GABRIEL ZEDECK FARIA RIBEIRO

O PAPEL SOCIAL DA LEI GERAL DE PROTEÇÃO DE DADOS NO BRASIL

CURSO DE DIREITO – UNIVERSIDADE EVANGÉLICA DE GOIÁS

2022

GABRIEL ZEDECK FARIA RIBEIRO

O PAPEL SOCIAL DA LEI GERAL DE PROTEÇÃO DE DADOS NO BRASIL

Monografia apresentada ao Núcleo de Trabalho de Curso da Universidade Evangélica de Goiás - UniEvangélica, como exigência parcial para a obtenção do grau de bacharel em Direito, sob a orientação da professora M.e. Camila Rodrigues de Souza Brito.

ANÁPOLIS – 2022

GABRIEL ZEDECK FARIA RIBEIRO

O PAPEL SOCIAL DA LEI GERAL DE PROTEÇÃO DE DADOS NO BRASIL

Anápolis, ___ de _____ de 2022.

Banca examinadora

_____

_____

RESUMO

A presente monografia tem o objetivo de analisar o papel social da Lei Geral de Proteção de Dados no Brasil. A metodologia utilizada é a de compilação bibliográfica e estudo de posicionamento jurisprudencial dos tribunais. Está dividida didaticamente em três capítulos. Inicialmente, aborda-se sobre a noção gerais, apontando a importância da sua proteção na atualidade, bem como distinguindo-a do direito à privacidade. O segundo capítulo ocupa-se na apresentação do instituto do consentimento frente à proteção dos dados pessoais. Por fim, o terceiro capítulo trata sobre a trajetória normativa do consentimento até a lei geral de proteção de dados pessoais do brasil. Logo, temos como o resultado o completo estudo da proteção dos dados pessoais de cada indivíduo, bem como apresentando-se a Lei Geral de Proteção de Dados e o posicionamento principal da doutrina e jurisprudência pátria.

Palavras-chave: Dados Pessoais. Direito Cibernético. Direto Digital. Lei Geral de Proteção de Dados.

SUMÁRIO

INTRODUÇÃO

O presente trabalho trata acerca do papel social da Lei Geral de Proteção de Dados no Brasil. Foram realizadas pesquisas na modalidade de compilação bibliográfica, baseando-se em doutrinas e jurisprudências.

É necessário entender o atual panorama da sociedade diante das várias mudanças decorrentes das inovações tecnológicas que se encontram cada dia mais velozes e frequentes no campo da informação e que afeta diretamente as relações entre as pessoas e suas próprias vidas.

Antes dessas mudanças, as atividades e situações eram concretizadas pessoalmente, hoje várias delas migraram para a forma virtual, transformando em boa parte, a maneira como nos relacionamos. Nessa nova configuração social, onde se tem a grande troca de informações de forma constante, estes começaram ser o cerne de um sistema econômico virtual gigantesco.

Em uma esfera cujas mídias digitais prestam seus serviços aos usuários sem que eles paguem alguma taxa ou imposto sobre isso diretamente, não se percebe que a conjuntura financeira vai além disso. Por mais que não existam boletos ou débito em conta para poder acessar determinado *website* ou rede social, o fim econômico, está na coleta dos dados dos usuários, que fornecem eles involuntariamente.

Assim, existe a coleta de dados que, além de passar por um tratamento, são, em vários casos, vendidos ou compartilhados com terceiros, girando enormes somas de dinheiro, resultado de um mercado que se apoia na publicidade direcionada.

É possível entender que os dados estão sendo trafegados em qualquer lugar da Internet, não importa se foi em uma busca, uma aquisição de assinatura em determinado aplicativo, a inscrição de perfis nas redes sociais ou a pesquisa de um determinado lugar em aplicativos e *websites* de localização.

Assim sendo, entende-se que todas essas atividades, realizadas no âmbito *on-line*, serão vistas como dados que serão armazenados e tratados, inclusive possibilitando transferência para outros países, seja com finalidade comercial ou até política, como poderá ser visto ao longo deste estudo.

Desta forma, o presente trabalho busca contribuir, mesmo que de forma modesta, com a bibliografia jurídica, sanando dúvidas e buscando uma melhor elucidação do tema proposto.

CAPÍTULO I – NOÇÃO GERAL SOBRE DADOS PESSOAIS

Este capítulo trata da noção geral sobre os dados pessoais, trazendo o seu conceito, bem como apontando a importância da proteção dos dados pessoais na sociedade de informação. Ainda, apontam-se os principais pontos entre a proteção de dados pessoais e o direito à privacidade.

1.1 Conceito

Os dados pessoais foram regularmente definidos através do Regulamento 2016/679 da União Europeia, em seu artigo 4º, nº 1, que *in verbis* estipula:

> Dados pessoais, informação relativa a uma pessoa singular identificada ou identificável (titular dos dados); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular. (JORNAL OFICIAL DA UNIÃO EUROPEIA, 2016, *online).*

Por mais que a Lei nº 12.965/2014 – Marco Civil da Internet – tenha entrado em vigor, não há definição legislativa para os dados pessoais nas leis brasileiras. Vale ressaltar que há outras leis internacionais, em especial na Europa, que também não definem seu conceito, porém, com o Regulamento 2016/679 da União Europeia e buscando apontar conceitos mais concretos adota-se a definição mais recente estipulada na Lei Europeia de Regulamentação de Dados Pessoais.

Nesse sentido, os dados pessoais coletados podem referir-se a uma universalidade de informações, partindo dos dados cadastrais como nome, endereço, e-mail, até o endereço de IP, dados biométricos, de raça, saúde (LIMA, 2014).

As redes sociais são destaque como plataformas de coleta desses dados, sendo feitos de forma atraente aos usuários, e que a partir do momento que se aceita ser usuário, tem-se o acesso a diversos dados como nome, idade, e-mail, e todas as fotos contidas no perfil do usuário (MENDONÇA, 2018).

> A fim de desenvolver o seu conceito, convém apontar alguns tipos de dados pessoais, quais sejam: dados biométricos, dados genéticos, dados relativos à saúde, e dados sensíveis. Conceitua a GDPR, em seu art. 4º, n. 14, que dados biométricos são resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos; nesse sentido, representam características únicas (variam a depender da pessoa em questão), permanentes (não variam no tempo), acessíveis e quantificáveis. E permitem, dessa forma, a identificação ou a autenticação do indivíduo. (CASTRO, 2005, p. 83).

Os dados biométricos podem ser segmentados em dois grupos: relativos a características físicas e dados relativos a características comportamentais. O primeiro engloba a impressão digital, a geometria da mão e dedos, das veias da face, ou da orelha, a íris, a retina, o odor, a voz, ou o DNA, o segundo abrange a assinatura escrita, a forma como toca nas teclas ou na forma como fala.

Com o intuito de complementar, a Diretiva 95/46 da União Europeia em seu art. 8º, nº 1, estabelece que:

> Os Estados-membros proibirão o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, bem como o tratamento de dados relativos à saúde e à vida sexual.

Assim sendo, dados pessoais são simplesmente os dados da pessoa, desde o número do documento até um número de telefone. Os dados pessoais devem estar restritos à apenas as pessoas que foram destinadas, não podendo ser divulgados.

1.2 A importância da proteção dos dados pessoais na sociedade da informação

Ainda no começo do século XIX, em virtude da utilização de novos métodos e instrumentos tecnológicos, o início dos debates sobre o direito à privacidade se deu

como consequência do grande acesso e divulgação de fatos relacionados à esfera privada dos indivíduos. Ressalta-se a associação feita entre o objeto vida privada e um direito desconhecido à época.

O direito à privacidade está diretamente relacionado com a inviolabilidade da personalidade, rompendo com uma tradição anterior que associava a proteção da vida privada à propriedade. Com isso, “o princípio que protege escritos pessoais e outras produções pessoais, não contra o furto ou a apropriação física, mas contra toda forma de publicação, é na realidade não o princípio da propriedade privada, mas da inviolabilidade da personalidade” (MENDES, 2008, p. 14).

Com o passar do século XX, a transformação da função do Estado, interligado à crescente revolução tecnológica, contribuiu para modificar o sentido e o alcance do direito à privacidade. Atualmente, a necessidade do reconhecimento desse direito observa-se pelo próprio estilo de vida pós-moderno, com relações que tornaram as pessoas mais sensíveis e expostas à publicidade, tornando a privacidade algo essencial.

> A doutrina coloca, então, o direito à privacidade relacionado com a aversão a qualquer intromissão não consentida na vida privada (definida como o espaço da vida doméstica e das relações sexuais), acerca da fundamentalização da proteção de dados pessoais. Dessa forma, fica fácil perceber que a proteção de dados pessoais, apesar de ter como fundamento o direito à privacidade, ultrapassa o seu âmbito29, podendo ser compreendida como um fenômeno coletivo, na medida em que os danos causados pelo tratamento impróprio desse material são, em razão de sua própria natureza, difusos, exigindo uma tutela jurídica coletiva específica. Naturalmente, tanto o direito à privacidade como a proteção de dados pessoais fundamentam-se, em última medida, na proteção da personalidade e da dignidade do indivíduo. (DONEDA, 2006, p. 139).

Ocorre que, a proteção de dados pessoais modifica os elementos da privacidade, aprofundando seus pedidos e tocando em certos pontos principais dos interesses em questão. Assim sendo:

> [...] nem todos os problemas advindos do processamento de dados pessoais são passíveis de serem plenamente examinados sob a ótica da privacidade. isso acontece vez que esse conceito não é capaz de abordar os problemas individuais e coletivos oriundos dos atuais sistemas de classificação e risco, como por exemplo, a utilização de

> dados genéticos dos pacientes por planos de saúde ou a discriminação por supermercados em razão do código postal (MENDES, 2008, p. 11).

Buscando pela limitação do tratamento de dados pessoais, a fim de que os indivíduos possam exercer seu poder de autodeterminação informativa, a doutrina desenvolveu alguns princípios norteadores. Diante da clara evolução do, é possível agrupar alguns objetivos e linhas de atuação, presentes em vários ordenamentos, em diversos graus.

Com isso, pode-se perceber uma forte convergência do tratamento da matéria nos diferentes ordenamentos indo em direção à consolidação de alguns princípios básicos e à vinculação cada vez mais estreita com os direitos fundamentais e a proteção dos dados pessoais. Os princípios possuem suas origens nas leis de primeira e segunda geração, podendo observar até mesmo aos princípios norteadores do National Data Center, ainda na década de 1960.

Pode-se citar pelo menos cinco princípios considerados como principais para a proteção dos dados, quais sejam: 1. Princípio da publicidade ou transparência; 2. Princípio da exatidão; 3. Princípio da finalidade; 4. Princípio do livre acesso e; 5. Princípio da segurança. Estes princípios passaram a ser encontrados em diversas apresentações acerca da proteção de dados, e passaram a ser chamados de *Fair Information Principles*. Esse núcleo comum se consolidou como tal principalmente a partir da Convenção de Strasbourg, e das guidelines da OCDE, no início da década de 80 (DONEDA, 2011).

1.3 Proteção dos dados pessoais *versus* Direito à Privacidade

O que se leva em consideração à Lei Geral de Proteção de Dados (Lei 13.709/18) passa necessariamente pelo entendimento adequado do significado e importância do direito à privacidade e à proteção de dados pessoais. É óbvio, mas é importante dizer que, ao se refinar o conceito desses direitos, existem boas polêmicas a serem enfrentadas.

A Lei Geral de Proteção de Dados utiliza palavras e expressões que indicam uma forma de insegurança do legislador. Em seu artigo 2º declara que a

proteção de dados tem como fundamento: I - o respeito à privacidade; II - a autodeterminação informativa e; III - a intimidade. São usadas quatro expressões que a doutrina encontra dificuldades em discriminar. Vale salientar que no extenso rol de conceitos trazidos pelo artigo 5º da lei, não há definição de proteção de dados, privacidade, autodeterminação informativa, intimidade.

> A lei reflete certa indefinição em torno do conceito jurídico de privacidade e proteção de dados pessoais. Um dos desafios do intérprete e aplicador da LGPD é, reitere-se, compreender adequadamente esses termos. A importância é ainda maior ao se considerar que a LGPD possui vários conceitos indeterminados e cláusulas gerais. Definir o sentido e alcance das referidas expressões — até mesmo para concluir que são faces de uma única ideia — é diretriz hermenêutica fundamental para aplicação correta e simplificação da norma (BESSA, 2021, *online)*

O direito à privacidade é gerado simbolicamente em meados de 1890, quando se publica, na *Havard Law Review,* o ensaio *"The right to privacy"*, de Samuel Warren e Louis Brandeis. O trabalho se deu devido a imprensa em divulgar mexericos do salão a respeito da mulher de Samuel Warren, que era filha de um senador, Louis Brandeis que foi influente integrante da Suprema Corte dos Estados Unidos.

> A privacidade estava associada ao direito de ser deixado em paz, a preocupação contemporânea se dirige a proteger o cidadão e consumidor em face dos modernos — e cada vez mais eficientes e sofisticados — mecanismos da informática de tratamento (coleta, armazenamento, difusão) de dados. A evolução tecnológica aumenta exponencialmente a capacidade e velocidade de processamento de dados pessoais. Em tempos de *big data*, o consumidor, o cidadão, está completamente vulnerável e exposto a uma permanente coleta, armazenamento e divulgação de seus dados pessoais. Na maior parte das vezes, sem qualquer transparência ou mesmo ciência sobre este tratamento. Dados pessoais são coletados a partir de navegação na internet, ao se baixar e utilizar inúmeros aplicativos para smartphones, em visitas a lojas virtuais, nas manifestações e curtidas nas redes sociais (BESSA, 2021, *online)*

Na posse de várias informações pessoais e através de algoritmos e inteligência artificial, são criados perfis digitais que representam o indivíduo no relacionamento diante da sociedade e governo. E é a partir desses perfis que se decide se o consumidor merece crédito, ou pode ingressar em algum estabelecimento, se a pessoa pode usufruir algum serviço público ou atravessar a fronteira do país vizinho.

A Lei Geral de Proteção de Dados Pessoais, reconhece a importância do tratamento de dados para desenvolvimento econômico e tecnológico, bem como objetiva conferir instrumentos para que a pessoa possua controle e autonomia em relação ao que é feito com seus dados. Por mais que se tenha alguma diferença nos conceitos, inclusive em relação à autonomia do direito à proteção de dados pessoais em relação à privacidade, existem alguns consensos que são importantes diretrizes hermenêuticas para a aplicação da lei.

> Entre as incertezas, algumas certezas precisam ser pontuadas: o direito à privacidade ou, para alguns, o direito à proteção de dados pessoais integra os direitos da personalidade, o que atrai para a compreensão dos atributos desses direitos. Destacam-se aqui duas caraterísticas: o *caráter absoluto* e o *grau de disponibilidade*. Quando se afirma que os direitos da personalidade são *absolutos* não significa que eles possuem superioridade com relação a outros direitos. O significado é de oponibilidade *erga omnes*, ou seja, o sujeito passivo são todos os outros, pessoas naturais ou jurídicas, de direito público ou privado (CANOTILHO; MACHADO, 2003, p. 57).

Por não ser um direito absoluto no sentido de superioridade hierárquica, o legislador, com base em outros valores constitucionais, como por exemplo o direito à informação, a liberdade de expressão, o desenvolvimento econômico, pode estabelecer pontuações e limites à privacidade.

O exemplo mais claro de possibilidade de limitação do direito à privacidade parte do Código de Defesa do Consumidor (Lei 8.078/90), em seu artigo 43, o qual possibilita o tratamento de dados pessoais do consumidor para fins de análise de risco de concessão de crédito. Independentemente da anuência do consumidor , permite-se que as dívidas vencidas e não pagas sejam registradas nas entidades de proteção ao crédito.

> Atendidos os pressupostos normativos específicos (informação verdadeira, comunicação prévia, limite temporal etc.), o fornecedor pode inscrever o nome do consumidor em banco de dados de proteção ao crédito. Cuida-se de exercício regular de direito que, por óbvio, não enseja qualquer sanção jurídica. Outro ponto merece ser destacado. A vontade do titular ganha dimensão especial em relação a alguns direitos da personalidade. É o que ocorre no direito à privacidade. A legislação reconhece a vontade como forma legitimadora do tratamento de dados pessoais. Se o titular, em ambiente de transparência e informação, manifesta concordância com o tratamento

> de seus dados, não há que se falar em ilicitude do tratamento de dados (BESSA, 2021, *online)*

Assim, a LGPD, no inciso I do artigo 7º, institui o consentimento do titular como base legitimadora do tratamento de dados pessoais. A importância da autonomia da pessoa evidencia-se também por ser hipótese autorizadora de tratamento de dados sensíveis. Essa prática aponta a liberdade e autonomia do indivíduo, bem como traz várias outras consequências.

Assim, a liberdade, a possibilidade de autodeterminação é um aspecto determinante da própria dignidade humana. Como observa Jorge Reis Novais, "a titularidade de uma qualquer posição de direito fundamental envolve, em princípio, o poder de disposição sobre todas as possibilidades de ação que dela decorrem, momento o poder de disposição acerca do 'se', do 'quando' e do 'como' do seu exercício (ou não exercício) fático" (2006, p. 286).

Não se trata de se impor obrigatoriamente proteção de privacidade, porém de oferecer instrumentos básicos que são necessários para determinar a medida e em que circunstâncias dados pessoais podem ser objeto de tratamento.

> O direito à privacidade deve centrar-se na proteção das decisões individuais em matéria de privacidade e não na promoção de uma determinada concepção acerca deste bem. É que numa sociedade composta por milhões de indivíduos portadores das mais diversas, incomensuráveis e antagônicas concepções mundividenciais e valorativas e, frequentemente, portadores de interesses e objectivos completamente diferentes, é impossível e indesejável impor a todos eles uma determinada concepção de privacidade e muito menos transformar unidimensionalmente o direito à privacidade num dever de privacidade (CANOTILHO; MACHADO, 2003, p. 57).

Desta forma, nas hipóteses em que não o legislador não dispõe sobre, impondo ou permitindo o tratamento de dados, não se deve deferir a tutela de dados pessoais como um dever a ser observado pelos titulares. A autodeterminação informativa prestigia a liberdade para exercício de escolhas individuais, a fim de decidir de forma livre o que fazer com seus dados pessoais.

Com a promulgação da Constituição Federal de 1988, muito se falou acerca da dicotomia referente as previsões constitucionais do direito à privacidade e demais

outros. Não há nenhum direito fundamental absoluto, e existem momentos em que é necessário esquecer por um leve prazo os direitos fundamentais individuais em detrimento da coletividade (VENOSA, 2016).

Ocorre que, não há razão para este debate e dicotomia entre os princípios, tendo em vista que a própria legislação brasileira traz conteúdo necessário para a solução desta divergência hermenêutica. A Constituição Federal é clara e rígida ao dispor sobre seus princípios fundamentais, e basear a conclusão dessa dicotomia e debate.

> O direito à dignidade, privacidade, intimidade, honra, imagem, e os demais direitos personalíssimos, possuem na Constituição Brasileira caráter de direito fundamental, com perfil de cláusula pétrea, incluído na carta magna entre os direitos civis, sociais, políticos e jurídicos, com função de garantir e perpetuar todos os direitos individuais e direitos coletivos alicerçados na Declaração Universal de Direitos Humanos entre outras recomendações e legislações que tem base nos direitos de primeira geração e na tríade da Revolução Francesa (qual seja: “Liberdade, Igualdade e Fraternidade”) (CANTELMO, 2021, *online).*

Referidos princípios são apresentados de início no Preâmbulo da Constituição Federal de 1988, sendo repetidos no artigo 1º, posteriormente citado nos artigos 3º e 4º, e, finalmente, referenciado no artigo 5º, um dos artigos mais importantes da Carta Magna (VENOSA, 2016).

O preâmbulo da Constituição Federal de 1988 anuncia que é objetivo do texto constitucional “instituir um Estado Democrático, destinado a assegurar o exercício dos direitos sociais e individuais, a liberdade, a segurança, o bem-estar, o desenvolvimento, a igualdade e a justiça como valores supremos de uma sociedade fraterna, pluralista e sem preconceitos (...)”(BRASIL, 1988, *online).*

Assim senso, se existe dúvida entre quaisquer princípios trazidos pela Constituição Federal, deve-se priorizar o que for destinado a assegurar o bem-estar e a justiça, buscando a fraternidade, e impedindo a criação de quaisquer tipos de preconceitos. Assim, o princípio da dignidade, honra e imagem devem ser prioridade.

> [...] partindo da compreensão que os princípios e fundamentos constitucionais estão previstos exatamente no preâmbulo e nos quatro

> primeiros artigos da Constituição Federal (com estes quatro artigos formando o Capítulo I da Carta Magna sob o título "*Dos Princípios Fundamentais*"), conclui-se como imperioso a proteção da cidadania, da dignidade da pessoa humana, da justiça, da erradicação dos preconceitos e desigualdades sociais (e quaisquer outras formas de discriminação) etc., bem como a construção de uma sociedade justa e solidária, que busca a solução pacífica dos conflitos, com prevalência dos direitos humanos (com todas essas expressões manifestadas taxativamente em diversos incisos distribuídos nos artigos 1º, 3º e 4º do texto constitucional) (CANTELMO, 2021, *online).*

O *Caput* do artigo 5º da Constituição Federal explica que "todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade". (BRASIL, 1988, *online).* Por mais que depois apresente incisos que disponham sobre princípios dicotômicos tais como o da liberdade de expressão, da transparência da informação, entre outros, o *caput* hierarquiza a dignidade da pessoa humana sobretudo ao garantir, entre outros, o direito à vida, igualdade e segurança.

Baseando-se em todos os princípios e fundamentos constitucionais, o artigo 5º da Constituição traz uma série de incisos listando direitos e garantias fundamentais, reforçando inúmeras vezes os direitos personalíssimos, principalmente o direito à dignidade, honra e imagem.

> O artigo 5º, inciso X, confirma o Princípio da Dignidade, Intimidade, Privacidade, Honra e Imagem das pessoas, admitindo tudo que fora atribuído entre os princípios e fundamentos constitucionais elencados no Preâmbulo, nos artigos 1º, 3º e 4º, e no *Caput* do artigo 5º da Constituição Federal de 1988. Vejamos o que diz o referido artigo 5º, X, da CF: "*são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação*" (lembrando que inciso V do mesmo artigo 5º aborda que "*é assegurado o direito de resposta, proporcional ao agravo, além da indenização por dano material, moral ou à imagem*") (CANTELMO, 2021, *online).*

Desta forma, decerto que o princípio da privacidade, dignidade, intimidade, privacidade, honra e imagem, entre outros, mesmo que não sejam direito absoluto, devem se sobrepor sobre quaisquer outros direitos se houver dúvida entre os princípios constitucionais, analisando de acordo com cada caso, conforme estabelece o Supremo Tribunal Federal.

CAPÍTULO II – O INSTITUTO DO CONSENTIMENTO FRENTE A PROTEÇÃO DOS DADOS PESSOAIS

O presente capítulo apresenta o instituto do consentimento diante da proteção dos dados pessoais. Inicia-se com a dualidade do consentimento, partindo para os pressupostos de validade, bem como distinguindo os consentimentos informado, livre e inequívoco, finalizando com as dificuldades e desafios do consentimento em relação ao fluxo informacional.

2.1 Dualidade do consentimento: autodeterminação informativa e meio de legitimação

O instituto do consentimento passou a designar a liberdade e autonomia dos usuários de redes, principalmente no que dispõe sobre a ciência de procedimentos a serem realizados com seus dados, concordando com referidas ações (CORRÊA, 2019).

Desta forma, os atos normativos que apresentam sobre a matéria apontam sobre o consentimento com o objetivo de colocar a pessoa no centro do controle da coleta e tratamento de suas informações, “preservando, assim, a sua capacidade de livre desenvolvimento da personalidade” (MENDES, 2014, p.60)

O Estado, diante do tema aqui tratado, teria como dever legislar acerca dos meios e formas pelos quais a pessoa tem à sua disposição quando do ato de controle. Desta forma:

> Por se constituir um direito sobre as informações pessoais, a proteção de dados pessoais tem um forte componente de autoconformação,

> tendo em vista que somente o indivíduo pode determinar o âmbito da própria privacidade, isto é, em que medida as suas informações pessoais podem ou não ser coletadas, processadas e transferidas. Nesse aspecto, nota-se que a proteção de dados pessoais é marcada por esse acentuado viés de autocontrole e de liberdade pelo titular (MENDES, 2014, p. 90).

O consentimento passa a ser um instrumento que o indivíduo utiliza, o qual possibilita o exercício da sua autodeterminação informática. Bioni (2018) aponta que o consentimento surge como uma carta regulatória, possuindo o objetivo de autorizar ou proibir em meio a um sistema de coletas e tratamentos de dados pessoais.

Assim sendo, é possível perceber que o indivíduo passa a ser visto como um ser central ao longo da evolução da proteção dos dados pessoais, chegando-se ao ponto de ser equiparada “ao direito do cidadão autogerenciar as suas informações pessoais (BIONI, 2018, p. 35).

Seria inapropriado considerar o consentimento como uma forma negocial, tendo em vista que se fosse dessa forma, poderia se incluir esse instituto nas estruturas contratuais, bem como se dificultaria o exercício das prerrogativas da personalidade a serem analisadas e respeitadas. Assim, é possível perceber que a fundamentação do consentimento está fundada na possibilidade da autodeterminação, ligada aos dados pessoais, devendo esta ser o principal elemento para se caracterizar a natureza jurídica e os efeitos do consentimento.

Ruaro, Rodrigues e Finger (2011) dispõem que o consentimento é identificado como uma forma de expressar a escolha da pessoa, ato contínuo. Se refere aos valores fundamentais relacionados. Desta forma, quando se identifica a autodeterminação informacional, percebe-se um importante instrumento de legitimação.

Em relação às possibilidades de revogação do consentimento declarado pelo indivíduo, tem-se a ideia de proteção da personalidade do titular. Caso houvesse a revogação, seria uma atribuição da própria natureza jurídica do consentimento, tendo em vista que como decorre da autodeterminação, a pessoa não se submete aos efeitos vinculantes da sua escolha, mas o que está autorizado a usar os dados e tem a revogação, nada pode fazer, pois está direcionado à natureza da atividade realizada.

De acordo com Mendes (2014), a revogação do consentimento do uso de dados sem qualquer justificativa que seja, é a vertente que aponta a realidade, pois está colocado de forma intrínseca à proteção dos dados pessoais. É possível perceber tal ato pois o indivíduo que possui os dados pessoais enfrenta várias dificuldades para que se possa calcular os riscos e consequências de seu consentimento.

A Escola Nacional de Defesa do Consumidor (2010), traz que a ideia de revogação deve ser posicionada de forma que os usuários a tenha por mecanismos ostensivos e fáceis para os usuários, pois sua autodeterminação não se encontra a restrição ao indivíduo das consequências de natureza obrigacional, vez que vinculariam ao seu consentimento já entregue.

2.2 Pressupostos de validade

A validade do consentimento se dá a partir de alguns pressupostos que merecem um maior esclarecimento no presente trabalho. São basicamente três pressupostos principais, quais sejam: a) o titular deve emitir o consentimento de forma espontânea; b) o consentimento deve se voltar para um fim em específico; c) deve ser proporcionada a devida informação ao usuário acerca dos objetivos da coleta de dados, processamento e uso, bem como as consequências de seu consentimento.

De acordo com Souza (2018, p. 30):

> [...] validade ao consentimento, declaração do indivíduo, devem perceber a coleta de seus dados, isto é, ser obtida antes da interferência de terceiros, a fim de servir como um instrumento de informação acerca do que será consentido, inclusive dos riscos e consequências de sua decisão.

Assim, além da possibilidade de revogação do consentimento, deve-se observar a relação de autorização para o tratamento, bem como para a circulação dos dados colhidos. A validade do consentimento se dá quando ele é fornecido por alguém que possua devida ciência dos riscos e consequências que acompanham a declaração de vontade, bem como que ele seja assegurado da coerção, autorizando de forma expressa, determinado o tratamento de dados específicos.

2.2.1 Consentimento informado

A questão do consentimento informado surge como um direito e um dever pelo tratamento dos dados pessoais. Para que o consentimento seja válido, é necessário que o titular possua informações suficientes para que possa decidir. Bioni (2018) aponta que consiste em dar forma e a sua importância é grande em relação ao ambiente de proteção de dados pessoais que o consentimento informado é visto apenas como ‘consentimento’.

O consentimento informado é posto como uma forma de garantia para que as decisões a serem tomadas sejam realizadas de forma racional e ponderada, bem como, se não o houvesse, poderia ser constatada uma quebra do princípio da autonomia. Diante disso, é importante apontar duas questões: a) deve-se considerar o elemento formal, para que se aponte fielmente a forma declarada de vontade do titular e; b) sobre a utilidade da informação prestada, deve ter o acréscimo do conhecimento ao usuário, proporcionando a devida proteção (BIONI, 2018).

Este é o modelo básico do consentimento, que possui duas etapas importantíssimas que devem ser analisadas. A primeira é o pedido pelo controlador e a segunda é a declaração de vontade do indivíduo, sendo assim é necessário que as ações dos interessados nos dados do indivíduo passam a ser vistas como um fornecimento de informações acerca do conteúdo e processo de cada consentimento, a fim de que o dono e titular dos dados possa tomar sua decisão.

Assim, Lisboa preceitua (2012, p. 28):

> O emitente deve buscar o equilíbrio ideal entre os elementos da mensagem, transmitindo a informação em um grau de originalidade e imprevisibilidade que, ao mesmo tempo, desperte a atenção do receptor e possibilite a sua compreensão. Agindo desta maneira, o emitente da informação terá maior êxito no processo comunicativo, podendo inclusive exercer legitimamente o convencimento necessário para que o destinatário adote a conduta dele esperada. A comunicação adequada e eficiente provoca a reação no destinatário da mensagem.

Mesmo assim, necessário se faz destacar que as informações apresentadas não abrangem o total do transmissor, tendo em vista que é de difícil

concretização, ou seja, é necessário transpassar a informação ao receptor leigo de forma mais clara.

É importante sempre saber acerca da procedência dos dados repassados, bem como as suas finalidades e procedimentos usados. O indivíduo deve possuir ciência que seus dados serão coletados e usados, bem como para quais fins serão utilizados, cientificando-se ainda sobre como pode consentir e quais meios pode usar para revogar o seu consentimento.

2.2.2 Consentimento livre

Baseado no histórico normativo, inclusive do brasileiro relacionado ao direito privado, é possível verificar que o instituto do consentimento esteve muitas vezes ligado aos defeitos do negócio jurídico, a fim de que a relação negocial fosse válida, seria necessário que o consentimento da parte fosse livre e consciente. Agora, a declaração de vontade tem que advir sem coação, física ou moral, partindo de uma escolha livre e espontânea vontade do indivíduo (MALHEIRO, 2017).

O consentimento estaria categorizado como um ato unilateral, estando separado em duas etapas: quando da declaração de vontade que concede o processamento dos dados e quando da autorização acerca do compartilhamento dos dados. Assim sendo, para que o processamento dos dados seja lícito, o consentimento deve indicar a concordância do indivíduo na sessão de seus dados. Para que seja válida, deverá ter sido entregue de forma livre e específica, numa real demonstração de vontade, independente do ambiente em que os dados foram coletados (SOUZA, 2018).

Bioni (2018, p. 197) dispõe que a análise deve estar diante do grau de assimetria existente para, então, entender quais eram as possibilidades de escolha do usuári, ou seja, todas as opções à disposição do cidadão definirão o quão livre é o seu consentimento:

> A questão central é sempre checar a existência de algum tipo de subordinação - assimetria de poder - que possa minar a voluntariedade do “consentimento, devendo haver uma análise

> casuística para se concluir se o “consentimento pode ser adjetivado ou não como livre.

Desta forma, ao se referir em ausência do controle de terceiros, o consentimento livre aponta que o usuário praticou o ato a partir de uma escolha “se recusar o consentimento não é uma escolha viável, ou por ser impossível, ou por trazer um impacto muito negativo ao titular dos dados, então não há uma escolha real e, portanto, não há consentimento” (MALHEIRO, 2017, p. 47). Assim sendo, quando a declaração de vontade acontece sem este adjetivo, o consentimento está viciado.

Conclui-se, assim, que a partir de um consentimento dito como livre e informado, é necessário que os indivíduos tenham concordado com as medidas impostas. A Escola Nacional de Defesa do Consumidor (2010, p. 66) assevera:

> Como condições para o consentimento livre e informado, é necessário que o monitoramento se processe de forma clara e transparente e que sejam fornecidas aos usuários informações sobre quais dados serão colhidos, a forma como eles serão utilizados e por quem serão utilizados, entre outras. informações essenciais. Além disso, é fundamental que o usuário tenha

Com isso, é possível entender que, para que os usuários possuam o julgamento sobre a conveniência, riscos e consequências da coleta e tratamento de seus dados, devem receber de início, informações necessárias que lhes permitiram optar pela cessão de seus dados de forma livre, tendo em vista que a decisão de entrega dos seus dados deverá ser dada em meio a tantas outras que poderiam ter sido feitas.

2.2.3 Consentimento inequívoco

Inicialmente é importante mencionar que o tratamento dos dados passa a ser uma atividade exercida com uma finalidade específica e explícita, ao passo que, ao relacionar com o instituto do consentimento, liga-se à imprescindibilidade de direção, possuindo função de como se fosse um caminho a ser perseguido para a verificação da informações passadas ao usuário que deu origem à declaração de vontade livre.

Partindo para uma carga participativa intermediária do indivíduo sobre seus dados, aparece a adjetivação com o termo inequívoco, onde se encontram

autorizações dentro do contexto do fluxo informacional. Assim, apresentam-se situações nas quais o consentimento torna-se prescindível, tendo em vista que se encontram dentro das legítimas expectativas do titular dos dados.

> Além do mais, ao atrelar o instituto do consentimento à inequívoca declaração, a declaração de vontade passa a ser um ato de origem do indivíduo que exponha a sua vontade. Já quanto à categorização de consentimento com finalidade determinada, a carga participativa do titular dos dados passa a ser pré-intermediária, tendo em vista que, por estar vinculado aos princípios de informação e transparência, tal adjetivação recebe uma maior importância (MALHEIRO, 2017, p. 47).

Sob este prisma, o consentimento deve estar ligado a um fim específico, excluindo-se propósitos genéricos que poderiam gerar emissões de espécie de "cheque em branco" aos coletores de dados, ou seja, afasta-se a possibilidade de uma declaração de vontade genérica por parte do titular dos dados e de uma interpretação extensiva além das que estariam previstas (DONEDA, 2006).

Conclui-se que, o instituto do consentimento encontra-se inserido em um contexto específico, de forma que a declaração de vontade que autoriza a coleta e o processamento de algum dado, em alguma situação, não se estende a outros ambientes diferentes daquele.

2.3 Dificuldades e desafios do consentimento em relação ao fluxo informacional

A sociedade ganhou um novo impulso com a era da informação que introduziu a reestruturação e organização de novos modos de se conviver no mundo. Decorrentes dessa dinâmica realidade ditada pelas tecnologias, foi gerada a criação de mecanismos e ferramentas cada vez mais rápidas e eficazes na coleta e transmissão de dados (BIONI, 2018).

Essa facilidade em ter informações fez com que o direito à privacidade fosse afetado, uma vez que a esfera privada deu espaço para que o avanço tecnológico ganhasse o seu, o que não ocorreu sem problemas. As novas formas de violação exigiram que fossem pensadas em outras estratégias de tutela e, considerando que os fluxos informacionais não respeitam as fronteiras do Estados, os contornos imprecisos da sociedade em rede exigem que se lance um olhar atento aos mecanismos internacionais no que tange à proteção dos dados pessoais.

> As primeiras legislações voltadas à proteção de dados são oriundas da União Europeia, e o marco desse surgimento foi na década de 70 do século XX, ocasião em que a Alemanha promulgou a Lei do Land alemão de Hesse, que tinha por objetivo regular os bancos de dados informatizados de dados governamentais (MACHADO, 2018, p. 123).

A Lei não foi suficiente para fornecer as garantias elencadas, tendo em vista que a prática adotada por ela fez com que gerasse insegurança na sociedade. O Estado pretendia criar um censo que continha 160 (cento e sessenta) perguntas de cunho pessoal, voltadas à obtenção de dados ligados à vida profissional, ideologias políticas e crenças religiosas, informações que seriam confrontadas com dados apresentados no registro civil. Quem não respondesse, estaria sujeito à multa, além de existir a possibilidade dos dados dessas pessoas serem direcionados às autoridades federais.

Por conta da exposição e das sanções trazidas, apresentava-se o medo da criação de um Estado super informado que, em vez de ajudar o seu povo, estaria prejudicando e isso geraria a inconstitucionalidade do censo, conforme anteriormente apresentada pela Corte Constitucional, que entendeu que a diversidade de finalidades do censo impediria as pessoas de determinarem como seriam utilizados os seus dados.

A nova Lei n.º 13.709, de 2018 é uma legislação que possui seu pilar principiológico, que evidencia que o Brasil começa a dar os primeiros passos em direção à proteção de dados, perfazendo a primeira etapa de uma longa trajetória já traçada em outros países. Constitui-se em uma das mais esperadas leis a ser editada nos últimos tempos, colocando em pauta a evolução atrasada dessa proteção em território nacional.

Sua inspiração é de origem europeia, baseando-se no Regulamento Europeu de Proteção de Dados, o qual traz referência para vários países do mundo quando se trata da proteção de dados, constituindo-se em um dos fatores impulsionadores da edição da novel legislação, sendo que sem ela o Brasil teria problemas para negociar com as empresas europeias por não dispor de nível de proteção adequado aos parâmetros lá vigentes (CORRÊA, 2019).

De acordo com Coêlho (2019, p. 44):

> Outras lacunas preenchidas pela MP que merecem destaque dizem respeito à instituição e regulamentação do agir da Autoridade Nacional de Dados Pessoais (ANDP). Vetada pelo Presidente Michel Temer quando do sancionamento, para ser aprovada por medida provisória, fora alterada na sua essência de vinculação hierárquica, agora subordinada à própria Presidência da República, mas com a devida autonomia técnica. É função da ANPD não só reguladora, como sancionadora das penalidades que estão previstas no texto normativo. As multas a serem concedidas por atos infracionais à norma chegam a valores vultosos de cinco milhões de reais, por exemplo

Apesar de os artigos 55, 56 e 57 da LGPD terem sofrido veto da Presidência da República, tendo em vista sua desconformidade com a regra que deveria passar pelo Poder Executivo e pela previsão orçamentária antes de se tornar Lei, a Autoridade Nacional se instituiu através da Lei n° 13.853, de 2019. Referida Lei assevera acerca de alterações feitas na Lei nº 13.709, de 2018 e acerca da criação da Autoridade Nacional que passa a ser um órgão integrante da Administração Pública Federal, sendo ele subordinado à Presidência da República e possível de ter sua natureza jurídica reanalisada em até dois anos, tendo em vista seu caráter transitório (BRASIL, 2019).

> Entre as competências da ANPD, estão as de zelar pela proteção dos dados pessoais e de elaborar diretrizes para a Política Nacional de Proteção de Dados e da Privacidade, de forma a inibir todo e qualquer ato de violação que possa partir dos agentes encarregados do tratamento das informações pessoais. Além dessas, há outras competências previstas no art. 55-J, que explicitam como será sua esfera de atuação, bem como a busca por certas garantias, a exemplo do tratamento de dados de idosos, para que seja efetuado da forma mais simplificada e clara possível, dispondo a eles acessibilidade, tudo em conformidade com o Estatuto do Idoso (MALHEIRO, 2018, *online*).

Muitas são as atribuições da ANPD, sendo uma delas enviar informes com previsão das medidas necessárias para cessar violações geradas do tratamento dos dados em poder da Administração Pública, bem como solicitar aos agentes detentores desses dados a publicação de relatórios que apresentem informações acerca do impacto referente à proteção de dados e formas e sugestões de boas práticas relacionadas a essa proteção.

Além disso, com a criação da ANPD, foram geradas várias expectativas relacionadas à fiscalização e ao cuidado no tratamento dos dados pessoais sensíveis,

principalmente em torno da atuação do Poder Público. É importante observar como este tratamento irá evoluir, principalmente diante da opção brasileira em vincular o órgão à Presidência da República, o que pode comprometer sua autonomia e também colocar em risco a proteção de dados pessoais no Brasil.

CAPÍTULO III – TRAJETÓRIA NORMATIVA DO CONSENTIMENTO ATÉ A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS DO BRASIL (LEI N. 13.709/18)

O presente capítulo aborda sobre a trajetória normativa do consentimento até o surgimento da Lei Geral de Proteção de Dados Pessoais do Brasil. De início, aborda-se sobre as principais normativas setoriais brasileiras anteriores à LGPD e, por fim, sobre a Lei Geral de Proteção de Dados Pessoais, propriamente dita.

3.1 As principais normas setoriais brasileiras anteriores à LGPD

Viktor Mayer-Scönberger, abordado por diversas doutrinas, traz que o traçado evolutivo das leis que apontam acerca da proteção dos dados pessoais em todo o mundo pode ser visto por quatro gerações distintas: parte-se de um cenário mais técnico e restrito para, enfim, ampliar as disposições e as técnicas referentes às tecnologias modernas (apud DONEDA, 2011).

O contexto apresentado à primeira geração de leis que regulamentam os dados pessoais está direcionado às aflições ocasionadas pelo processamento de dados pessoais colacionado à construção do Estado Moderno, além de definir uma reação às ideologias de concentração dos imensos bancos de dados nacionais (MENDES, 2014).

Os regulamentos vão ao encontro especificamente para a própria tecnologia, analisada então como um meio que necessitava de orientação para se encaixar dentro dos valores democráticos. A realidade da época está relacionada à

ideia de arquitetar "normas rígidas que tomassem o uso da tecnologia" (BIONI, 2018, p. 114).

Doneda (2006) aponta fielmente acerca dessa pontuação, dizendo que os núcleos destes normativos estavam ligados com a entrega do consentimento dos titulares dos dados para a criação dos bancos de dados, além do controle a *posteriori* por órgãos públicos, o que fez com que o Estado fosse colocado como o destinatário principal desses regulamentos.

Mendes (2014, p. 39) expressa:

> Ademais, ao priorizar o controle rígido dos procedimentos, as normas desse periodo deixavam para segundo plano a garantia do direito individual à privacidade, o que pode ser percebido a partir do próprio jargão técnico utilizado nas normas.

Ocorre que, com o passar do tempo, a primeira geração tornou-se obsoleta, como virtualmente ineficaz para uma proteção, por se basear em um simples centro de autorizações, taxado pela rigidez, e que ainda exigia um minucioso acompanhamento (apud DONEDA, 2006).

Nesse sentido, Bioni (2018, p. 114) diz que, “tendo em vista o exponencial crescimento das ferramentas tecnológicas, o tratamento de dados pessoais passou a ir além do domínio governamental, trazendo novos autores na relação e a necessidade de uma evolução, também, na legislação sobre o tema: surge, assim, a segunda geração de leis de proteção de dados pessoais.

Após a guerra, o mundo ficou concentrado em seus esforços em conseguir os direitos mínimos a todos os cidadãos, podendo citar principalmente a Declaração Universal de Direitos Humanos:

> Artigo 12 - Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques.

Esta diligência com a privacidade foi aperfeiçoada, transcrita no artigo 5º, inciso X, da Constituição Federal de 1988, que estabelece que “são invioláveis a

intimidade, a vida privada, a honra e a imagem das pessoas assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação" (BRASIL, 1988, *online)*.

Viviane Maldonado (2019, p. 13) aponta que,

> [...] para entender a evolução legislativa que deu a autonomia aos dados pessoais, torna-se importante a compreensão de dois instrumentos da legislação europeia: a) a Carta dos Direitos Fundamentais da União Europeia de 2000, artigo 8º; e b) o Tratado de Funcionamento da União Europeia (TFUE), artigo 16, ambas que preconizam que "Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.

A emancipação do direito, ligada à proteção de dados pessoais e à privacidade, somada a um contexto de fluxo de dados dos vários estados membros da União Europeia, apresentou a necessidade da edição de uma lei que desse segurança jurídica aos seus jurisdicionados, o que trouxe a devida relevância para a discussão da temática.

Diane disso, em 2012 iniciou-se o trâmite da proposta de criação de um Regulamento Geral Europeu que pudesse se aplicar a todos os estados-membros, sendo aprovada em abril de 2016 e com início de sua eficácia em 2018. Foi criada a GDPR (General Data Protection Regulation), que encarregou-se de unir todas as normas relacionadas ao tema de forma coesa, aplicando extraterritorialidade nos casos em que o agente de tratamento ofertar produtos ou serviços à União Europeia ou tratar os dados pessoais de seus residentes (MALDONADO, 2019).

> Além disso, houve a imposição de restrições às contratações das empresas europeias que, a partir daquele momento, somente poderiam contratar empresas de países estrangeiros se no país do contratado houvesse grau de proteção similar ou superior ao estabelecido pela lei, o que naquela época excluía o Brasil (OLIVEIRA, 2020, p. 30).

Assim sendo, houve um efeito em cascata na cadeia de fornecimento das empresas europeias, sendo que o Brasil ainda em 2018 promulgou a Lei Geral de Proteção de Dados – LGPD (Lei 13.709/18). Porém, quando a LGPD foi aprovada, o Brasil não estava desamparado no assunto de proteção aos dados pessoais, pois já

existia no país uma lei que desse um pouco de respaldo, trata-se do Marco Civil da Internet (Lei 12.965/2014) e seu Decreto Regulador (Decreto 8.771/2016).

3.2 A Lei Geral de Proteção de Dados Pessoais

Por mais que não seja essencial que o operador do direito seja um especialista em tecnologia dos meios de informação para entender a Lei Geral de Proteção de Dados, alguns conceitos a serem apresentados ajudarão a expandir o entendimento da sociedade de forma geral.

Maldonado (2019), aponta que embora os esforços das mais diversas regulamentações acerca da proteção de dados pessoais, há o convívio em um mundo de *big data*, onde as informações são processadas por qualquer pessoa, pelas empresas, e a todo momento, em um volume incomparável com o volume de antigamente:

> Os estudos sobre privacidade embora tenham ganhado contorno mais acentuado na era da informação, estão presentes desde a antiguidade, como é possível ser visto na distinção Aristotélica entre vida pública e vida privada, ou polis e oikos, respectivamente. Contudo, como vivemos em uma sociedade dinâmica e, para garantir a efetividade da proteção à privacidade, qualquer definição, natureza e mecanismos desta proteção devem ser constantemente atualizadas (MALDONADO, 2019, p.12).

Após um certo tempo, passou-se a compreender a privacidade como um direito individual. Nos dias atuais, o avanço da tecnologia é um dos principais responsáveis pelo avanço nas pontuações sobre a privacidade. O simples conhecimento de que a qualquer momento suas informações são processadas por vários agentes e que, decisões automatizadas, são tomadas, sem qualquer participação, colocou o sujeito em uma posição de passividade.

Como leciona Bioni, (2019, p.64), “há uma economia de vigilância, onde o titular transforma-se em um mero expectador do fluxo de seus dados, estes que são a base de sustentação deste novo mercado”. Na sociedade informacional, a geração de riqueza está sempre observando os comportamentos de cada pessoa que, unidas, são capazes de construir padrões e fazer com que a mensagem publicitária fique cada vez mais eficiente.

Além da publicidade ser aparentemente sutil, de forma gradativa, ela se torna mais agressiva, pois considera todos seus padrões de consumo, o contínuo processamento de dados pessoais, podendo ser utilizado para várias finalidades, desde a segurança pública até práticas consideradas discriminatórias.

Bioni (2019, p.64) aponta que é essencial a conciliação entre os interesses econômicos e o empoderamento do titular dos dados. Este é o ponto principal para o sucesso de qualquer legislação que venha a regular acerca dos dados pessoais, a inobservância de qualquer um destes dois aspectos acarretará o fracasso da lei.

Um grande avanço na legislação acerca da proteção de dados, foi o Marco Civil da Internet. Palhares, Prado e Vidigal (2021, p. 33), apontam que, para o correto entendimento do Marco Civil da Internet, é necessário relembrar qual era o contexto na época de sua aprovação. Em 2013, o mundo ficava assustado com o vazamento de documentos de espionagens realizadas pelo Estados Unidos, apresentados pelo então ex-agente da CIA, Edward Snowden. Nos documentos restou comprovado que o Brasil vinha era um dos principais países objetos desta vigília, inclusive tendo o e-mail da ex-Presidente Dilma Rouseff, sido alvo desta espionagem.

Bioni (2019, p. 186) ressalta que,

> [...] à época tentava-se criar uma lei com traços do direito criminal para regular o uso da internet, através de uma técnica legislativa que seria prescritiva e restritiva das liberdades individuais, o que viria a travar qualquer inovação advinda da internet e teria consequências sociais e econômicas devastadoras.

Com a vulnerabilidade devidamente escancarada, aos quais os dados pessoais, inclusive da presidente do país, estavam expostos, o Brasil aprovou em 23 de junho de 2014 o Marco Civil da Internet, com o intuito de regular o uso da internet. Alguns conceitos importantes foram utilizados para a criação da LGPD, a saber “especialmente os de dados pessoais e de tratamento, a privacidade como um princípio, direitos dos usuários, padrões de segurança para guarda, armazenamento e tratamento de dados pessoais” (OLIVEIRA, 2020, p.35), bem como vários princípios que norteiam atualmente o tratamento de dados pessoais.

Dos principais princípios abordados pelo Artigo 3º do MCI, dois deles apontam principal relevância para a posterior compreensão da LGPD e do papel do legítimo interesse, a saber: inciso III – proteção dos dados pessoais, na forma da lei; e inciso VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios da lei (BIONI, 2019).

Um leigo ao ouvir pela primeira vez sobre a LGPD, tende a entender que ela protege igualmente os dados empresarias, tanto os segredos de negócio como os dados identificadores. Porém, em uma leitura mais atenta, é possível entender que a legislação busca tutelar tão somente os dados pessoais, o que não necessariamente exclui os dados que possam igualmente dizer respeito a pessoas jurídicas (OLIVEIRA, 2020).

O Direito Penal, por exemplo, em alguns artigos busca proteger a vida (homicídio, Art. 121, CP) e, em outros, a propriedade (furto, Art. 151, CP). A Constituição em seus artigos. 5º, XIII, 6º e 7º, estabelece o trabalho como um fundamento da República, possuindo normas que proíbem trabalho infantil, forçado e com carga superior ao permitido em lei. Da mesma forma, Ricardo Oliveira e Márcio Cots asseveram:

> O principal bem jurídico resguardado pela LGPD é a privacidade. Ao contrário das pessoas jurídicas, as pessoas naturais (de carne e osso) se formam durante a vida e necessitam de ambiente propício para seu desenvolvimento, mas tal ambiente não é gerado por si mesmas. (...) A importância da privacidade para o desenvolvimento humano é atestada pelas grandes religiões da humanidade, pois, via de regra, há sempre momentos em que o retiro, seja para o deserto, seja para dentro de si mesmo, é essencial para a construção do ser humano e sua visão de si mesmo. (OLIVEIRA; COTS, 2020, p. 44)

A proteção da privacidade tem o intuito de proteger o desenvolvimento do ser humano. Desta forma, a LGPD ficou encarregada de preservar os dados pessoais das pessoas naturais, visando à tutela da privacidade destas, uma vez que pessoas jurídicas não gozam dessa proteção. De acordo com Palhares, Prado e Vidigal (2021), existem exceções no direito empresarial que muitas vezes confundem uma pessoa jurídica com uma pessoa física, criando vários dilemas para definir a abrangência do conceito de “titular de dados”.

Alguns exemplos são o Empresário Individual e do Microempreendedor Individual (MEI), que inúmeras vezes realizam o registro no Cadastro Nacional de Pessoas Jurídicas tão somente para fins tributários. Para estes casos, “exige-se o mesmo grau de cautela e conformidade com a LGPD que aqueles dados das pessoas naturais convencionais” (PALHARES; PRADO; VIDIGAL, 2021, p. 118).

É importante destacar o conceito de dado pessoal e de titular de dados elencados na lei de proteção de dados:

> Art. 5º Para os fins desta Lei, considera-se: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável; V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

É possível observar que a LGPD não trouxe um rol taxativo do que é um dado pessoal, de forma que a avaliação se determinada informação consiste ou não como um dado pessoal deve ser sempre feita de maneira contextual. (MALDONADO, 2019).

Como por exemplo, o número de matrícula de um funcionário sem nenhuma outra informação pode não representar algo, contudo, este número no contexto da organização facilmente leva a identificação de alguém, devendo este dado ser tratado nos termos da lei:

> No campo prático, o conceito de dado pessoal vai além daqueles dados comumente utilizados em cadastros (como nome, endereço, profissão, documentos de identidade) e, na maioria das vezes, inclui qualquer tipo de informação que possa ser útil à individualização de uma pessoa natural (física), como conjunto de hábitos, comportamentos, preferências, registros eletrônicos (inclusive dados de acesso e uso de internet). Trata-se portanto, de um conceito aberto, sendo praticamente impossível cravar se determinado dado é ou não pessoal sem a análise do contexto em que se insere. (PALHARES; PRADO; VIDIGAL, 2021, p. 117)

Quanto a propriedade dos dados, é válido dizer que ela não é transmitida do titular ao agente de tratamento, uma vez que o que o agente possui é apenas um direito de uso sobre os mesmos. Assim sendo, mesmo que uma empresa use de esforços para a coleta e manutenção de dados pessoais de acordo com a lei, os dados nunca serão somente dela, sendo a titularidade mantida na pessoa natural (OLIVEIRA, 2020).

A técnica legislativa utilizada na LGPD se adequou ao que diz respeito à sobrevida da lei ao tempo, pois ao invés de optar por uma lei restritiva e punitiva, o legislador elaborou uma lei principiológica. Considerando que a LGPD é uma lei que gera impacto no setor público e no privado, empresas diversas nas quais somente nos dias atuais possuíram as reflexões acerca da proteção de dados pessoais e ganharam especial atenção, a adoção de princípios pelo legislador foi a melhor opção para garantir a eficácia da lei. De acordo com a doutrina, os princípios podem ser entendidos como normas base para qualquer operação jurídica:

> [...] princípios, no plural, significam as normas elementares ou os requisitos primordiais instituídos como base, como alicerce de alguma coisa [...] revelam o conjunto de regras ou preceitos, que se fixam para servir de norma a toda espécie e ação jurídica, traçando, assim, a conduta a ser tida em qualquer operação jurídica [...] exprimem sentido mais relevante que o da própria norma ou regra jurídica [...] mostram-se a própria razão fundamental de ser das coisas jurídicas, convertendo-se em perfeitos axiomas [...] significam os pontos básicos, que servem de ponto de partida ou de elementos vitais do próprio Direito. (SILVA, 2001, p. 639)

Com a escolha por uma lei principiológica, a LGPD pode se tornar referência à produção de leis que vierem a ser promulgadas, que venham a tutelar hipóteses específicas, ou auxiliar na interpretação de outras normas que tenham como tema o tratamento de dados pessoais. Por mais que os princípios sejam norteadores da aplicação da lei, a jurisprudência europeia aponta que um número considerável das penalidades é tomado com base na violação destes (PALHARES; PRADO; VIDIGAL, 2021).

Conforme levantamento de sanções aplicadas pelas autoridades europeias, tem-se 160 multas aplicadas pela não observância de princípios, que somadas, podem chegar ao valor de mais de 780 milhões de euros. Os principais princípios que norteiam a LGPD são: a) princípio da boa-fé; b) princípio da finalidade; c) princípio da adequação; d) princípio da necessidade e; e) princípio da transparência.

Importante ressaltar que, com o advento da nova disciplina, o agente de tratamento é obrigado a encontrar ao menos uma legislação ou fundamento legal que

autorize sua atividade de tratamento. Destaca-se que a “base legal nada mais é do que um motivo justo e lícito, aos olhos da legislação para que os dados pessoais possam ser tratados” (PALHARES; PRADO; VIDIGAL, 2021, p. 144), assim, caso não seja possível enquadrar-se em nenhum dos fundamentos jurídicos, o mesmo deve ser imediatamente interrompido.

Quando o Marco Civil da Internet)e seu decreto eram considerados os principais normativos relacionados com a proteção de dados pessoais, tinha-se uma visão “consentimentocentrista”, em que o consentimento era a única forma que o controlador de dados pessoais era autorizado a realizar um tratamento. Com a LGPD, houve uma grande evolução quanto a este pensamento, tendo em vista que ampliou-se o rol de hipóteses autorizadoras ao tratamento de dados, fazendo com que a lei fosse aderente à realidade social. Assim abordou Bioni:

> É interessante notar que, na primeira versão do anteprojeto de lei colocada sob consulta pública em 2010, o consentimento era, em termos topográficos, a única base legal para o tratamento de dados pessoais. Isso se repetiu na segunda consulta pública em 2015, quando o que hoje são as demais bases legais da LGPD eram hipóteses nas quais o consentimento poderia ser dispensado. Após tais consultas públicas, o texto enviado ao Congresso Nacional, que depois veio a ser aprovado e sancionado, acabou por posicionar o consentimento como sendo uma das hipóteses legais e não na cabeça do dispositivo. Isso significa que, em termos de técnica legislativa, o consentimento não só deixou de ser a única base legal para o tratamento de dados, como também foi alocado topograficamente sem ser hierarquicamente superior às demais bases legais por estarem todos elas horizontalmente elencadas em incisos do art. 7º da LGPD. (BIONI, 2019, p.188).

Não obstante, o correto enquadramento do tratamento em uma base legal ainda é considerado um desafio, pois a doutrina nacional é fraca e a agência reguladora não emitiu pontuações neste sentido. Afim de contornar este problema, é possível identificar que os profissionais de proteção de dados buscam recorrer à doutrina europeia, para, então, garantir a conformidade de suas empresas/clientes.

Sendo assim, por mais que os dados estejam circulando no meio de redes sociais e afins, ainda existem problemas a serem combatidos, principalmente legislações a serem feitas para que se possa defender e guardar melhor ainda os dados de quaisquer pessoas que sejam.

CONCLUSÃO

Ao identificar o processo de construção da Lei Geral de Proteção de Dados, foi possível compreender que, antes desta legislação ser sancionada, ou antes de ela entrar em vigor, já existiam várias normas no ordenamento jurídico brasileiro acerca da proteção de dados pessoais, como por exemplo o próprio Código de Defesa do Consumidor, o Marco Civil da Internet, a Lei de Acesso à Informação, entre outras.

Ao analisar referidas leis, entendia-se que havia um quebra-cabeças, várias peças espalhadas, que não possuíam sintonia, sendo difícil poder agrupá-las. Assim, compreende-se que com a promulgação da nova lei, surgiu um impacto positivo, pois antes não era possível estruturar um sistema completo, mesmo havendo grande regulamentação acerca do assunto.

É possível concluir que por mais que haja várias leis setoriais de proteção de dados pessoais, elas representavam um grande emaranhado, tendo em vista que todas essas normas e regras estavam espalhadas, e faltando ainda a maior peça desse quebra-cabeça, que é a LGDP brasileira. Com isso, tornava-se possível ver todos os conceitos básicos condensados em uma única legislação, o que facilitava o trabalho de todos os órgãos e cidadãos que queriam estar em conformidade com as novas regras.

O objetivo é proporcionar mecanismos efetivos e capazes na manutenção de garantias relacionadas à vida privada, com a devida transparência neste processo. Com o entendimento acerca dos dados pessoais e sensíveis, possível é de se entender melhor a questão do consentimento.

A LGPD é regida por princípios que podem instigar a iniciativa pública e privada a transformar a internet em uma esfera mais democrática. Imprecisões, erros ou intrusões podem ocorrer, porém, observa-se que ainda assim, haverá mais proteção jurídica.

Desta forma, no caminho da previsibilidade, a segurança jurídica vem para preservar os direitos. É notório o desafio contínuo em relação aos obstáculos que as companhias acabam encontrando para obter coerência com a LGPD, desenvolvendo e renovando suas políticas de proteção e tratamento, a fim de manter em equilíbrio com o amparo legal estabelecido, além de sempre atualizar os termos legais que propõem para com as informações de seus usuários, como parâmetros no que se refere ao uso e ao período de obtenção de dados pessoais. Desta forma, as empresas deverão adequar-se o mais rápido possível, pois estarão lidando com direitos fundamentais.

REFERÊNCIAS

BESSA, Leonardo. **LGPD:** direito ou dever de privacidade? Conjur. Fevereiro de 2021. Disponível em: https://www.conjur.com.br/2021-fev-08/leonardo-bessa-lgpd-direito-ou-dever-privacidade. Acesso em: 01 jun. 2022

BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. Rio de Janeiro: Forense, 2018.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Portal da Legislação. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 05 jun. 2022.

BRASIL. **Lei Geral de Proteção de Dados** Pessoais (LGPD). Brasília, DF: Presidência da República, [2020]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/**lei**/l14020.htm. Acesso em: 20 out. 2022.

CANOTILHO, J. J. Gomes; MACHADO, Jónatas E. M. **Reality shows e liberdade de programação.** Coimbra: Coimbra, 2003. p. 57.

CANTELMO, Fernando. A Lei Geral de Proteção de Dados e o conflito entre direito de privacidade versus direito de informação e publicidade dos atos públicos: Noções legais sobre divergências constitucionais consolidadas pela LGPD. **Revista Jus Navigandi**, ISSN 1518-4862, Teresina, ano 26, n. 6609, 5 ago. 2021. Disponível em: https://jus.com.br/artigos/92061. Acesso em: 5 jun. 2022.

CASTRO, Catarina Sarmento e. **Direito da Informática, Privacidade e Dados Pessoais**. Coimbra: Almedina, 2005.

COÊLHO, Amanda Carmen Bezerra. **A Lei Geral de Proteção de Dados Pessoais Brasileira Como Meio de Efetivação dos Direitos da Personalidade**. Orientador: Alfredo Rangel Ribeiro. 2019. 52 f. Trabalho de Conclusão de Curso (Bacharelado em Direito) - Universidade Federal da Paraíba, João Pessoa, 2019.

CORRÊA, Ana Carolina Mariano. **Análise do consentimento na Lei de Proteção de Dados Pessoais no Brasil e sua aplicação no mundo jurídico.** Trabalho de conclusão de curso (Bacharelado em Direito) – Universidade Presbiteriana Mackenzie, São Paulo, 2019.

DONEDA, Danilo. **A proteção de dados pessoais como direito fundamental**, vol. 12, n° 2. Joaçaba: Espaço Jurídico, 2011.

DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais**. Rio de Janeiro: Renovar, 2006.

DONEDA, Danilo. **A proteção de Dados Pessoais como um Direito Fundamental.** Revista Espaço Jurídico, Joaçaba, v. 12, n. 2, p. 91-108, jul/dez. 2006. Disponível em: https://dialnet.unirioja.es/descarga/articulo/4555153.pdf. Acesso em: 12 set 2022.

JORNAL OFICIAL DA UNIÃO EUROPEIA. **Regulamentos.** 27 de abril de 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN

LIMA, Caio César Carvalho. **Marco Civil da Internet**: Garantia da privacidade e dados pessoais à luz do marco civil da internet. Organizadores: George Salomão e Ronaldo Lemos. São Paulo: Atlas, 2014.

MACHADO, José Mauro Decoussau; SANTOS, Matheus Chucri dos; PARANHOS, Mario Cosac Oliveira. **LGPD e GDPR**: uma Análise Comparativa entre as Legislações. São Paulo, 2018. Disponível em: http://www.pinheironeto.com.br/publicacoes/lgpd-e-gdpr-uma-analisecomparativa-entre-as-legislacoes. Acesso em: 10 set. 2022.

MALDONADO, Viviane. **A Lei Geral de Proteção de Dados:** objeto, âmbito de aplicação, requisitos, segurança e a necessidade de sua correta implementação. In: MALDONADO, Viviane (coord.). LGPD Lei Geral de Proteção de Dados Pessoais: Manual de Implementação. 5. ed. São Paulo: Thomson Reuters, 2019.

MALHEIRO, Luíza Fernandes. **O consentimento na proteção de dados pessoais na Internet:** uma análise comparada do Regulamento Geral de Proteção de Dados europeu e do Projeto de Lei 5.276/2016 / Luíza Fernandes Malheiro – Brasília/DF, 2017.

MENDES, Gilmar Ferreira (et al). **Curso de Direito Constitucional**. São Paulo: Ed. Saraiva, 2008.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor:** linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MENDES, Laura Schertel. **Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo**. Departamento de Pós-Graduação Unb. Brasília, 2008.

MENDONÇA, Renata. **Como os testes de Facebook usam seus dados pessoais - e como empresas ganham dinheiro com isso**. 2018. Disponível em: http://www.bbc.com/portuguese/salasocial-43106323

NOVAIS, Jorge Reis. **Renúncia a direitos fundamentais.** In: Miranda, Jorge (Org.). *Perspectivas constitucionais*: nos 20 anos da Constituição de 1976. Coimbra: Coimbra, 2006, p. 286.

OLIVEIRA, Ricardo. COTS, Márcio Cots. **O LEGÍTIMO INTERESE E A LGPD**: Lei Geral de Proteção de Dados Pessoais. 2ª. ed. São Paulo: Thomson Reuters, 2020.

PALHARES, Felipe; PRADO, Luis; VIDIGAL, Paulo. **COMPLIANCE DIGITAL E LGPD.** 1ª. ed. Brasil: Thomson Reuters, 2021.

RUARO, Regina Linden; Rodrigues Daniel Pinheiro; FINGER, Brunize. **O direito à proteção de dados pessoais e a privacidade.** Revista da Faculdade de Direito UFPR, Curitiba, PR. V. 53, jun. 2011.

SILVA, De Plácido. **Vocabulário Jurídico**. 18 ed. Rio de Janeiro: Forense, 2001.

SOUZA, Thiago Pinheiro Vieira de. **A proteção de dados pessoais como direito fundamental e a [in]civilidade do uso de cookies.** Trabalho de Conclusão de Curso (Bacharelado em Direito) – Universidade Federal de Uberlândia, Minas Gerais, 2018.

VENOSA, Sílvio de Salvo. **Direito Civil:** Parte Geral. 16ª ed. São Paulo: Atlas, 2016