A PROTEÇÃO DOS DADOS PESSOAIS NO MEIO DIGITAL COMO UM DIREITO FUNDAMENTAL[1]

THE PROTECTION OF PERSONAL DATA IN THE DIGITAL MEDIA AS A FUNDAMENTAL RIGHT

Mariana Martins RIBEIRO[2]

Cildo GIOLO JÚNIOR[3]

RESUMO
Este trabalho busca relacionar a proteção de dados pessoais aos direitos fundamentais garantidos pela Constituição Federal e como seu uso indevido pode interferir, negativamente, no exercício da democracia e na tomada de decisões por meio de políticas públicas, tendo em vista o avanço tecnológico e a digitalização de vários serviços. Para atingir os objetivos propostos, recorre-se à investigação teórica, com predomínio do método dedutivo e análise de obras e artigos centrados no direito constitucional e civil.
Palavras-chave: Dados Pessoais, Direitos Fundamentais, Constituição Federal, Lei Geral de Proteção de Dados, Internet, Democracia, Poder Público.

[1] O presente artigo sintetiza a monografia de conclusão da pesquisa, realizada para o Programa Interno de Bolsas de Iniciação Científica (PIBIC 2020-2021) da Faculdade de Direito de Franca (FDF), Franca/SP.

[2] Discente da Faculdade de Direito de Franca (FDF), Franca/SP. Bolsista do Programa Interno de Bolsas de Iniciação Científica (PIBIC 2020-2021).

[3] Pós-Doutor em Direitos Humanos pelo "Ius Gentium Conimbrigae" (IGC/CDH) da Faculdade de Direito da Universidade de Coimbra (Portugal). Doutor em Direito pela Universidade Metropolitana de Santos, Santos - São Paulo (Brasil). Doutor em Ciências Jurídicas e Sociais pela UMSA, Buenos Aires - Capital Federal (Argentina). Mestre em Direito Público pela Universidade de Franca. Especialista em Direito Processual Civil na Faculdade de Direito de Franca. Graduado em Direito pela Faculdade de Direito de Franca. Professor Titular das cadeiras de Direito Civil na Faculdade de Direito de Franca e de Direito Processual Civil na Universidade do Estado de Minas Gerais, tendo sido admitido em ambas por concursos públicos de provas e títulos. Docente e Advogado. Avaliador do MEC/INEP para os Cursos de Direito.

ABSTRACT
This work seeks to relate the protection of personal data to the fundamental rights guaranteed by the Federal Constitution and how its misuse can negatively interfere in the exercise of democracy and decision-making through public policies, in view of the technological advance and the digitalization of several services. To achieve the proposed objectives, theoretical research is used, with a predominance of the deductive method and analysis of works and articles centered on constitutional and civil law.
Keywords*: Personal Data, Fundamental Rights, Federal Constitution, General Data Protection Law, Internet, Democracy, Public Power*

1 INTRODUÇÃO

É inegável que a sociedade esteja passando por mudanças significativas desde o advento da tecnologia, e desse modo, as relações sociais também se alteram. O Direito, como instrumento de regulação da vida social, tem o dever de acompanhar tais mudanças a fim de aplicar e adequar as normas jurídicas a essa nova realidade, buscando garantir cada vez mais, a proteção aos direitos fundamentais para o pleno desenvolvimento da sociedade.

A inovação tecnológica, conforme demonstrado ao longo da história da civilização, se mostra como um fator de grande importância para o aprimoramento do meio técnico, científico e informacional, inaugurando um novo espaço público e permitindo que as informações sejam trocadas de maneira instantânea por meio da tecnologia de dados: *big data, machine learning*, *dataveillance*, entre outros, conceitos que serão devidamente explicados no presente artigo.

Castells (2003) menciona acerca da modificação da vida social em decorrência desta inovação tecnológica:

> A Galáxia Internet é um novo ambiente de comunicação. Como a comunicação é a essência da atividade humana, todos os domínios da vida social estão sendo modificados pelos usos disseminados da Internet (...). Uma nova forma social, a sociedade de rede, está se construindo em torno do planeta, embora sob uma diversidade de formas e com consideráveis diferenças em suas consequências para a vida das pessoas.

Assim, a tecnologia e a informação incidem constantemente sobre as ações humanas, determinando, entre outras coisas, a quais propagandas publicitárias o usuário da *internet* terá acesso, influenciando

em seus hábitos de consumo, entre outras infinitas possibilidades que acabam por influenciar e categorizar a vida de um indivíduo.

Pode-se dizer que a discussão sobre a proteção aos dados pessoais ganhou maior relevância após os escândalos envolvendo a empresa Cambridge Analytica e as eleições norte-americanas no ano de 2016, apesar de o tema já ser uma preocupação após o atentado em setembro de 2001 no World Trade Center, contexto no qual o governo norte americano passou a vigiar sistematicamente, em nome da "Guerra ao Terror" e à segurança nacional, tanto os seus cidadãos quanto os outros países utilizando-se da tecnologia de dados.

Desse modo, o presente trabalho objetiva discutir acerca da importância de uma proteção efetiva e constitucional aos dados pessoais destacando seu caráter fundamental, uma vez que os dados pessoais são o que representam o indivíduo perante a sociedade e o identificam como tal. Pretende-se ainda, discutir sobre de que forma a inobservância a tal proteção pode impactar, negativamente, o pleno exercício da cidadania e da democracia.

Para a consecução dos objetivos propostos, utiliza-se a pesquisa teórica de caráter bibliográfico, com predominância do método dedutivo e análise de obras e artigos centrados no Direito Constitucional, Direito Civil e Público. Utiliza-se também a pesquisa documental, procedendo à análise de julgados e dispositivos normativos.

2 CONTEXTUALIZAÇÃO DOS DADOS PESSOAIS NO MEIO DIGITAL

Antes de discorrer sobre os impactos negativos do uso indevido dos dados pessoais, é necessário compreender de que forma esses dados são utilizados no meio digital e para quais finalidades, especialmente no cenário brasileiro.

A revolução tecnológica e a democratização do acesso à internet caminham no sentido de permitir que mais da metade da população brasileira possua acesso a dispositivos eletrônicos conectados à rede mundial de computadores ou por meio da internet das coisas (IoT). Permitem ainda, a digitalização de serviços públicos com a finalidade de facilitar e melhorar as demandas da população.

Desse modo, toda vez que se acessa sites e páginas da *web*, são baixados *cookies*, que são arquivos nos quais são armazenadas diversas

informações do usuário como o IP (número de registro do dispositivo), nome, interesses pessoais, geolocalização, entre outros, que são utilizados com a finalidade de reconhecer o usuário da próxima vez que ele acessar o site novamente, de forma a tornar a navegação mais rápida e preencher campos automaticamente, como login e senhas. Muitas vezes, esses dados são obtidos de maneira que o seu titular não esteja consciente de tal atividade, seja por desconhecimento ou por, simplesmente, ignorar as permissões e termos de uso muitas vezes apresentados em textos extensos.

A cessão desses dados funciona como uma permuta para que o usuário possa utilizar os serviços ofertados pelo site, podendo ser vendidos para terceiros visto que o processamento dos dados é útil para que as empresas conheçam o perfil de seus consumidores e criem estratégias de direcionamento de produtos que correspondam aos interesses do consumidor em específico.

Segundo Rodotá (2003, p. 19):

> Los datos así recogidos pueden ser utilizados para distintos fines, elaborando, por ejemplo, perfiles de ciudadanos «activos» o fichando opiniones, preferencias, orientaciones. Si este conjunto de informaciones es utilizado para actividades de control o de simple interferencia en la esfera privada, o así lo percibe el ciudadano, existe el riesgo de desincentivar la participación al objeto de evitar consecuencias no deseadas.[4]

Tendo em vista que os dados adquiriram caráter econômico, aumenta-se a preocupação quanto à segurança dos usuários e quanto à autodeterminação informativa do titular, isto é, ter controle sobre os próprios dados de forma transparente para que não haja consequências graves para os direitos fundamentais que moldam o Estado de Direito.

[4] Os dados coletados podem ser usados para diferentes fins, criando, por exemplo, perfis de cidadãos "ativos" ou registrando opiniões, preferências ou orientações. Se esse conjunto de informações é utilizado para atividades de controle ou simples interferência na esfera privada, ou assim o cidadão o percebe, corre-se o risco de desestimular a participação para evitar consequências indesejadas. (RODOTÀ, 2003, p. 19, tradução nossa)

2.2 DADOS PESSOAIS, ALGORITMOS E COLETA

Para prosseguir, é necessário compreender o significado de dados pessoais, sendo esse um conceito fundamental para a presente pesquisa. Dados pessoais são informações relativas a uma pessoa identificada ou identificável, ou o conjunto de informações que podem levar à identificação de determinado indivíduo. Essa é a definição utilizada pela União Europeia no Regulamento Geral sobre a Proteção de Dados (RGPD ou GDPR, *General Data Protection Regulation*) servindo de base para outras legislações sobre o tema, inclusive para a Lei Geral de Proteção de Dados no Brasil.

São, acima de tudo, informações fragmentadas antes de serem transmitidas, visto ser a partir do conjunto de vários dados que será possível a identificação de um indivíduo. Assim, são dados pessoais as informações como nome, CEP, data de nascimento, número de documentos de identidade, número de celular, dados bancários, contatos da agenda telefônica entre outros.

Os dados pessoais sensíveis, por sua vez, são aqueles que demandam uma maior proteção, sendo que não poderão ser processados, em hipótese alguma, para fins de diferenciação, discriminação ou abusos a direitos. São aqueles dados relativos à origem racial, convicção religiosa, opinião política, sexualidade, dados genéticos e biométricos conforme dispostos no artigo 5º, inciso II da LGPD.

O regulamento 2016/679 da União Europeia dispõe com mais propriedade sobre os dados pessoais sensíveis:

> Merecem proteção específica os dados pessoais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, dado que o contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e liberdades fundamentais. Deverão incluir-se neste caso os dados pessoais que revelem a origem racial ou étnica, não implicando o uso do termo "origem racial" no presente regulamento que a União aceite teorias que procuram determinar a existência de diferentes raças humanas. (...) Tais dados pessoais não deverão ser objeto de tratamento, salvo se essa operação for autorizada em casos específicos definidos no presente regulamento, tendo em conta que o direito dos Estados-Membros pode estabelecer disposições de proteção de dados específicas, a fim de adaptar a aplicação das regras do presente regulamento para dar

> cumprimento a uma obrigação legal, para o exercício de funções de interesse público ou para o exercício da autoridade pública de que está investido o responsável pelo tratamento.

Observa-se que os dados pessoais se assemelham aos direitos fundamentais assegurados pela Constituição Federal por estarem, diretamente, relacionados à personalidade do indivíduo. Desse modo, o uso inadequado pode acarretar sérios riscos aos direitos e liberdades fundamentais, exigindo-se uma proteção igualmente constitucional e adequada, somada a uma fiscalização por parte da Agência Nacional de Proteção de Dados acerca das atividades de coleta e tratamento de dados.

Algoritmo, por sua vez, é o conjunto de instruções e diretrizes seguidas pelos dispositivos eletrônicos, compreendendo procedimentos lógicos aplicados aos dados e que são capazes de solucionar problemas e identificar objetos. Os algoritmos realizam tarefas que substituem os esforços humanos e para isso, são "ensinados" por meio da aprendizagem mecânica, responsável por processar dados continuamente para a realização de certas atividades, por meio do processamento de linguagem natural, a capacidade da máquina de reconhecer a linguagem humana e por fim, a habilidade de identificar imagens (CRESPO, 2016).

Para melhor ilustrar, toma-se o exemplo das recomendações da *Netflix* baseadas em buscas recentes e interesses demonstrados pelo usuário do aplicativo – o que se chama de perfil comportamental – a fim de tornar o uso deste aplicativo mais personalizado e atraente. A problemática reside no fato de que os algoritmos podem "aprender" com o ser humano, por meio de comportamentos repetidos, e acabar por reproduzir preconceitos e discriminação na realização de suas tarefas. Além disso, passam a reproduzir viés de confirmação por meio dos filtros-bolhas, inviabilizando o exercício democrático no espaço virtual.

Outro conceito recorrente em matéria de dados pessoais é a coleta de dados, que consiste no recolhimento de certos dados pelo site ou plataforma que o titular esteja utilizando. Segundo o Instituto Gartner 2,2 milhões de *terabytes* de novos dados são gerados todos os dias. Isso se dá através de cadastros realizados em sites, acesso a redes sociais, postagem de fotos, compartilhamento de conteúdo entre outras atividades corriqueiras na *internet*. Dados são coletados a todo instante e de diversas maneiras e de acordo com a Serasa Experian, as principais formas de coleta se dão por meio de anúncios publicitários, mídias sociais e sites de empresas.

Os questionários e testes *online* se tornaram verdadeiros fenômenos e são os meios mais eficazes para a coleta de dados. Vinculados às redes sociais, os questionários são acessados por usuários que pretendem descobrir qual o seu tipo de personalidade ou com qual personagem mais se parecem, submetendo-se a perguntas estritamente pessoais. Esses aplicativos, na verdade, coletam os dados para traçar um perfil comportamental e psicológico do usuário que será usado para finalidades diversas do apresentado.

Esta técnica de coleta de dados e categorização de indivíduos de acordo com o perfil psicológico foi desenvolvida pela Universidade de Cambridge sendo possível deduzir, com certa precisão, a etnia do indivíduo, a orientação sexual, tendências políticas e problemas familiares. Tal técnica foi utilizada em 2015, pela empresa de tecnologia Cambridge Analytica para influenciar pessoas, através da publicidade dirigida, na campanha eleitoral dos Estados Unidos, o que representou uma das maiores transgressões a proteção de dados pessoais e à liberdade dos usuários nos últimos anos.

Importante observar o disposto no artigo 7º da LGPD sobre hipóteses em que se pode proceder à coleta e processamento de dados pessoais.

Percebe-se que o processo de coleta e tratamento de dados pessoais, quando feito de maneira ilícita e fora do estabelecido pela LGPD, pode afetar de maneira significativa a privacidade de seu titular ao invadir e recolher aquilo que não queira que venha a público. Certo é que uma informação isolada pode não levar a identificação do indivíduo, mas o conjunto de informação, quando sequenciadas e organizadas, permite a realização de suposições sobre alguém.

O respeito à privacidade deve ser concreto e efetivo também no espaço digital, ainda mais quando se leva em consideração a espontaneidade e a velocidade com que a informação circula, não se limitando ao tempo e ao espaço, visto que a informação pode circular, eternamente, pelas plataformas digitais. Entender a proteção dos dados pessoais é fundamental para garantir o desenvolvimento do Estado Democrático e a garantia dos direitos fundamentais.

3. A RELAÇÃO ENTRE A PROTEÇÃO DOS DADOS PESSOAIS E OS DIREITOS FUNDAMENTAIS

3.1 O DIREITO À PRIVACIDADE

O conceito de privacidade depende de contextos sociais, culturais e históricos divergentes, sofrendo alterações no espaço e no tempo. Inicialmente, a privacidade se restringia aos bens patrimoniais, isto é, ao direito de não ter sua propriedade invadida, não englobando, contudo, aspectos como a imagem e a honra, necessidades pelas quais o âmbito de proteção deste direito vem sendo reformulado de acordo com a evolução da sociedade.

Em 1888, o juiz americano Thomas Cooley desenvolveu a ideia do direito de estar só, conhecido como *the right to be let alone*. Tal ideia se deu a partir do exacerbado individualismo que marcou o *Welfare State* norte americano no qual o indivíduo passou a ser enxergado como sujeito de direitos desde o seu nascimento, competindo ao Estado a garantia dos direitos fundamentais e a promoção da dignidade humana. Contudo, os primeiros julgados fundamentados com a ideia do direito de estar só eram, marcadamente, elitistas e atendia mais na divulgação de imagens de celebridades.

Com efeito, o desenvolvimento tecnológico suscitou a expansão da tutela do direito à privacidade ao ambiente virtual, devendo ser entendida como uma liberdade que o ser humano possui para determinar o que deseja ter divulgado sobre si mesmo, exercer o controle sobre informações e atributos que não se dissociam de sua personalidade. É a partir desse distanciamento de uma noção patrimonialista, que o direito à privacidade passa a integrar o ser como um todo, tanto na privacidade referente a seus aspectos mais íntimos, quanto a atributos que o formam como ser humano.

O atual Código Civil insere o direito à privacidade em seu capítulo II juntamente com o direito à personalidade:

> Art. 20. Salvo se autorizadas, ou se necessárias à administração da justiça ou à manutenção da ordem pública, a divulgação de escritos, a transmissão da palavra, ou a publicação, a exposição ou a utilização da imagem de uma pessoa poderão ser proibidas, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a boa fama ou a respeitabilidade, ou se se destinarem a fins comerciais
>
> Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as

> providências necessárias para impedir ou fazer cessar ato contrário a esta norma.

Faz-se necessária a distinção entre a dimensão do direito à privacidade propriamente dito e a proteção aos dados pessoais no contexto da sociedade da informação. A privacidade remete a uma ideia de reclusão e de se retirar da vida pública, assim, tem uma dimensão mais interna. No contexto digital e principalmente nas questões envolvendo políticas públicas, a privacidade em seu sentido literal se torna inviável. Seria pouco procedimental que o indivíduo desejasse se retirar do espaço público quando as políticas públicas de desenvolvimento que o beneficiam dependem de certos dados pessoais.

Fala-se em proteção aos dados pessoais não como uma proteção absoluta, mas como uma tutela que deve ser exercida com certas limitações acerca das informações obtidas por um controlador. Focando na questão das políticas públicas, é essencial que o poder público tenha informações seguras e verídicas para que possa traçar e executar projetos que atendam às demandas da população.

A ideia individualista da proteção à privacidade deve ser superada tendo em vista os frequentes vazamentos de dados de sistemas públicos, tais como aplicativos e sistemas de tribunais, que demonstram as falhas de segurança e a vulnerabilidade de um sistema que deveria primar pela proteção aos dados, sobretudo em plena digitalização dos processos e dos serviços públicos. Tal ataque representa uma invasão à privacidade, visto que no processo há provas e informações sigilosas sobre a vida das partes, sendo inadmissível que o indivíduo tenha os seus direitos violados ao recorrer à Justiça.

3.2 O DIREITO À PERSONALIDADE

O direito à personalidade é um direito humano reconhecido internacionalmente e positivado pelo Estado brasileiro como um direito fundamental. Trata-se de um direito personalíssimo e intransmissível reconhecido à pessoa humana tomada em suas projeções perante a sociedade, abrangendo o complexo valorativo intrínseco, podendo ser exercido somente pelo seu titular.

A constitucionalização deste direito se dá como forma de limitar as intervenções do Estado por meio das políticas públicas (BITTAR,

2015), e também por outros meios, assegurando que não ocorram violações aos direitos autorais, de imagem e a coleta de dados pessoais para fins indevidos.

Nessa perspectiva, pode-se dizer que os dados pessoais são uma extensão da personalidade humana uma vez que tais dados servem como elementos caracterizadores e individualizadores de uma pessoa, permitindo que quem colete esses dados faça suposições e identifique seu titular.

Dessa forma, a coleta de dados pessoais no meio digital deve ter como premissa o consentimento expresso do titular. O agente de tratamento de dados deve especificar as finalidades e por quanto tempo se dará a coleta e o tratamento dos dados, as condições de uso e os prazos que regem a concessão de tais informações cedidas. A LGPD em seu artigo 5º, inciso XII, considera o consentimento como uma "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada".

O artigo 8º e seus parágrafos tratam especificamente acerca do consentimento do titular, que deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular, sendo vedado o tratamento de dados pessoais mediante vício de consentimento. O consentimento deve se referir a finalidades previamente determinadas e especificadas, sendo nulas as autorizações genéricas. Pode ainda, ser revogado a qualquer momento pela manifestação do titular.

Vislumbra-se que o consentimento é o meio pelo qual o titular dos dados permite que uma informação a seu respeito se torne pública, ou, pelo menos, acessível para determinada pessoa física ou jurídica. Retoma-se do capítulo anterior, que a privacidade é justamente a pretensão de o indivíduo determinar quando e como determinada informação sobre ele será comunicada a terceiros (DANTAS, Ribeiro). Ainda, de acordo com a Ministra Rosa Weber, em seu voto proferido na ADI 5527, "o direito à privacidade está alinhado com do seu papel social na própria preservação da personalidade e no desenvolvimento da autonomia individual".

Levando-se em consideração a conjugação dos direitos fundamentais à privacidade e à personalidade em matéria de proteção de dados pessoais, tem-se como resultado a autodeterminação informativa, que é justamente o exercício de controle sobre as informações que o titular cedeu a outra pessoa para a persecução de determinada finalidade.

A expressão apareceu pela primeira vez na Alemanha, tendo influenciado demais ordenamentos jurídicos, inclusive a legislação brasileira referente à proteção de dados. Tal direito (reconhecido pela Corte Constitucional Alemã em 1983) surgiu da proteção da personalidade como direito fundamental e do livre desenvolvimento dessa, representando uma "proteção do mínimo de liberdade de ação humana, sem a qual o homem não é capaz de desenvolver sua essência como personalidade mental e moral". (KUBE, 2009, p. 90; JARASS, 1996, p. 89-90 apud MENDES, 2001, p. 2).

Mais tarde, a Corte Constitucional Alemã afirmou entendimento de que a Constituição garante à pessoa humana valor social e respeito, sendo vedado ao Estado catalogar um indivíduo com todas as informações que envolvem sua personalidade de forma coercitiva, o que não seria compatível com a dignidade humana (daí a importância do consentimento nas normas de proteção de dados). Além disso, o Tribunal considerou que no livre desenvolvimento da personalidade deve existir um "espaço interior" (*Innenraum*, do alemão) no qual o indivíduo possa ter a posse de si mesmo. (BVerfGE 27, 1 Mikrozensus[5]).

Como anteriormente mencionado, a autodeterminação informativa surge após a coleta dos dados e do processamento da informação mediante prévio consentimento do titular. Visto que nem todo levantamento estatístico de dados viola a personalidade humana em sua dignidade ou afeta seu direito à autodeterminação, seria mais adequado substituir a esfera estritamente privada por uma abordagem orientada à informação e que ao mesmo tempo, garanta proteção a um direito fundamental (STEINMÜLLER et al., 1971, p. 88; 93 apud MENDES, 2001, p. 10).

Desse modo, o aspecto procedimental da autodeterminação informativa e da proteção aos dados pessoais (lembrando-se sempre da distinção entre essa e a privacidade) quanto aos dados coletados para fins de políticas públicas será devidamente explicado em momento oportuno.

---

[5] Decisão do Tribunal Constitucional Federal Alemão (*Bundesverfassungsgericht*) sobre a constitucionalidade das estatísticas representativas (*Zur Verfassungsmäßigkeit repräsentativer Statistiken*), decisão nº 27,1 de 16 de julho de 1969. Disponível em: https://www.servat.unibe.ch/dfr/bv027001.html

3.3 A DEMOCRACIA DIGITAL À LUZ DOS DIREITOS FUNDAMENTAIS

As plataformas digitais têm ampliado a existência do espaço público para o espaço virtual, no qual se apresenta em uma via de mão dupla: não só se recebe informações, como também é possível se expressar e se comunicar com os demais. Os meios digitais permitem realizar o ideal da democracia, isto é, o poder de exercer opiniões com liberdade – na medida da Constituição Federal e com respeito aos direitos fundamentais – além de propiciar a participação e o engajamento da sociedade civil nos assuntos públicos.

Desse modo, os intermediários entre a sociedade civil e o Estado são suprimidos no meio digital e o cidadão passa a se comunicar diretamente com o sistema político e seus membros sem tais instituições intermediárias, como a burocracia e os partidos políticos. Assim, a chamada democracia digital é uma digitalização de determinadas dimensões dos Estados democráticos. (GOMES, 2010, p. 4).

A democracia no meio digital pode ser exercida com objetivos políticos ou cívicos sem interação com o Estado, abrangendo o ativismo e a militância, a mobilização eleitoral, por meio da liberdade de imprensa e pela troca de informações. Pode ainda ser exercida utilizando-se do espaço virtual para a participação em processos legislativos (e-democracia).

A primeira forma de se exercer a democracia no espaço virtual apresenta-se como a mais comum e usual, por meio da expressão de ideias, opiniões e posicionamentos políticos. Nesse espaço, as informações se dão em uma quantidade massiva e infinitamente superior à capacidade de serem processadas, dessa forma, os usuários acabam por consumir apenas aquilo que está de acordo com suas predileções e com seu viés de confirmação.

É nesse cenário que surge fenômenos como os filtros-bolhas que funcionam de maneira a personalizar, automaticamente, o conteúdo a ser consumido, vez que o *machine learning* (de acordo com as preferências do usuário bem como os caminhos por ele percorrido na internet) possibilita essa filtragem direcionada para que o consumo e o tempo de permanência deste usuário nas redes sociais sejam maiores. Esses filtros limitam ou até mesmo suprimem conteúdos que vão de encontro com o viés ideológico do usuário e inibem os debates

construtivos que fundamentam a democracia, podendo, fatalmente, resultar em discursos de ódio e intolerância.

Essas filtragens geram lucros para algumas empresas: o fornecimento de dados pessoais que possibilita traçar um perfil comportamental do usuário gera capitalização dos dados, e quanto mais dados forem vendidos e comprados pelos provedores para as mais variadas finalidades, maior o lucro. Evgeny Morozov (2013, p. 149) aponta os riscos dos filtros-bolha a partir da premissa de um solucionismo que busca implantar a tecnologia para se evitar a política:

> Esses novos filtros podem ser mais rápidos, mais baratos e mais eficientes, mas velocidade, custo e eficiência estão apenas perifericamente relacionados aos papeis cívicos que tais filtros e algoritmos exercerão em nossas vidas. Ao não submeter estes ao devido escrutínio ético, corremos o risco de incidir sobre uma das muitas falácias do "solucionismo" e de celebrar melhorias relacionadas a problemas menos importantes em detrimento temas mais quentes, apesar de menos óbvios.

Não são raros os casos de empresas de marketing direcionado que compram dados com a intenção de usá-los para o impulsionamento de propagandas eleitorais. Tais empresas coletam os dados pessoais através de redes sociais e formulários que são facilmente encontrados e acessados pela *internet*. Cita-se brevemente o escândalo envolvendo a Cambridge Analytica às vésperas das eleições norte-americanas em 2016. A empresa trabalha com marketing de dados direcionados combinando a mineração e a análise de dados pessoais para elaboração de conteúdos estratégicos, por meio de uma análise psicográfica e comportamental dos indivíduos conhecida pela expressão *behavioral sciences*.[6]

Desse modo, elaboraram um formulário de personalidade que poderia ser acessado pelo *Facebook*, e abordava questões sobre posicionamentos e predileções políticas, religião, idade, além da coleta de dados por meio de *cookies* e por meio de informações previamente cadastradas no perfil do usuário. A finalidade do questionário – embora

[6] A *behavioral sciences* atua na identificação de cinco perfis: 1) abertura: receptividade da pessoa a novas experiências; 2) nível de consciência: cuidado do indivíduo com organização e eficiência; 3) extroversão: grau de sociabilidade e tendência a encarar positivamente os acontecimentos; 4) amabilidade: nível de empatia, sensibilidade e cooperação com os outros; e 3) instabilidade emocional ou neurose: intensidade emocional ao obter informações e condição de reação (FLORES, 2017).

nenhum usuário tivesse conhecimento – era a de segmentar, individualmente, a personalidade de cada pessoa que preencheu o questionário para que manchetes sensacionalistas e inverídicas e propagandas eleitorais fossem direcionadas exclusivamente para cada tipo de personalidade.

Aqui se faz um alerta para os riscos que as *fakes news* oferecem para a democracia, considerando que estas são rapidamente disseminadas dadas as suas características alarmistas e apelativas que estimulam a descrença nas instituições políticas que já se encontram, de certo modo, fragilizadas.

A desinformação se diferencia das notícias falsas, pois aquelas são informações imprecisas que são disseminadas independentemente da vontade de enganar. De acordo com o mencionado na obra Democracy and Fake News (Politics, Media and Political Communication) publicada pela Routledge, as *fakes news* podem ser entendidas como uma versão avançada e tecnológica da desinformação, sendo que essas possuem a intenção de enganar e manipular a opinião pública com uma construção falsa ou alternativa da realidade. Tal fenômeno pode resultar na pós-verdade política, uma subversão da verdade que consiste em aceitar como verdadeiros os argumentos baseados em suas próprias emoções e convicções.

Desse modo, resta evidente que a *internet* e o uso de dados pessoais estão, de certo modo, relacionados com a forma com que exercemos a democracia. Implicam na análise acerca dos limites das liberdades individuais de se manifestarem publicamente, tendo em vista que a disseminação de informações e ideias é extremamente mais rápida do que nos meios convencionais. A disseminação cada vez mais frequente e intencional de notícias falsas restringe o acesso à informação verdadeira, limitando a capacidade de um debate crítico e construtivo na sociedade, afastando-se do ideal democrático participativo.

Ainda, a coleta de dados feita de maneira indevida pode impactar, negativamente, as relações internacionais e diplomáticas entre os Estados, como é o caso da Agência de Segurança Nacional (NSA) dos Estados Unidos em 2001, que passou a vigiar, sistematicamente, outros países e qualquer pessoa que entrasse em seu território com a justificativa de combater o terrorismo. Essa forma de espionagem recebeu o nome de *dataveillance* por Roger Clarke em 1988 e significa um monitoramento sistemático por meio de dados pessoais com a finalidade de governar seu comportamento e prever acontecimentos.

O episódio de 11 de setembro foi o estopim para que diversos países passassem a se preocupar efetivamente com leis de proteção de dados, sendo que de outubro de 2013 a abril de 2014, o Brasil se debruçou na elaboração do Marco Civil da Internet, primeira legislação tratando sobre internet e dados pessoais. Logo após, iniciou-se o processo de elaboração de um anteprojeto que mais tarde, viria a ser a atual LGPD. Assim, a proteção aos dados pessoais e o cumprimento da LGPD precisam ser eficazes, vez que se conjugam os direitos da privacidade, da personalidade, da autodeterminação informativa e do exercício da democracia.

4. O USO DA TECNOLOGIA DE DADOS PELO PODER PÚBLICO

É por meio das políticas públicas que há a efetivação de direitos fundamentais e a realização de objetivos socialmente relevantes que são demandados pela população. É também por meio das políticas públicas como um dever de prestação positiva do Estado, que se faz cumprir com os objetivos fundamentais da República Federativa do Brasil dispostos pela Constituição Federal.

Como bem conceitua Maria Paula Bucci (2002):

> Políticas públicas são programas de ação governamental visando a coordenar os meios à disposição do Estado e as atividades privadas para a realização de objetivos socialmente relevantes e politicamente determinados. Políticas públicas são "metas coletivas conscientes" e, como tais, um problema de direito público, em sentido lato.

O avanço tecnológico e a digitalização dos serviços públicos facilitaram a coleta de informações pelo Poder Público, propiciando um maior conhecimento das demandas da população.

Não é de hoje que governos no mundo inteiro têm aderido à tecnologia como forma de facilitar a comunicação com seus cidadãos ou tornar mais eficaz a execução de políticas públicas. No entanto, apenas recentemente, as preocupações e indagações quanto à proteção dos dados e a garantia a tais direitos vieram à tona, tanto por parte de acadêmicos quanto pela própria sociedade.

Inúmeros aplicativos são desenvolvidos pelo governo federal, estadual e municipal e colocados à disposição da população para a digitalização de serviços públicos e para dar celeridade às demandas sociais. Tais aplicativos pedem a concessão de inúmeros dados pessoais e dados pessoais sensíveis (nome, idade, sexo, dados clínicos de saúde, biometria *etc.*) sendo de extrema importância que o tratamento desses dados se dê de maneira limitada a atingir os objetivos pelos quais foram coletados, sempre visando à proteção e o não fornecimento desses para terceiros.

O capítulo IV da Lei Geral de Proteção de Dados é destinado a regular o tratamento de dados pelo Poder Público, enfatizando a persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público sempre fornecendo informações claras sobre a finalidade e os procedimentos realizados durante o tratamento.

Importante mencionar o art. 25 da referida lei:

> Art. 25. Os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral.

No sistema de interoperabilidade é adotado o "padrão aberto", que significa um sistema disponível publicamente não controlado por governos ou outras empresas. Desse modo, é possível uma comunicação totalmente transparente seja com o público em geral, seja com outros sistemas informatizados.

Conforme mencionado no parágrafo 39 da Declaração de Princípios da Cúpula Mundial sobre a Sociedade da Informação, o uso de padrões abertos e transparentes são os pilares para o desenvolvimento de uma sociedade mais digitalizada e centrada nas pessoas, devendo-se prezar os benefícios do uso das TIC´s para o desenvolvimento de políticas públicas mais eficientes.

Primeiramente, é de se ressaltar a necessidade do consentimento do titular como base legal para o acesso a determinados dados, que consiste em uma manifestação livre e espontânea, informada e inequívoca, autorizando a coleta e o tratamento dos dados para um determinado fim. A LGPD conta ainda com outros requisitos para que a

administração pública possa exercer atividades relacionadas ao uso de dados: a) quando necessário à execução de políticas públicas previstas em leis; b) para a realização de pesquisas (como censo populacional e escolar, por exemplo); c) execução de contratos celebrados entre o titular e a administração pública para a concessão de serviços públicos; d) para o exercício regular de direitos em processo judicial e administrativo; e) para a tutela da saúde (há permissão para o tratamento sem o consentimento do titular em alguns casos); f) para a proteção de crédito.

Para que o Poder Público possa coletar e tratar dados pessoais, não deve observar apenas as normas dispostas na LGPD, mas conjugá-las com outras leis, como o Marco Civil da Internet, a Lei de Acesso à Informação, Lei do Habeas Data, Lei Geral do Processo Administrativo e o Código de Defesa do Consumidor.

Os órgãos da administração pública devem ainda registar todas as operações de tratamentos de dados elaborando relatórios que contenham a descrição dos dados coletados, a metodologia utilizada para garantir a segurança e os mecanismos de mitigação de riscos, sempre indicando o encarregado pelo tratamento dos dados de forma pública e objetiva, para que esse possa adotar providências a serem tomadas mediante comunicação com os titulares ou com a ANPD. Devem ainda conceder o acesso imediato à informação disponível para que o titular exerça seu direito da autodeterminação informativa.

Atualmente, tem crescido o número de cidades interessadas em implantar a chamada *smart city*, ou cidade inteligente, que tem como premissa o uso da tecnologia e o uso de dados pessoais. Em outras palavras, *smart city* significa a contratação de soluções tecnológicas pelo poder público (ZANATTA, MOROZOV, 2019) com a finalidade de buscar soluções para problemas sociais e políticos por meio da infraestrutura de coleta e análise de dados dos cidadãos.

Evgeny Morozov e Francesca Bria (2019) apontam dois motivos pelos quais o Poder Público pode optar pelas soluções da cidade inteligente, sendo eles normativos e pragmáticos. O motivo normativo se traduz pelo empenho em inserir a tecnologia para alcançar metas políticas, fomentar a participação cidadã nas decisões políticas e a personalização dos serviços públicos atendendo às demandas da população. O motivo pragmático, por sua vez, se traduz em buscar as tecnologias visando uma economia no fornecimento de serviços públicos (muitas vezes através de empresas privadas) e reforçar a segurança

pública por meio da vigilância direcionada a áreas até então pouco alcançadas.

Contudo, o excesso de vigilância pode impactar, negativamente, a privacidade, visto que para a consecução de segurança pública, por exemplo, a coleta de dados sobre endereço e classe social pode gerar um policiamento preditivo (*predictive policing*) e reforçar desigualdades. O policiamento preditivo é uma estratégia de segurança pública que consiste na indicação de prováveis crimes tendo como base a análise de dados criminais passados para predizer atividades criminais futuras (BACHNER, apud JOH, 2014, p. 42), que podem ser obtidos por bancos de dados do Estado, Sistemas de Justiça Criminal, dados socioeconômicos e demográficos e até mesmo de redes sociais.

Em alguns casos, são desenvolvidos *softwares* que geram listas para identificar pessoas, locais e situações com maiores possibilidades de estarem cometendo delitos. Alguns estudos sobre a eficácia desse tipo de sistema foram feitos e apontaram uma diminuição na porcentagem de assaltos e furtos. Contudo, por ser um sistema preditivo, muitas pessoas acabam sendo presas por crimes que não cometeram, ficando afastado o princípio da presunção de inocência.

Além disso, essa prevenção primária ou preditiva não evita o crime, mas desloca a sua prática. Desse modo, o Poder Público estaria coletando a armazenando dados para atingir objetivos que não são tão claros e eficientes, aumentando o risco de se criminalizar certos elementos sociais e condutas.

No entanto, o uso de dados pessoais para fins de segurança pública não está no escopo de proteção da LGPD, devendo ser regida por lei específica e prever medidas proporcionais e estritamente necessárias ao interesse público, observados os princípios gerais de proteção de dados e o devido processo legal. Até hoje, tal lei não foi elaborada, criando um cenário panóptico, tal como concebido por Bentham, no qual um único vigilante observa a todos, sem que ninguém saiba quando está de fato sendo vigiado.

Assim, as políticas públicas, como um dever de prestação positiva do Estado, que se faz cumprir com os objetivos fundamentais da República, devem ser meios de efetivar também os direitos humanos e fundamentais reconhecidos pela Constituição e pelos Tratados Internacionais. Desse modo, o Estado ao formular políticas públicas que venham a atender as demandas sociais, não deve ser ator de violação da proteção aos dados pessoais.

CONSIDERAÇÕES FINAIS

Tendo discorrido sobre como a *internet* tem possibilitado a digitalização do espaço público para o virtual, no qual o usuário passa a viver social e politicamente, desenvolvendo sua personalidade e exercendo seu direito de informação e expressão, faz-se necessária uma proteção jurídica aos dados pessoais visto que esses são a representação do indivíduo perante a sociedade.

Restou demonstrada a facilidade com que os dados pessoais podem ser acessados e coletados, fugindo ao controle do usuário que vê desrespeitado o seu direito à privacidade, à autodeterminação informativa, isto é, a capacidade de controlar seus próprios dados e de ter o conhecimento sobre como esses estão sendo usados.

Esta facilidade pode ainda favorecer a criação e a divulgação de notícias falsas e restringir o acesso a informações verídicas, pois como mencionado, o desenvolvimento cada vez mais acentuado da tecnologia permite ter o conhecimento do comportamento do usuário para que a ele seja direcionado determinado conteúdo. A coleta massiva de dados e *cookies* (fragmentos que o usuário deixa pelos caminhos trilhados na *internet*) favorece ainda a formação de filtros-bolhas que acabam por restringir o tipo de conteúdo acessado.

Dessa forma, a Lei Geral de Proteção de Dados surgiu com o propósito de mitigar esses e outros problemas relacionados ao uso indevido de dados pessoais, seja por pessoas jurídicas, seja pela administração pública. A referida lei representou um avanço do país no sentido de dar maior segurança aos usuários bem como de impor procedimentos a serem observados pelos operadores de dados, além de inserir o Brasil no rol de países determinados em estabelecer uma proteção jurídica para as atividades realizadas no meio digital.

Tal proteção deve ser tida como um direito fundamental e autônomo, não bastando apenas que decorra do direito à privacidade ou da dignidade da pessoa humana em seus desdobramentos. É necessário de pleno mérito, que tal proteção seja integrada ao rol dos direitos fundamentais já consolidados no artigo 5º da Constituição Federal, como uma forma de se evitar que futuras leis possam permitir o uso indevido dos dados pessoais e, consequentemente, prejudicar os seus titulares.

REFERÊNCIAS

BITTAR, C. A. **Os Direitos da Personalidade.** 8. ed. São Paulo: Saraiva, 2015.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. **Lei de Acesso à informação.** Brasília, 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm Acesso em: 10 out. 2020.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Brasília, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 01 out. 2020.

BUCCI, Maria Paula Dallari. **Direito administrativo e políticas públicas**. São Paulo: Saraiva, 2002. p. 241.

CASTELLS, Manuel**. A Galáxia Internet: reflexões sobre a Internet, negócios e a sociedade.** Rio de Janeiro: Jorge Zahar Ed., 2003. Tradução: Maria Luiza X. de A. Borges.

COTRIM, Gilberto. **Fundamentos da Filosofia**. São Paulo: Saraiva, 2006, p. 96.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço jurídico,** Joaçaba, v.12, n. 2, p. 91-108, jul./dez. 2011.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

FARIA, Cristiano Ferri Soares de. **O Parlamento aberto na era da internet**: pode o povo colaborar com o legislativo na elaboração das leis? Brasília: Câmara, 2012. p. 96

GENAVA. World Summit on the Information Society. **Declaration of Principles Building the Information Society:** a global challenge in the new Millennium. Geneva, 12 de dezembro de 2003. Disponível em: http://www.itu.int/net/wsis/docs/geneva/official/dop.html Acesso em: 06 jan. 2021

GRASSEGGER, Hannes; KROGERUS, Mikael. The Data That Turned the World Upside Down. Nova Iorque: **Vice,** 2017. Disponível em: https:// www.vice.com/en_us/article/4x4x8n/the-data-that-turned-the-world-upside-down Acesso em: 20 out. 2020.

JOH, E. E. Policing by numbers: Big data and the 4th Amendment. **Washington Law Review**, v. 89, 2014. Disponível em: https://digitalcommons.law.uw.edu/wlr/vol89/iss1/3/ Acesso em: 15 jan. 2020

MAYBIN, Simon. Sistema de algoritmo que determina pena de condenados cria polêmica nos EUA. ***In*** BBC News Brasil, 31 out. 2016. Disponível em: https://www.bbc.com/portuguese/brasil-37677421 Acesso em: 07 out. 2020.

MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. **Pensar Revista de Ciências Júridicas Universidade de Fortaleza** (Unifor), Fortaleza, v. 25, n 4, p. 1-18, out./dez. 2020. Disponível em: https://periodicos.unifor.br/rpen/article/view/10828 Aceso em: 01 jul. 2021.

MOROZOV, Evgeny; BRIA, Francesca. **A cidade inteligente.** Tecnologias Urbanas e Democracia. 1. ed. Ubu Editora, 2020.

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho (**General Data Protection Regulation**). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679 Acesso em: 10 set. 2020.

RODOTÀ, Stefano. Democracia y protección de datos. **Cuadernos de Derecho Público**, nº. 19-20. 2003.

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

SCHWAB, Klaus. **A quarta Revolução Industrial**. Tradução de Daniel Moreira Miranda São Paulo: Edipro, 2016.