FACULDADE DE DIREITO DE VITÓRIA
CURSO DE GRADUAÇÃO EM DIREITO

FERNANDA GOMES SALUME

PROTEÇÃO DE DADOS PESSOAIS NO CONTEXTO DA LEI GERAL DE PROTEÇÃO DE DADOS: ANÁLISE DA RESPONSABILIDADE ESTATAL.

VITÓRIA
2021

FERNANDA GOMES SALUME

PROTEÇÃO DE DADOS PESSOAIS NO CONTEXTO DA LEI GERAL DE PROTEÇÃO DE DADOS: ANÁLISE DA RESPONSABILIDADE ESTATAL.

Trabalho de Conclusão de Curso apresentado ao Curso de Direito da Faculdade de Direito de Vitória – FDV, como requisito parcial para obtenção do título de bacharel em Direito, orientada pela professora Me. Ivana Bonesi Rodrigues Lellis.

VITÓRIA

2021

SUMÁRIO

RESUMO

O reconhecimento dos direitos da personalidade e a tentativa de proteção dos dados pessoais no direito internacional, foi expressamente garantido no direito brasileiro com a promulgação da Constituição Federal de 1988. Consolidando essa proteção de forma mais específica, o Brasil aprovou a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) que dispõe sobre o tratamento de dados pessoais nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado. Pode-se aferir que embora o termo de consentimento do titular seja imprescindível em determinadas finalidades, ele não é sempre exigido, desse modo, faz-se necessário distinguir as práticas legitimas das abusivas. Nessa toada, na perspectiva dos direitos fundamentais, a limitação do uso de dados pessoais pela LGPD respeita o princípio da dignidade da pessoa humana, especialmente, no tocante à proteção dos direitos à liberdade, privacidade e personalidade intrínsecos ao ser humano. Portanto, é imprescindível que a Administração Pública se adeque a LGPD, embora o Estado, nas figuras da administração direta ou indireta, goze de tratamento diferenciado, enquanto controlador de dados pessoais, sendo-lhe asseguradas algumas prerrogativas não permitidas aos entes privados.

INTRODUÇÃO

O tratamento autônomo da proteção de dados pessoais no Brasil tornou-se necessário na medida em que as relações sociais se moldaram em uma nova forma de organização, marcada por um fluxo informacional que não encontra objeções físicas distanciais. Sendo maior sua maleabilidade e utilidade, cada vez mais ela se torna elemento fundamental de um crescente número de relações e aumenta sua possibilidade de influir no cotidiano.

É inegável que as informações pessoais, cedidas a empresas e estabelecimentos, são comercializadas livremente e em larga escala no mercado, de forma a identificar padrões de consumo e registrar as atividades realizadas pelos consumidores. Ainda,

os dados coletados são utilizados como capital e moeda do mercado, sendo que o valor desses dados nunca foi tão subestimado pela sociedade que os fornece.

Informações sobre preferências de consumo, uso de telecomunicações, aplicativos, histórico de crédito, hábitos ao assistir a televisão e navegar na internet, são armazenados sistematicamente no banco de dados e são transformados em informações úteis para tomada de decisões mercadológicas a longo prazo. Por exemplo, é muito comum que organizações se associem, visando ao compartilhamento e cruzamento de dados pessoais.

Nessa sentido, embora o indivíduo tenha direito à autodeterminação informativa através da qual ele tem autonomia para autorizar, ou não, o fluxo dos seus dados pessoais, de modo a controlá-los; evidencia-se um desequilíbrio entre as entidades ou órgãos que coletam e processam os dados e o individuo que os fornece, por isso, medidas que meramente reconhecem o direito à autodeterminação informativa não parecem suficientes para solucionar a questão.

Diante disso, o presente trabalho busca analisar e compreender quais são as consequências do tratamento e disponibilização dos dados pessoais e sensíveis coletados, bem como verificar a responsabilidade do Estado na observância dos princípios da publicidade e transparência, conectados ao direito à informação, frente ao direito à privacidade e os direitos da personalidade.

1. CONTEXTO LEGISLATIVO PRÉ LEI GERAL DE PROTEÇÃO DE DADOS

O marco inicial da compreensão da necessidade de proteção do fluxo informacional tecnológico se deu após a Segunda Guerra Mundial, através das *guidelines,* da Organização para a Cooperação e Desenvolvimento Econômico (OCDE), que estabeleciam padrões normativos para a proteção dos dados pessoais, a fim de assegurar o livre fluxo de informações entre os países-membros.

Em 1980, uma das problemáticas enfrentadas pelos países-membros era o processamento dos dados pessoais, e, diante do desenvolvimento econômico e social, era imprescindível ponderar os eventuais conflitos entre a proteção dos direitos da personalidade com os avanços da tecnologia da informação.

Desta forma, a OCDE emitiu dois documentos, *privacy guidelines* em 1980 e *declaration on transborder data flows* em 1985, que vinculavam os países- membros a adoção dos princípios previstos, além disso, fomentaram o desenvolvimento da proteção dos dados pessoais mundialmente. Em síntese, Bruno Bioni (2019, p. 115) alude:

> Trata-se de normas que elevam o próprio titular dos dados pessoais como o seu grande protagonista. A própria noção do que seja um tratamento de dados pessoais justo e lícito é vinculada ao consentimento do indivíduo.

Para além disso, a Convenção 108, da década de 1980, de Strasbourg, do Conselho da Europa e União Europeia, é resultado do movimento promovido pela OCDE que propiciou a compatibilização das legislações de proteção de dados, entre os países-membros. À luz disso, Bruno Bioni (2019, p. 118) revela:

> A diretiva europeia irá adjetivar o consentimento na tentativa de operacionaliza-lo, a sua qualificação como devendo ser livre, informado, inequívoco, explícito e/ou específico é uma das características marcantes do progresso geracional das leis de proteção de dados pessoais, na medida em que procura resolver a problemática em torno do controle ilusório ou pouco efetivo das informações pessoais por parte do seu titular e quem as processa.

O cenário acima delineado, marcado, inicialmente, pelo reconhecimento dos direitos da personalidade e a tentativa de proteção dos dados pessoais no direito internacional, foi transportado para o Brasil com a promulgação da Constituição da República Federativa do Brasil de 1988, têm-se início uma nova etapa de conquista dos cidadãos brasileiros com a consagração expressa de uma gama variada de direitos fundamentais individuais e coletivos.

Os direitos fundamentais são o resultado da personalização e positivação constitucional de determinados valores básicos e decisões essenciais que

caracterizam sua fundamentalidade, assim, servem como parâmetro para o controle dos atos normativos estatais (SARLET, 2017).

Em síntese, destaca-se a ponderação feita por Daury Cesar Fabriz (2008, p. 227): “A Constituição, nesse cenário, se revela como uma esfera pública, na qual as práticas quotidianas, ao se firmarem, passam a firmar os seus comandos, que, por sua natureza, devem ser notados em sua incompletude”.

No paradigma do Estado Democrático de Direito, acentua-se a importância da tutela dos direitos fundamentais em apreço, visando a assegurar as garantias à liberdade (art. 5, IX da CF/88) e o direito à informação (art. 5, XIV da CF/88), que deverão ser equacionados com a proteção do direito à privacidade (art. 5, X da CF/88) e com o livre desenvolvimento da personalidade da pessoa natural.

Nesse sentido, cabe pontuar que o direito não tem o condão de impor condutas ao psiquismo humano, bem como não pode obrigar o indivíduo a pensar, agir ou nutrir sentimentos em um determinado sentido; mas pode corrigir as distorções nas relações jurídicas e vincular os atores sociais ao respeito à norma jurídica. (DUQUE, B. L.; PEDRA, A. S., 2013, p. 153).

Na legislação infraconstitucional, a proteção dos dados pessoais teve seu destaque no Código de Defesa do Consumidor, consubstanciado na Lei 8.078/90, que no seu artigo 43 estabeleceu uma série de direitos e garantias para o consumidor em relação às suas informações pessoais presentes em “banco de dados e cadastros” (DONEDA, 2011, p. 103). À luz disso, Laura Schertel Mendes (2018) aponta:

> O direito básico do consumidor a proteção de dados pessoais envolve uma dupla dimensão: a tutela da personalidade do consumidor contra os riscos que ameaçam a sua personalidade em face da coleta, processamento, utilização e circulação dos dados pessoais e a atribuição ao consumidor da garantia de controlar o fluxo de seus dados na sociedade.

Concomitantemente, o artigo 51, parágrafo primeiro e seus incisos da referida lei, ao abordar as cláusulas abusivas, em complemento à dignidade da pessoa humana, a promoção do bem estar geral, sem discriminações de qualquer tipo (art. 3, IV da CF/88), proíbem a existência de discriminações ou a busca de fins discriminatórios

ilícitos ou abusivos, com fundamento em religião, origem étnica, vida sexual, opinião política, dentre outros, no tratamento dos dados pessoais.

Como regra geral, a matéria atinente a proteção dos dados pessoais é tipicamente ligada ao mercado de consumo, dessa forma, em primeiro momento pensa-se no Código de Defesa do Consumidor, mas isso não impede que seja realizado um diálogo de fontes, utilizando também as normas do Código Civil para regular a obtenção e o tratamento dos dados pessoais.

O Código Civil ao abordar os direitos da personalidade (art. 12 do CC) elenca um rol exemplificativo, o que abre caminhos para o reconhecimento da proteção dos dados pessoais como um novo direito da personalidade. Dessa forma, os direitos da personalidade não representam somente uma inovação no ordenamento jurídico brasileiro, trata-se também, de um componente central de uma nova hermenêutica que coloca o ser humano como o "coração do direito civil contemporâneo". (BIONI, 2019, p. 51)

Ademais, consolidando a opção do legislador em adotar a autodeterminação informativa no nosso ordenamento, a temática encontra respaldo na Lei do Cadastro Positivo (Lei nº 12.414/2011), na medida em que sistematiza a formação do banco de dados atinente à capacidade financeira e ao histórico de adimplemento para fins de concessão de crédito, garantindo ao titular dos dados pessoais o direito de gerenciá-los.

Em termos gerais, embora a Lei do Cadastro Positivo autorize a abertura de cadastro (art. 4º, I, da LCP) de forma automática, podendo ser realizada pelo próprio gestor, o titular dos dados pessoais tem a possibilidade de requerer a exclusão dos seus dados do banco de dados. Ainda, a referida lei impõe limites ao gestor da base de dados, na forma do artigo art. 3º, § 3º, incisos I e II, de modo coibir a coleta de informações excessivas e sensíveis para análise de crédito, além de vedar a utilização para outra finalidade que não a creditícia (art. 5º, VII, da LCP).

Nesse contexto, a tendência do direito brasileiro, consagrada no artigo 43 do Código de Defesa do Consumidor e na Lei do Cadastro Positivo, seguia o sentido de

disciplinar, especialmente, os bancos de dados relativos a informações de crédito, não se ocupando com as outras formas de coleta e tratamento de dados pessoais.

Contudo, a edição da lei 12.965/2014, conhecida como Marco Civil da Internet (MCI), trouxe definições importantes acerca das regras gerais de proteção de dados, mesmo que aplicáveis somente em relação ao fluxo de informações na Internet. Dessa forma, Bruno Bioni (2019, p.124) pondera:

> O Marco Civil da Internet procurou, de forma principiológica, assegurar os direitos e garantias do cidadão no ambiente eletrônico, sendo o seu traço marcante a distância de uma técnica normativa prescritiva e restritiva das liberdades individuais, própria do âmbito criminal, que poderia ter efeitos inibitórios para a inovação e a dinamicidade da internet.

Importa destacar que a proteção de dados pessoais é fixada como princípio da disciplina do uso da internet e dentre os direitos previstos, encontra-se a proteção da privacidade e dos dados pessoais, na forma do artigo 3º, incisos II e III, do MCI. Para além disso, o artigo 7º, incisos VI, VIII, IX e XI, pontuam a necessidade do consentimento do usuário para a coleta, o uso, o armazenamento e o tratamento dos dados pessoais, qualificando o consentimento como livre, expresso e informado.

Diante disso, no que tange a ideia da liberdade de contratar, Enzo Roppo (2009, p. 34) elucida que:

> Na sociedade moderna as relações tendem a ser, cada vez mais, fruto de uma escolha livre dos próprios interessados, da sua iniciativa individual e da sua vontade autônoma, que encontra no contrato o seu símbolo e seu instrumento de atuação, de modo que os contraentes interessados devem, na sua soberania individual de juízo e de escolha, decidir e estipular um certo contrato, determinando com plena autonomia o seu conteúdo.

Assim, a “Teoria da Vontade Declarada”, de Enzo Roppo, assegura que para que um contrato seja considerado juridicamente relevante e produza seus efeitos jurídicos, é necessário que a vontade seja socialmente conhecida, isto é, manifestadamente declarada (ROPPO, 2009, p. 93). Desta forma, seguindo a lógica contratual, o titular dos dados pessoais assume o papel de protagonista, sendo responsável por controlar e autoproteger as suas informações pessoais.

Atualmente, a proteção de dados pessoais tem sido compreendida como o direito de o indivíduo autodeterminar as suas informações pessoais, fazendo com que, por meio da vontade manifestadamente declarada, o cidadão emita autorizações sobre o fluxo dos seus dados pessoais, controlando-os.

Em verdade, sustenta-se hoje o modelo normativo no qual a força obrigatória do contrato repousa na expressão livre e concreta das partes, na medida em que o pensamento jurídico identifica na vontade não apenas um elemento essencial do contrato, mas precisamente a razão de ser da sua força obrigatória (NEGREIROS, 2006, p. 219).

À luz disso, temos o direito à autodeterminação informativa, na medida em que as normas de proteção de dados pessoais procuram assegurar a participação do titular das informações. Nesse sentido, Laura Schertel Mendes (2008, p. 49) pondera:

> Para que o indivíduo possa exercer o seu poder de autodeterminação informativa, faz- se necessário um instituto jurídico por meio do qual se expresse a sua vontade de autorizar ou não o processamento de dados pessoais: o consentimento. Este é o mecanismo que o direito dispõe para fazer valer a autonomia privada do cidadão, o consentimento não representa a ausência de interesse do indivíduo na tutela dos dados pessoais, mas, constitui um ato de escolha no âmbito da autodeterminação individual.

Entretanto, a autodeterminação informacional carrega consigo a problemática do controle ilusório ou pouco efetivo, por parte do titular, em torno da movimentação das suas informações pessoais, na medida em que as relações sociais se moldaram em uma nova forma de organização, marcada por um fluxo informacional que não encontra óbices físicos distanciais.

Diante disso, ressalta-se que boa parte das informações que livremente se expõe fica armazenada em plataformas digitais de comunicação digital, assim, não é possível controlar a reprodução e o acesso posterior a elas, ocorrendo uma fusão das fronteiras entre o público e o privado, perde-se a autodeterminação informativa, o direito ao esquecimento e a possibilidade de resguardar a privacidade (PINHEIRO, V. S.; BONNA, A. P., 2020, p. 368).

Isto porque, a coleta, o processamento, o uso e a transmissão dessas informações, em particular por processos automatizados, é uma atividade de risco que se concretiza na possibilidade da exposição e utilização indevida ou abusiva dos dados coletados. Sob essa perspectiva, Bruno Bioni (2019, p. 72) lista seis fatores de risco: o volume dos dados, a natureza dos dados, a cadeia da atividade de tratamento de dados, gerenciamento de identidades e segmentação, cláusulas contratuais e atualização contínua.

Na sociedade atual, as oportunidades e a participação social estão condicionadas ao fornecimento de dados pessoais, de modo que, para fazer parte das relações, deve-se concordar com os termos contratuais que impõem um cheque em branco no que se refere à utilização dos dados pessoais. Dada esta dinâmica contratual, os usuários não têm poder de barganha para colocar em curso as suas preferencias de privacidade. (BIONI, 2019, p. 157).

Em verdade, pode-se aferir que a igualdade se apresenta como um princípio ameaçado, na medida em que a vigilância realizada por organismos privados e estatais, a partir de informações obtidas em bancos de dados, pode acarretar a classificação e a discriminação dos indivíduos, afetando expressivamente as suas oportunidades sociais (MENDES, 2008, p. 58).

Desta forma, evidencia-se um desequilíbrio entre as entidades ou órgãos que coletam e processam os dados e o individuo que os fornece, por isso, o mero reconhecimento do direito à autodeterminação informativa não é suficiente para solucionar a questão. Tal constatação fundamenta-se nas dificuldades acima mencionadas, assim, entende-se melhor evitar a transposição do consentimento negocial, aplicado aos mecanismos contratuais tradicionais, à disciplina da proteção de dados (DONEDA, 2006, p. 376).

2. A LEI GERAL DE PROTEÇÃO DE DADOS, ANÁLISE DOS DIREITOS À LIBERDADE, PRIVACIDADE E PERSONALIDADE, DIANTE DA UTILIZAÇÃO DE DADOS PESSOAIS

Diante do cenário exposto, o Brasil aprovou a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) que dispõe sobre o tratamento de dados pessoais nos

meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Nessa toada, elementos como consentimento informado e legítimo interesse, além do princípio da finalidade, por exemplo, são parâmetros utilizados para preservar a autonomia da vontade e o controle, pelos cidadãos, do uso dos dados e informações a seu respeito. À luz disso, é interessante ressaltar o que pontuou Bruno Bioni (2019, p. 127):

> Na primeira versão do anteprojeto de lei, colocada sob consulta pública em 2010, o consentimento era a única base legal para o tratamento de dados pessoais. Isso se repetiu na segunda consulta publica em 2015, quando o que hoje são as demais bases legais da LGPS era 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 a 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.

Assim, o consentimento livre, informado, inequívoco e explícito do titular dos dados, é uma das hipóteses que legitimam o tratamento de dados pessoais, conforme art. 7º, inciso I da LGPD. Ainda, o art. 8º, §5º da referida lei estabelece que "o consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação".

Cabe pontuar, ainda, que o consentimento pode ser considerado nulo, na forma do art. 9º, §1º da LGPD, quando a informação sobre o tratamento de dados não for apresentada previamente de forma clara, transparente e inequívoca, ou quando a informação prestada tenha conteúdo enganoso ou abusivo.

Pelo exposto, pode-se aferir que embora o termo de consentimento do titular seja imprescindível em determinadas finalidades (art. 8º, §4º da LGPD), ele não é sempre exigido, na medida em que o art. 7º e o art. 11, inciso II, ambos da LGPD preveem

hipóteses em que o consentimento é dispensado, tanto para o tratamento de dados pessoais ordinários (art. 5º, I da LGPD) quanto para o de dados pessoais sensíveis (art. 5º, II da LGPD).

Ressalta-se que a LGPD disciplina hipóteses de não aplicabilidade, previstas no seu artigo 4º, como também estabelece a possibilidade de tratamento de dados anônimos para fins estatísticos, nos termos do artigo 5º, inciso III da referida lei, relativos “a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento”, na medida em que não são considerados dados pessoais (art. 12 da LGPD).

Portanto, além do consentimento livre e previamente informado do titular, o controlador de dados deverá atuar com boa-fé, em conformidade com os princípios que norteiam a atividade de tratamento de dados pessoais, sendo eles: o princípio da transparência, o princípio da exatidão, o princípio da finalidade, o princípio do livre acesso e o princípio da segurança.

O princípio da transparência indica que a existência de um banco de dados pessoais deve ser de conhecimento público. Já o princípio da exatidão se refere a exigência de que as informações de um banco de dados reflitam a realidade. Outro princípio relevante é o da finalidade, ele indica a correlação necessária existente entre o tratamento dos dados pessoais e a finalidade comunicada ao titular na coleta dos dados. Quanto ao princípio do livre acesso, ele assegura ao interessado a disponibilidade dos dados armazenados. Por fim, o princípio da segurança refere-se à exigência de proteção do banco de dados contra desvios não autorizados pelos interessados. (MENDES, 2008, p. 56)

Nesse sentido, no que se refere ao principio da boa-fé contratual, Teresa Negreiros (2.206, p. 117) pondera:

> A fundamentação constitucional do principio da boa-fé assenta na clausula geral de tutela da pessoa humana – em que esta se presume parte integrante de uma comunidade, e não um ser isolado, cuja vontade em si mesma fosse absolutamente soberana, embora sujeira a limites externos. Mais especificamente, é possível reconduzir o principio da boa-fé ao ditame constitucional que determina como objetivo fundamental da República a

> construção de uma sociedade solidária, na qual o respeito pelo próximo seja um elemento essencial de toda e qualquer relação jurídica.

Para além disso, destaca-se que o artigo 5º, inciso VI da LGPD, conceitua o controlador de dados como uma "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais", dessa forma, é o responsável pelas decisões atinentes ao processamento dos dados pessoas, devendo orientar corretamente o operador que irá realizar o tratamento das informações coletadas.

O controlador tem o dever de garantir ao titular dos dados a comunicação e a transparência das informações, além disso, tem responsabilidade sobre o operador, na medida em que responde solidariamente pelos prejuízos causados ao titular, se do tratamento resultar danos patrimoniais, morais, individuais ou coletivos.

Como visto, os maiores riscos do tratamento de dados dos consumidores pelas empresas referem-se a violação da igualdade, como a discriminação no mercado de consumo em razão de dados sensíveis, e da liberdade, quando ocorre a limitação do acesso a bens e serviços a partir de informações incorretas (MENDES, 2008, p. 119).

Desta forma, cabe ressaltar que o princípio da não discriminação é um dos mais importantes, no que se refere ao tratamento de dados sensíveis, na medida em que é ponto fundamental diante do uso de dados sensíveis potencialmente lesivos, em decorrência de sua capacidade discriminatória, seja por entes privados ou por entes públicos (MULHOLLAND, 2018, p. 166).

Ainda, no que tange ao tratamento dos dados pessoais, vale destacar o que elucida Priscilla Regan (2002, p. 387):

> Em uma sociedade de risco, qualquer instituição que lida com um indivíduo coleta informações desse indivíduo e sobre as suas atividades. A sociedade de risco requer a vigilância como forma de gerenciar o risco. Mas a vigilância gera uma insaciável sede de mais e mais informações sobre riscos que existem e que são gerados pelos indivíduos em particular. O conhecimento gerado pelo sistema de vigilância não gera uma sensação de segurança e de confiança, mas produz, ao invés, novas incertezas, acarretando mais vigilância e coleta de informações.

Importa destacar que a coleta massiva de informações sobre os hábitos e os comportamentos dos consumidores molda as relações de consumo, na medida em que as empresas adquirem a capacidade de ofertar produtos especializados, singularizados e direcionados ao perfil do consumidor desejado. À luz disso, Laura Schertel Mendes (2008, p. 80) afirma:

> O tratamento de dados pessoais pelas empresas privadas objetiva atingir, principalmente, as seguintes finalidades no mercado: i) previsibilidade e diminuição de riscos, ii) fidelização e interação com o consumidor, iii) diferenciação de produtos e iv) diferenciação de serviços.

Sob essa perspectiva, o princípio da vulnerabilidade é um dos mais relevantes consagrados pelo CDC, na medida em que reconhece o estado de risco e fragilidade do sujeito de direitos inserido no mercado de consumo que propicia o acesso desigual à informação, isto porque, o consumidor possui menos informações que o fornecedor a respeito do fluxo de seus dados.

Concomitantemente, vale destacar que o direito contratual assegura a proteção do contratante vulnerável frente à disparidade de poder negocial e condição de barganha contratual, nesse sentido, Teresa Negreiros (2006, p. 307) afirma:

> Com efeito, as inovações no direito contratual contemporâneo, refletidas sobretudo na legislação de proteção ao contratante vulnerável, transformaram o juízo acerca da validade do contrato num juízo voltado não apenas para o processo de formação e de manifestação da vontade geradora do vinculo contratual, mas igualmente voltado para o efetivo resultado produzido pelo acordo de vontades. Nesse sentido, diz-se que o contrato se materializou, reconhecendo-se, como nunca, a relevância jurídica do seu conteúdo.

Nessa toada, o fluxo de dados pessoais representa um dever de vigilância constante na nossa sociedade, por isso, faz-se necessário aludir o modo como é realizado o tratamento dos dados pessoais, de modo a distinguir as práticas legítimas das abusivas, visando à preservação dos direitos fundamentais (MENDES, 2008, p. 86).

Portanto, conforme artigo 5º, X da LGPD, o tratamento das informações pessoais envolve a coleta, o registro, a organização, a conservação, a adaptação ou a alteração, a recuperação, a consulta, a utilização, a comunicação por transmissão, a difusão e a comparação, como também o bloqueio, o apagamento ou a destruição.

Diante da extensão das atividades que envolvem o processamento de dados pessoais e, por consequência, sofrerão a limitação da Lei Geral de Proteção de Dados, pode-se aferir que o integral cumprimento das obrigações asseguradas pela Lei requer a observação do imperativo de vigilância em todas as fases atribuídas ao processamento das informações armazenadas nos bancos de dados, de modo que só é possível cumprir ou descumprir integralmente os deveres legais impostos.

2.1 DOS DIREITOS À LIBERDADE, PRIVACIDADE E PERSONALIDADE

A Lei Geral de Proteção de Dados Pessoais visa à garantia dos direitos fundamentais de liberdade, de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Desta forma, o artigo 2º da LGPD estabelece que a proteção de dados tem como fundamentos: o respeito à privacidade; a autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

À luz disso, João Carlos Zanon (2013, p. 160) pondera que:

> O direito à proteção dos dados pessoais, como direito fundamental, possui duas dimensões: uma subjetiva (status negativo) ao delimitar uma esfera de proteção que não pode sofrer intervenção indevida do poder estatal ou privado, exigindo a abstenção do Estado nesse âmbito; e, também, uma dimensão objetiva (status positivo), na medida em que reclama ações do Estado para garantir tal proteção.

Com efeito, a proteção de dados pessoais garantida pela LGPD é um direito fundamental de status positivo, na medida em que o Estado tem o dever de criar

políticas públicas e estabelecer órgãos públicos competentes para fiscalizar o tratamento de dados pessoais.

Nessa toada, na perspectiva dos direitos fundamentais, a limitação do uso de dados pessoais pela LGPD respeita o princípio da dignidade da pessoa humana, especialmente, a proteção dos direitos à liberdade, privacidade e personalidade intrínsecos ao ser humano.

O princípio da dignidade da pessoa humana salvaguarda todos os direitos individuais, sendo o principio estruturante do sistema constitucional e do Estado Democrático de Direito, na forma do art. 1º, inciso III da Constituição Federal, para a interpretação adequada dos direitos e garantias conferidos ao cidadão brasileiro. Em outras palavras, é o Estado que passa a servir como instrumento para o reconhecimento, respeito, proteção, promoção e desenvolvimento da dignidade das pessoas (SARLET, 2017, p. 340).

Nesse sentido, o direito à liberdade conjuntamente com vida, igualdade, propriedade e segurança constituem um conjunto de direitos que fundamentam a própria República. Assim, no que se refere à proteção de dados, a garantia à liberdade pretende manter sob a tutela do indivíduo a decisão de compartilhar tais dados e em qual extensão, de modo que o acesso e disposição desses dados pessoais a terceiros encontra-se na órbita de poder individual.

Sob essa perspectiva, Rizzatto Nunes (2018, p. 48) aduz:

> aplicado o conceito à realidade social, o que se tem é o fato de que o objetivo constitucional da construção de uma sociedade livre significa que, sendo a situação real de necessidade, o Estado pode e deve intervir para garantir a dignidade humana.

Concomitantemente, o direito à privacidade é assegurado expressamente no artigo 5º, inciso X da CF/88, ao estabelecer que: “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação.” Nesse sentido, a gravidade da violação ao direito à privacidade não está necessariamente ligada ao grau de intimidade ou de

segredo da informação armazenada, mas, principalmente, do seu potencial discriminatório.

Aplicado à LGPD, mais especificamente nos casos de dados sensíveis, o referido direito garante ao cidadão a prerrogativa de negar a divulgação de informações a respeito de sua vida pessoal, protegendo a privacidade do indivíduo em face do desenvolvimento tecnológico que propicia o compartilhamento e a sistematização das informações pessoais, de modo que não ocorram violações ao direito.

Ante o exposto, importa destacar a lição de José Joaquim Gomes Canotilho e Vital Moreira (2007, p. 467) quando sustentam que:

> O direito à reserva da intimidade da vida privada e familiar analisa-se principalmente em dois direitos menores: (a) o direito a impedir o acesso de estranhos a informações sobre a vida privada e familiar e (b) o direito a que ninguém divulgue as informações que tenha sobre a vida privada e familiar de outrem. Alguns outros direitos fundamentais funcionam como garantias deste: é o caso da proibição de tratamento informático de dados referentes à vida privada.

Assim como o direito à liberdade e à privacidade, o direito ao livre desenvolvimento da personalidade torna-se ameaçado no âmbito virtual, na medida em que o processamento de dados pessoais mapeia e armazena os hábitos e as características dos indivíduos, transmitindo suas preferências e afazeres, de modo a utilizar essas informações para gerar receita própria. Nesse contexto, cabe ressaltar a análise feita por Ingo Wolfgang Sarlet (2017, p. 566):

> Ressalta-se o nexo entre o direito de liberdade pessoal e a proteção da personalidade, posto que o direito de personalidade, embora tenha por objeto a proteção contra intervenções na esfera pessoal, é também um direito de liberdade, no sentido de um direito de qualquer pessoa a não ser impedida de desenvolver sua própria personalidade e se determinar de acordo com suas opções. Como direitos fundamentais, encontram-se, em geral, submetidos ao mesmo regime jurídico, com destaque para os aspectos relacionados com sua titularidade, destinatários e proteção contra intervenções por parte do Estado e de terceiros.

Em termos gerais, diante da universalização da conexão, o fluxo informacional tornou-se elemento fundamental de um crescente número de relações, aumentando sua possibilidade de influir no cotidiano. Por isso, a facilidade de acesso aos dados

pessoais pode resultar em violação dos referidos direitos fundamentais, à liberdade, privacidade e personalidade, cujo uso e disposição cabem somente ao seu titular.

Para Zygmunt Bauman (2008, p. 76) o “objetivo do consumo na sociedade de consumidores é a modificação ou recomodificação do consumidor, ou seja, elevar a condição dos consumidores à de mercadorias vendáveis”. Na lógica da comercialização dos dados pessoais, as informações particulares dos consumidores são tidas como insumo da economia, com elevado potencial lucrativo atribuído, formando um caminho de discriminação sistematizado na bolha de algoritmos.

Nas palavras de Tânia Carolina Gonçalves (2019, p. 35) os algoritmos seriam mais especialistas no conhecimento de um indivíduo do que ele próprio,

> As pessoas, com isso, passariam a ter suas vidas constantemente monitoradas e guiadas por uma rede de algoritmos eletrônicos criados para, em tese, proporcionar uma experiência ou qualidade de vida melhor. Para que isso se concretize, não há necessidade de um algoritmo externo que me conheça perfeitamente e que nunca cometa nenhum erro; basta que esse algoritmo me conheça melhor do que eu me conheço e que cometa menos erros do que eu. Então fará sentido confiar a eles cada vez mais decisões e escolhas na vida.

Esta organização e direcionamento a partir dos algoritmos faz com que o indivíduo seja monitorado e esteja vinculado aos conteúdos baseados nas informações coletadas, cerceando a sua liberdade de escolha do que deseja ver, ler, consumir, discutir e se posicionar, na medida em que há um juízo de valor externo acerca das suas preferências e o direcionamento do seu desejo de consumo e opiniões publicas, a partir de uma leitura superficial e automatizada.

Esse cenário demonstra uma flagrante violação da dignidade humana e do direito à liberdade de escolha e desenvolvimento da personalidade, que, por vezes, podem ser definitivos, tendo em vista a complexidade humana e a redução do indivíduo ao filtro que o algoritmo impõe. Nesse sentido cabe destacar a ponderação feita por Laura Schertel Mendes (2008, p. 94), vejamos:

> É interessante observar como o ambiente virtual é propenso às violações da privacidade, de uma forma mais imperceptível e silenciosa que o ambiente físico. Isso porque o espaço físico possibilita a constatação mais nítida do nível de privacidade disponível e permite que a pessoa tome as decisões a fim de aumentar ou diminuir a sua privacidade, o que nem sempre é possível no espaço virtual, vez que não se sabe quais informações estão sendo capturadas, nem o momento em que esse controle é realizado.

Portanto, com a participação social condicionada ao fornecimento de dados pessoais e a exposição da pessoa ao ambiente virtual, a Lei Geral de Proteção de Dados reconhece a proteção de dados como direito identicamente protegido os atributos inerentes da personalidade e da dignidade humana, reconhecidos pela Constituição como direitos fundamentais.

3 POSSIBILIDADE DA SUJEIÇÃO DA ADMINISTRAÇÃO PÚBLICA À LGPD

A Administração Pública sempre teve um papel de destaque no que tange o acesso à informação, isto porque o Estado foi e é responsável por criar a cultura de estatística dos cidadãos, com a coleta dos dados do censo demográfico e educacional, que contém informações sobre idade, nível de renda, raça, etnia, gênero e localização geográfica, dos programas de assistência social, do uso da biometria e do reconhecimento facial para identificação, tanto nos órgãos públicos como nos aplicativos do governo.

Para além disso, o Poder Público é um empregador em massa e controla, mesmo que indiretamente, o acesso aos órgãos e departamentos públicos, a vida financeira, o acesso à saúde, eventuais processos judiciais, dados educacionais, dados trabalhistas do cidadão e de seus funcionários, entre outros (ROSSO, 2019).

Na forma do artigo primeiro da Lei Geral de Proteção de Dados, esta se aplica às pessoas naturais e as pessoas de direito público e privado, estabelecidas no Brasil ou que oferecem produtos e serviços ao mercado brasileiro, na medida em que coletam e tratam dados de pessoas que estejam no país. Para além disso, o paragrafo único do referido artigo assegura a necessidade de todos os entes da federação observarem as disposições contidas na lei.

Nessa toada, é imprescindível que a Administração Pública se adeque a LGPD, embora o Estado, na administração direta ou indireta, possui prerrogativa de tratamento diferenciado, enquanto controlador de dados pessoais, permitindo-lhe alguns tratamentos não permitidos aos entes privados.

À luz disso, o artigo 24 da LGPD aduz que as empresas públicas e sociedades de economia mista devem se adequar a depender do caso concreto: ao explorar atividade econômica devem atuar conforme os requisitos do art. 173, CF/88, que versa sobre o tratamento de dados pessoais; já nos casos em que a finalidade do tratamento for a persecução do interesse público devem seguir os ditames do tratamento de dados pessoais pelo Poder Público.

Nesse sentido, quando observar-se a necessidade de tratar dados pessoais, o ente público primeiramente deve verificar sua condição de atuação, tendo em vista que os requisitos a serem atendidos e as sanções previstas em lei variam dependendo do regime adotado, podendo ser concorrencial ou de finalidade pública (ROSSO, 2019).

A finalidade pública é identificada pelo art. 4º, da referida lei, nos casos em que as atividades se revestem de caráter puramente estatal, afastando a incidência da LGPD no tratamento de dados pessoais para fins exclusivos de segurança pública, defesa nacional, segurança do estado ou atividades de investigação e repressão de infrações penais.

Diante disso, o art. 7º, inciso III da LGPD traz o requisito permissivo para o tratamento de dados pessoais pela Administração Pública, quando estes forem necessários para a execução das políticas públicas previstas em leis, regulamentos ou respaldadas em contratos, convênios e instrumentos congêneres, observadas as disposições do Capítulo IV que versa sobre o tratamento de dados pessoais pelo Poder Público.

Não obstante, o termo políticas públicas é amplo e, consequentemente, suscita dificuldades de controle e administração dos dados pessoais e sensíveis coletados pelo setor público, abrindo margem para a manipulação extensiva dos dados

pessoais, uma vez que é inerente à própria existência do Estado a consecução de políticas públicas. Nesse sentido, cabe destacar o posicionamento do Superior Tribunal de Justiça nas decisões mais recentes, vejamos:

> PROCESSUAL CIVIL E ADMINISTRATIVO. AGRAVO INTERNO NO MANDADO DE SEGURANÇA. CÓDIGO DE PROCESSO CIVIL DE 2015. APLICABILIDADE. PROCESSO ADMINISTRATIVO DISCIPLINAR CONTRA AUDITOR DA RECEITA FEDERAL. OBTENÇÃO DE DADOS FISCAIS DIRETAMENTE PELA CORREGEDORIA. ILEGALIDADE. INEXISTÊNCIA. ARGUMENTOS INSUFICIENTES PARA DESCONSTITUIR A DECISÃO ATACADA. APLICAÇÃO DE MULTA. ART. 1.021, § 4º, DO CÓDIGO DE PROCESSO CIVIL DE 2015. DESCABIMENTO. I Consoante o decidido pelo Plenário desta Corte na sessão realizada em 09.03.2016, o regime recursal será determinado pela data da publicação do provimento jurisdicional impugnado. In casu, aplica-se o Código de Processo Civil de 2015. II A controvérsia gravita em torno de eventual ilegalidade na obtenção, por parte do Escritório de Corregedoria da Receita Federal, do histórico de movimentação fiscal do Impetrante, Auditor Fiscal, após constatar indícios de infração disciplinar, relacionada à sua participação na administração de empresa de consultoria da área fiscal. III - Em questão idêntica, esta Corte compreendeu não se configurar a violação ao sigilo fiscal o uso de tais dados pela própria Receita Federal no exercício do poder disciplinar, na linha do que definiu o Supremo Tribunal Federal que, ao julgar conjuntamente as ADI 2.386/DF, ADI 2.390/DF, ADI 2.397/DF e ADI 2.859/DF, assentou inexistir quebra de sigilo na hipótese de haver intercâmbio de informações sigilosas no âmbito da Administração Pública, de acordo com o art. 1º da Lei Complementar n. 104/2001, ao inserir o § 1º, inciso II, e o § 2º ao art. 198 do CTN (1ª T., AREsp 1.068.263/RJ, Rel. p/ Acórdão Ministro Benedito Gonçalves, DJe 05.03.2020). IV - Ao julgar as apontadas Ações Diretas de Inconstitucionalidade, o Supremo Tribunal Federal, dentre as teses firmadas, registrou que, para se falar em "quebra" de sigilo fiscal, necessário seria vislumbrar a exposição da informação ao público externo, circunstância inocorrente com o simples acesso do órgão detentor dos dados. V - Não se configurando quebra de sigilo fiscal o compartilhamento de dados entres os órgãos distintos, ante o compromisso de sigilo de ambos, menos ainda há de se cogitar em ilegalidade quando os dados fiscais são utilizados pela própria Receita Federal, no exercício do poder disciplinar, visando preservar a integridade da Administração Tributária, atividade essencial ao funcionamento do Estado, consoante art. 37, XXII, da Constituição da República. VI ? Não apresentação de argumentos suficientes para desconstituir a decisão recorrida. VII ? Em regra, descabe a imposição da multa, prevista no art. 1.021, § 4º, do Código de Processo Civil de 2015, em razão do mero improvimento do Agravo Interno em votação unânime, sendo necessária a configuração da manifesta inadmissibilidade ou improcedência do recurso a autorizar sua aplicação, o que não ocorreu no caso. VIII ? Agravo Interno improvido. (STJ - AgInt nos EDcl no MS: 21328 DF 2014/0263274-0, Relator: Ministra REGINA HELENA COSTA, Data de Julgamento: 29/06/2021, S1 - PRIMEIRA SEÇÃO, Data de Publicação: DJe 01/07/2021)

> PENAL E PROCESSO PENAL. AGRAVO REGIMENTAL NO RECURSO ESPECIAL. COMPARTILHAMENTO DE DADOS DA RECEITA FEDERAL COM ÓRGÃOS DE PERSECUÇÃO PENAL. PRECEDENTE DO STF. REPERCUSSÃO GERAL (TEMA 990). VIABILIDADE. INÉPCIA DA DENÚNCIA. SENTENÇA PROLATADA. COGNIÇÃO EXAURIENTE. PREJUDICIALIDADE. INDEFERIMENTO DE DILIGÊNCIA. DECISÃO FUNDAMENTADA. POSSIBILIDADE. GRAVE DANO À COLETIVIDADE.

> ART. 12, I, DA LEI N. 8.137/1990. CAUSA DE AUMENTO. VALOR DO CRÉDITO TRIBUTÁRIO SONEGADO DESCRITO NA DENÚNCIA. DESNECESSIDADE DE PERÍCIA. PRECEDENTE. AGRAVO DESPROVIDO. 1. É válido o compartilhamento dos relatórios de inteligência financeira da UIF e da íntegra do procedimento fiscalizatório da Receita Federal do Brasil (RFB), que define o lançamento do tributo, com os órgãos de persecução penal para fins criminais, sem a obrigatoriedade de prévia autorização judicial, devendo ser resguardado o sigilo das informações em procedimentos formalmente instaurados e sujeitos a posterior controle jurisdicional. Precedente do STF. Repercussão Geral (tema 990). 2. Após a prolação de sentença condenatória, em que é realizado um juízo de cognição mais amplo, perde força a discussão acerca de eventual inépcia da denúncia. Precedentes. 3. Caso em que o Tribunal de origem justificou o indeferimento da diligência com base na desnecessidade de produção da prova requerida, bem como na falta de comprovação do motivo excepcional a justificar o pedido de ouvida da testemunha só ao término da instrução. O argumento justificado sobre ser prescindível a diligência requerida afasta a violação ao art. 402 do CPP. Precedentes do STJ. 4. A descrição, na denúncia, do valor do crédito tributário sonegado é suficiente para que o juízo delibere sobre o grave dano à coletividade e, consequentemente, sobre a incidência da causa de aumento do art. 12, I, da Lei n. 8.137/1990. Precedentes do STJ. 5. Agravo regimental desprovido. (STJ - AgRg no REsp: 1836170 SP 2019/0264400-9, Relator: Ministro RIBEIRO DANTAS, Data de Julgamento: 18/08/2020, T5 - QUINTA TURMA, Data de Publicação: DJe 25/08/2020)

Assim, o artigo 23 da LGPD estabelece requisitos que devem ser observados e cumpridos pelo Estado quando for manipular os dados pessoais, quais sejam: a informação clara, atualizada e precisa quando, no exercício de suas competências, realizar o tratamento de dados, destacando a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para o exercício desta atividade, sem a possiblidade de tratamento futuro quando incompatível com a finalidade anteriormente exposta.

Em verdade, o princípio da transparência previsto no art. 6º da LGPD garante aos titulares dos dados pessoais a consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a extensão integral das informações coletadas. Ademais, o referido artigo elenca os princípios que devem ser observados no tratamento de dados, sendo eles: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, segurança, prevenção, não discriminação, responsabilização e prestação de contas.

Concomitantemente, o princípio da publicidade previsto no artigo 5º, XXXIII, XXXIV, LXXII, da Constituição Federal dispõe que a Administração Pública deve obrigatoriamente atender ao interesse público e dar conhecimento do ato

administrativo ao público em geral, como meio de exercer suas funções com transparência e clareza, de modo a permitir o controle social dos atos administrativos.

Nesse cenário, Tânia Carolina Gonçalves (2019, p. 30) aduz que “a disponibilização de dados pessoais, a transparência e o grau de publicidade estão relacionados ao nível de agregação e à verificação da sensibilidade de determinadas informações no caso concreto”. Assim, pondera:

> O governo transparente não é tão simples como parece à primeira vista. A possibilidade de reorganizar os dados por meio de processos novos e melhores, abrindo repositórios de dados governamentais para os cidadãos, de forma acessível, organizada e neutra, sem afetar a privacidade de informações ou exposição de dados sensíveis que podem prejudicar a função do Estado torna-se uma tarefa titânica.

Por isso, Sônia Aguiar do Amaral (2002, p. 28) afirma que “imperioso que o interesse público a sobrepujar o particular, em termos de vida privada, seja indispensável, ou seja, só se justifica o seu sacrifício, na exata medida da necessidade e se o interesse superior não puder ser satisfeito por outra forma, seja ele de natureza pública ou privada”.

Nessa toada, conforme preceitua o art. 25 da LGPD, os dados pessoais geridos pelo setor público deverão ser mantidos em formato inoperável e estruturado para o uso compartilhado, visando à execução de políticas públicas, prestação de serviços públicos e disseminação do acesso a informação relativos à atividade pública.

O artigo 26, por sua vez, veda o compartilhamento dos dados em posse da Administração Pública com entidades privadas, ressalvadas as hipóteses previstas taxativamente nos seus incisos, em que a transferência atende a finalidade pública ou quando os dados forem acessíveis publicamente, houver previsão legal ou pretende coibir fraudes e irregularidades.

Ainda, o art. 27 da LGPD garante ao titular a faculdade de consentir com a transmissão das suas informações pela pessoa jurídica de direito público a pessoa jurídica de direito privado, bem como assegura a comunicação da atividade à autoridade nacional. Entretanto, nos seus incisos trazem exceções em que o consentimento é

dispensado, quando a transferência das informações pessoais for necessária para a execução da atividade pública e nas exceções referentes ao artigo 26, aludidas acima.

Pelo exposto, os entes públicos ao fazerem a mineração de dados se submetem às sanções dispostas no art. 52, §3º da Lei Geral de Proteção de Dados, envolvendo: advertência, com indicação de prazo para adoção de medidas corretivas; publicização da infração após sua ocorrência ser apurada e confirmada; bloqueio dos dados pessoais a que se refere a infração até a sua regularização e/ou eliminação dos referidos dados pessoais.

Observa-se que para a Administração Pública, atuando em prol do interesse público, não estão previstas as punições de multa simples e diária, porém se submete à Lei de Acesso à Informação, Lei de Improbidade Administrativa e ao Estatuto do Servidor Público Federal. Já as empresas públicas e sociedades de economia mista que atuam sob o regime de concorrência se submetem à sanção pecuniária.

3.1 A LEI GERAL DE ACESSO A INFORMAÇÕES PÚBLICAS E A RESPONSABILIDADE DO ESTADO PELOS DADOS DOS USUÁRIOS DE SERVIÇOS PÚBLICOS

Atualmente, pode-se perceber que a gestão de dados pelos órgãos da Administração Pública direta e indireta não tem se dado de forma uniforme, isso porque alguns optam por utilizar sua própria infraestrutura para armazenamento, sistematização e tratamento dos dados. Enquanto outros firmam contratos com o Serviço Federal de Processamento de Dados (Serpro) ou com a Empresa de Tecnologia e Informações da Previdência (Dataprev), tratam-se de empresas públicas vinculadas ao Ministério da Fazenda (GONÇALVES, 2019).

Para além disso, cabe ressaltar que o próprio conceito de privacidade, aludido anteriormente, ganha contornos diferentes a depender a situação e do contexto em que está inserido. Assim, Danilo Doneda (2006, p. 64) afirma:

> A privacidade é um termo que se presta a uma certa manipulação pelo próprio ordenamento – pois não raro ela é utilizada para suprir necessidades

> estruturais dele próprio, assumindo determinado sentido em função de determinadas características de um ordenamento e dificultando ainda mais a sua redução a um sentido comum.

Nessa toada, a Lei de Acesso a Informações Públicas (Lei n. 12.527/2011) representou um avanço na gestão governamental democrática da República brasileira, na medida em que garantiu o acesso à informação de caráter público por qualquer cidadão, sem exigir nenhuma motivação para o pedido, assim, no seu artigo 3º, inciso I, propõe a "observância da publicidade como preceito geral e do sigilo como exceção".

Entende-se como informação pública, todos os registros mantidos por órgão público, sob essa ótica Toby Mendel (2009, p. 34) pontua:

> para efetivar o direito à informação na prática, não basta simplesmente exigir que os órgãos públicos atendam a pedidos de informação. O acesso efetivo para muitas pessoas depende de que esses órgãos publiquem e divulguem, efetivamente, voluntariamente, de forma pró-ativa, sem necessidade de requisição, categorias-chave de informação, mesmo na ausência de um pedido.

Em termos gerais, enquanto a LAI tem como principal finalidade dar transparência aos atos praticados pela administração pública direta ou indireta, nos poderes Judiciário, Legislativo e Executivo, em todas as esferas governamentais; a LGPD visa assegurar a proteção dos dados pessoais enquanto informações particulares inerentes à personalidade e privacidade do indivíduo.

À luz disso, a título de exemplo, o STF fixou no tema de Repercussão Geral nº 483 que: "É legítima a publicação, inclusive em sítio eletrônico mantido pela Administração Pública, dos nomes dos seus servidores e do valor dos correspondentes vencimentos e vantagens pecuniárias"; isto porque, nas palavras do ministro Carlos Ayres Britto, "é o preço que se paga pela opção por uma carreira pública no seio de um Estado republicano". (ARE 652777/ SP, 2015, p.9)

Desta forma, o art. 31, §§ 3º e 4º da LAI prevê hipóteses em que entidades e órgãos públicos podem divulgar ou conferir o acesso de informações pessoais, independentemente do consentimento do titular, quando destinadas à realização de pesquisas científicas, do cumprimento de ordem judicial, da defesa de direitos

humanos, da proteção de interesse público geral e preponderante ou de ações voltadas para a recuperação de fatos históricos de maior relevância.

Assim, foi criado o Sistema Eletrônico do Serviço de Informação ao Cidadão (e-SIC), que consiste num sistema que permite que qualquer pessoa, física ou jurídica, encaminhe pedidos de acesso à informação para qualquer órgão da administração pública direta ou indireta, estabelecendo as regras, trâmites e prazos que devem ser observados pelas partes (GONÇALVES, 2019).

Não obstante, o pedido é analisado pelo Ministério da Transparência e Controladoria-Geral da União (CGU), podendo ser negado o acesso à informação quando se tratar de dados pessoais e informação sigilosa de acordo com a legislação especifica ou conforme a Lei no 12.527/201, de acordo com o Relatório de Pedidos de Acesso à Informação (GONÇALVES, 2019).

Nesse sentido, importa destacar, a elucidação feita por Tânia Carolina Gonçalves e Marcelo D. Varella (2018, p. 519),

> os princípios da publicidade e da transparência compartilham de natureza relativa, ao dispor sobre as informações pessoais, a Lei prescreve que o tratamento dado a elas deve respeitar a intimidade, a vida privada, a honra e a imagem das pessoas, bem como as liberdades e garantias individuais. Todos são princípios constitucionais e, como tais, não há hierarquia entre eles. Trata-se de uma antinomia aparente, devendo haver, tão somente na análise do caso concreto, o processo de harmonização e ponderação entre eles.

Todavia, informações como como Cadastro de Pessoas Físicas (CPF), registro geral (RG) e endereço residencial a Suprema Corte, no tema de Repercussão Geral n. 483, estabeleceu que são classificadas como pessoais e, por isso, em razão do direito à intimidade, à vida privada ou à honra devem ser preservadas, sendo proibida a sua publicização.

Com a aprovação da Lei Geral de Proteção de Dados, essa lacuna jurídica relativa a proteção das informações pessoais dos cidadãos brasileiros foi preenchida, trazendo segurança jurídica e impactando diretamente a Lei de Acesso à Informação, isso porque, a LAI já apontava a necessidade de tratamento de dados pessoais.

Desse modo, pode-se aferir que quando se tratar de informações que tornam um indivíduo identificável, o que hoje conhecemos como dados pessoais sensíveis, estas devem ser preservadas pela Administração Pública. Com efeito, ambas as leis garantem a proteção da privacidade, a honra e a imagem das pessoas, bem como as liberdades e direitos individuais, por isso, elas se complementam ao tutelarem direitos fundamentais específicos, sendo a proteção à privacidade e o direito à informação.

O Poder Público ao desenvolver os aplicativos de internet como estratégia para se aproximar de cidadãos e facilitar o acesso à informação e a prestação de determinados serviços, através dos aplicativos do Bolsa Família, Caixa Econômica Federal, Anatel Consumidor, FGTS, Meu INSS, SNE (Sistema de Notificação Eletrônica, do Denatran), Meu Imposto de Renda e CNH Digital, este deve observar os termos de privacidade no uso dos dados sob a sua guarda e gestão (GONÇALVES, 2019).

Sob esse aspecto, busca-se melhorar a colaboração e o compartilhamento de informações entre as instituições governamentais, tanto para alcançar o almejado governo eletrônico e acessível a todos como para garantir a segurança nacional (GONÇALVES, 2019). Nesses casos, embora a Administração esteja perseguindo o interesse público, ainda sim deve prestar informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, conforme estabelece o art. 7º, inciso I da LGPD.

Todavia, Felipe Demartini (2008) pontua que o estudo realizado pela InternetLab detectou “flagrantes violações da privacidade dos cidadãos, principalmente no que toca a coleta de informações sem autorização e sem necessidade, uma vez que tais dados não são essenciais para a utilização dos aplicativos”. Ainda, apontou-se que as informações de localização dos usuários, a permissão de acesso à câmara para reconhecimento facial ou ao sensor biométrico são informações sensíveis coletadas sem necessidade específica.

Para além disso, constatou-se que os aplicativos analisados não solicitaram o consentimento expresso, inequívoco e específico para acessar os dados pessoais dos usuários dos serviços públicos, bem como não explicaram a destinação das informações coletadas, na medida em que apenas solicitam uma autorização genérica no momento da instalação (DEMARTINI, 2008). Portanto, na forma do art. 9º, §1º da LGPD o consentimento pode ser considerado nulo.

Outra questão, envolve o fato de que se trata de um contrato de adesão, condicionador da participação social, em que a autonomia da vontade do consumidor e/ou cidadão é usurpada pelo modelo do "tudo ou nada" aludido anteriormente, em que o usuário não tem poder de "barganha", isto é, não pode negociar o conteúdo das cláusulas atinentes as suas próprias informações.

Pelo exposto, verifica-se a ilegalidade e abusividade dos termos condicionadores do uso dos aplicativos governamentais, na medida em que não observam a necessidade de transparência e confiança, ofertando a possibilidade de negar o compartilhamento de dados; a necessidade do consentimento real e espontâneo do consumidor e a necessidade de vinculação entre os dados coletados e o serviço prestado.

Portanto, pautando-se nas sanções dispostas no art. 52, §3º da LGPD, a Administração Publica deve ser responsabilizada pelas referidas infrações cometidas às normas dispostas nesta Lei, com a advertência e indicação de prazo para adoção de medidas corretivas; a publicização da infração e o bloqueio dos dados pessoais fornecidos indevidamente até a sua regularização e/ou sua eliminação.

CONSIDERAÇÕES FINAIS

No contexto da globalização, do desenvolvimento tecnológico e acessibilidade, evidenciou-se a necessidade da proteção de dados pessoais, de modo a regulamentar a coleta, o fluxo e o processamento das informações disponibilizadas pelos cidadãos ao poder Público, como também ao setor privado.

Essa questão envolve o direito à autodeterminação informativa e o condicionamento do exercício da vida social particular aos interesses velados, ou não, das entidades ou órgãos que formam bancos de dados.

Na Europa, a Organização para a Cooperação e Desenvolvimento Econômico (OCDE) emitiu dois documentos que estabeleceram padrões normativos para a proteção dos dados pessoais, visando a assegurar a proteção do fluxo de informações entre os países-membros. Nesse sentido, a Convenção 108 de Strasbourg, do Conselho da Europa e União Europeia, propiciou a compatibilização das legislações de proteção de dados entre os países-membros.

No Brasil, a proteção dos dados pessoais teve seu destaque no Código de Defesa do Consumidor, no Código Civil, na Lei do Cadastro Positivo, no Marco Civil da Internet, e, posteriormente, na Lei Geral de Proteção de Dados.

Por sua vez, a LGPD impõe o consentimento informado e o legítimo interesse como parâmetros para preservar a autonomia da vontade, garantindo ao titular dos dados pessoais a faculdade de consentir com o tratamento e a transmissão das suas informações pela pessoa jurídica de direito público à pessoa jurídica de direito privado. Todavia, o art. 7º e o art. 11, inciso II, ambos da LGPD preveem hipóteses em que o consentimento não é exigido, tanto para o tratamento de dados pessoais ordinários quanto para o de dados pessoais sensíveis.

Nessa toada, o princípio da vulnerabilidade reconhece o estado de risco e fragilidade do sujeito de direitos inserido no mercado de consumo e na vida social, na medida em que o próprio titular dos dados possui menos informações que o fornecedor a respeito do fluxo de suas informações.

Assim, os direitos fundamentais à liberdade e à privacidade, o direito ao livre desenvolvimento da personalidade mostram-se ameaçados no âmbito virtual, tendo em vista a complexidade humana e a redução do indivíduo ao filtro que o algoritmo impõe, na medida em que o processamento de dados pessoais mapeia e armazena

os hábitos e as características dos indivíduos, direcionando os hábitos, o consumo e o cotidiano do cidadão.

A Administração Pública, enquanto coletora de dados pessoais dos cidadãos, está amparada por regime especial, desta forma, ao realizar o tratamento das informações deve observar sua condição de atuação, a fim de verificar se a atividade está pautada na finalidade pública, na forma do art. 4º da LGPD, afastando-se a incidência da LGPD, assim como no art. 7º, inciso III da LGPD que permite o tratamento quando necessário para a execução das políticas públicas previstas. Já as empresas públicas e sociedades de economia mista que exploram a atividade econômica, no regime de concorrência, devem adequar o tratamento de dados aos ditames da LGPD, na medida em que se submetem à sanção pecuniária.

Pelo exposto, ainda que o Poder Público deva observar os princípios da publicidade e transparência, deve também cumprir o que dispõe o art. 7º, inciso I da LGPD e prestar informações claras e completas sobre coleta, uso, armazenamento e tratamento dos dados pessoais.

Logo, ao não solicitar o consentimento expresso para acessar os dados pessoais dos usuários dos serviços públicos e condicionar o uso dos aplicativos governamentais aos termos genéricos de adesão verifica-se a ilegalidade e abusividade dos seus atos, sendo possível a sua responsabilização.

REFERÊNCIAS:

BAUMAN, Zygmunt. Vida para consumo: a transformação das pessoas em mercadorias – Rio de Janeiro: Jorge Zahar Ed., 2008.

BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 2. Ed. – Rio de Janeiro: Forense, 2019.

BRASIL. Lei Federal nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: outubro 2021.

BRASIL. Lei Federal nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: outubro 2021.

BRASIL. Lei Federal nº 12.414, de 09 de junho de 2011. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: outubro de 2021.

BRASIL. Lei Federal nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: outubro de 2021.

BRASIL. Lei Federal nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: outubro de 2021.

BRASIL. Lei Federal nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: outubro de 2021.

BRASIL. Ministério da Transparência e Controladoria-Geral da União. **E-SIC:** Relatório de pedidos de acesso à informação e solicitantes. Disponível em: <https://esic.cgu.gov.br/sistema/Relatorios/Anual/Relatorio- AnualPedidos.aspx>. Acesso em: 09 ago. 2018.

CANOTILHO, José Joaquim Gomes; MOREIRA, Vital. Constituição da República Portuguesa anotada. 1. Ed. São Paulo: Revista dos Tribunais, 2007.

DEMARTINI, Felipe. Apps do governo estão invadindo privacidade dos usuários, diz estudo. Canatech, 28 mai. 2018. Disponível em: <https://canaltech.com.br/seguranca/apps-do-governo-estao-invadindo-privaci- dade-dos-usuarios-diz-estudo-114680/>. Acesso em: 01 outubro de 2021.

DONEDA, Danilo. A PROTEÇÃO DOS DADOS PESSOAIS COMO UM DIREITO FUNDAMENTAL. ESPAÇO JURÍDICO, v. 12, n. 2, p. 91-108, 2011. Disponível em: https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315

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

DUQUE, Bruna Lyra; PEDRA, Adriano Sant'Ana. OS DEVERES FUNDAMENTAIS E A SOLIDARIEDADE NAS RELAÇÕES PRIVADAS. Revista de Direitos Fundamentais e Democracia, Curitiba, v. 14, n. 14, p. 147-161, julho/dezembro de 2013.

FABRIZ, Daury Cesar. A Eficácia dos Direitos Sociais após duas décadas da Constituição brasileira de 1988. Publicações Seriadas do Centro de Estudos Sociais, Coimbra, n. 315, p. 1-13, out. 2008.

GONÇALVES, Tânia Carolina Nunes Machado. Gestão de dados pessoais e sensíveis pela Administração Publica Federal: desafios, modelos e principais impactos previstos com a nova lei. 2019. Dissertação (Mestrado em Direito) – Centro Universitário de Brasília, 2019.

GONÇALVES, Tânia Carolina Nunes Machado; VARELLA, Marcelo D. OS DESAFIOS DA ADMINISTRAÇÃO PÚBLICA NA DISPONIBILIZAÇÃO DE DADOS SENSÍVEIS. Revista de Direito GV, São Paulo, v. 14 n. 2, p. 513-536, maio/ago. 2018.

MENDEL, Toby. Liberdade de informação: um estudo de direito comparado. Brasília: Unesco, 2009.

MENDES, Laura Schertel; DONEDA, Danilo. Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018): o novo paradigma da proteção de dados no Brasil. Revista de Direito do Consumidor, São Paulo, v. 120, 2018.

MENDES, Laura Schertel. Transparência e Privacidade: violação e proteção da informação pessoal na sociedade de consumo. Dissertação (Mestrado em Direito) – Faculdade de Direito da Universidade de Brasília. Brasília, 2008.

MULHOLLAND, Caitlin Sampaio. DADOS PESSOAIS SENSÍVEIS E A TUTELA DE DIREITOS FUNDAMENTAIS: uma análise à luz da Lei Geral de Proteção de Dados (Lei 13.709/18). Revista de Direitos e Garantias Fundamentais, Vitória, v. 19, n. 3, p. 159-180, set./dez. 2018.

NEGREIROS, Teresa. Teoria do Contrato: novos paradigmas. 2. Ed. – Rio de Janeiro: Renovar, 2006.

NUNES, Rizzato. Curso de Direito do Consumidor. 12. Ed. – São Paulo: Saraiva Educação, 2018.

PINHEIRO, Victor Sales; BONNA, Alexandre Pereira. SOCIEDADE DA INFORMAÇÃO E DIRETO À PRIVACIDADE NO MARCO CIVIL DA INTERNET: Fundamentação Filosófica do Estado de Direito em John Finnis. Revista Direitos e Garantias Fundamentais, Vitória, v. 21, n. 3, p. 365-394, set./dez. 2020.

REGAN, Priscilla M. (2002) 'Privacy as a Common Good in the Digital World', In: Information, Communication & Society, 5:3.

ROPPO, Enzo. O contrato. Coimbra: Edições Almedina, 2009.

ROSSO, ANGELA MARIA. LGPD E SETOR PÚBLICO: aspectos gerais e desafios. 2019. Disponível em: https://www.migalhas.com.br/depeso/300585/lgpd-e-setor-publico--aspectos-gerais-e-desafios

SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. Curso de Direito Constitucional. 6. Ed.- São Paulo: Saraiva, 2017.

Superior Tribunal de Justiça - AgInt nos EDcl no MS: 21328 DF 2014/0263274-0, Relator: Ministra REGINA HELENA COSTA, Data de Julgamento: 29/06/2021, S1 - PRIMEIRA SEÇÃO, Data de Publicação: DJe 01/07/2021. Disponível em: <https://stj.jusbrasil.com.br/jurisprudencia/1263958604/agravo-interno-nos

embargos-de-declaracao-no-mandado-de-seguranca-agint-nos-edcl-no-ms-21328-df-2014-0263274-0>. Acesso em: 1 de outubro de 2021.

Superior Tribunal de Justiça - AgRg no REsp: 1836170 SP 2019/0264400-9, Relator: Ministro RIBEIRO DANTAS, Data de Julgamento: 18/08/2020, T5 - QUINTA TURMA, Data de Publicação: DJe 25/08/2020. Disponível em: <https://stj.jusbrasil.com.br/jurisprudencia/923455751/agravo-regimental-no-recurso-especial-agrg-no-resp-1836170-sp-2019-0264400-9>. Acesso em: 1 de outubro de 2021.

Supremo Tribunal Federal. SS 3902 AgR-segundo Relator(a): Min. AYRES BRITTO, Tribunal Pleno, julgado em 09/06/2011, DJe- 03-10-2011 EMENT VOL-02599- 01 PP-00055 RTJ VOL-00220-01 PP 00149. 2011. Disponível em: <http://www.stf.jus.br/portal/jurisprudencia/visualizarEmenta.asp?s1=000181369&base=baseAcordaos>. Acesso em: 1 de outubro de 2021.

VIEIRA, Sônia Aguiar do Amaral. Inviolabilidade da vida privada e da intimidade pelos meios eletrônicos. São Paulo: Editora Juarez de Oliveira, 2002.

ZANON**,** João Carlos. Direito à Proteção dos Dados Pessoais. São Paulo, Revista dos Tribunais, 2013.