ISSN 1982-0496

INDEPENDÊNCIA DA AUTORIDADE FISCALIZADORA E EFETIVIDADE DA PROTEÇÃO DE DADOS PESSOAIS NA SOCIEDADE EM REDE

INDEPENDENCE OF SUPERVISORY AUTHORITY AND EFFECTIVENESS OF PROTECTION OF PERSONAL DATA IN THE NETWORK SOCIETY

Paulo Jorge Silva Santos

Doutorando em Direito pela Universidade de Brasília – UNB (2020). Mestre em Direito pela Universidade de Marília - UNIMAR (2020). Especialização em Direito Imobiliário e Urbanístico. (2017). Especialização em Direito Tribuário (2017). Graduação em Direito – UFAC (2011). Professor de Direito da Faculdade da Amazônia Ocidental - FAAO, Professor de Direito do Instituto Federal de Educação, Ciência e Tecnologia do Acre – IFAC. Advogado.

Mariana Ribeiro Santiago

Pós-Doutorado em Direito Civil pela Justus-Liebig-Universität Gießen (Alemanha), sob a supervisão da Prof. Dr. M.A. LL.M. S.J.D. (Harvard) Marietta Auer. Doutora (2011) e Mestre (2004) em Direito Civil Comparado pela Pontifícia Universidade Católica de São Paulo, sob a orientação da Profa. Dra. Maria Helena Diniz. Especialista em Direito Contratual pela Pontifícia Universidade Católica de São Paulo (2002). Graduada em Direito pela Universidade Federal da Bahia (1999). Professora do Programa de Mestrado e Doutorado em Direito e da Graduação em Direito da Universidade de Marília - UNIMAR. Professora visitante da Univerdidad Católica de Colombia. Associada ao Instituto dos Advogados de São Paulo – IASP. Membro da Comissão Permanente de Estudos de Direito da Mulher do IASP. Advogada.

Resumo

O presente artigo busca demonstrar a importância de se conceder independência e autonomia à Autoridade de Proteção de Dados Pessoais, instituição que se constitui como base para a eficácia e efetividade da Lei Geral de Proteção de Dados Pessoais, através de sua transformação em autarquia especial federal. Para este fim, é apresentado um desenho do atual contexto por que passa a sociedade e, consequentemente, a economia mundial, os quais ganharam os novéis conceitos de sociedade em rede e economia da informação. Procede-se a uma análise do que venha ser *Big Data*, com o intuito de sedimentar o caminho para se entender o contexto em

que nasceram as leis de proteção aos dados pessoais em todo o mundo. Percorre-se a evolução dos normativos de proteção da privacidade e dados pessoais, os quais foram delineados em quatro gerações. Explica-se o conceito, a função, a importância e a posterior ineficácia do papel do consentimento como instrumento único de proteção de tais direitos. Por fim, busca-se demonstrar a importância de dotar tal entidade de um mínimo de independência e autonomia, imperativo para que essas instituições alcancem a finalidade para a qual foi criada. O método de abordagem utilizado é o dedutivo, com o auxílio do método de pesquisa bibliográfico. Conclui-se que a independência de uma autoridade nacional de proteção de dados amplia a efetividade da legislação específica sobre a matéria.
Palavras-chave: Autoridade Nacional de Proteção de Dados. *Big Data.* Economia da informação. Lei Geral de Proteção de Dados Pessoais.

Abstract

This article seeks to demonstrate the importance of granting independence and autonomy to the Personal Data Protection Authority, an institution that is the base to effectiveness and effectiveness of the General Law of Protection of Personal Data, through its transformation into a special federal authority. To this end, it is presented a drawing of the current context through which society and, consequently, the world economy pass, which have gained the noble concept of networked society and information economy. An analysis is made of what Big Data will be, with the aim of laying the groundwork for understanding the context in which personal data protection laws were born all over the world. The evolution of the norms of protection of the privacy and personal data, which have been delineated in four generations, is traversed. The concept, function, importance and subsequent ineffectiveness of the role of consent as a single instrument for the protection of such rights is explained. Finally, it seeks to demonstrate the importance of providing such entities with a minimum of independence and autonomy, imperative for these institutions to achieve the purpose for which they were created. The method used is the deductive method, with the aid of bibliographic research method. The conclusion is that the independence of a national data protection authority increases the effectiveness of specific legislation about the subject.
Keywords: Big data. General Law of Protection of Personal Data. Information economy. National Authority for Data Protection.

1. CONSIDERAÇÕES INICIAIS

O progresso exponencial vivido pela humanidade, ocorrido principalmente na segunda metade do século XX, trouxe, a reboque, grandes desafios para a ciência jurídica. Trata-se do processo de disrupção causado pelas tecnologias da informação, que transformou substancialmente todas as bases da sociedade mundial. Na seara econômica, houve a transição de uma economia pautada na produção em massa de produtos e serviço para produção de informação, a qual tem como insumo principal a coleta, análise e tratamento de dados dos indivíduos em sociedade.

Bancos, empresas de seguros, planos de saúde, mercadores em geral e até o próprio Poder Público se pautam nos resultados advindos do processamento de

informação para direcionarem suas ações. Chega-se a um processo em que a informação tratada gera mais informação, com uma carga valorativa maior. Bancos conseguem avaliar melhor para quem podem oferecer seus créditos, bem como o grau de risco envolvido. Empresas de seguros conseguem ter maior previsibilidade em suas ações e atuações, não obstante operarem com contratos aleatórios, aumentando exponencialmente seus lucros. Planos de saúde conseguem adequar suas ações de acordo com o a clientela, direcionando e alterando os preços com base na informação gerada sobre os dados coletados de seu público. Tudo isso se constitui o atual cenário denominado big data.

Nesse cenário, surgem dúvidas sobre qual o ponto de equilíbrio entre a sanha irrefreável dessa nova economia, que se sustenta na absorção de dados pessoais, e a privacidade do titular de tais dados, mormente diante da magnitude constitucional dos direitos envolvidos. Outro ponto que merece análise é o papel de uma autoridade central na regulamentação, fiscalização e proteção integrada e efetiva do direito de privacidade das pessoas.

O Brasil, seguindo a mesma trilha dos países Europeus, promulgou a Lei Geral de Proteção de Dados Pessoais - LGPD e se insere em um contexto mundial de vanguarda a respeito da proteção à privacidade. Não obstante, peca em não conceder autonomia a sua Autoridade Nacional de Proteção de Dados - ANPD, fato que pode colocar em xeque a total efetividade da própria LGPD.

Nessa linha, o objetivo deste artigo é analisar a importância do Brasil conceder independência e autonomia para ANPD prevista na LGPD, através de sua transformação em autarquia especial pertencente à Administração Pública Indireta Federal, e como isso impacta de fato a defesa da privacidade em relação aos titulares dos dados.

Para tal desiderato, de início, explica-se o atual contexto porque passa a sociedade mundial, qual recebeu o nome de “sociedade da informação” pelo sociólogo Manuel Castells, o conceito de *big data*, bem como sua utilização em uma novel economia, denominada de economia da informação. Após isso, apresenta-se um panorama dos diplomas de proteção de dados, bem como o funcionamento desse sistema regulatório e a sua repercussão na proteção ao direito de privacidade. Por fim, examina-se a real necessidade da independência de uma autoridade nacional de proteção de dados para a efetividade da legislação específica sobre a matéria.

Quanto à questão metodológica, o método de abordagem utilizado é o dedutivo, partindo-se da análise da norma geral para alcançar a compreensão dos casos particulares. O método de pesquisa é o bibliográfico, com recurso a obras técnicas especializadas.

2. SOCIEDADE EM REDE, BIG DATA E A ECONOMIA DA INFORMAÇÃO

A história é marcada por diversos fatos e acontecimentos que vão moldando o desenvolvimento do homem. Alguns, todavia, em virtude do grande impacto causado nesse cenário de contínuo desenvolvimento, acabam por se destacar e se diferenciar dos demais fatos históricos.

A abrangência e impacto da tecnologia atual na vida do homem são de significativa densidade, a ponto de causar uma disrupção em sua evolução. Por disrupção entenda-se a interrupção do curso normal de um processo (HOUAISS, 2001). Entender o conceito de disrupção é o primeiro passo para compreender o vocábulo revolução usado pela maioria dos pesquisadores para se referir aos grandes acontecimentos da história humana que ocasionaram um salto singular, incomum e profundamente impactante no processo evolutivo do homem.

Revolução agrícola, primeira e segunda revoluções industriais são exemplos de acontecimentos que causaram essa disrupção na estrutura da sociedade. A partir do momento em que o homem passou a dominar as técnicas agrícolas, deixou de ser nômade e passou a conviver com seus pares, formado um núcleo social. A partir da interação social, houve a aglomeração de pessoas no mesmo espaço territorial, dando início às cidades. Mais tarde, o acúmulo de produtos agrícolas diferenciados deu início à troca de produtos, ou seja, ao comércio.

Assim como a revolução agrícola deu início a uma série de fatos sociais e históricos disruptivos, a primeira e segunda revoluções industriais desempenharam o mesmo papel de destaque, mudando totalmente o modo de ser dos humanos.

Atualmente, nossa sociedade está absorvendo as consequências da última grande revolução por que passou a humanidade: a revolução das tecnologias da informação. Conforme assinala Castells (2005a, p. 67), “o surgimento de um novo paradigma tecnológico, organizado com base na tecnologia de informação começa a remodelar a base material da sociedade em ritmo acelerado”. Esta revolução, tal como

as outras que a antecederam, desencadeou um processo de disrupção em nossa sociedade, estabelecendo um novo paradigma ou um padrão de descontinuidade.

De acordo com Castells (2005a, p. 67-69), este novo paradigma pode ser assim descrito:

> Meu ponto de partida, e não estou sozinho nesta conjetura, é que no final do século XX vivemos um desses raros intervalos na história. Um intervalo cuja característica é a transformação de nossa "cultura material" pelos mecanismos de um novo paradigma tecnológico que se organiza em torno da tecnologia da informação. O que caracteriza a atual revolução tecnológica não é a centralidade de conhecimentos e informação, mas a aplicação desses conhecimentos e dessa informação para a geração de conhecimentos e dispositivos de processamento/comunicação da informação, em um ciclo de realimentação cumulativo entre a inovação e seu uso.

A disrupção ou padrão de descontinuidade pode ser entendido como a característica de penetrabilidade desta revolução em todos os domínios da atividade humana. O cerne da transformação que se vivencia atualmente são as tecnologias da informação, processamento e comunicação. Dessa forma, o que caracteriza a revolução em referência não é acumulação de conhecimentos e informação, mas a aplicação destes para a produção de mais conhecimentos e de dispositivos de processamento e comunicação da informação, desenhando um ciclo em que ocorre a realimentação cumulativa da inovação ao seu uso.

Esse padrão de descontinuidade é que vem causando uma série de mudanças econômicas, sociais e culturais. Dentre as principais transformações que ensejaram esse novo paradigma, deve-se destacar a que ocorreu na área da economia, qual seja, a migração para uma economia centrada na informação (BENKLER, 2006, p. 15). Isso é facilmente perceptível com a ascensão de serviços financeiros, *software* e ciência, na atribuição de valor aos produtos por meio de marcas, em nítida manipulação de símbolos, na produção cultural, com a indústria de filmes e música e, principalmente, na manipulação de dados, notadamente os pessoais, como insumo propulsor dessa nova engrenagem econômica (BENKLER, 2006, p. 13).

A terminologia usada por Castells para denominar esse fenômeno é "sociedade em rede". De acordo com este sociólogo (CASTELLS, 2005b, p. 20):

> A sociedade em rede, em termos simples, é uma estrutura social baseada em redes operadas por tecnologias de comunicação e informação fundamentadas na microelectrónica e em redes digitais de computadores que

> geram, processam e distribuem informação a partir de conhecimento acumulado nos nós dessas redes.

Informacional, global e em rede são as características fundamentais e diferenciadas que molduram essa nova economia e enfatizam a sua interligação. Informacional porque a competitividade e produtividade dependem basicamente da capacidade de gerar, processar e aplicar eficientemente a informação baseada em conhecimentos. Global porque as principais atividades produtivas, seus substratos, a circulação e o consequente consumo estão dispostos em escala mundial. Em rede porque a produtividade é gerada e a competitividade é feita em uma rede de interação global entre os setores empresariais (CASTELLS, 2005a, p. 119).

Os avanços no setor da tecnologia da informação transformaram radicalmente o modo de viver do ser humano. Se antes, para ter acesso a conhecimento, precisava-se ir a uma biblioteca, tendo-se que se contentar com seu limitado acervo, hoje isso é facilmente feito da própria casa, onde a pessoa, através da internet, consegue, de forma simples, acessar as mais variadas e profundas pesquisas científicas e produções literárias. O modo de se fazer entretenimento mudou. Houve uma democratização do acesso à mídia. Antes, esse acesso estava sob o monopólio das grandes empresas de mídia televisiva; hoje, qualquer pessoa pode postar um vídeo no *youtube* e, da noite para o dia, virar uma celebridade. Investir nas bolsas de valores mobiliários não era uma realidade palpável para outras classes afora a alta sociedade, que sequer conseguiam ser atendidas por uma corretora de valores, a qual focava suas atenções para o grande investidor. Os bons professores ou as boas universidades só poderiam ser alcanças por aqueles nasciam e se criavam nos grandes centros, tendo a oportunidade, financeira ou social, de conseguir adentrar a esses grandes centros do conhecimento; hoje, a internet possibilita o ensino à distância, democratizando a educação de ponta.

Esses são poucos exemplos de uma gama de transformações vivenciadas pela sociedade desde o começo da segunda metade do Século XX. Essa nova realidade levou à criação do conceito de onipresença ou ubiquidade dos meios informáticos (BENKLER, 2006, p. 20).

Com o alvorecer da Revolução Industrial, inaugurou-se um modelo econômico de produção em massa, com fornecimento a baixo custo de grandes quantidades de serviços e de produtos, quase sempre padronizados. Na atual sociedade em rede, o

modelo econômico assumiu uma nova roupagem, mais flexível, dando ensejo a uma produção customizada e marketing individualizado. Nessa nova conjuntura, *commodities* como o ferro, petróleo, madeira, ouro, gás natural, dentre outros, vão perdendo espaço e atratividade para a informação, a qual se constitui como novo insumo dessa economia alicerçada na capacidade de prospectar, obter, tratar, gerenciar e lapidar dados.

Atualmente, a assertiva que está em constante evidência é a que afirma que os dados são o novo petróleo ou o combustível que impulsiona a economia do Século XXI (TOONDERS, 2018). Para se referir a esse cenário, utiliza-se muito o termo *big data.* Dessa forma, necessário compreender o seu significado.

O professor Viktor Mayer-Schonberger da Universidade Oxford conceitua o termo como (GOMES, 2019):

> Big data refers to things one can do at a large scale that cannot be done at a smaller one, to extract new insights or create new forms of value, in ways that change markets, organizations, the relationship between citizens and governments, and more.

O Article 29 Working Party, criada pela Diretiva 95/46/EC do Parlamento Europeu como uma organização de caráter consultivo e independente conceitua *big data* como:

> Big data refers to the exponential growth both in the availability and in the automated use of information: it refers to gigantic digital datasets held by corporations, governments and other large organizations, which are then extensively analyzed (hence the name: analytics) using computer algorithms. Big data can be used to identify more general trends and correlations but it can also be processed in order to directly affect individuals.[1]

Já conforme o Instituto de Tecnologia e Sociedade do Rio de Janeiro – ITS (2016), Big Data é:

> [...] conjunto de dados cuja existência só é possível em consequência da coleta massiva de dados que se tornou possível nos últimos anos, graças à onipresença de aparelhos e sensores na vida cotidiana e do número crescente de pessoas conectadas a tais tecnologias por meio de redes digitais e também de sensores.

[1] Tradução livre: Big data se refere ao crescimento exponencial tanto na disponibilidade quanto no uso automatizado de informação: refere-se a conjuntos de dados digitais gigantescos detidos por empresas, governos e outras organizações de grande porte, que são amplamente analisados (daí o nome: analytics) usando algoritmos de computador. Big data pode ser usado para identificar tendências mais gerais e correlações, mas também pode ser processado, de modo a afetar diretamente os indivíduos.

Em síntese, o significado do termo *big data* transcendeu seu real sentido para, atualmente, referir-se a um verdadeiro fenômeno cultural e tecnológico (BOYD; CRAWFORD, 2012, p. 663). Neste sentido, no intuito de delimitar seu conceito para os fins propostos neste trabalho, é possível entender o vocábulo *big data* como o processo de coleta e análise de uma enorme quantidade de dados, de forma automatizada por algoritmos, com o objetivo de extrair informação útil, ou seja, aquela que possa trazer um resultado prático ou outros benefícios para seu detentor ou usuário.

Mas a função extraída do *big data* não se encerra somente em coletar e analisar. Há, conforme aponta Laura Schertel Mendes (2014, p. 33), uma "utilização secundária dos dados", que consiste na combinação ou cruzamento de dados, resultando em informações derivadas, que acabam adquirindo um novo valor. Sendo assim, essa geração de valor não se resume a apenas armazenar e analisar um volume maciço de dados, mas, além disso, extrair da combinação, cruzamento, enfim, do tratamento desses dados, outras novas informações com muito mais valor agregado.

Para se entender o que está sendo afirmado, tem-se como exemplo a utilização secundária das informações extraídas da análise de mais de 350 milhões de *tweets* pela Organização das Nações Unidas, com o objetivo de ajudar o Poder Público a combater a fome em locais mais carentes[2].

Outro exemplo é a coleta de dados pessoais relacionados à área da saúde. Existem muitos aplicativos no mercado que se propõem a monitorar para seus usuários hábitos de dieta, batimentos cardíacos, distâncias percorridas, calorias queimadas, quantidade de passos, entre outros. Em um primeiro momento, há uma coleta de dados que baseia o usuário da sua tomada de decisões. Já com a utilização secundária desses dados podem se extrair e gerar informações que serão por demais úteis e valiosos para empresas de seguro e planos de saúde, as quais terão um indicador preciso para pautarem suas decisões, ou para profissionais da saúde, os

[2] "When correlations between social media conversations on food-related topics and official inflation data started to emerge, Jakarta's Global Pulse analysts were able to flag the likely local impacts of the crisis and deploy resources accordingly. In 2014, Global Pulse implemented over 25 joint data innovation projects worldwide. Implementation involved the analysis of over 350 million tweets" (GOMES, 2019).

quais terão substratos para tomar decisões de mercados, tal como direcionamento de um serviço para determinados públicos-alvo específicos (ENISA, p. 13).

Um típico exemplo do uso do *big data* pode ser demonstrado no caso do supermercado britânico Tesco, descrito por Vinícius Fortes, Salete Boff e Fernando Ayuda (2016, p. 24-48). A partir do Tesco Clubcard, um programa de fidelidade criado pela rede de supermercados, é possível coletar dados de compras feitas no "mundo real" que são mapeadas e cruzadas com compras feitas na internet. Nas palavras dos autores:

> In this way, the network began to store details of every consumer in the United Kingdom, from the domicile to a range of demographic characteristics, socioeconomic and lifestyle. By means of an artificial intelligence system called Zodiac, was possible to create intelligent profiles and segmentation of customer data. So the client profile can be classified as your enthusiasm for promotions, its fidelity to brands and other buying habits. On top of that, the company went on to sell access to the database named Crucible to companies from different segments, such as Sky (paid TV), Gillette (razors and cosmetics) and Orange (television and internet services provider). Together, the Crucible and the Zodiac can generate a map of how an individual often thinks, works and stores. Furthermore, the map is able to classify consumers in 10 categories: (i) wealth; (ii) promotions; (iii) trips; (iv) charity; (v) 'green' consumption; (vi) financial difficulties; (vii) credit; (viii) lifestyle; (ix) habits; (x) adventures[3].

Assim, é possível verificar a importância adquirida pelo *big data* na atual conjuntura econômico-social, possibilitando-se ter uma noção do valor gerado pela coleta, acumulação e processamento de dados, os quais geram mais informações que agregam enorme valor para quem delas irá se utilizar. Todavia, esse novo insumo econômico não poderia passar ao largo do Direito, tendo em vista que a sua origem, em sua maior parte, advém do ser humano.

[3] Dessa forma, a rede passou a armazenar detalhes de cada consumidor no Reino Unido, desde o domicílio até uma série de características demográficas, socioeconômicas e de estilo de vida. Por meio de um sistema de inteligência artificial chamado Zodiac, foi possível criar perfis inteligentes e segmentação de dados de clientes. Assim, o perfil do cliente pode ser classificado como seu entusiasmo por promoções, sua fidelidade a marcas e outros hábitos de compra. Além disso, a empresa passou a vender o acesso ao banco de dados chamado Crucible para empresas de diferentes segmentos, como Sky (TV paga), Gillette (aparelhos de barbear e cosméticos) e Orange (provedora de serviços de televisão e internet). Juntos, o Crucible e o Zodiac podem gerar um mapa de como um indivíduo pensa, trabalha e armazena com frequência. Além disso, o mapa é capaz de classificar os consumidores em 10 categorias: (i) riqueza; (ii) promoções; (iii) viagens; (iv) caridade; (v) consumo "verde"; (vi) dificuldades financeiras; (vii) crédito; (viii) estilo de vida; (ix) hábitos; (x) aventuras.

3. DIPLOMAS LEGAIS DE PROTEÇÃO DE DADOS PESSOAIS: EVOLUÇÃO HISTÓRICA E ATUAIS MODELOS DE REGULAMENTAÇÃO

A preocupação, em âmbito mundial, com a proteção de dados não é recente. Mayer-Schönberger ensina uma perspectiva histórico-evolutiva para entender como se deu a evolução dos diplomas legais voltados à proteção de dados, explicando em quatro diferentes gerações de leis (MENDES, 2014, p.32).

A preocupação com a regulamentação se iniciou na década de 70, como resposta ao processamento de dados nas empresas privadas e Administração Pública centralizado em grandes bancos de dados nacionais. A forma de regulamentação se pautava na concessão de autorizações para a criação desses bancos de dados, bem como o controle destes pelo Estado. Tem como exemplos de marco regulatório as leis do Estado alemão de Hesse de 1970, a Lei de Dados da Suécia de 1973, além do Privacy Act norte-americano de 1974 (DONEDA, 2011, p. 91-108).

A segunda geração de leis começou a surgir no final da década de 70. O primeiro marco dessa geração foi a *Bundesdatenschutzgesetz,* a lei federal da República Federativa da Alemanha sobre proteção de dados pessoais, de 1977, seguida pela Lei Francesa de Proteção de Dados Pessoais, intitulada *Informatique et Libertées* (DONEDA, 2011, p. 97). Tais regulamentos inovaram por criar um sistema jurídico que fornecia instrumentos legais postos à disposição do cidadão para identificar o uso indevido de seus dados pessoais e, em caso positivo, demandar a tutela correspondente.

Na década de 80 surgiu a terceira geração de leis que, basicamente, continuou focada em dar meios ao cidadão para identificar e combater o mau uso de seus dados, inovando apenas em dar maior efetividade a esse sistema.

A quarta e última geração, ao verificar que apenas tutelar o indivíduo de meios jurídicos para agir não era suficiente – o que será exposto mais à frente -, buscou regulamentar a questão dos dados pessoais de forma integral e sistêmica, retirando a base de atuação legal do enfoque apenas individual. Dentre esses marcos regulatórios de quarta geração, pode-se destacar as Diretivas europeias em matérias de proteção de dados, principalmente as Diretivas 95/46/CE e 2002/58/CE, que deram

origem ao recente Regulamento Geral sobre a Proteção de Dados - GDPR de 2018[4], bem como a Lei Geral de Proteção de Dados Pessoais - LGPD brasileira, Lei nº 13.709/2018.

Especificamente no Brasil, antes da Lei nº 13.709/2018, o regramento a respeito da proteção de dados começou a surgir no final da década de 80, com a própria Constituição Federal, que protegeu, de forma bastante abstrata, o direito à privacidade no artigo 5º, inciso X. Não obstante, tal dispositivo estabelece a norma base de proteção à privacidade.

Segundo Laura Mendes (2014, p. 171), o artigo 5º, X da Constituição faz com que seja:

> [...] possível extrair uma tutela ampla da personalidade e da vida privada do cidadão, nas mais diversas situações em que ele se encontra. Não faria sentindo excluir exatamente as situações em que a sua vida privada está sujeita a uma maior violação, como é o caso do processamento de dados pessoais. Afinal, muitas vezes, o tratamento de dados configura, hoje, uma ameaça muito mais grave à intimidade e à vida privada do homem médio do que os perigos "tradicionais", [...]. Assim, não há dúvidas de que a Constituição Federal protege o homem médio desses riscos, que raramente ocorrem na vida real, não haveria sentido em negar-lhe a proteção constitucional perante os bancos de dados, que constituem um risco constante e diário para todos os cidadãos.

Em matéria infraconstitucional, o primeiro diploma a regulamentar especificamente a questão dos dados pessoais foi o Código de Defesa do Consumidor, ao disciplinar, em seu artigo 43, banco de dados e cadastros de consumidores. Após, foi promulgada a Lei do Cadastro Positivo, Lei n. 12.414/2011, que veio a disciplinar a formação de banco de dados sob um conjunto de dados relativos às operações financeiras e de adimplemento para fins de concessão de crédito. Pouco tempo depois o ordenamento jurídico brasileiro foi inovado com a Lei n. 12.964/2014, o Marco Civil da Internet - MCI, que inaugurou uma normativa específica para os direitos e garantias do cidadão nas relações travadas na Internet. O direito à privacidade foi tido como um dos pilares do MCI, ao lado da neutralidade de rede e da liberdade de expressão (BIONI, 2019). Por fim, em 2018, houve a

[4] A GDPR é a versão atualizada da Diretiva 95/46/CE. Ou seja, a GDPR revogou a Diretiva 95/46/CE. Tornou-se necessário elaborar uma nova versão porque, na época da elaboração da anterior, empresas com negócios baseados na Internet (como, por exemplo, o Facebook) não tinham o tamanho que possuem hoje em dia. Como consequência, a lei de 1995 não aborda a dinâmica atual dos dados na rede, como armazenamento, compartilhamento e risco de vazamento.

promulgação da Lei Geral de Proteção de Dados Pessoais no Brasil, trazendo todo um sistema de normas com o escopo de regulamentar especificamente todos os conflitos de interesses que venham a existir a respeito da questão.

A Lei n. 13.709/18 é estruturada, mormente, com base no livre consentimento, tal como os outros regulamentos mundiais que tratam da mesma matéria. Contudo, por ser fruto da quarta geração de leis de proteção de dados, a LGPD também se utiliza de outros mecanismos de proteção. Esta temática será abordada em capítulo próprio.

Não obstante o grande avanço experimentado pelo ordenamento jurídico brasileiro com a promulgação da LGPD, algumas intercorrências que aconteceram durante o processo legislativo de sua criação deram origem a alguns pontos fracos no sistema legal de proteção do cidadão e de seus dados pessoais. Trata-se do veto presidencial aos artigos 55 a 59, os quais tratavam da criação da Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade.

4. DO SISTEMA DE PROTEÇÃO DE DADOS PESSOAIS E SUA REPERCUSSÃO NO DIREITO FUNDAMENTAL À PRIVACIDADE

Conforme explicado anteriormente, a respeito da evolução dos normativos que se propuseram a regulamentar e proteger a coleta e uso de dados pessoais nessa novel economia global que retira da informação a sua mola propulsora de desenvolvimento, tais sistemas de proteção tiveram como alicerce de sua estrutura de funcionamento, a partir da segunda geração de leis, o consentimento.

Essa transição é bem explicada por Bruno Ricardo Bioni (2019):

> Com isso, percebe-se que seria inviável a estratégia regulatória anterior em que incumbia ao Estado licenciar a criação e o funcionamento de todos os bancos de dados. A segunda geração de leis transfere para o próprio titular dos dados a responsabilidade de protegê-los. Se antes o fluxo das informações pessoais deveria ser autorizado pelo Estado, agora cabe ao próprio cidadão tal ingerência que, por meio do consentimento, estabelece as suas escolhas no tocante à coleta, uso e compartilhamento dos seus dados pessoais. Destaca-se, nesse sentido, o referencial teórico de Alan Westin que compreendia a privacidade como a "reivindicação dos indivíduos, grupos e instituições de determinar, por eles mesmos, quando, como e em qual extensão suas informações pessoais seriam comunicadas aos outros". Dá-se ênfase à autonomia do indivíduo em controlar o fluxo de suas informações pessoais.

Dessa forma, verifica-se que o consentimento é o mecanismo jurídico que possibilita o controle do titular sobre seus dados pessoais. Pelo exercício desse direito, o titular pode exercer o controle sobre a possibilidade de se coletar, analisar, tratar, compartilhar seus dados pessoais, determinando um maior ou menor nível de fluxo e proteção. Nos dizeres de Laura Schertel Mendes (2014, p. 60):

> Para que o indivíduo possa exercer o seu papel 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 artigo 5, inciso XII, da LGPD, conceitua o consentimento como "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada".

Entretanto, apenas o consentimento, *de per si*, não traz a efetividade de proteção de dados pessoais almejada pelos normativos que têm esse objetivo. E os motivos defendidos neste artigo serão abordados a seguir.

O primeiro e mais enfático se trata do grau de indispensabilidade que alguns serviços de aplicativos ou software adquiriram no atual contexto da sociedade em rede. Stefano Rodotà (2008, p. 76) já criticava o consentimento como única forma de proteção de dados pessoais, asseverando que o acesso a determinado bem ou serviço, no atual momento da sociedade, somente seria possível com o fornecimento de dados pessoais, relevando a ineficácia do consentimento em razão da assimetria de poder entre o fornecedor do bem ou serviço e o usuário, que não teria outra escolha senão consentir.

Pense-se, por exemplo, na situação de um indivíduo que não tem uma conta no Instagram, Facebook, Twitter, Linkedin, WhatsApp entre outros aplicativos. Essa pessoa, apesar de fisicamente inserida no seio de uma sociedade, está destinada a uma segregação tecnológica informacional. Atualmente, os serviços desses aplicativos se tornaram indispensáveis para o bom relacionamento social, para a própria inserção do indivíduo em sociedade.

Esses serviços, em sua maioria, não exigem uma contraprestação pecuniária. E é preciso atenção nesse detalhe. Não se estar a dizer que se trata de serviços gratuitos. Seria inimaginável que em uma sociedade capitalista fosse possível oferecer serviços tecnológicos avançados sem custos e sem alguma espécie de

contraprestação. Em verdade, a contraprestação imediata dada pelo usuário do aplicativo são seus dados pessoais. Trata-se do *zero-price advertisement business* (BIONI, 2019).

Enfatize-se que é a própria pessoa quem fornece seus dados, pois é ela mesma quem procura o aplicativo, disponibiliza seus dados pessoais e autoriza o tratamento destes, tudo em troca de poder fazer parte de uma sociedade informacional estruturada em rede. Ao fazer isso, a pessoa diminui os custos que seriam gastos na coleta dos dados pessoais, tendo em vista que é o próprio indivíduo que assume esse trabalho de alimentação do sistema com dados pessoais. Esses, por sua vez, após coletados, armazenados e analisados acabam sofrendo um processo de tratamento onde o resultado é a agregação de mais valor através das novas informações extraídas desse tratamento, conforme explicado no capítulo a respeito do *big data.*

Esse cenário já havia sido identificado à época da segunda geração de leis de proteção de dados pessoais, conforme explica Danilo Doneda (2011):

> Estas leis[5] apresentavam igualmente seus problemas, o que motivou uma subsequente mudança de paradigma: percebeu-se que o fornecimento de dados pessoais pelos cidadãos tinha se tornado um requisito indispensável para a sua efetiva participação na vida social. O que era exceção veio a se tornar regra. Tanto o Estado quanto os entes privados utilizavam intensamente o fluxo de informações pessoais para seu funcionamento, e a interrupção ou mesmo o questionamento deste fluxo pelo cidadão implica muito frequentemente a sua exclusão de algum aspecto da vida social. [...] A autodeterminação informativa era, porém, o privilégio de uma minoria que decidia enfrentar os custos econômicos e sociais do exercício dessas prerrogativas.

Na segunda geração de leis de proteção de dados pessoais começaram, assim, os questionamentos a respeito da eficácia do consentimento como única ferramenta de proteção de dados pessoais em um sistema jurídico. Como poderia uma pessoa simplesmente escolher não fornecer seus dados se tal decisão acarretasse um prejuízo maior que a própria manipulação de seus dados pessoais por outra entidade? Esse fenômeno é muito similar ao que ocorre com a patologia da sociedade de consumo. Mariana Ribeiro Santiago e Livia Gaigher B. Campelo (2016, p.124-125) conseguem explicar essa patologia em poucas palavras:

> Nesse sentido, a expressão “sociedade de consumidores” verbaliza mais do que a postura dos seus membros de gastar tempo e esforços

[5] Segunda geração de leis de proteção de dados pessoais.

> visando ampliar seus prazeres, refletindo a percepção de que a política de vida dos indivíduos tende a ser remodelada com base nos meios e objetos de consumo, segundo as linhas da síndrome consumista. “Necessitando” consumir para definir o seu papel na sociedade, para alcançar o padrão pregado pela cultura de consumo, os indivíduos se lançam em aquisições impensadas, consequência de uma avaliação deturpada das suas possibilidades e má administração das suas finanças, o que já produz efeitos na economia do país e na questão da sustentabilidade.

Em síntese, o consumidor tem a (pseudo) liberdade de optar entre consumir um determinado bem ou serviço, todavia, na fase atual da sociedade de consumidores, o consumismo deixou de ser uma opção e se transformou em um fenômeno social indispensável para o ser humano se sentir inserido dentro de um contexto social. Nesse cenário, garantir a liberdade para o indivíduo não resolve o problema social. O mesmo pode-se dizer a respeito do consentimento no âmbito da proteção de dados pessoais.

Outro motivo da ineficácia do consentimento como único mecanismo de proteção dos dados pessoais são as filigranas envolvidas no processo de manifestação do consentimento. De acordo com Solove (2019), há diversos obstáculos para um consentimento eficaz, tais como o fato de que as pessoas não leem as políticas de privacidade. Quando leem, muitas vezes não as entendem. Quando conseguem entender, muitas das vezes não lhe são oferecidas escolhas em que possam personalizar como será o uso de seus dados pessoais.

A quarta geração de leis de proteção a dados pessoais, ciente da ineficácia do consentimento como único mecanismo de proteção da privacidade, buscou equacionar essa deficiência através de proposições normativas que retiram da esfera de liberdade do indivíduo a escolha sobre o tratamento de certos tipos de dados, como por exemplo os dados pessoais sensíveis.

A noção tradicional de consentimento demanda uma revisão em tal contexto. É preciso considerar que a liberdade deve ser entendida como um conceito limitado e relativo, que está em constante modificação à medida que se impõem novas necessidades ao homem, ou seja, trata-se de uma ideia dinâmica que se modifica no curso da história (STRENGER, 1968, p. 104).

Quanto ao consentimento, este não foi simplesmente deixado de lado, mas sofreu algumas mudanças, permanecendo, ainda, no centro da estrutura regulatória

das leis de proteção da privacidade. Bruno Ricardo Bioni (2019) consegue bem sintetizar o novo patamar assumido pelo consentimento:

> Ao mesmo tempo, contudo, esse progresso geracional não eliminou o protagonismo do consentimento. A sua centralidade permaneceu sendo o traço marcante da abordagem regulatória. Tanto é verdade que, em meio a esse processo evolutivo, o consentimento passou a ser adjetivado, como devendo ser livre, informado, inequívoco, explícito e/ou específico, tal como ocorreu no direito comunitário europeu. Essa distribuição de qualificadores acaba, portanto, por desenhar um movimento refratário em torno do papel de destaque do consentimento quase como sendo sinônimo de autodeterminação informacional.

Fora desse quadro, torna-se difícil garantir o próprio direito constitucional à privacidade e à intimidade dos usuários, que permanecem sem autonomia para defender os próprios dados e informações geradas a partir destes sobre seu estilo de vida.

Sobre o tema, Gilberto Haddad Jabur (2000, p. 260) ensina que “o conceito de intimidade abriga o direito à quietude, à paz interior, à solidão e ao isolamento da curiosidade pública, de tudo o quanto possa interessar a pessoa, impedindo que se desnude sua vida particular”. Na mesma linha, entende Rui Stoco (199, p. 682):

> Intimidade compreende esfera exclusiva da vida privada de cada um, velada à indiscrição alheia; e a própria imagem participa dessa esfera privada. Quem, portanto, retrata a imagem de um homem no recesso, sem o seu consentimento, está a invalidar-se a intimidade, independentemente do prejuízo que possa causar-lhe à honra.

Entre as mudanças advindas com a quarta geração de leis de proteção de dados pessoais, a mais importante foi ideia a respeito de criação de autoridades independentes para a aplicação dos referidos regulamentos. A importância dessas autoridades e sua necessária independência, é o tema abordado a seguir.

5. DA IMPORTÂNCIDA DA INDEPENDÊNCIA DA AUTORIDADE FISCALIZADORA PARA A EFETIVIDADE DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS - LGPD

A promulgação da Lei Geral de Proteção de Dados Pessoais no Brasil, embora seja considerada um avanço, levanta questões que estão diretamente ligadas à característica da efetividade, e é nesse ponto que se pode aferir a importância da independência da autoridade fiscalizadora.

Importante esclarecer, de plano, o sentido utilizado para o termo técnico efetividade. A efetividade de uma norma engloba tanto a decisão pela sua efetiva aplicação (eficácia jurídica), quanto o resultado concreto decorrente da sua aplicação (eficácia social). Está no âmbito da realização do Direito, do desempenho concreto de sua função social (SARLET, 2009, p. 240).

Conforme já abordado neste artigo, em agosto de 2018 foi promulgada a Lei n. 13.709/18, Lei Geral de Proteção de Dados Pessoais - LGPD. Todavia, referida Lei sofreu mudança no final do processo legislativo. Na fase de sanção do projeto de lei que iria dar origem à LGPD, o Presidente da República vetou os artigos 55 a 59, que travam justamente da criação da Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, sua composição e atribuições administrativas.

A razão do veto se resumiu na assertiva de que os dispositivos incorrem em inconstitucionalidade do processo legislativo, por afronta ao artigo 61, § 1º, II, 'e', cumulado com o artigo 37, XIX da Constituição. Em apertada síntese, após a aprovação do PLC nº 53/2018 pelo Congresso Nacional e o seu encaminhamento para a sanção presidencial, foram expostos questionamentos sobre a constitucionalidade da criação da Autoridade Nacional de Proteção de Dados (ANPD), autarquia especial, por meio de emenda parlamentar, já que, no projeto originário encaminhado pelo Poder Executivo, as atribuições ora conferidas à ANPD seriam exercidas por órgão da Administração direta.

Em 27 de dezembro de 2018, foi editada a Medida Provisória n. 869/18, a qual alterou a Lei n. 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados e outras providências.

Todavia, houve uma grande alteração nessa recriação da Autoridade Nacional de Proteção de Dados. Diferente do que havia sido previsto no projeto de lei aprovado pelo Congresso Nacional, quando detinha natureza jurídica de autarquia especial, na disposição contida na Medida Provisória 869/18 a ANPD passou a deter natureza jurídica de órgão da Administração Pública Direta Federal, ou seja, está subordinada à Presidência da República.

Apesar de parecer um detalhe simples, essa mudança gera o risco de se retroceder em toda construção científica histórica da estrutura jurídica de proteção à

privacidade dos dados pessoais. Por este motivo que não foi despicienda a explicação neste artigo a respeito da evolução dos normativos de proteção à privacidade. Foi comprovado que o consentimento, mola propulsora dessa estrutura jurídica, acabou se relevando ineficaz se usado isoladamente dentro do contexto jurídico da proteção de dados pessoais. Verificou-se que na transição para uma quarta geração de leis de proteção dos dados pessoais, uma das maiores contribuições científicas foi a conclusão de que haveria de ser criada uma autoridade de proteção desses direitos, com o principal objetivo de regulamentar a aplicação da lei e equacionar a assimetria de poder fático existentes entre as entidades que colhem e tratam os dados e os titulares destes.

Tudo que foi exposto mostra a relevância da ANPD, mas a importância da sua independência reside no fato de que o próprio Estado é um dos que coleta, analisa e trata dados de seus cidadãos. E tal como qualquer iniciativa estatal, deve-se moldar aos princípios expostos na Constituição e na LGPD, bem como se submeter a mecanismos de fiscalização e controle. Dessa forma, se o próprio Estado deve-se submeter à fiscalização da ANPD, esta deve se encontrar em posição que lhe permita atuar sem intervenções indevidas, ou seja, precisa de um mínimo de independência e autonomia.

A título de ilustração, um dos primeiros casos emblemáticos em torno de conflito de interesses sobre a temática em questão surgiu na Alemanha, através de decisão do Tribunal Constitucional Alemão de 1982, no julgamento da “Lei do Recenseamento de População, Profissão, Moradia e Trabalho”. Essa decisão marcou a transição para a terceira geração de leis de proteção de dados. Nesse julgamento histórico, o Tribunal entendeu pela inconstitucionalidade parcial da Lei de Recenseamento, tendo como fundamento central a existência de um direito à autodeterminação informativa, protegendo amplamente o controle que deveria o titular de dados ter sobre o fluxo de informações da sociedade (MENDES, 2014, p.30).

A importância de uma ANPD independente influência nas relações travadas pelo Estado Brasileiro e outros países que possuem legislações semelhantes sobre a temática em questão. A título de exemplo, garantir independência à ANPD é um dos requisitos para que a LGPD brasileira seja reconhecida como adequada ao modelo de tratamento de dados pessoais estabelecidos na Europa por meio do Regulamento Geral sobre a Proteção de Dados – GDPR. Isso implica na facilitação de fluxos

internacionais de dados entre os diferentes sistemas jurídicos adotados por países distintos, principalmente os situados na Europa, visto que estão sujeitos ao GDPR. A esse respeito, veja-se o que dispõe o artigo 36, 2, (b) do GDPR (EUROPEAN Union, 2016):

> Transferências com base numa decisão de adequação
> 1. Pode ser realizada uma transferência de dados pessoais para um país terceiro ou uma organização internacional se a Comissão tiver decidido que o país terceiro, um território ou um ou mais setores específicos desse país terceiro, ou a organização internacional em causa, assegura um nível de proteção adequado. Esta transferência não exige autorização específica.
> 2. Ao avaliar a adequação do nível de proteção, a Comissão tem nomeadamente em conta os seguintes elementos:
> [...]
> b) A existência e o efetivo funcionamento de uma ou mais autoridades de controle independentes no país terceiro ou às quais esteja sujeita uma organização internacional, responsáveis por assegurar e impor o cumprimento das regras de proteção de dados, e dotadas de poderes coercitivos adequados para assistir e aconselhar os titulares dos dados no exercício dos seus direitos, e cooperar com as autoridades de controlo dos Estados-Membros;[6]

A independência da Autoridade Nacional de Proteção na Europa é tão importante que no velho continente referida independência é considerada, desde o ano 2000, um direito fundamental, consoante previsto no artigo 8º da Carta dos Direitos Fundamentais da União Europeia (2000). Ainda, desde a aprovação da Diretiva 95/46/CE já existia a obrigação para os Estados-membros da União Europeia estabelecerem autoridades de proteção de dados que teriam a função de fiscalizar a aplicação das disposições da referida Diretiva no seu território.

No caso da LGPD, a autoridade se constitui como o esqueleto de todo o sistema normativo. Para se ter uma noção, as referências à Autoridade Nacional aparecem na Lei. n. 13.709/18 mais de cinquenta vezes. Não há como negar a

[6] Article 36
Transfers on the basis of an adequacy decision
1. Member States shall provide that a transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.
2. When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:
[...]
b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with data protection rules, including adequate enforcement powers, for assisting and advising data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States;

importância dessa instituição no sistema normativo de proteção de dados pessoais, bem como a preocupação a respeito de sua necessária independência, para uma melhor aplicação, fiscalização e proteção do direito à privacidade.

No contexto da estrutura administrativa brasileira, a instituição jurídica que melhor se adequaria às necessidades exigidas pela Autoridade Nacional de Proteção de Dados seria a autarquia federal especial, que, nas palavras de Celso Antônio Bandeira de Mello (1968, p. 5-6):

> [...] refere-se ao instituto jurídico correspondente a uma determinada técnica de administração pública: a técnica de administrar interesses públicos através de demiurgos, pessoas jurídicas auxiliares da administração central [...]; estar-se-á diante do fenômeno das autarquias sempre que o Estado lançar mão da técnica de criar pessoas para perseguir mencionados interesses, seja para prestação de serviços, seja para polícia de certas atividades, desde que, ao criá-las, não as coloque expressamente sob o regime jurídico das relações privadas.

Por fim, salienta Luís Roberto Barroso (2002, p. 121):

> Tais autarquias, porém, são dotadas de um conjunto de privilégios específicos que a lei lhes outorgou, tendo em vista a consecução de seus fins, pelo que são consideradas autarquias de regime especial. A pedra de toque desse regime especial das agências reguladoras é sua independência em relação ao Poder Público. No desempenho de suas atribuições, as agências precisam ver preservado seu espaço de legítima discricionariedade, imune a injunções de qualquer natureza, sob pena de falharem em sua missão.

Portanto, não há como negar a importância de se garantir independência à Autoridade Nacional de Proteção de Dados brasileira através da reformulação de sua estrutura organizativa base, ou seja, através de sua transformação em uma autarquia especial, instituição de direito público pertencente à Administração Indireta. Ao assim se proceder, colocar-se-á o Brasil em um cenário de destaque no que diz respeito à proteção de dados pessoais, ao lado dos países que fazem parte da União Europeia.

6. CONSIDERAÇÕES FINAIS

Diante do exposto, é possível concluir que a partir da segunda metade do Século XX, toda a sociedade mundial, incluindo-se, desta forma, o setor da economia, sofreram mudanças profundas em sua base de estruturação. Mudou-se desde o modo de ser do cidadão, sua forma de interagir em sociedade até os insumos mais usados no processo econômico mundial. Deu-se início a uma economia lastreada na

informação como insumo principal para o crescimento e desenvolvimento, fato que acabou sendo nominado de economia da informação.

Esse processo de disrupção penetrou em todos os âmbitos da sociedade, dando início a um cenário cultural e social denominado *big data*, paradigma sustentado na coleta, análise, cruzamento, processamento e tratamento de dados, como objetivo principal de gerar cada vez mais valor com as novas informações obtidas através do tratamento de tais dados.

A partir da absorção dos efeitos colaterais advindos do *big data*, principalmente a respeito dos limites de sua atuação à luz do direito à privacidade e autodeterminação informacional, o Direito começou a agir, dando início a um processo progressivo de criação de leis, que foram divididos em quatro gerações, com o intuito de proteger a privacidade da pessoa humana.

O fato em comum das gerações de leis é a estrutura normativa pautada no consentimento como forma de proteção do direito à privacidade e consequente uso de dados pessoais por outras entidades ou órgãos. Todavia, na transição para a quarta geração de leis, verificou-se que o consentimento, isoladamente, não poderia ser o único escudo contra o abuso no tratamento de dados pessoais. Foi a partir dessa geração de leis que foi inaugurada a necessidade de se ter uma autoridade central com atribuições de regulamentar e fiscalizar o tratamento de dados pessoais. A experiência, principalmente na Europa, vanguarda na proteção da privacidade na sociedade da informação, demonstrou que tais autoridades devem ter um mínimo de independência e a autonomia para alcançarem suas finalidades.

No Brasil, apesar do projeto de lei nº 53/2018 prever em seu bojo a Autoridade Nacional de Proteção de Dados - ANPD com estrutura de autarquia especial, na última fase no processo legislativo foram vetados os artigos que cuidavam de sua criação, estruturação, composição e atribuições, sob o fundamento de vício formal, uma vez que a iniciativa não partiu do Poder Executivo. Poucos meses depois, foi editada a Medida Provisória n. 869/18, que criou a ANPD com natureza jurídica de órgão da Administração Pública Direta Federal, ou seja, subordinada à Presidência da República.

Conclui-se que tal movimento legislativo põe em xeque a total efetividade da Lei Geral de Proteção de Dados Pessoais, visto que sua independência e autonomia

perante o próprio Estado é um imperativo para que se possa alcançar a excelência no que diz respeito à proteção da privacidade relativo aos dados pessoais.

REFERÊNCIAS

BANDEIRA DE MELLO, Celso Antônio. **Natureza e Regime Jurídico das Autarquias**. São Paulo: Revista dos Tribunais, 1968.

BARROSO, Luís Roberto. Apontamento sobre as Agências Reguladoras. In: MORAES, Alexandre de (Coord.). **Agências reguladoras**. Atlas, São Paulo, 2002.

BENKLER, Yochai. The wealth of networks: how social production transforms markets and freedom. In: **New Haven and London**: Yale University Press, 2006, p. 13. Disponível em: http://www.benkler.org/Benkler_Wealth_Of_Networks.pdf. Acesso em dez. 2018.

BRASIL. **Constituição da República Federativa do Brasil**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em dez. 2018.

BRASIL. **Lei n. 13.709 de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em dez. 2018.

BRASIL. **Medida Provisória Nº 869**, de 27 de dezembro de 2018. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Mpv/mpv869.htm. Acesso em fev. 2019.

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

BIONI, Bruno. **Xeque-mate***:* o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil. Disponível em: http://gomaoficina.com/wp-content/uploads/2016/07/XEQUE_MATE_INTERATIVO.pdf. Acesso em fev. 2019.

BOYD, Danah; CRAWFORD, Kate. Critical questions for big data. Provocations for a cultural, technological, and scholarly phenomenon. “We define big data1 as a cultural, technological, and scholarly phenomenon”. **Information, Communication & Society**, Vol. 15, Issue 5. 2012. Disponível em: http://dx.doi.org/10.1080/1369118X.2012.678878. Acesso em jan. 2019.

CASTELLS, Manuel. **A Sociedade em rede**. 8. ed. Tradução de Roneide Venâncio Majer. São Paulo: Paz e Terra, volume I, 2005a.

CASTELLS, M. A Sociedade em Rede: do Conhecimento à Política. In: CASTELLS, M.; CARDOSO, G. **A Sociedade em rede**: do conhecimento à ação política. Belém: Imprensa Nacional – Casa da Moeda, 2005b. p. 20. Disponível em: http://www.egov.ufsc.br/portal/sites/default/files/ anexos/a_sociedade_em_rede_-do_conhecimento_a_acao_politica.pdf. Acesso em dez. 2018.

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

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**. Joaçaba, V. 12, n. 2, p. 91-108, Ago.-Dez./2011.

EUROPEAN UNION. DIRECTIVE (EU) 2016/680 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. **Official Journal of the European Union**, 27 April 2016. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=EN. Acesso em fev. 2019.

FORTES, Vinícius B. BOFF, Salete O. AYUDA, Fernando G. The fundamental right to privacy in Brazil and the internet privacy rights in regulating personal data protection. **Revista Eletrônica do Curso de Direito da UFSM**, v. 11, n. 1 /2016, p. 24-48, 2016.

GOMES, Rodrigo Dias de Pinho. **Desafios à privacidade**: Big Data, consentimento, legítimos interesses e novas formas de legitimar o tratamento de dados pessoais. Disponível em: https://itsrio.org/wp-content/uploads/2017/03/Rodrigo-Gomes.doc-B.pdf. Acesso em janeiro de 2019.

HOUAISS, Antonio. **Dicionário Houaiss da língua portuguesa**. Rio de Janeiro: Objetiva, 2001.

INSTITUTO DE TECNOLOGIA & SOCIEDADE DO RIO - ITS. Big data no projeto Sul Global. **Relatório sobre estudos de caso**. Rio de Janeiro, 2016. Disponível em:http://itsrio.org/wp-content/uploads/2016/03/ITS_Relatorio_Big -Data_PT-BR_v2.pdf. Acesso em: dez. 2018.

JABUR, Gilberto Haddad. ***Liberdade de pensamento e direito à vida privada****:* conflitos entre direitos da personalidade. São Paulo: Revista dos Tribunais, 2000.

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

RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, s/d.

SANTIAGO, Mariana Ribeiro; CAMPELLO, Livia Gaigher Bósio. Função social e solidária da empresa na dinâmica da sociedade de consumo. **Scientia Iuris**. Londrina, v. 20, n. 1, p.119-143, abr. 2016.

SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais**: uma teoria geral dos direitos fundamentais na perspectiva constitucional. 10. ed. Porto Alegre: Livraria do Advogado, 2009.

SOLOVE, DJ. Privacy self-management and the consent dilemma. **Harvard Law Review** 126: 1880–1903. Disponível em: https://harvardlawreview.org/2013/05/introduction-privacy-self-management-and-the-consent-dilemma/. Acesso em fev. 2019.

STOCO, Rui. **Responsabilidade Civil e Sua Interpretação Jurisprudencial**. 4 ed. São Paulo: Revista dos Tribunais, 1999,

STRENGER, Irineu. **Autonomia da vontade em direito internacional privado**. São Paulo: Revista dos Tribunais, 1968.

TOONDERS, Joris. **Data is the new oil of the digital economy**. Disponível em: https://www.wired.com/insights/2014/07/data-new-oil-digital-economy/. Acesso em: dez. 2018.

UNIÃO EUROPEIA. **Carta dos Direitos Fundamentais da União Europeia**. Parlamento Europeu, Conselho da União Europeia e Comissão Europeia. 2000. Disponível em: http://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso em fev. 2019.

Recebido em 16/10/2019
Aprovado em 30/08/2021
Received in 16/10/2019
Approved in 30/08/2021