawn, and is robust to data perturbation and mistakes in the adversary's knowledge.

> Therefore, we expect that it can be successfully used against any dataset containing anonymous multi-dimensional records such as individual transactions, preferences, and so on [1].(NARAYANAN, Arvind; SHMATIKOV, Vitaly, sem data, p. 13-14)

Dessa forma, vai de regra, prepondera a teoria expansionista em que o dado pessoal é aquele que identifica diretamente um indivíduo ou tem potencial para identificá-lo, haja vista que sempre existirá a possibilidade de uma base de dados anonimizada ser agregada a outra para a sua reidentificação (BIONI, 2019, p. 108).

A LGPD ainda conceitua o banco de dados como conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico (BRASIL, 2018).

Partindo-se do pressuposto de que os dados pessoais exprimem informações que tem aptidão de caracterizar seu titular, bem como ser munição para tratamento discriminatório no caso de dados sensíveis, é acertado identificá-los como um direito atinente à personalidade.

2.2 Fundamento Jurídico (Proteção dos Dados Pessoais Como Direito Fundamental)

Os reflexos das novas tecnologias são diretamente observados no direito, posto que este deve revelar-se adequado para solucionar disfunções acarretadas por elas preservando como valor fundamental a pessoa humana e, simultaneamente, fornecendo segurança necessária para que haja a previsibilidade e segurança devidas para a viabilidade da estrutura econômica dentro da tábua axiológica constitucional (DONEDA, 2020, p. 37).

Importante, nesse sentido, é reportar-se a decisão da Corte Constitucional alemã no caso da Lei do Censo de 1983 (Volkszählunsgesetz)[2], que

[1] Apresentamos uma metodologia de “desanonimar” microdados esparsos e demonstramos sua aplicabilidade prática mostrando como “desanonimar” os registros de visualização de filmes lançados no conjunto de dados do Netflix Prize. Nosso “ScoreboardRH de-anonymizationalgorithm” trabalha sob hipóteses muito gerais sobre a distribuição da qual os dados são extraídos, e é robusto para perturbação de dados e erros no conhecimento do adversário. Portanto, esperamos que ele possa ser usado com êxito contra qualquer conjunto de dados que contenha registros multidimensionais anônimos, como transações individuais, preferências e assim por diante (tradução nossa).

[2] A Lei do Censo de 1983 (Volkszählunsgesetz) determinou que os cidadãos na Alemanha concedessem vários dados pessoais com o fim de se observar disposição na extensão da população naquele território, bem como possível análise cruzada com outros dados para programas generalizados de administrativos. Tal lei foi julgada pela Corte Constitucional Alemã como parcialmente

inovou na esfera de proteção de proteção de dados pessoais ao passo que declarou a proteção de dados pessoais como um direito de personalidade autônomo ao passo que verifica a autodeterminação informacional como um direito da personalidade, haja vista que A capacidade do indivíduo de autodeterminar seus dados pessoais seria parcela fundamental do seu direito em livremente desenvolver sua personalidade (BIONI, 2019, p. 129).

Nesse diapasão, a mobilização para a regulamentação a respeito da proteção de dados em vários ordenamentos jurídicos provocou:

> uma tendência que, a princípio, parecia apenas destinada a mudar determinado patamar tecnológico e a solicitar previsões pontuais no ordenamento, mas que, em seus desdobramentos, veio a formar as bases para o que vem sendo tratado, hoje, como um direito fundamental à proteção de dados (DONEDA, 2011, p. 96)

Certo é que tal tendência pode ser notada no ordenamento jurídico pátrio quando se visualiza a Proposta de Emenda Constitucional nº 12 de 2019[3], que visa alterar a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.

A proposta para declaração da proteção de dados pessoais como um direito da personalidade e desdobramento da dignidade da pessoa humana, elencada na Carta Magna, fixa os dados pessoais como direitos extrapatrimoniais, inabdicável, refletindo na forma como se depreende a responsabilização dos agentes de tratamento em caso de algum acidente.

Ainda, complementa Rafael Pinheiro Rotundo (2017, p. 10) que:

> O direito à proteção de dados não se limita à proteção da personalidade humana, sua intimidade e vida privada. A proteção de dados visa permitir gama muito maior de relações, ou, de outra parte, evitar que se criem barreiras para a fruição de todos os direitos e garantias. É fonte de fomento para igualdade social. (ROTUNDO, 2017, p. 10)

inconstitucional com fundamento de que os dados coletados deveriam única e exclusivamente ter por fim à atividade de recenseamento.

[3] Atualmente aguarda apreciação do Senado Federal.

Assim, na condição de direito fundamental, o direito a proteção de dados se revela em duas dimensões: subjetiva e objetiva. Na primeira dimensão, o direito à proteção de dados pessoais se

> decodifica em um conjunto heterogêneo de posições subjetivas de natureza defensiva (negativa), mas também assume a condição de direito a prestações, cujo objeto consiste em uma atuação do estado mediante a disponibilização de prestações de natureza fática ou normativa (SARLET, 2018, p. 288).

Nesse contexto, a proteção de dados deve ser vislumbrada como uma prerrogativa de não ofensa ou intromissão à dimensão privada do indivíduo, encontrando arcabouço de fundamento no artigo 5º, inciso X, da Constituição Federal, bem como no artigo 21 do Código Civil de 2002 em que impõe a inviolabilidade da vida privada da pessoa natural (BIONI, 2020, p. 92-93).

Essa não intromissão se refere a uma condutada almejada não somente por entidades privadas como também do próprio Estado. Isso se justifica, haja vista que, conforme entende Jacinto Nelson de Miranda Coutinho (2016, p. 200), a

> privacidade, a día de hoy, se pone en riesgo por las escuchas telefónicas, microcámaras poderosas que captan conversaciones a larga distancia, por la invasión de una prensa en ocasiones sensacionalista e irresponsable, por la circulación de datos individuales previstos para un determinado fin y utilizados para otro, por la violación de la confidencialidad constitucional, especialmente por las comisiones parlamentares de investigación, por las intervenciones corporales realizadas por la policía bajo la sospecha de haber cometido delito, en fin por una serie de atentados potenciales, solamente posibles en una sociedad tecnológica y económicamente compleja en que el ciudadano, para convivir y para salir del aislaminto proprio del siglo XX y XXI, es obligado a estabelecer relaciones sociales y económicas y, así, exponer a público uma parte considerable de su intimidad y de su familia. [4]

Conclui-se, portanto, que pela perspectiva subjetiva, a privacidade deve ser compreendida pela concepção de liberdade negativa, direito de retrai aspectos de

[4] A privacidade, hoje, é posta em risco pelos grampos telefônicos, potentes microcâmeras que captam conversas à distância, pela invasão de uma imprensa às vezes sensacionalista e irresponsável, pela circulação de dados individuais destinados a um fim e usados para outro , pela violação do sigilo constitucional, em especial pelas comissões parlamentares de inquérito, pelas intervenções corporais realizadas pela polícia sob suspeita de crime, em suma, por uma série de ataques potenciais, apenas possíveis numa sociedade tecnológica e economicamente complexo em que o cidadão, para conviver e sair do isolamento dos séculos XX e XXI, é obrigado a estabelecer relações sociais e econômicas e, assim, expor ao público parte considerável de sua privacidade e de sua família (tradução nossa).

sua vida do domínio público e estar a salvo de interferências alheias (BIONI, 2020, p. 92).

Por outro lado, pela perspectiva objetiva da proteção dos dados pessoais, emerge um dever ao Estado de instituir meios eficazes para assegurar a proteção dos dados pessoais perante a terceiros:

> Neste sentido o Estado tem o dever de proteger o direito à vida perante eventuais agressões de outros indivíduos (é a ideia trazida pela doutrina alemã na fórmula Schutzpflicht). O mesmo acontece com numerosos direitos como o direito de inviolabilidade de domicílio, o direito de protecção de dados informativos, o direito de associação. Em todos estes casos, de garantia constitucional de um direito resulta o dever do Estado adoptar medidas positivas destinadas a proteger o exercício dos direitos fundamentais perante atividades perturbadoras ou lesivas dos mesmos praticadas por terceiros. Daí o falar-se da função de proteção perante terceiros. (CANOTILHO, 1993, p. 409).

É neste momento, portanto, que surge a exigência de se criar um legislação que devidamente estruturada que regulamente e crie meios necessários para a efetiva proteção dos dados pessoais, tal qual fez a LGPD ao prever como deve ser realizado os tratamentos dos dados pessoais, a Autoridade Nacional de Proteção de Dados, principalmente, deve zelar pela observância da proteção dos dados pessoais conforme estipulado pela legislação, e sanções administrativas, aplicadas pela ANPD, para aqueles que infringi-la.

Faz-se necessário frisar que a LGPD expressamente estabeleceu que não será aplicada no contexto de tratamento de dados pessoais quando for realizado para fins exclusivamente particulares e não econômicos, jornalísticos, artísticos, acadêmicos, segurança pública, defesa nacional, segurança do Estado e atividades de investigação e repressão de infrações penais (artigo 4º, da Lei 13.709, de 2018).

2.3 A Comercialização dos Dados Pessoais

Conforme já abordado, a sociedade da informação passa a almejar os dados como grande fonte potencializadora da efetividade de difusão e comércio de seus produtos sobretudo em relação à segmentação de bens de consumo (*marketing*) e promoção (publicidade), utilizando-os como base para construção de perfis que auxiliarão na previsibilidade de compatibilização do produto comercializado com as preferências do titular.

Segundo Bruno Bioni (2019, p. 40):

> A Internet e a sua camada de aplicações, principalmente a web com blogs, redes sociais, websites etc., capilarizou esses painéis de opiniões. Os consumidores compartilham e trocam, com mais frequência, em diversos canais e quase em tempo real, informações sobre as suas experiências de consumo: um blog em que consumidores de vinhos comentam as suas aspirações de sommelier, ou, simplesmente, um consumidor que reclama sobre uma determinada funcionalidade de um produto em uma rede social. Em todas essas situações, eles passam a ser “ouvidos” por seus milhares de pares, parametrizando o próprio movimento de consumo.

A metáfora do sorvete social elucida de forma efetiva o processo de transformação com o advento de recursos de compartilhamento de saberes e informação. A situação se passa na cidade de Scoopville, conhecida pela produção dos mais variados tipos de sorvetes por seus moradores. Certo dia, um dos comerciantes posicionou um mural em frente do seu estabelecimento para que seus clientes deixassem sua avaliação sobre as inúmeras variedades de sorvete que era ofertado.

Essas avaliações começaram a interferir na produção dos sorvetes, posto que o comerciante optou por produzir aqueles sabores mais bem avaliados e, por conseguinte, influiu também no consumo das pessoas que ali iam visitar.

Nesse contexto, o consumidor assume uma função de assistente de vendas sem custo, além de ele divulgar o bem de consumo, a informação por ele produzida auxilia em seu processo de produção. (BIONI, 2019, p. 40).

Nesse contexto Laura Schertel Mendes e Marcela Mattiuzzo afirmam que:

> A função mais importante de Big Data é elaborar previsões baseadas em um grande número de dados e informações: desde desastres climáticos até crises econômicas, do surto de uma epidemia até o vencedor de um campeonato de esportes, do comportamento de um consumidor até a solvência dos clientes. Assim, as análises de Big Data podem ser utilizadas para elaborar prognósticos, tanto com relação à economia, à natureza ou à política, quanto sobre comportamento individual. No que se refere ao assunto aqui discutido, a predição do comportamento individual é de grande interesse, na medida em que gerar informação e conhecimento sobre o comportamento de uma pessoa a partir de dados pessoais oferece base para tomada de decisões.

Nota-se, portanto, que há um enorme interesse das grandes mídias digitais em se obter dados sobre seus usuários para que consigam direcionar produtos, notícias, publicidades em geral de empresas patrocinadoras para aqueles

usuários considerados mais aptos a consumir os produtos desta, tendo em vista o perfil traçado com base na sua atividade e dados proporcionados às mídias digitais.

É o que ocorreu no emblemático caso de vazamentos de dados do Facebook a Cambridge Analytica, companhia que trabalhava na campanha para de Donald Trump, em que haveria interferido no resultado da eleição para a presidência dos Estados Unidos, bem como no plebiscito para o Brexit. As informações apenas vieram à tona em 2018 quando um delator divulgou à mídia que a companhia havia empregado cerca de 50 (cinquenta) milhões de dados para o registro de perfis de eleitores norte-americanos e realização do *marketing* político extremamente particularizado, sem qualquer informação de finalidade e consentimento dos titulares.

Verificando-se a crescente importância dos dados no mercado, surge a necessidade de se examinar até que ponto é razoável a manipulação dos dados dos usuários para estratégias de marketing e de modelo de negócio sob o ponto de vista jurídico, e até que ponto essa manipulação poderia cercear a liberdade de escolha dos usuários ao serem direcionados determinados produtos, anúncios e notícias em detrimento de outros e até mesmo ferir a sua privacidade.

Nesse caso, havendo qualquer agressão ao direito do titular dos dados, surge a necessidade de reparação pelos danos a estes pelos agentes de tratamento.

3 RESPONSABILIDADE CIVIL NA LGPD ACERCA DO TRATAMENTO DE DADOS

Quando se fala em responsabilidade civil está se referindo necessariamente a uma situação de dano. A lei brasileira, que pode ser considerada como uma lei geral que trata da responsabilidade civil e que, portanto, traz os elementos fundamentais da responsabilidade civil é o Código Civil Brasileiro.

O Código Civil traz, nos artigos 186, 187 e 927 e seguintes, toda uma diretiva genérica sobre esses elementos que constituem o que se chama de responsabilidade civil, ou seja, o dano, a culpa ou o risco, que são dois fatores que justificam a obrigação de indenizar, e o nexo de causalidade. Assim, é possível dizer que toda vez que se tem um dano, que é o pressuposto da responsabilidade civil, a vítima desse dano terá que comprovar que a situação desfavorável foi causada a ela em razão de uma conduta culposa ou uma atividade de risco ligada causalmente àquele resultado.

Em poucas palavras, pode-se se referir a reponsabilidade civil, a partir da visão de uma teoria geral, como a constituição de três elementos: dano, culpa ou risco, e causalidade, que uma vez comprovados gerarão a obrigação de indenizar.

Deste modo, ao lado do Código Civil, que traz as normas genéricas, tem-se inúmeras outras legislações que tratarão da responsabilidade civil de maneira específica. A segunda lei mais importante que trata a responsabilidade civil por conta da sua incidência concreta é o Código de Defesa do Consumidor.

O Código de Defesa do Consumidor traz um aspecto importante sobre a responsabilidade civil que é o fato de que o fornecedor do produto ou do serviço são obrigados a indenizar o consumidor pelos danos que forem causados a ele de forma objetiva, ou seja, está expressamente previsto, tanto no artigo 12 quanto no artigo 14 do CDC, que, se o consumidor sofrer um dano, o fornecedor responderá independentemente de culpa por este. Assim, o fornecedor é obrigado a indenizar aquele dano sem que o consumidor precise comprovar que houve uma conduta culposa por parte do fornecedor, recaindo a prova basicamente sobre a existência da relação de consumo e o dano que foi concretamente observado.

É possível dizer que há conexão entre esses dois códigos com a Lei Geral de Proteção de Dados ao passo que há que se interpretar toda legislação dentro de um ambiente que é integral, então faz-se a interpretação da Lei Geral levando em

consideração o Código Civil e o Código de Defesa do Consumidor naquilo em que se denomina de diálogo das fontes legislativas.

A Lei Geral de Proteção de Dados não trouxe uma identificação sobre qual é o fundamento dessa responsabilidade atinente ao dano causado na circunstância de tratamento de dado, assim não se tem clareza se o agente de tratamento de dados, especificamente o controlador, é obrigado a indenizar o dano causado ao titular de dados de forma objetiva ou de forma subjetiva, ou seja, a lei não trouxe de forma explicita essa justificativa para a obrigação de indenizar, o que leva a necessidade de interpretação.

Além do mais, o tema da responsabilidade civil na Lei Geral de Proteção de Dados já começa polêmico pelo simples fato de que houve uma alteração de posicionamento em relação aos projetos de lei que já tramitavam 8/9 anos, tanto no Senado quanto na Câmara, e o resultado que se tem hoje após a aprovação e sanção do texto da lei. Com isso busca-se referir especificamente ao fato de que nos projetos, originalmente, havia o reconhecimento expresso de que a responsabilidade civil pelos danos causados por violação aos direitos dos titulares de dados, seriam respondidos pelos ofensores (agentes de tratamentos) independentemente da existência de culpa. Ou seja, havia nos projetos de lei abertamente a adoção da responsabilidade civil objetiva.

Tanto é assim, que no relatório final do deputado Orlando Silva a respeito do projeto de Lei nº 4.060 de 2012, que dispunha sobre o tratamento de dados, proposto pelo deputado Milton Monti, o qual expressamente aduzia em seus artigos 42 a 45 a adoção da hipótese de responsabilidade civil por risco, fazendo uma leitura sistemática da Lei Geral com o Código Civil de 2002, foi afirmada a aplicação da responsabilidade objetiva e solidária, tendo em vista que a atividade de tratamento de dados pessoais constitui atividade de risco e que usualmente há o tratamento de dados por mais de um agente, não devendo, por conseguinte, recair ao titular de dados o ônus de se investigar dentro do uma rede econômica quem teria dado causa ao dano.

Atualmente, em razão da ausência de determinação legislativa que expresse categoricamente sobre a adoção da responsabilidade objetiva ou subjetiva, paira-se diversos entendimentos com os mais sortidos fundamentos na doutrina.

3.1 Da Responsabilidade Civil Objetiva dos Agentes de Tratamento de Dados

O Código Civil de 2002, estabelece que estará caracterizada a natureza objetiva da responsabilidade civil quando, independente de culpa, houver previsão em lei ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem (artigo 927, § único).

Caio Mario da silva Pereira (2018, p. 325) enuncia que:

> A doutrina objetiva, ao invés de exigir que a responsabilidade civil seja a resultante dos elementos tradicionais (culpa, dano, vínculo de causalidade entre uma e outro) assenta na equação binária cujos polos são o dano e a autoria do evento danoso. Sem cogitar da imputabilidade ou investigar a antijuridicidade do fato danoso, o que importa para assegurar o ressarcimento é a verificação se ocorreu o evento e se dele emanou o prejuízo. Em tal ocorrendo, o autor do fato causador do dano é o responsável. Com a teoria do risco, diz Philippe Le Tourneau, o juiz não tem de examinar o caráter lícito ou ilícito do ato imputado ao pretenso responsável: as questões de responsabilidade transformam-se em simples problemas objetivos que se reduzem à pesquisa de uma relação de causalidade.

Caitlin Mulholland (2021, p. 15) adota e vem sustentando em artigos doutrinários que a Lei Geral de Proteção de Dados traz no seu corpo legislativo o reconhecimento da responsabilidade civil objetiva baseada no risco, através da leitura sistemática da Lei Geral junto ao Código Civil (artigo 927, § único).

Em outras palavras, considera que a responsabilidade do controlador é uma responsabilidade objetiva baseada na concepção de que o dano ocasionado ao titular de dados será justificado ou pelo tratamento irregular – há uma extensa literatura que considera a semelhante o tratamento irregular com o defeito na prestação de um serviço – ou pela violação da lei.

Como fundamento específico da responsabilidade civil objetiva na Lei Geral de Proteção de Dados, é importante fazer uma digressão e uma análise do programa da Lei Geral de Proteção de Dados, fazendo uma avaliação dos fundamentos principiológicos da Lei Geral que são justamente as bases por meio das quais será possível identificar qual é a mens legis, ou seja, qual foi a intenção do legislador quando ao enumerar uma série de princípios que servirão como cobertor da lei, a intenção do legislador era justamente proporcionar um arcabouço a uma série de direitos, de sanções e de regulamentações específicas sobre a proteção de dados que devem se servir desses princípios para que possam alcançar o objetivo da lei que é justamente proteger o titular de dados.

Ademais, A própria estrutura da Lei Geral de Proteção de Dados é muito semelhante, por exemplo, ao Código de Defesa do Consumidor, principalmente, e ao Marco Civil da Internet também. Faz-se uma menção direta ao CDC justamente em razão de sua estrutura principiológica e os princípios fundamentando todos os demais direitos e regulamentações decorrentes daqueles princípios, que são muito semelhantes. Daí o porquê que, também, pode-se interpretar esses princípios como sendo fundamentais para se identificar a responsabilidade civil na Lei Geral como sendo objetiva.

Segundo Mulhlland (2021, p. 11-12), dos dez princípios expressamente trazidos na LGPD, ressalta-se três que podem ser considerados fundantes da responsabilidade civil por risco, quais sejam: princípio da segurança, o princípio da prevenção e o princípio da responsabilização e da prestação de contas. Esses três princípios trazem toda uma fundamentação que permite ao intérprete considerar que está diante de uma lei que protege o titular de dados e concede a ele um direito a ser indenizado pelos danos sofridos, com base na chamada teoria do risco.

Assim, em que pese ser válida a fundamentação por essa perspectiva sobre a adoção da responsabilidade objetiva baseada no risco, essa conclusão não decorre simples e exclusivamente da análise desses princípios, mas estes ditam o tom do que se espera no tratamento de dados em eventuais danos que sejam ocasionados nesse tratamento, sendo, portanto, de extrema valia para o estudo.

Para instaurar a análise sobre a natureza jurídica da responsabilidade civil que é adotada na Lei Geral de Proteção de Dados, é extremamente necessário prestar atenção, principalmente, em três artigos, quais sejam, artigos 42, 44 e 46 da Lei Geral de Proteção de Dados, sendo que é certo que a parte especifica da responsabilidade civil na LGPD está entre os artigos 42 e 45, e o artigo 46 está fora do capítulo da responsabilidade civil, e trata especificamente de governança de dados, de boas práticas e segurança de dados.

O artigo 42 traz da sua própria leitura três requisitos para que se estabeleça a responsabilidade civil do agente de tratamento de dados, seja controlador, seja operador, que é a existência de um exercício efetivo de uma atividade de tratamento de dados. Observando o primeiro requisito, que é atividade de tratamento de dados, remete-se ao artigo 5º, inciso X, da Lei Geral, em que apresenta vinte possibilidades exemplificativas de exercício de tratamento de dados.

O segundo requisito consiste na comprovação da existência de um dano causado ao titular de dados, que, via de regra, é extrapatrimonial, mas que pode também ter conotação patrimonial (GONDIM, 2021, p. 26-28), seja ele um dano individual seja ele um coletivo, devendo ser resultado do exercício de uma atividade de tratamento de dados - aqui está, portanto, a relação de causalidade. Dessa forma, o dano deve ser decorrência causal do exercício de uma atividade de tratamento de dados.

Quanto ao segundo requisito, são apontadas críticas baseadas na compreensão da identificação da existência de um dano, pois normalmente é associado a existência de um dano à comprovação de um desvalor patrimonial ou um desvalor psíquico. No caso de violação decorrente de dano aos dados, a prova do desvalor patrimonial muito possivelmente será ínfima em algumas hipóteses, por exemplo, quando há incidentes de segurança como os mega vazamentos de dados – para que consiga identificar que se sofreu um dano em decorrência desse incidente de segurança é bem difícil, além de que a prova de sua relação causal fica bastante comprometida (CAITLIN, 2021, p. 17).

Além disso, outra crítica que se estabelece é que o dano moral se caracteriza pela violação de uma situação jurídica subjetiva existencial, qual seja, qualquer situação em que haja a violação de um direito da personalidade ou de um direito fundamental, e no caso, proteção de dados é um direito fundamental, que será reconhecido pela aprovação da Proposta de Emenda Constitucional 17 de 2019, ou já pode ser reconhecido pela interpretação do artigo 5º, incisos V e X que tratam da privacidade. Então, o dano moral estará constituído toda vez que houver a violação de um dado justamente porque terá o dano *in re ipsa*, significando que houve em si só a violação de um direito fundamental.

Nesse sentindo, corrobora Maria Celina Bodin de Moraes (2019, p. 134) que:

> Estando a Constituição no ápice do ordenamento e sendo fundamento axiológico primeiro de todo o sistema, a introdução da cláusula geral de tutela da pessoa humana contida no art. 1º III impõe a proteção da privacidade não somente a partir da ótica proprietária segundo a qual os dados pessoais seriam bens móveis objeto de mera apropriação mas, ao revés, da prevalência do aspecto não patrimonial dos dados pessoais (como atributos indissociáveis à sua dignidade) em face de seu aspecto patrimonial.

O terceiro requisito trazido pelo artigo 42 é a existência da violação da lei. Veja, o artigo 42 em momento algum se refere a um elemento de culpa ou a um elemento do risco. Não é feita qualquer menção ao fator de atribuição, a uma qualificação da conduta do agente de tratamento. Em suma, são utilizados apenas os três critérios: a existência de atividade de tratamento de dados e o dano decorrente do exercício de uma atividade de tratamento de dados justamente pela violação da lei, entendendo-se como lei no sentido do ordenamento jurídico de uma forma geral. Assim, no artigo 42 não há qualquer menção a qualquer fator de atribuição de responsabilidade.

O artigo 43, por sua vez, seria o artigo que pode ser comparado ao artigo 12 e artigo 14, § 3º, do Código de Defesa do Consumidor, ao passo que de forma semelhante, traz as hipóteses de excludente de responsabilidade, utilizando a seguinte locução: os agentes de tratamento só não serão responsabilizados quando provarem.

Por sua vez, o artigo 44 traz o tema do tratamento irregular. Enquanto o artigo 42 da Lei Geral fala sobre o dano causado no exercício de tratamento de dados pela violação da lei, o artigo 44 inova ao trazer a qualificação de tratamento como sendo um tratamento irregular, aquele, portanto, que geraria a responsabilidade.

Os critérios do artigo 44 seriam a existência da violação da lei ou quando houver uma legítima expectativa do titular dos dados em relação a segurança daquele tratamento (ou do uso daqueles dados dentro daquela determinada base de dados), o que de certa forma se assemelha a maneira como o legislador se referiu no artigo 12, § 1º, do Código de Defesa do Consumidor ao conceito de defeito. De um lado tem-se que o produto será defeituoso quando não atender a legítima expectativa de segurança do consumidor, e de outro que o tratamento será irregular – o tratamento será “defeituoso” – quando violar a lei ou quando violar a legitima expectativa de segurança esperada pelo titular de dados.

O artigo 44 provoca um desarranjo, posto que, enquanto a leitura do artigo 42 por si só levaria a uma conclusão que a Lei Geral, apesar de não ter usado a locução “independentemente de culpa” – uma expressão que remete a uma responsabilidade objetiva baseada no risco –, o artigo 44 inverte a ordem quando estabelece o conceito de tratamento irregular como sendo aquele que viola a segurança, quando o agente de tratamento de dados deixa de adotar determinada

medidas de segurança, que é o que está previsto no artigo 46. Assim, observa-se a grande confusão que há na Lei Geral de Proteção de Dados.

Por outro lado, tem-se posicionamentos que não vislumbram a atividade de tratamento de dados como gerador de risco por si só, devendo se realizar uma avaliação casuística garantindo um olhar mais cuidadoso aos dados sensíveis, haja vista que, por exemplo, no caso de dados sensíveis tratados em um contexto de inteligência artificial e big data, representam um risco não só para o titular de dados, mas para toda a humanidade, já que tais informações carregam consigo demasiado potencial lesivo ao titulares quando utilizados com finalidade discriminatória, como já pode ser observado em tecnologias de reconhecimento facial.

Valendo-se sobre a menção sobre a representação de risco pelo tratamento dos dados bem como sobre as tecnologias de reconhecimento facial, é importante destacar o episódio ocorrido em São Paulo, em que a concessionária responsável pela linha 4 do metrô na Capital do Estado de São Paulo, ViaQuatro, instalou nas plataformas de embarque e desembarque painéis que exibiam publicidade e capitavam a imagem de seus usuários por uma câmera neles instaladas sem o devido consentimento realizando a contabilização de quantas pessoas passavam em frente à tela e, ainda, faziam o reconhecimento facial.

O Instituto Brasileiro de Defesa do Consumidor (IDEC), com auxílio técnico o Programa de Educação Tutorial da Universidade de São Paulo e a Rede Latino-Americana de Estudos de Vigilância (LAVITS), ajuizou ação civil pública[5] em face da concessionária requerendo a retirada imediata das câmeras instaladas nos painéis, haja vista que estas possuíam tecnologia capaz de realizar uma análise sobre gênero, faixa etária e a identificação das emoções esboçadas pelos passageiros que ali passavam, sendo considerada pelo autor ilegal tal prática, pois operaria como uma forma de uma pesquisa opinião forçada sem que o titular dos dados saiba.

[5] Processo nº 1090663-42.2018.8.26.0100. Em primeira instância, a 37ª Vara Cível de São Paulo, em maio de 2021, condenou a concessionária ViaQuatro ao pagamento de dano morais coletivos no valor de R$ 100,00 (cem mil reais) em virtude da utilização de equipamentos gravação de imagens dos usuários para fins publicitários e estatísticos nas estações que estavam sob sua administração, sem a comprovação, pela requerida, de que os equipamentos não armazenavam dados pessoais dos usuários da plataforma, que não realizavam gravação ou filmagem dos usuários, bem como o efetivo emprego do material obtido. Com a interposição de recurso de apelação pela Defensoria Pública do Estado de São Paulo pleiteando a reforma da decisão para condenar a requerida em danos morais individuais e determinar a majoração dos danos morais coletivos O processo se encontra, atualmente, tramitando em segunda instância (verificado no dia 02 de outubro de 2021).

Além disso, não teria ficado comprovado que os aparelhos não utilizariam as tecnologias instaladas nas estações para outras finalidades que não foram divulgadas publicamente nem que os dados biométricos dos usuários seriam armazenados e utilizados posteriormente, sendo o referido incidente um caso marcante no âmbito jurídico de tratamento e proteção de dados pessoais no Brasil.

Como já abordado, o artigo 43 da Lei Geral de Proteção de Dados estabelece as hipóteses de exclusão de responsabilidade civil, sustentando através da dicção de que os agentes de tratamento de dados somente não responderão se não realizaram o tratamento que lhes fora imputado, ou, embora realizado, cumpriram o que a lei estabelece, ou se o dano decorrer de atividade exclusiva do titular de dados ou de terceiros.

Analisando as excludentes contidas no artigo 43, chega-se à conclusão de que se aproximam demasiadamente com as excludentes previstas no parágrafo terceiro, do artigo doze do Código de Defesa do Consumidor. Por isso, ficaria clara a natureza jurídica da responsabilização objetiva na LGPD, pois, se fosse adotada a modalidade subjetiva de responsabilização, não haveria necessidade de se ter esse rol taxativo de excludentes, bastaria demonstrar que não houve culpa.

Ademais, levando-se em consideração a estruturação da Lei Geral sobre as diretrizes dos princípios da responsabilização e prestação de contas (*accountability*), que impõe que os controladores e operadores demonstrem que adotaram todas as medidas estabelecidas em lei, bem como a coerente posição do legislador em trazer a possibilidade do ônus da prova no parágrafo segundo, do artigo 42, desponta nova oportunidade para se mencionar a similitude de tratamento do conteúdo entre esta legislação com o Código de Defesa do Consumidor, mais especificamente em seu inciso oitavo do artigo sexto.

Certa é a posição majoritária dos consumeristas no sentido de que não se pode confundir inversão do ônus da prova, que é um instituto processual, com responsabilidade civil, que é um instituto de direito material. E além disso, a inversão do ônus da prova é uma possibilidade mediante a verificação de alguns requisitos que a lei traz – verossimilhança das alegações, a hipossuficiência, no CDC, do consumidor e, na LGPD, do titular de dados.

Isto posto, no entanto, não se mantém a tese de que com apenas a análise da inversão do ônus da prova seja o fundamento para determinação da natureza jurídica da responsabilidade civil.

Parte-se, portanto, para análise da possibilidade de se considerar as relações de tratamentos de dados como relações de consumo. Nesse sentindo, relevante se faz o entendimento do STJ expresso no julgamento do Resp. 1156616/MG:

> RISCO INERENTE AO NEGÓCIO. INEXISTÊNCIA. CIÊNCIA DA EXISTÊNCIA DE CONTEÚDO ILÍCITO. RETIRADA IMEDIATA DO AR. DEVER. DISPONIBILIZAÇÃO DE MEIOS PARA IDENTIFICAÇÃO DE CADA USUÁRIO. DEVER. REGISTRO DO NÚMERO DE IP. SUFICIÊNCIA.
> 1. A exploração comercial da internet sujeita as relações de consumo daí advindas à Lei n. 8.078/90.
> 2. O fato de o serviço prestado pelo provedor de serviço de internet ser gratuito não desvirtua a relação de consumo, pois o termo "mediante remuneração", contido no art. 3º, § 2º, do CDC, deve ser interpretado de forma ampla, de modo a incluir o ganho indireto do fornecedor.
> 3. A fiscalização prévia, pelo provedor de conteúdo, do teor das informações postadas na web por cada usuário não é atividade intrínseca ao serviço prestado, de modo que não se pode reputar defeituoso, nos termos do art. 14 do CDC, o site que não examina e filtra os dados e imagens nele inseridos.
> 4. O dano moral decorrente de mensagens com conteúdo ofensivo inseridas no site pelo usuário não constitui risco inerente à atividade dos provedores de conteúdo, de modo que não se lhes aplica a responsabilidade objetiva prevista no art. 927, parágrafo único, do CC/02.
> 5. Ao ser comunicado de que determinado texto ou imagem possui conteúdo ilícito, deve o provedor agir de forma enérgica, retirando o material do ar imediatamente, sob pena de responder solidariamente com o autor direto do dano, em virtude da omissão praticada.
> 6. Ao oferecer um serviço por meio do qual se possibilita que os usuários externem livremente sua opinião, deve o provedor de conteúdo ter o cuidado de propiciar meios para que se possa identificar cada um desses usuários, coibindo o anonimato e atribuindo a cada manifestação uma autoria certa e determinada. Sob a ótica da diligência média que se espera do provedor, deve este adotar as providências que, conforme as circunstâncias específicas de cada caso, estiverem ao seu alcance para a individualização dos usuários do site, sob pena de responsabilização subjetiva por culpa in omittendo.
> 7. Ainda que não exija os dados pessoais dos seus usuários, o provedor de conteúdo que registra o número de protocolo (IP) na internet dos computadores utilizados para o cadastramento de cada conta mantém um meio razoavelmente eficiente de rastreamento dos seus usuários, medida de segurança que corresponde à diligência média esperada dessa modalidade de provedor de serviço de internet.
> 8. Recurso especial provido.
> (REsp. 1186616/MG, Rel. Ministra NANCY ANDRIGHI, TERCEIRA TURMA, julgado em 23/08/2011, DJe 31/08/2011)

Tomando-se como base o supramencionado entendimento, infere-se que não há risco inerente às atividades desempenhadas pelos provedores de aplicação de internet, bem como que as relações de consumo incorporadas em um contexto de exploração comercial da Internet, em que há a comprovação de

remuneração – e bastando ser remuneração indireta que vem por meio da publicidade – se do outro lado demonstrar que o titular de dados se encaixa na figura do consumidor (destinatário final ou figuras equiparadas – como a coletividade, as vítimas dos acidentes de consumo e também as pessoas expostas as práticas comerciais), são regulamentadas pela lei nº. 8.078/90, Código de Defesa do Consumidor.

Assim, de forma análoga, pode-se entender que, demonstrando-se que um titular de dados pessoais se encaixa nessas categorias, seja o consumidor *standart*, seja as figuras equiparadas, de um outro lado tem-se o fornecedor, e portanto, seria regulamentada pelo CDC. À atividade de tratamento de dados é muito comum que se desenvolva ou numa atividade empresarial típica, a exemplo da mera atividade de realização de exames laboratoriais, precede-se a coleta de dados, inclusive sensíveis, sendo, portanto, um caso típico de uma relação de consumo.

Mas além disso, assim podem ser consideradas também a utilização de cookies e outras informações pessoais, das redes sociais, por exemplo, que são utilizadas com uma aparente gratuidade, mas que se obtém a remuneração pela publicidade.

Caso venha a ser demonstrado em uma relação jurídica esses pressupostos subjetivos e objetivos da relação jurídica de consumo, não há dúvidas de que se deve aplicar o Código de Defesa do Consumidor, e, com ele, a responsabilidade é objetiva.

O STF discute a inconstitucionalidade do artigo 19 do Marco Civil da Internet que estabeleceu um regime jurídico de responsabilização dos provedores de aplicação diverso do que estabelece o Código de Defesa do Consumidor. Então, para evitar esse intenso ativismo judicial que pode gerar um ambiente de insegurança e incertezas, o ideal seria que a lei tivesse sido clara.

Os juristas que apoiam a concepção de que a Lei Geral de Proteção de Dados emprega a responsabilidade civil subjetiva respaldam-se no fundamento de que, embora haja similitude entre a abordagem da responsabilidade civil na LGPD com o CDC, esta pode ter ocorrido devido a uma frustrada tentativa do legislador adotar a responsabilidade civil objetiva, havendo diferenças fundamentais entre as duas legislações.

3.2 Da Responsabilidade Civil Subjetiva dos Agentes de Tratamento de Dados

Entende-se que, se analisar a LGPD do primeiro ao último artigo, é simples perceber que ela impôs, não só para o controlador, mas para o operador dos dados também uma série de deveres, e, diante disso, não haveria congruência entre a instituição de vários encargos aos controladores e operadores de dados sendo que mesmo os cumprindo ainda assim serão responsabilizados.

Ao comparar o artigo 42 da LGPD com o artigo 12 e 14 do CDC, consegue-se notar que uma das diferenças fundamentais entre a LGPD e o CDC é que tanto no artigo 12 quanto no artigo 14 há expressão adoção da responsabilidade objetiva, fazendo uso da expressão “independentemente de culpa”.

Em contrapartida, diferentemente do artigo 14 do Código de Defesa do Consumidor, o artigo 42 da Lei Geral não deixa claro a adoção de que modalidade de responsabilidade que adota, apenas menciona que “o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo”, sem qualquer alusão direta à responsabilidade objetiva.

No Código Civil a responsabilidade civil objetiva não está só prevista por meio de uma cláusula geral, mas também espalhada em diversos outros dispositivos do código, e observa-se que em todos eles há expressa definição da natureza objetiva da responsabilidade, não só pelo uso da expressão independentemente de culpa, como também da expressão “salvo motivo de força maior, como ocorre no artigo 734 do código em que se aborda a responsabilidade do transportador.

Além do mais, a lógica da responsabilidade objetiva não se adequaria a uma imposição de deveres, e a concretização da responsabilidade objetiva independe da violação de qualquer dever jurídico. Segundo Maria Celina Bodin de Moraes (2006, p. 28), a responsabilidade objetiva “[...] independe completamente de negligência, imprudência, imperícia ou mesmo da violação de qualquer dever jurídico por parte do agente. São danos (injustos) causados por atos ilícitos, mas que, segundo o legislador, devem ser indenizados”. Dessa forma, surgiria, então, o questionamento sobre o porquê o legislador imporia múltiplos deveres para posteriormente pronunciar que a responsabilidade é objetiva.

Também se apoia a concepção de que há alguns indícios na legislação de que existe de fato uma opção por uma responsabilidade civil de natureza subjetiva. A cláusula específica sobre tratamento de dados na Lei Geral, artigo 42, diz que os agentes de tratamento que, em razão do exercício da atividade de tratamento de dados pessoais, causarem dano em violação à legislação de proteção de dados, são obrigados à repará-lo. Veja-se que há um primeiro elemento que traz um indício de qualificação da conduta do agente, qual seja, violação da legislação de proteção de dados.

Isso aparece novamente quando o artigo 42, parágrafo primeiro, inciso primeiro, aborda sobre a responsabilização do operador, que é aquele que atua sob comando do controlador, na seguinte dicção:

> 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;

Partindo-se da análise do trecho destacado “quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador**”,** que se vislumbra como mais um indício de que o legislador reconhecendo a necessidade de equilíbrio virtuoso entre a lei que tutela direitos fundamentais, mas que ao mesmo tempo tem normas de indução econômica, optou por uma qualificação da conduta do agente, nesse caso o operador, trazendo de volta a ideia de uma responsabilidade subjetiva.

Deve-se admitir, da mesma forma, que o artigo 43 da Lei Geral é muito parecido com o parágrafo terceiro do artigo 12 do Código de Defesa do Consumidor. No entanto, quando se analisa, principalmente, os incisos primeiro e terceiro das duas codificações, entende-se que se relacionam com o nexo de causalidade, e como este é um elemento presente em qualquer espécie de responsabilidade civil não trariam qualquer embasamento para a definição da natureza da responsabilidade.

Em contrapartida, compreende-se que o referente artigo que traz a dicção de quando os agentes de tratamentos provarem que não realizaram o tratamento, ou que realizaram o tratamento, mas que não houve violação à legislação, ou que houve culpa exclusiva do titular e de terceiro seriam elementos que exonerariam a responsabilidade do agente ainda que tenha havido dano.

Segundo Maria Celina Bodin de Moares (2019, p. 4), esse artigo mostra-se especialíssimo ao passo que:

> configurando-se como a principal novidade da lei, e reflete a determinação do disposto no inciso X do art. 60 da Lei, que prevê o princípio da "responsabilização e prestação de contas, isto é, a demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas'.

O aspecto de diferenciação localizar-se-ia no inciso dois, pois, enquanto o CDC declara que o fabricante, construtor e o produtor não será responsabilizado quando provar que, embora tenha colocado o produto no mercado, o defeito inexiste, estaria relacionado ao nexo de causalidade, o inciso dois da LGPD não teria relação com nexo de causalidade, mas sim com a análise do elemento subjetivo da responsabilidade, a culpa.

No artigo 44 compreende-se as circunstâncias em que se há tratamento irregular, apontando que é tratamento irregular quando se deixar que observar a legislação ou não fornecer a segurança que se espera.

Dessa forma, existiria, portanto, a necessidade de demonstração da violação da legislação ou a falha da segurança, sendo, novamente, dois qualificadores da conduta – dentro do trinômio conduta, dano, nexo causal – que precisariam ser demonstrados, até porque, quando se fala em tratamento de dados pessoais, há uma grande massa de dados que não estão em uma relação de consumo e que não representam per se uma atividade de risco.

Voltando-se os olhos para o parágrafo único do artigo 44 da Lei Geral, Gisela vislumbra uma menção indireta à culpa, pois entende que se o controlador e o operador adotarem as medidas de segurança impostas pelo legislador e mesmo assim gerar um dano, eles não responderão pela lesão.

O artigo 46 declara que os agentes devem adotar medidas de segurança técnica e administrativas aptas a proteger os dados pessoais, ou seja, fala de medidas aptas a garantir a segurança dos dados.

Ainda que se pense em termos de segurança, o problema da segurança que ensejou uma alteração, uma comunicação, uma destruição, uma perda, um vazamento de dado ou um tratamento ilícito, poderia se pensar no instituto da responsabilidade civil objetiva imprópria, fazendo uma analogia presume-se a culpa

do motorista que bate o carro atrás do outro, mas se esse motorista vier a provar que houve um engavetamento, ele certamente deve ser exonerado dessa culpa.

Assim, parece que mesmo que a organização ofereça as melhores técnicas no contexto do tratamento, com as melhores atualizações possíveis e ainda assim um grupo de hackers superespecializados consegue invadir o banco de dados, por exemplo, parece que será objeto de discussão para analisar se de fato houve um descumprimento da lei.

Destarte, segue-se para a apreciação das atribuições de responsabilização: se ela é solidária ou se é subsidiária. Ao que tudo indica, a tendência é pela cláusula geral de responsabilidade solidária, o que teria acertado o legislador ao passo que a especialidade da cadeia de tratamento é muito complexa para o titular dos dados, não fazendo sentindo o titular tentar identificar no emaranhado contratual quem de fato cometeu o ilícito e descumpriu a lei. Dessa forma, o titular dos dados lesado deve reclamar contra algum agente em específico, ou contra todos, e, a própria lei no artigo 42, parágrafo quarto, garante direito de regresso àquele operador ou controlador que entendeu que não tinha culpa e mesmo assim for responsabilizado e precisou arcar com os custos indenizatórios.

Deste modo, na Lei Geral, basicamente tem se uma cláusula geral de responsabilização por ilícitos de proteção de dados dentro da natureza subjetiva e solidária, resguardadas as relações de consumo, o que nesses casos há a cláusula específica da relação de consumo.

Conclui-se isso, pois, ao analisar a Lei Geral de Proteção de Dados busca-se sopesar seus princípios informadores e *intra legem,* tendo como macro princípio a responsabilidade, transparência e prestação de contas. Não faria sentido a lei estabelecer a responsabilidade subjetiva sendo que ela é uma lei procedimental. Traria um grande desincentivo à cadeia de tratamento em empregar as melhores práticas, em ter uma governança e uma arquitetura de dados de primeira linha com pessoas capacitadas se no final a responsabilidade é objetiva. Seria uma norma com um desincentivo econômico à proteção dos direitos fundamentais do titular, pois todos os titulares saberiam que não haveria necessidade de apontar o ilícito – houve ou não consentimento, relatório de impacto com fundamento legal no legítimo interesse foi ou não feito. O titular do dado simplesmente apontaria eventual dano e então seria ressarcido.

4 OS PRINCÍPIOS NA LGPD E A AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

Há muito tempo já se comentam sobre a maior inserção da tecnologia no dia a dia dos indivíduos, suas implicações e os reflexos no mundo jurídico. No entanto, com a crise gerada pela pandemia do COVID-19, que impôs o isolamento social e a utilização da tecnologia como alternativa para a manutenção das relações interpessoais, estudos e trabalhos, houve um aprofundamento da relação entre as pessoas e a tecnologia, e uma brutal imersão no mundo digital.

Em que pese as mídias digitais serem uma grande ferramenta que possibilitou a manutenção da maioria das atividades humanas no período de isolamento social, a maior utilização desses meios digitais acarreta, direta ou indiretamente, na exposição de dados do usuário a essas mídias digitais, que os utilizam como bem entendem.

Nota-se que há um enorme interesse dessas grandes mídias digitais em se obter dados sobre seus usuários para que consigam direcionar produtos, notícias, publicidades em geral de empresas patrocinadoras para aqueles usuários considerados mais aptos a consumir os produtos desta, tendo em vista o perfil traçado com base na sua atividade e dados proporcionados às mídias digitais.

Verificando-se a crescente importância dos dados no mercado, surge a necessidade de se examinar até que ponto é razoável a manipulação dos dados dos usuários para estratégias de marketing e de modelo de negócio sob o ponto de vista jurídico, e até que ponto essa manipulação poderia cercear a liberdade de escolha dos usuários ao serem direcionados determinados produtos, anúncios e notícias em detrimento de outros e até mesmo ferir a sua privacidade.

Todo esse avanço tecnológico fez com que fosse visto como uma exigência a implementação – e em alguns cenários o aprimoramento – de uma regulamentação sobre o assunto, não apenas visando proteger a intimidade e privacidade dos titulares de dados, mas também para estipular balizas de regramento para a manipulação dos dados pessoais para realização de um tratamento transparente e sem causar qualquer infortúnio ao utilizar informações para finalidades econômicas, posto que a informação se tornou um produto extremamente cobiçado nos mercado.

A União Europeia contava desde 1995 com a Diretiva nº 95/46/CE do Parlamento Europeu e do Conselho da União Europeia que tratava acerca da proteção de dados pessoais. No entanto, houve a necessidade amoldar seu regramento às demandas que surgiram, apontando assim a *General Data Protection Regulation* (GDPR).

O Brasil, por sua vez, não possuía uma legislação individual que tratasse de forma sistematizada a proteção de dados. A tutela consagrada à essa demanda era encontrada em legislações esparsas sem uma sistematização bem definida e estruturada.

Essa omissão foi suprida, quando em 2018 a Lei nº 13.709 foi aprovada Lei Geral de Proteção de Dados (LGPD), legislação genuinamente inspirada no modelo europeu, que proporcionou um respeitável rol de regramento para a proteção de dados pessoais, possuindo diretrizes que guiarão o tratamento de dados, além de prever a Autoridade Nacional de Proteção de Dados, que tem como objetivo dar efetividade à legislação.

Assim, a partir de análises histórica, comparativa, doutrinária e jurisprudência, devolverá essa construção cientifica buscando elucidar as indagações supramencionadas, destrinchando a Lei Geral de Proteção de Dados.

4.1 Dos Princípios

Os ordenamentos jurídicos contemporâneos, em particular o brasileiro com o advento da Magna Carta de 1988, caracterizam-se por conter, entre outros atributos, a existência de princípios e cláusulas gerais que, conforme Miguel Reale (1986, p. 60) podem ser conceituados por:

> [...] verdades ou juízos fundamentais, que servem de alicerce ou de garantia de certeza a um conjunto de juízos, ordenados em um sistema de conceitos relativos à dada porção da realidade. Às vezes também se denominam princípios certas proposições, que apesar de não serem evidentes ou resultantes de evidências, são assumidas como fundantes da validez de um sistema particular de conhecimentos, como seus pressupostos necessários

Nesse sentido, a Lei Geral de Proteção de Dados (LGPD) é elaborada trazendo expressamente em seu artigo 6º um rol de princípios que deverão nortear a atividade de tratamento dos dados pessoais, sem prejuízo do emprego de outros

princípios relacionados ao assunto, conforme é assertivamente declarado no artigo 64 da legislação em análise.

O primeiro princípio constatado é o princípio da boa-fé, contemplado logo no caput do artigo 6º da LGPD. Conforme é pacificamente entendido pelos juristas, há duas vertentes da boa-fé no ordenamento jurídico: a subjetiva e a objetiva.

Na primeira vertente, o entendimento que se deve ter é o de antônimo de má-fé, sendo relacionada, portanto, com a intenção do sujeito de direito. A imprescindibilidade de obediência à boa-fé em seu aspecto subjetivo verifica-se ao longo de toda a Lei Geral, no entanto, encontra previsão expressa em seu artigo 52, parágrafo primeiro, inciso II, LGPD. Já a segunda vertente, relaciona-se com a conduta do sujeito, concebendo um padrão comportamental baseado na probidade e fidelidade de atitude (MARTINS-COSTA, 2018, p. 43-44).

Segundo leciona Silvano Flumignan e Wévertton Flumignan (2020, p. 127), em capítulo da obra Comentários à Lei Geral de Proteção de Dados, ao estudar o caput do artigo 6º da LGPD deve-se entender que o aspecto da boa-fé ali utilizado é a objetiva, haja vista que, de forma análoga ao tratamento da boa-fé objetiva como cláusula geral dos contratos no Código Civil de 2002, é justo que, no meio virtual em que a maioria das relações são estabelecidas através de contratos por adesão entre usuários e provedores de internet, o comportamento almejado seja de lealdade e confiança entre os sujeitos, resguardando, assim, os direitos dos usuários (LEITE, 2020, p. 127).

Esse aspecto proporciona a análise de que a relação entre usuários e provedores de internet deve ser nutrida pela confiança a fim de realizar o propósito maior que é proporcionar segurança ao usuário, haja vista que se está diante de um cenário de uma relação que, via de regra, protrai-se no tempo, e que o consentimento inicial dado pelo usuário pode não mais corresponder com futuro contexto em que estará envolvido os fluxos informacionais.

Assim, em se tratando de uma relação passível de muitas mudanças, já que é um vínculo em constante modificação a julgar pela evolução tecnológica e as mudanças sociais, o consentimento expresso de todos os termos contratuais se torna inviável ao passo que se vislumbra o desdobramento contratual de tratamento dos dados nos meios digitais. Assim, é necessário que haja a compatibilidade entre o tratamento dos dados pessoais frente a anuência do usuário, possibilitando certa

manutenção da autodeterminação informacional do usuário sobre os desígnios em relação aos seus dados pessoais.

Como bem pontua Bruno Bioni (2019, p. 320), essa relação baseia-se na:

> [...] fidelidade depositada pelo emissor de uma informação ao(s) seu(s) recipiente(s), na legítima expectativa de que seus dados pessoais serão usados e compartilhados de acordo com o contexto de uma relação preestabelecida ou a razão pela qual foi publicizado um dado; particularmente, na esperança de que o trânsito das suas informações pessoais não minará e trairá a sua capacidade de livre desenvolvimento da personalidade e de participação social.

Dado isso, surge o fundamento da LGPD que se ampara no respeito à autodeterminação informativa, que é um conceito que teve origem na jurisprudência do Tribunal Constitucional Federal da Alemanha (PEREIRA, 2015, p. 27-30), que tem uma nova roupagem ao trazer no contexto da Lei Geral a ideia de dar ao titular dos dados pessoais o controle do fluxo dos seus dados. A LGPD concretiza esse direito quando cria os próprios direitos dos titulares, como o de ter conhecimento de quais dados são coletados, para quem e para que estão coletando seus dados, bem como a possibilidade de poder controlar e interferir nesse fluxo.

Esses direitos também são resguardados pelo princípio do livre acesso e da transparência, ao passo que esse garante que, aos titulares, deverão ser transmitidas informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, resguardando os segredos comercial e industrial, e aquele garante a exigência de acesso eficaz e gratuito às informações sobre forma, duração do tratamento e integridade dos dados.

Isto posto, destrincha-se a percepção de que não pode ser compartilhado dados a terceiros de forma a se ocultar do titular tal fluxo. Aos titulares deve ser informado se há repasse de seus dados a terceiro, ainda que esse seja operador fundamental à efetivação da atividade.

Outro princípio trazido expressamente na LGPD é o da finalidade. Esse princípio deve ser vislumbrado como decorrência da boa-fé objetiva, pois se espera um manejo dos dados pelos agentes de tratamento compatível com o informado ao titular, de modo que o tratamento dos dados pessoais não seja realizado ao bel prazer de quem os controle. A partir disso, então, surge o entendimento de que qualquer modificação de diretriz acerca dos dados abrangidos e do objetivo do tratamento

deverá ser notificado ao titular para ter ciência da nova diretriz bem como para concordar ou não com a disponibilização de seus dados para a nova finalidade de tratamento.

Precisos exemplos são dados por Silvano Flumignan e Wévertton Flumignan no qual menciona que um usuário que consinta a um aplicativo de transporte armazenar seus dados não poderá ter alterado a forma de tratamento de seus dados sem antes a empresa lhe dar oportunidade para apresentar seu legítimo e prévio consentimento, ou que uma startup que utiliza o e-mail do cliente unicamente para acesso à plataforma online não poderá instantaneamente usar esse e-mail para enviar ofertas e propaganda.

Além do mais, o princípio da finalidade está estreitamente relacionado com o princípio da adequação, necessidade e transparência, os dois primeiros abordados mais a frente, ao passo que determina que o tratamento dos dados deve ser realizado para “propósitos legítimos, específicos, explícitos e informados ao titular, sem a possibilidade de tratamento posterior de forma incompatível com essas finalidades” (Art. 6º, I, LGPD).

Desta feita, é oportuno elucidar que o princípio da adequação possui como escopo a “compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto de trabalho” (Art. 6º, II, LGPD). Ora, a partir desse preceito, não é concebível que uma empresa de transporte queira ter acesso aos dados sobre saúde de seus usuários, por exemplo, pois não há uma justificativa verossímil para tal interesse.

Além disso, tem-se que o princípio da necessidade fundamenta a apreensão de que o tratamento deve se limitar ao mínimo necessário para que se consiga atingir suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados. (LGPD, art. 6, III)

Há que se observar que tal princípio traz a reflexão de que se proporciona a garantia ao controlador no sentido de que quanto menos se coleta dados, menos risco se corre de vazamentos e de violação dos dados dos usuários.

O princípio da segurança instaura que o tratamento de dados deve se utilizar de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão (art. 6, VII, LGPD).

Esse princípio juntamente com o princípio da prevenção, que visa adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais (art. 6º, VIII, LGPD), instituem que o tratamento de dados deve ser realizado com o emprego de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos de terceiros, tal como o que ocorre em um ataque de hackers.

Assim, atua-se de forma preventiva inclusive, pois, ao passo que se adota medidas de proteção eficazes, busca-se evitar um incidente de qualquer tipo de prejuízo por efeito do tratamento, não concebendo a ideia de que se proporcione ao responsável pelo tratamento que se tome qualquer iniciativa somente depois de já instaurado o imbróglio – tutela ressarcitória (comentários à LGPD, p. 133).

A importância de uma atitude precavida e, portanto, antes de eventual dano, adotada pelos responsáveis pelo tratamento dos dados pessoais assume particular importância em razão de se tratar de meios digitais que tem a capacidade de propagação de informações em altíssima velocidade e abrangência, tornando-se extremamente difícil voltar ao *status quo ante* uma vez que há algum vazamento de dado (FLUMIGNAN , 2018, p. 35).

As medidas de segurança, técnicas e administrativas capaz de proteger os dados pessoais de acessos não permitidos e de eventos acidentais ou ilícitos de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, devem ser adotadas pelos agentes de tratamento, conforme expressamente é indicado no artigo 46 da LGPD, devendo manter essas informações em segurança mesmo após o término do tratamento.

Em caso de qualquer incidente de segurança que tenha capacidade de provocar risco ou lesão grave aos titulares, o controlador deverá informar à autoridade nacional e ao titular dos dados.

Outro princípio com extrema pertinência é o da não discriminação, em que se revela a diligência do legislador ao demonstrar o desígnio de tolher qualquer utilização de dados para tratamento com fito a discriminação ilícita ou abusiva, consonante aos preceitos contidos na Constituição Federal de 1988, notadamente a tutela do princípio da isonomia.

Em que pese a abrangência desse princípio ao tratamento de todos os dados pessoais, a LGPD trouxe regras exclusivas quanto ao tratamento dos dados pessoais sensíveis.

Tendo em vista que o conteúdo desses dados são relativos à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico (Art. 5º, II, LGPD), de uma pessoa natural, portanto, dados que compreendem uma especial vulnerabilidade em razão de seu conteúdo, podem ser utilizados de forma mais discriminatória, tornando-se, portanto, uma obrigação salvaguardá-los não apenas em virtude do direito à privacidade, com também em razão aos preceitos da liberdade, igualdade e, principalmente, da dignidade da pessoa humana.

Pode-se citar como de desrespeito ao princípio da não discriminação onde banco ou financeira, por exemplo, desrespeitam os limites legais de utilização do sistema “credit scoring”, que é uma prática comercial lícita de avaliação de risco de concessão de crédito, utilizando informações excessivas, sensíveis, ou nos casos de recusa de crédito pelo uso de dados incorretos ou desatualizados.[6]

O último princípio expresso na LGPD é o da responsabilização e prestação de contas, previsto no inciso X, do artigo 6º, da LGPD. A partir desse princípio, desponta o dever do agente de demonstrar que se adotou medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais ao longo do tratamento, demonstrando também a eficácia de cada medida (art. 6, X, LGPD).

Esse princípio estabelece que, além de corresponder completamente a LGPD, os agentes que manuseiam os dados pessoais para a realização de seu tratamento devem comprovar todas as medidas adotadas a fim de atestar sua boa-fé e diligência.

É com fulcro nesse princípio que a Autoridade Nacional de Proteção adquire especial magnitude, pois se trata do órgão da administração pública responsável exatamente por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território brasileiro, nos termos do seu inciso XIX, artigo 5º.

Posto isto, é relevante analisar tal figura em apartado.

---

[6] Veja-se o sistema de credit scoring que foi analisado pelo STJ (Recurso Especial n. 1.419.697 – Relator Paulo de Tarso Sanseverino).

4.2 Da Autoridade Nacional de Proteção de Dados

A Autoridade Nacional de Proteção de Dados é composta pelo Conselho Diretor, Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, Corregedoria, Ouvidoria, órgão de assessoramento jurídico próprio e unidades administrativas e unidades especializadas necessárias à aplicação do disposto nesta Lei.

A princípio, no anteprojeto nº 5.276/16 do poder executivo não fora previsto expressamente a figura da Autoridade Nacional de Proteção de Dados sequer fora regulamentada como se estruturaria, embora mencionado no item nº 16 da exposição de motivos da esplanada lei a concepção de um órgão competente para a proteção de dados e sua relevância para a efetivação da lei.

> Com o objetivo de dar efetividade à regulamentação sugerida, a proposta prevê um órgão competente para a proteção de dados pessoais no país. Será sua responsabilidade elaborar diretrizes de uma Política Nacional de Proteção de Dados Pessoais e Privacidade, promover entre a população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais, bem como das medidas de segurança, estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, entre outras medidas (BRASIL, 2016).

O Projeto de Lei nº 4.060, de 2012, de iniciativa do Deputado Milton Monti, que ensejou na Lei Geral de Proteção de Dados (LGPD) previa em seu Título II (artigos 21 a 23) regras para fiscalização em que determinava a autorregulamentação estruturada a partir de “Conselhos de Autorregulamentação” instaurados pelas entidades representativas dos responsáveis pelo tratamento de dados pessoais, de forma semelhante ao Conselho Nacional de Autorregulamentação de Publicitária – CONAR.

Algumas críticas foram feitas a esse modelo de autorregulação:

> o CONAR mesmo não fazendo parte da administração pública direta ou indireta – por isso não tem seus poderes e atribuições definidas em lei –, recebe denúncias de consumidores, de autoridades e de associados sobre violação do Código e aplica sanção administrativa, porém sem coerção legal. Não nos parece adequado esse modelo de sistema fiscalizador e sancionatório quanto à proteção dos dados pessoais, por diversas razões. Primeira: a descentralização não seria conveniente em um setor tão sensível, como o da proteção de dados pessoais, pois fomentaria incertezas e insegurança no que diz respeito às regras e padrões técnicos exigidos, pois caberia ao Judiciário definir essas questões com todas as prerrogativas e garantias que a lei lhe assegura. Portanto, o livre convencimento motivado do

> juiz viabilizaria situações nas quais cada juiz poderia decidir diferentemente um do outro, o que iria criar insegurança quanto às regras de tratamento de dados pessoais. Por exemplo, cada juiz poderia compreender de maneira diversa a anonimização... Para evitar essas situações indesejáveis, a LGPD centralizou na ANPD a atribuição de editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade (art. 55-J, inc. XIII da LGPD) e de editar normas, orientações e procedimentos simplificados e diferenciados (art. 55-J, inc. XVIII da LGPD); dessa forma, é possível conhecer e se adequar a priori a essas regras. Segunda razão: o próprio CONAR não tem poder de polícia, o que pode tornar esse sistema pouco eficaz na medida em que os titulares dos dados pessoais, para exercerem seus direitos, deveriam recorrer necessária e exclusivamente ao Poder Judiciário, o que demandaria tempo e dinheiro, sendo, tampouco, conveniente ao Judiciário, que já está assoberbado pela quantidade das demandas. Se considerarmos o volume de dados na sociedade informacional, esses números aumentariam exponencialmente, podendo até mesmo inviabilizar a eficiência do provimento jurisdicional. Por isso, deve-se conceder à ANPD poder de polícia, pois entre suas atribuições estão: fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação (art. 55-J, inc. IV da LGPD); apreciar petições de titular contra controlador após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação (art. 55-J, inc. V da LGPD). Terceira razão: deve-se prestigiar a independência e autonomia da ANPD; por isso, não seria confiável um sistema no qual o ente que fiscaliza é composto por representantes dos fiscalizados, ou seja, os próprios controladores. Daí ser muito interessante a composição multissetorial do Conselho Nacional de Proteção de Dados e Privacidade, haja vista o art. 58-A da LGPD, composto por representantes da sociedade civil, da academia, do Poder Público e do mercado. Em outras palavras, para a efetividade do sistema de proteção de dados, essa entidade deve ter absoluta independência funcional e autonomia financeira para que possa tomar decisões imparciais. Nesse sentido, o art. 55-B da LGPD assegura a autonomia técnica e decisória da ANPD. (DE LUCCA; LIMA, 2020, p. 374).

Como resultado de todos os motivos supracitados, no Projeto de Lei n. 53 do Senado Federal e Projeto de Lei n. 5.276-A da Câmara dos Deputados foi prevista a criação da Autoridade de Proteção de dados, que, inicialmente, seria um órgão integrante da administração pública federal indireta, submetida a regime autárquico especial e vinculado ao Ministério da Justiça.

No entanto, o Projeto de Lei n. 5.276-A foi apensado ao Projeto de Lei n. 4.060 afetando-a com um vício de iniciativa de proposta, haja vista que a Constituição Federal determina que a criação de tal órgão deve se de iniciativa do Poder Executivo.

A aparição da figura da Autoridade de Proteção de Dados Pessoais (ANPD) no projeto de lei ainda causou resistência, pois a criação do órgão geraria aumento de gastos e dotação orçamentária.

Todavia, a aprovação da Lei Geral de Proteção de Dados sem a pretensão de se implantar tal órgão se transformaria em uma sistematização inócua e

incapaz de concretizar todo o complexo projetado, haja vista que para isso, a atuação da Autoridade Nacional de Proteção de Dados é fundamental, além de não permitir que o Brasil tivesse sua legislação reconhecida pela União Europeia como de mesmo nível que a *General Data Protection Regulation* (GDPR).

A GDPR é a regulamentação vigente na União Europeia que versa sobre a privacidade e a proteção dos dados pessoais de seus cidadãos. Essa lei se tornou uma referência para elaboração da LGPD e conseguinte regulamentação da proteção de dados no Brasil, sendo grande impulso para a sua elaboração devido a condição contida na GDPR que estipula que os dados pessoais dos europeus só podem ser disponibilizados a países com um nível adequado de proteção de dados.

> GDPR – Regulamento 679/2016, art. 45: "1. Pode ser realizada uma transferência de dados pessoais para um país terceiro ou uma organização internacional se a Comissão tiver decidido que o país terceiro, um território ou um ou mais setores específicos desse país terceiro, ou a organização internacional em causa, assegura um nível de proteção adequado. Esta transferência não exige autorização específica." A regra já estava prevista na Diretiva 95/46/CE: Artigo 25: "1. Os Estados-membros estabelecerão que a transferência para um país terceiro de dados pessoais objeto de tratamento, ou que se destinem a ser objeto de tratamento após a sua transferência, só pode realizar-se se, sob reserva da observância das disposições nacionais adoptadas nos termos das outras disposições da presente diretiva, o país terceiro em questão assegurar um nível de proteção adequado. (UNIÃO EUROPEIA, 2016 apud DE LUCCA; LIMA, 2020, p. 378).

O critério utilizado para verificar o nível adequado de proteção de dados é realizado pela Comissão Europeia de proteção de dados e não pode basear-se em subjetivismo, devendo analisar, conforme disposto no artigo 45, 2, da GDPR, se há presença no país da legislação analisada se constitui um Estado de Direito, se possui Autoridade de Controle Independente e Compromissos Internacionais, especialmente em relação à proteção de dados (I.T.S., 2019, p. 12).

Assim, para corrigir tais óbices, o Presidente da República a época, Michel Temer, vetou os artigos relacionados à Autoridade Nacional de Proteção de Dados mediante sanção da Lei n. 13.709, de 14 de agosto de 2018, e, posteriormente, elaborou a Medida Provisória n. 869, de 27 de dezembro de 2018, por meio da qual criou o órgão, frisando em sua justificativa que o veto não se deu por ser contrário à criação da ANPD, inclusive a considerava fundamental, sendo que seu veto se deu unicamente por prevenção, pois observava-se iminente vício formal atinente a matéria

de competência exclusiva do Poder Executivo para a criação do órgão contida nos artigos 61, § 1º, II, “e”, e artigo 37, XIX da Constituição Federal.

A Autoridade Nacional de Proteção de Dados foi criada, portanto, sem aumento de despesas (artigo 55-A da LGPD), “pois a estruturação da Autoridade será realizada com a utilização de cargos e funções alocados em estruturas vigentes de órgãos e entidades do Poder Executivo”,[7] e constituindo órgão da administração pública direta integrante da Presidência da República, a quem inclusive fica encarregado de escolher e nomear os membros do Conselho Diretor da ANPD (parágrafo 1º do artigo 55-D da LGPD).

A estruturação da Autoridade Nacional de Proteção de Dados em uma entidade da Administração Pública Indireta, de modo diferente do concebido pela Câmara dos Deputados, não agradou a maioria dos doutrinadores brasileiros, pois estes observam que essa forma em que foi implantado o órgão compromete a caracterização deste como uma entidade autônoma e independente, haja vista a sua direta subordinação ao Presidente da República.

Como menciona Roberto Pfeiffer (2019), apesar do artigo 55-B mencionar que é assegurada autonomia técnica e decisória à ANPD (BRASIL, 2018), justamente em razão dessa subordinação haveria consequências negativas, considerando-se que as decisões da ANPD poderiam ser revistas através de recurso administrativo pelo Presidente da República, o que pode interferir cabalmente na sua autonomia na tomada de decisões.

Igualmente se vê bem prejudicada a independência da ANPD diante da ausência de autonomia financeira, pois esta encontra-se condicionada à expressa autorização da lei orçamentária anual e à permissão na lei de diretrizes orçamentárias (BRASIL, 2018), ou seja, os seus recursos financeiros estarão condicionados ao repasse do governo federal do montante integral da receita que é destinada à presidência da república.

Não obstante, pode-se observar que fora estabelecido no mesmo dispositivo que a receitas da ANPD seriam constituídas também por doações, valores obtidos com a venda ou aluguel de bens móveis e imóveis de sua propriedade, resgate de valores contabilizados em aplicações no mercado financeiro, entre outras

---

[7] Medida provisória n. 869. https://legis.senado.leg.br/sdleg-getter/documento?dm=7904411&ts=1594019736542&disposition=inline

possibilidades (BRASIL, 2018). Faz-se necessário salientar que, de forma símia legislações estrangeiras, não é permitido que as multas integrem o orçamento.

Ao analisar a Lei 13.709/18, verifica-se que a Autoridade Nacional de Proteção de Dados tem natureza jurídica transitória, podendo ser transformada pelo Presidente da República em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República, sendo que a análise sobre a modificação da natureza jurídica da ANPD se dará em até dois anos de sua entrada em vigor.

O Brasil adotou a opção da corregulação, assim dizendo, a Autoridade Nacional de Proteção de Dados executará atribuições de fiscalização, regulação e sanção. Em que pese tal implementação, o Brasil continua sendo avaliado pela Comissão Europeia de proteção de dados como um país com nível não adequado de proteção de dados.

São considerados países com legislação adequada à proteção de dados pessoais na América do Sul a Argentina e o Uruguai, conforme é observado nas decisões prolatadas pela Comissão Europeia:

> ARGENTINA: 2003/490/CE: Decisão da Comissão, de 30 de Junho de 2003, nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de proteção de dados pessoais na Argentina (Texto relevante para efeitos do EEE). Jornal Oficial no L 168 de 05/07/2003 p. 0019 – 0022. (14) A lei argentina abrange todos os princípios básicos necessários para assegurar um nível adequado de proteção das pessoas singulares, embora também preveja exceções e limitações de modo a salvaguardar interesses públicos importantes. A aplicação destas normas é garantida por uma reparação judicial rápida específica para a proteção de dados pessoais, conhecida como habeas data, juntamente com as reparações judiciais gerais. A lei prevê a criação de um organismo de controlo responsável pela proteção de dados encarregado de realizar todas as ações necessárias para dar cumprimento aos objetivos e às disposições da lei e dotado das competências de investigação e de intervenção. Nos termos do regulamento, a “Direção Nacional de Proteção de Dados Pessoais” foi criada como organismo de controlo. A lei argentina prevê sanções dissuasivas eficazes de natureza tanto administrativa como penal. Por outro lado, as disposições da lei argentina no que respeita à responsabilidade civil (contratual e extracontratual) aplicam-se no caso de tratamento ilícito prejudicial para as pessoas em causa. (15) O Estado argentino apresentou explicações e deu garantias sobre o modo como a legislação argentina deve ser interpretada e garantiu que as regras de proteção de dados na Argentina são aplicadas de acordo com essa interpretação. A presente decisão baseia-se nessas explicações e garantias e, consequentemente, depende delas. [...] (UNIÃO EUROPEIA, 2003)

> URUGUAI: DECISÃO DE EXECUÇÃO DA COMISSÃO, de 21 de agosto de 2012, nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de proteção de dados pessoais pela República Oriental do Uruguai no que se refere ao tratamento automatizado

> de dados [notificada com o número C(2012) 5704]. (Texto relevante para efeitos do EEE) (2012/484/UE). (6) As normas de proteção dos dados pessoais da República Oriental do Uruguai baseiam-se em grande medida nas normas da Diretiva 95/46/CE e encontram-se estabelecidas na Lei n. 18.331 de proteção dos dados pessoais e ação de habeas data (Ley n. 18.331 de protección de datos personales y acción de habeas data), de 11 de agosto de 2008, que é aplicável tanto às pessoas singulares como às pessoas coletivas. (7) A referida lei é regulamentada pelo Decreto n. 414/009, de 31 de agosto de 2009, aprovado no intuito de clarificar diversos elementos da lei e regular a organização, os poderes e o funcionamento da autoridade nacional de proteção de dados. O preâmbulo deste decreto indica que, quanto a esta questão, a ordem jurídica nacional deve ser adaptada ao regime jurídico comparável mais comumente aceite, sobretudo o estabelecido pelos países europeus através da Diretiva 95/46/CE.[...] (10) A aplicação das normas de proteção de dados é garantida pela existência de vias de recurso administrativas e judiciais, em especial pela ação de habeas data, que permite à pessoa a quem se referem os dados intentar uma ação judicial contra o responsável pelo tratamento dos dados, a fim de exercer o direito de acesso, retificação e supressão, e por um controlo independente efetuado pela Unidade Reguladora e de Controlo de Dados Pessoais (Unidad Reguladora y de Control de Datos Personales – URCDP), que tem poderes de investigação, intervenção e sanção, seguindo o disposto no artigo 28.o da Diretiva 95/46/CE, e que atua de forma totalmente independente. Além disso, qualquer parte interessada pode recorrer aos tribunais para pedir uma indenização por danos sofridos em consequência do tratamento ilícito dos seus dados pessoais. (UNIÃO EUROPEIA, 2003)

Em face de todo o exposto, consegue-se extrair a importância de se ter uma regulamentação atinente a proteção dos dados pessoais, como também de se ter uma entidade independente, autônoma e com corpo técnico qualificado para monitorar a efetivação da norma, tanto para efetivar o direito relativo a proteção de dados, minorar riscos, vazamentos e incidentes que podem ocorrer durante o tratamento dos dados, quanto para o próprio Brasil se manter como um lugar economicamente atrativo no cenário internacional, principalmente pelos países integrantes da União Europeia, em virtude da atuação comprometida com a proteção dos direitos dos titulares de dados.

Essa análise se faz relevante também em relação aos países do Mercosul, pois, como já mencionado, a Argentina e o Uruguai já possuem selo de adequação à GDPR pela União Europeia, e a presença de uma Autoridade de Proteção de Dados sólida e autônoma, poderá impulsionar a relação comercial e a cooperação internacional entre os países do bloco (ITSRIO, 2018).

O Regulamento europeu estabelece que as autoridades de proteção de dados deverão ter orçamentos anuais próprios a fim de desfrutar de independência financeira e recursos suficientes para desenvolver de forma eficaz suas competências (UNIÃO EUROPEIA, 2016).

No entanto, esse modelo não foi integrado em sua totalidade na estrutura das autoridades desses países da América do Sul, sendo o mais próximo do modelo europeu o que se apresenta na Argentina, em que apesar de possuir orçamento próprio, a autoridade integra a *La Agencia* e esta tem a incumbência de dispor sobre os recursos disponibilizados para sua atuação, haja vista que as receitas designado ao órgão de proteção estão incorporadas a demais receitas (IDEC, 2019).

5 CONCLUSÃO

A presente pesquisa se propôs analisar a diversa literatura atinente ao tema de proteção de dados a fim de definir o alvo e a maneira de atuação da recém-vigente Lei Geral de Proteção de Dados através de uma análise principiológica.

Buscou-se delinear a estrutura que compõe a Autoridade Nacional de Proteção de Dados, fazendo um paralelo entre as razões motivadoras para sua implementação e os moldes em que de fato foi implementada através de uma avaliação de seu tramite legislativo.

Além disso, buscou-se analisar a natureza da reponsabilidade civil estabelecida pela LGPD através de análise de forma ampla através de pesquisa doutrinária, estudo principiológico e comparativa com as demais legislações brasileiras.

Ainda, foi necessário realizar uma comparação entre a sistematização da ANPD no Brasil com algumas entidades equivalentes no ordenamento estrangeiro, qual seja a Autoridade implementada na União Europeia, a do Uruguai e da Argentina, averiguando possível compatibilidade entre esses modelos de modo que fosse possível formar uma unidade no exercício de fiscalização e cumprimento da lei, segurando os direitos dos titulares de dados perante ofensas e vazamentos que vieram a ocorrer.

Diante de todo o exposto ao longo desse estudo, em relação à responsabilização civil, chega-se à conclusão que se adota a modalidade objetiva, afastando o elemento de culpa para a aparição do dever de reparar. Assim, a responsabilidade civil objetiva dos agentes de tratamento se fundamenta no artigo 927 do Código Civil de 2002, que prevê a responsabilização, independente de culpa, quando a atividade exercida provocar risco, *per si*, a outrem, bem como no Código de Defesa do Consumidor.

No que tange a Autoridade Nacional de Proteção de Dados, infere-se que para de seja um órgão eficiente e conceituado perante as nações estrangeiras em virtude de sua notável atuação e cumprimento autêntico da Lei Geral de Proteção de Dados, é necessário que haja um órgão com atuação independente com autonomia técnica e decisória no plano fático.

Dessa forma, garantindo essas prerrogativas no plano fático, será possível que haja fidedigno cumprimento dos preceitos atribuídos pela Lei Geral de Proteção

de Dados, posicionando o Brasil em um local de visibilidade e credibilidade frente a outros países dentro de um contexto de relacionamento comercial.

REFERÊNCIAS

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais:** a função e os limites do consentimento. Ed 1. Vol. Único. Rio de Janeiro: Forense, 2019

BIONI, Bruno Ricardo. **Xeque-Mate:** o tripé de dados pessoais das iniciativas legislativas Brasileiras. São Paulo: GPoPAI/USP (Grupo de Pesquisa em políticas públicas para acesso à informação da USP), 02 de julho de 2015.

BRASIL. **Código de Defesa do Consumidor. Lei Nº 8.078, de 11 de setembro de 1990.** Brasília, DF: Presidência da República [1990]. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 16 jul. 2021

BRASIL. **Comissão Especial Destinada a Proferir Parecer ao Projeto de Lei no 4060, de 2012**. Disponível em: https://www.chttps//www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=548066. Acesso em: 15 jul. 2021.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018**.** (Redação dada pela Lei nº 13.853, de 2019). Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da República Federativa do Brasil**. Brasília, DF, 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 20 fev. 2021.

BRASIL. **Projeto de Lei nº 5276/2016**. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378. Acesso em: 20 Jun 2021.

BRASIL. Senado Federal. Proposta de Emenda Constitucional nº 17/2019. **Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.** Brasília, DF. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=node0t1zu0ajget2o1jk7mm52sogg288149.node0?codteor=1773684&filename=PEC+17/2019 Acesso em: 15 jun. 2021.

CANOTILHO, José Joaquim. **Direito Constitucional**. 6ª Ed. Vol. Único. Coimbra: Livraria Almedina, 1993.

CASTRO, Maria Eugênia Bordinassi de. **A estrutura e a natureza jurídica da Autoridade Nacional de Proteção de Dados com base na lei nº 13.853/2019.** In: MAGRO, Américo Ribeiro; TEIXEIRA, Tarcísio (coords.). Proteção de Dados - Fundamentos Jurídicos. 1. ed. Salvador; JusPODIVM; 2019.

COSTA, J. M. **A boa-fé no direito privado:** critérios para a sua aplicação. São Paulo: Editora Saraiva, 2018. 9788553601622. Disponível em:

https://integrada.minhabiblioteca.com.br/#/books/9788553601622/. Acesso em: 20 jun. 2021.

COUTINHO, Jacionto Nelson de Miranda. El Derecho a La Intimidad Y Las Nuevas Tecnologías. In: DE LUQUE, Luis Aguiar; GUERRA, Luis López; TREMPS, Pablo Pérez. El Derecho a la Intimidad.Valencia: Titant Lo Blanch, 2016.

DE LUCCA, Newton; LIMA, Cintia Rosa Pereira de. Autoridade Nacional de Proteção de Dados Pessoais (ANPD) e Conselho Nacional de Proteção de Dados Pessoais e da Privacidade. In: LIMA, Cintia Rosa Pereira de (Coord). **Comentários à Lei Geral de Proteção de Dados: Lei n. 13.709/2018, com alteração da Lei n. 13.853/2019**. São Paulo: Almedina, 2020. *E-book.*

DONEDA, Danilo. **A Proteção dos Dados Pessoais Como Um Direito Fundamental.** Joaçaba: Espaço Jurídico, v.12, n. 2, p. 91-108, jul/dez, 2011.

DONEDA, Danilo. **Da Privacidade à Proteção De Dados Pessoais**. 2ª Edição. São Paulo: Revista dos Tribunais, 2020.

FLUMIGNAN, Silvano José Gomes; FLUMIGNAN, Wéverton Gabriel Gomes. Princípios que Regem o Tratamento de Dados no Brasil. In: LIMA, Cintia Rosa Pereira de (Coord). **Comentários à Lei Geral de Proteção de Dados: Lei n. 13.709/2018, com alteração da Lei n. 13.853/2019**. São Paulo: Almedina, 2020. *E-book.*

FLUMIGNAN, Wévertton G. G. **Responsabilidade civil dos provedores no Marco Civil da Internet (Lei n. 12.965/14).** Dissertação de Mestrado. Faculdade de Direito, Universidade de São Paulo, 2018.

GONDIM, Glenda Gonçalves. **A RESPONSABILIDADE CIVIL NO USO INDEVIDO DOS DADOS PESSOAIS**. Revista IBERC. v. 4, n. 1, p. 19-34, jan./abr. 2021 Disponível em: https://revistaiberc.responsabilidadecivil.org/iberc/article/view/140/119. Acesso em 13 jun. 2021.

IDEC - INSTITUTO BRASILEIRO DE DEFESA DO CONSUMIDOR. **AUTORIDADES DE PROTEÇÃO DE DADOS NA AMÉRICA LATINA:** UM ESTUDO DOS MODELOS INSTITUCIONAIS DA ARGENTINA, COLÔMBIA E URUGUAI. Disponível em: file:///C:/Users/55189/Downloads/relatorio-autoridade-de-protecao-de-dados-na-america-latina-idec.pdf. Acesso em: 20 Jun 2021.

ITS – INSTITUTO DE TECNOLOGIA E SOCIEDADE DO RIO. **Transferência de dados entre Europa e Brasil:** Análise da Adequação da Legislação Brasileira. Rio de Janeiro: ITS; 2019. Disponível em: Relatorio_UK_Azul_INTERACTIVE_Justificado.pdf (itsrio.org). Acesso em: 10 mai. 2021.

ITSRIO - INSTITUTO DE TECNOLOGIA E SOCIEDADE DO RIO. **Proposta para a criação da Autoridade Brasileira de Proteção de Dados Pessoais.** Rio de Janeiro: ITSRIO; 2018.

MARCACINI, Augusto Tavares Rosa. Regras Aplicadas ao Tratamento de Dados Pessoais. In: LIMA, Cintia Rosa Pereira de (Coord). **Comentários à Lei Geral de Proteção de Dados: Lei n. 13.709/2018, com alteração da Lei n. 13.853/2019**. São Paulo: Almedina, 2020. *E-book.*

MATTIUZZO, Marcela; MENDES, Laura Schertel. Discriminação Algorítmica: Conceito, Fundamento Legal e Tipologia. In: Revista de Direito Univille, vol. 16, n. 90, pp. 39-64, nov-dez 2019. Disponível em: file:///C:/Users/55189/OneDrive/Documentos/Toledo/MONOGRAFIA%20I/Discrimina%C3%A7%C3%A3o%20Algor%C3%ADtmica%20Conceito,%20Fundamento%20Legal%20e%20Tipologia.pdf. Acesso em: 28 Jun 2021.

MENDES, Laura Schertel. **A vulnerabilidade do consumidor quanto ao tratamento de dados pessoais**. In: Revista de Direito do Consumidor, vol. 102, pp. 19-43 (acesso online pp. 1-21), Nov-Dez/2015. Disponível em: https://revistadedireitodoconsumidor.emnuvens.com.br/rdc/article/view/441/385. Acesso em: 20 Jul 2021.

MORAES, Maria Celina Bodin de**. Risco, solidariedade e responsabilidade objetiva**. In: Revista dos Tribunais, vol. 854. São Paulo: Revista do Tribunais, dez 2006.

MORAES, Maria Celina Bodin de; QUEIROZ, João Quinelato de. **Autodeterminação informativa e responsabilização proativa. In: Proteção de dados pessoais: Privacidade versus avanço tecnológico.** Cadernos Adenauer. Rio de Janeiro, ano XX, p. 113-135, n. 3, 2019.

MORAES, Maria Celina Bodin de Moares. **LGPD: um novo regime de responsabilização civil dito "proativo".** Editorial à Civilistica.com. Rio de Janeiro: a. 8, n. 3, 2019. Disponível em: <http://civilistica.com/'lgpd-um-novo-regime/>. Data de acesso em: 28 fev. 2021.

MULHOLLAND, Caitlin Sampaio. **Dados pessoais sensíveis e a tutela de direitos fundamentais:** uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). Revista de Direitos e Garantias Fundamentais, Vitória, v. 19, n. 3, set./dez. 2018.

MULHOLLAND, Caitlin Sampaio. **Responsabilidade civil por danos causados pela violação de dados sensíveis e a Lei Geral de Proteção de Dados Pessoais (lei 13.709/2018).** 2021. Disponível em: IBERC_Responsabilidade-civil-e-dados-sensíveis - Caitlin Mulholland.pdf. Acesso em: 15 jul. 2021.

NARAYANAN, Arvind; SHMATIKOV, Vitaly. **Robust De-anonymization of Large Sparse Datasets**. The University of Texas in Austin. Disponível em: https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf. Acesso em: 28 de jun. 2019.

PEREIRA, Alexandre Libório Dias. **O direito à autodeterminação informativa na jurisprudência portuguesa:** breve apontamento. In: Ars Iuris Salmanticensis. Salamanca, Vol. 5, ed. 2, (Dec 2017): p.27-30. Disponível em:

file:///C:/Users/55189/Downloads/18011-Texto%20del%20art%C3%ADculo-61571-1-10-20180315.pdf. Acesso em: 20 jun. 2021.

PEREIRA, Caio Mario da Silva. **Responsabilidade Civil.** 12. ed. rev. atual. e aum. Rio de Janeiro: Forense, 2018.

PFEIFFER, Roberto Augusto Castellanos. **ANPD em busca de sua autonomia:** é preciso aperfeiçoar a MP 869/2018. Revista Consultor Jurídico. Disponível em: https://www.conjur.com.br/2019-mai-01/garantias-consumo-anpd-busca-autonomia-preciso-aperfeicoar-mp. Acesso em: 10 mar. 2021.

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

REALE, Miguel. Filosofia do Direito. 11. Ed. São Paulo: Saraiva, 1986.

ROTUNDO, Rafael Pinheiro. **PROTEÇÃO DE DADOS**. Revista de Direito Privado. Vol. 74/2017. São Paulo: Revista dos Tribunais, 2017.

SARLET, Ingo Wolfgang. **A Eficácia dos Direitos Fundamentais:** uma teoria geral dos direitos fundamentais na perspectiva constitucional. 13. ed. Porto Alegre: Livraria do Advogado, 2018.

UNIÃO EUROPEIA. **Decisão nº 2003/490/CE de 30 de Junho de 2003, nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de protecção de dados pessoais na Argentina**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32003D0490. Acesso em: 20 jun. 2021.

UNIÃO EUROPEIA. **Regulamento Geral de Proteção de Dados 2016/679**. Disponível em: https://bit.ly/2JJYHmK. Acesso em: 21 jun. 2021.

UNIÃO EUROPEIA. **REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO.** Bruxelas: Jornal Oficial da União Europeia, 2016. Disponível em: EUR-Lex - 32016R0679 - EN - EUR-Lex (europa.eu). Acesso em: 20 jun. 2021.