INOVAÇÃO NA GESTÃO PÚBLICA E OS DESAFIOS DA IMPLEMENTAÇÃO DE UMA POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS

RESUMO
O presente estudo se propõe a analisar os desafios da implementação de uma política de proteção de dados pessoais por parte da administração pública em geral. Sob a metodologia da pesquisa bibliográfica, o trabalho traz uma análise acerca do que é inovação no setor público, e como ela se aplica ao progresso tecnológico. Ademais, o artigo apresenta os marcos normativos da proteção de dados pessoais, abordando o direito a privacidade e, em especial, a Lei Geral de Proteção de dados pessoais (Lei 13.709/2018) com enfoque em elucidar os dispositivos que devem nortear a atuação da administração pública a partir de sua entrada em vigor.

Palavras-chave: Gestão pública; Dados pessoais; Direito à privacidade;

INTRODUÇÃO

A administração pública tem vivenciado inúmeras transformações ao longo das últimas décadas, produto das constantes modificações econômicas, políticas, sociais e tecnológicas em um mundo mais globalizado e em rede. Os economistas, a exemplo de Schumpeter, apontam essas transformações como ondas, e cada onda representa um ciclo econômico, cuja característica principal é deter uma fase de prosperidade, seguida por uma recessão, induzindo a um processo de melhoria, que é princípio de uma nova fase de prosperidade nessa onda, seguindo, assim, um processo de "destruição criadora".

Nesses termos, a inovação é o fator que abre novos horizontes, pois é o fator que inaugura uma nova onda, induz a saída do estado de inércia, e quando essa fase se satura, é necessário vir uma nova onda. Importante salientar que o espaço entre as ondas vêm decrescendo geometricamente, e percebe-se que cada vez mais uma onda nasce próxima da sua onda anterior -estima-se que estamos na sexta onda Shumpeteriana, que diz respeito a economia baseada no mundo digital, em softwares, em novas mídias, onde os produtos não são mais físicos, e sim digitais.

Nesse tipo de sociedade, a informação é valiosa, pois pode identificar padrões comportamentais, de consumo, anseios sociais, ascendendo ao posto de verdadeira commodity, de forma a provocar uma intensa corrida das nações pelo

desenvolvimento de meios de coleta, produção, armazenamento e processamento de dados, provocando a aceleração e a banalização da prática de coleta e tratamento de dados pessoais.

Outrossim, no ano de 1974, o Privacy act norte americano lançou as primeiras inquietações acerca do potencial de risco que a informática pode trazer ao uso e tratamento de informações pessoais. Nesse mesmo ano, o jornal francês Le Monde publicou uma matéria intitulada "Safari ou caça aos franceses" em que divulgou um projeto de iniciativa governamental cujo objetivo era reunir, sistematicamente, cem milhões de fichas nominativas existentes nos arquivos oficiais do governo.

Outro escândalo envolvendo dados pessoais emergiu no ano de 2018, quando os jornais "New York Times" e "Guardian" revelaram que os dados de mais de 50 milhões de usuários da rede social Facebook foram compartilhados sem o consentimento dos titulares para a empresa britânica Cambridge Analytica. Estima-se que o número total de afetados, na realidade foi de 87 milhões de usuários.

Dessa forma, baseado na imprescindibilidade de uma legislação capaz de enfrentar as novas questões impostas pela economia digital, no ano de 2018 foi editada a Lei 13.709/2018, denominada de Lei Geral de Proteção de Dados Pessoais (LGPD). Essa normativa, cujas sanções entrarão em vigor em maio de 2021, fundamenta-se em assegurar a toda pessoa natural a titularidade de seus dados pessoais e a garantia dos direitos fundamentais de liberdade, intimidade e privacidade. Para tanto, se faz necessária a adesão de todos os setores públicos aos ditames dessa Lei.

É importante que cada governo estadual, na condição de controlador dos dados pessoais informados pelos titulares, institua sua própria Política Estadual de Proteção de Dados Pessoais (PEPD), que vise contemplar o conjunto de diretrizes, normas e ações para a adaptação e execução da LGPD no âmbito da administração pública.

O presente estudo visa identificar os desafios para a implementação de uma política estadual de proteção de dados pessoais pelo Poder Executivo, bem como discorrer sobre propostas de adequação, a partir do estudo dos novos conceitos abordados na LGPD.

A INOVAÇÃO NA GESTÃO PÚBLICA

A administração pública tem vivenciado inúmeras transformações ao longo das últimas décadas, produto das constantes modificações econômicas, políticas, sociais e tecnológicas em um mundo mais globalizado e em rede. Com essas transições, surgem novos desafios, demandas e problemáticas a serem resolvidas, assim como surge a necessidade de se garantir o conhecimento e o respeito aos direitos fundamentais daqueles que participam dos processos administrativos, sejam eles funcionários da administração pública ou os próprios administrados.

Dessa forma, a adaptação de tais metamorfoses tem levado os órgãos administrativos a discutir novas práticas de se resolver os desafios e entraves que a assolam. Nesse contexto, as demandas para aumento da produtividade e

eficiência se encontram na necessidade de se fazer algo diferente, a qual tenderia a refletir em novos resultados. Surge a ideia de inovação, que do ponto de vista do economista Schumpeter (1934) seria sinônimo de mudança, de realizar algo diferente, em um processo de "destruição criadora", na medida em que se desfaz de uma ideia antiga e gera novas possibilidades.

Após Schumpeter, as análises acerca do tema inovação foram ampliadas, ainda estando relacionadas a percepção de descontinuidade com o passado, vinculada a trazer melhorias em processos organizacionais, implementação de novos produtos, procedimentos, serviços, políticas ou sistemas (CAVALCANTE e CUNHA, 2017, p. 16). Em outra definição, com foco no setor público, Osborne e Brown (2005, apud CAVALCANTE e CUNHA, 2017, p. 16) argumentam que a inovação significa a introdução de novos elementos na administração pública, por meio de novos conhecimentos, nova organização, ou nova habilidade de gestão ou processual.

Assim, inovação no setor público, em um cenário complexo de globalização, busca atender as demandas contínuas da sociedade por maior transparência, qualidade, eficiência e eficácia de suas ações (OCDE, 2005) e está diretamente relacionado à busca pela máxima efetivação de direitos, e mínimo impacto sobre esses. Nesses termos, é possível destacar alguns princípios e diretrizes da gestão que vem norteando as inovações na condução da máquina pública, dentre elas o aperfeiçoamento dos mecanismos de controle, de transparência, fiscalização, responsabilização e prestação de contas (*accountability*), incremento da participação social e desenvolvimento de novas tecnologias (TORMES, 2017).

Além disso, com o desenvolvimento dos modelos políticos e econômicos, gradativamente, a questão da gestão de informações assume um novo papel de destaque na administração pública, inaugurando uma nova forma de organização social, política e econômica denominada de Sociedade da Informação (VIEIRA, 2007, p. 15). Na expressão do jurista italiano Stefano Rodotà (1973, apud DONEDA 2014, P. 140), a novidade introduzida pelas máquinas é de transformar a informação, que antes era dispersa, em informação organizada.

Dessa forma, sem negar os inúmeros benefícios que o progresso tecnológico traz à nossa vida cotidiana, a prática comum da coleta e tratamento de informações pessoais pelas entidades governamentais não pode arriscar um direito maior de respeito à vida privada.

DADOS PESSOAIS E DIREITO A PRIVACIDADE

Conceitua-se informação pessoal como aquela que se refere a uma pessoa determinada ou determinável, de forma a poder revelar algo de concreto sobre aquela pessoa. Ela se refere aos seus atributos legais, como o nome civil ou o domicílio, por exemplo, mas também podem se referir às características físicas e pessoais, às manifestações de opiniões, dados de consumo e como aquela pessoa em específico se relaciona na sociedade.

Nesse sentido, o direito inerente ao controle das informações privadas, chamado de direito privacidade é uma expressão do direito a dignidade da pessoa

humana, diretamente ligado ao conceito de liberdade, e que diz respeito a relação entre um indivíduo e o conjunto de informações acerca de sua vida pessoal, quais sejam: seu modo de vida doméstico, suas relações familiares e afetivas, fatos, hábitos, local, nome, imagens, pensamentos, segredos, suas origens e planos futuros desse indivíduo.

Outrossim, o direito à privacidade possui duas dimensões: uma objetiva e outra subjetiva. Sua dimensão subjetiva diz respeito a faculdade pela qual tem cada pessoa tem de impedir que pessoas estranhas se intrometam em sua vida privada, de exercer, com consciência, o seu poder de autodeterminação acerca dos já mencionados tipos de informação. Nas palavras do Juíz americano Cooly (1873 apud SILVA, 2005, p. 205), seria este o direito de toda pessoa tomar sozinha as decisões na esfera da sua vida privada (Right to be alone). Já a dimensão objetiva desse direito diz respeito a essência do Estado democrático de Direito, quando este proporciona ao indivíduo o livre exercício da sua consciência, de suas crenças e da forma como deseja expressá-las.

Esse direito também pode ser visto sob uma ótica positiva e sob uma ótica negativa. O aspecto negativo diz respeito ao direito pelo qual o titular das informações tem de exigir a não intromissão do Estado e de terceiros em sua vida privada. Outrossim, o enfoque positivo diz respeito a faculdade que este titular detém de exigir uma atuação do poder público a fim de criar pressupostos fáticos que vedem a omissão estatal diante das ameaças provenientes de terceiros (VIEIRA, 2007, p. 17).

MARCOS NORMATIVOS DA PROTEÇÃO DE DADOS PESSOAIS

Partindo-se do aspecto positivo do direito a privacidade, fundamentado na exigência da intervenção do poder público, as discussões acerca desse aspecto despertam a partir da década de 1970, onde há uma tendência mundial de preocupação com a proteção de informações pessoais e da privacidade, substanciada no amadurecimento, em diversos países, da proteção de dados pessoais. Em 1974, o Privacy act norte americano lançou as primeiras inquietações acerca do potencial de risco que a informática pode trazer ao uso e tratamento de informações pessoais (CASTRO, 2002, p. 42).

Nesse mesmo ano, o jornal francês Le Monde publicou uma matéria intitulada “Safari ou caça aos franceses” em que divulgou um projeto de iniciativa do Ministério do Interior cujo objetivo era reunir sistematicamente, em um único sistema, cem milhões de fichas nominativas existentes nos arquivos oficiais do governo.

A comoção em torno dessa reportagem culminou, no ano de 1978, na Lei de Informática e Liberdade, a qual foi pautada na Declaração dos Direitos do Homem e do Cidadão. Esta Lei criou um órgão autônomo chamado de Comissão Nacional de Informática e Liberdades – CNIL, incumbido de zelar pela transparência e fixação de regras no tratamento de informações pessoais. Importante destacar que tal normativa se destinou a regular a atividade estatal, prevendo a necessidade de autorização por lei ou decreto, para a criação de tratamentos de dados pessoais no Âmbito governamental (CASTRO, 2002, p. 42).

No plano europeu, em 1981 o Conselho da Europa aprovou a Convenção número 108, cujo teor firmou as bases principiológicas e terminológicas das atuais legislações de proteção de dados pessoais. Seguindo esta tendência, no ano de 1995, o Parlamento Europeu e o Concelho da Europa aprovaram a Diretiva 95/46/CE objetivando harmonizar as legislações europeias e permitir, assim, a circulação de dados em todo território da União Europeia.

O debate sobre privacidade e proteção de dados em âmbito internacional se acirrou após escândalos envolvendo espionagem e compartilhamento de dados pessoais dos usuários, em especial no ano de 2013, quando o ex-funcionário da Agência Nacional de Segurança norte-americana (NSA), Edward Snowden, forneceu documentos ao jornal britânico The Guardian, revelando que empresas de telecomunicações foram obrigadas pelo governo americano a fornecer milhões de registros telefônicos feitos por cidadãos americanos. Também foi revelada a existência de um programa desenvolvido pela NSA com a finalidade de revelar informações de pessoas em todo o mundo que utilizam serviços de grandes empresas dos Estados Unidos, como Apple, Microsoft, Google e Facebook (EXAME, 2013).

Posteriormente, uma reportagem veiculada pelo periódico brasileiro O Globo informa que o Brasil também foi alvo da espionagem americana, sendo o país mais vigiado na América Latina. Segundo informações divulgadas pelo jornalista Glenn Greenwald, milhões de telefonemas e e-mails de cidadãos brasileiros passaram pela análise da NSA (EXAME, 2013).

Devido a imprescindibilidade de uma legislação capaz de enfrentar as novas questões impostas pela economia digital, na data de 25 de maio de 2016 foi aprovado o Regulamento Geral de Proteção de Dados (General Data Protection Regulation - GDPR) na Europa, buscando unificar a proteção de dados pessoais na União Europeia. Esse regulamento é diretamente aplicável a todos os membros dessa organização, não sendo necessária qualquer transposição para suas legislações nacionais. Ele também adota, em seu Art. 4°, um conceito expansionista de dados pessoais, que vai além do dado que efetivamente identifica uma pessoa natural, englobando:

> “qualquer informação relacionada a uma pessoa natural identificada ou identificável. Uma pessoa natural identificável é alguém que pode ser identificada, direta ou indiretamente, principalmente por meio de referência a um identificador único como nome, número de identificação, dado locacional, identificador eletrônico ou um ou mais fatores específicos a identidade física, psicológica, genética, mental, econômica, cultural ou social da pessoa natural” (COUTO 2016, apud GDPR, 2016)

A principal característica da GDPR, é que ela não se aplica somente aos cidadãos europeus. Ela alcança os órgãos e empresas ofertam bens, serviços, ou atividades que se relacionam com a União Europeia e que coletam dados de cidadãos europeus. Portanto, sua implementação modificou substancialmente a forma como a Sociedade Internacional vem tratando os dados pessoais, tendo em vista que o mercado consumidor europeu é abastecido por produtos e serviços de inúmeras nações, inclusive do Brasil.

Seguido dessas novas normativas, outro escândalo envolvendo dados pessoais emergiu no ano de 2018, quando os jornais "New York Times" e "Guardian" revelaram que os dados de mais de 50 milhões de usuários da rede social Facebook foram compartilhados sem o consentimento dos titulares para a empresa britânica Cambridge Analytica (G1, 2018). Estima-se que o número total de afetados, na realidade foi de 87 milhões de usuários. Destaca-se que a empresa Cambridge Analytica trabalhou ainda com a equipe responsável pela campanha de Donald Trump à Presidência dos Estados Unidos, nas eleições de 2016, sinalizando mais ainda a necessidade de que cada nação normatizasse sobre a proteção de dados em seu território.

PROTEÇÃO DE DADOS NO DIREITO BRASILEIRO

Para mais, analisando a problemática da proteção de dados pessoais a partir do panorama brasileiro, verifica-se a introdução dos princípios da proteção de dados pessoais na Constituição Federal de 1988, especificamente em seu art. 5º, item X, o qual refere-se à privacidade e à intimidade com as seguintes palavras: “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas” e no artigo 21 do Código Civil, este que qualifica como inviolável a vida privada da pessoa natural.

No que diz respeito a proteção desse tipo de informação, o poder público vem atuando efetivamente, desde o ano de 2010, no que se considera “tratamento de dados pessoais”. Nesse ano, o Ministério da Justiça lançou uma consulta pública sobre o anteprojeto de uma lei de proteção desses dados. No ano de 2011, foi sancionada a Lei de Acesso à Informação, que dispõe acerca dos dados pessoais de acesso público. Nesse mesmo ano, foi proposto o projeto de lei nº 2126 sobre o marco civil da internet, estipulando direitos e deveres dos usuários e dos provedores. Por sua vez, o Marco Civil entrou em vigor no ano de 2014. Com ênfase em uma maior efetividade, e baseado na estrutura inaugurada pelo GDPR, no ano de 2018 foi editada a Lei 13.709/2018, denominada de Lei Geral de Proteção de Dados Pessoais (LGPD). Essa normativa fundamenta-se em assegurar a toda pessoa natural a titularidade de seus dados pessoais e a garantia dos direitos fundamentais de liberdade, intimidade e privacidade.

DESAFIOS DA GESTÃO PÚBLICA NA IMPLEMENTAÇÃO DE UMA POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS

A Lei geral de proteção de dados pessoais conceitua os dados pessoais como “aquelas informações relacionadas a pessoa natural identificada ou identificável” (Art. 5º, I da LGPD), e expõe que o tratamento de dados pessoais pode ser realizado por dois agentes de tratamento chamados de controlador e operador. O controlador é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (art. 5º, VI da LGPD), e o operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (art. 5º, VII da LGPD).

Em seu artigo 5º, a Lei 13.709/2018 conceitua também o titular, o encarregado, determina o que são dados sensíveis, explica o que se entende por

tratamento, bloqueio, consentimento, eliminação, transferência, anonimização, bem como dispõe sobre o uso compartilhado de dados e o relatório de impacto à proteção de dados pessoais.

Sobre a aplicação da LGPD pela administração pública, destacam-se os seus artigos 23 a 30 cujo teor evidencia que a realização do tratamento de dados deverá se submeter ao atendimento de finalidade pública, na persecução do interesse público e na execução de políticas públicas, com o objetivo de executar as competências determinadas em Lei ou cumprir atribuições legais do serviço público (arts. 23, caput e 26, caput da LGPD).

Nesse sentido, o poder público deve obedecer aos princípios de proteção de dados pessoais elencados no art. 6º desta Lei, que se fundamentam na necessidade de comunicação aos usuários de todos os propósitos decorrentes da realização e tratamento dos dados que são coletados, sem haver possibilidade de tratamento posterior desses dados de forma incompatível com as finalidades já informadas, limitando-se ao mínimo necessário para a realização de suas finalidades, e garantindo o livre acesso e consulta dos titulares sobre a forma de tratamento e sua duração, bem como sobre a integralidade de seus dados pessoais.

De acordo com LARA (2020):

> 'Trata-se (...) de buscar a adequação entre a transparência que deve reger as atividades da Administração Pública e o regime jurídico de proteção de dados inaugurado pela LGPD, o que, certamente, traduz um grande desafio ao gestor público.

No que diz respeito à segurança, a administração pública necessita de transparência em relação a forma de tratamento e aos respectivos agentes de tratamento de dados, se preocupando em desenvolver projetos que visem estipular medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão dessas informações (art. 6, VII da LGPD).

É importante que todos os entes federativos, na condição de controladores dos dados pessoais, estudem e confeccionem um relatório de impacto à proteção de dados pessoais. Este documento visa descrever os processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais dos cidadãos, e estabelece possíveis medidas, salvaguardas e mecanismos de mitigação de risco (art. 6º, XVII da LGPD).

Outros pontos estratégicos dizem respeito à adoção de medidas preventivas, as quais seriam utilizadas caso haja ocorrência de algum dano em virtude do tratamento de dados pessoais, e também a prestação de contas, pelo agente público, visando relatar quais medidas estão se mostrando eficazes no cumprimento e observância das normas de proteção de dados pessoais (art. 6º, VIII e X da LGPD).

Outrossim, o principal dispositivo que permite o tratamento de dados pessoais pela Administração Pública é o artigo 7º, III da LGPD, o qual expõe que o tratamento de dados pessoais somente poderá ser realizado pela administração pública para "tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres".

Portanto, a execução de políticas públicas é um conceito muito amplo, que pode servir de justificativa para que o setor público realize qualquer tipo de tratamento de dados, uma vez que é um conceito genérico e inerente à existência do próprio Estado (ROSSO, 2019).

Importante destacar também que o inciso III do art. 7º da LGPD estipula um rol de bases legais que podem autorizar o tratamento de dados pessoais (ROSSO, 2019). Dentre elas estão as Leis, os regulamentos, contratos, convênios e instrumentos congêneres, em consonância com o Art. 6º inciso I que dispõe acerca da necessidade de se expor as finalidades para que esses instrumentos autorizariam o tratamento de dados, observados os propósitos legítimos, específicos, explícitos e informados ao titular, e sem possibilidade de tratamento posterior de forma incompatível.

Ademais, quando se tratam de condicionantes para que o setor público compartilhe dados pessoais que detém posse, o artigo 26 veda o compartilhamento desses dados com entidades privadas, exceto em casos que a transferência seja necessária, com o fim específico e determinado de execução descentralizada da atividade pública. São os casos onde o ente privado atua executando um serviço em nome do Estado. Como exemplos temos a atuação das empresas públicas, autarquias, sociedades de economia mista, fundações, consórcios, e quando a execução de um serviço público ocorre por meio de concessões, autorizações e permissões.

O artigo 27 determina que deve existir consentimento do proprietário dos dados para que eles possam ser compartilhados com algum ente privado, com exceção dos casos em que ocorre dispensa de consentimento, expressos no artigo 7º, §4º, ou quando se tratam de dados manifestamente públicos pelo titular, e sem fornecimento de consentimento do titular, nas hipóteses previstas no artigo 11, II:

> a) cumprimento de obrigação legal ou regulatória pelo controlador;
> b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
> c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
> d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
> e) proteção da vida ou da incolumidade física do titular ou de terceiro;
> f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou
> g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Ademais, o Art. 4º da LGPD, em seu inciso III aborda os casos onde a incidência dessa lei é afastada, são eles a segurança pública; a defesa nacional; a segurança do Estado; e atividades de investigação e repressão de infrações penais.

CONCLUSÃO

Assim, tendo em vista a problemática da proteção de dados pessoais nas esferas públicas e privadas, surge a necessidade de se "fazer algo diferente", conforme Schumpeter lecionava. Precisamos destruir as antigas bases em que se fundamentava o direito de privacidade, cujas lacunas permitiram que empresas e órgãos estatais trocassem informações desenfreadamente. Para tanto, é necessário evocar o enfoque positivo do direito à privacidade, onde a atuação de cada agente público é fundamental.

Dessa forma, cabe aos entes federativos estabelecerem um conjunto de diretrizes, normas e ações para a adaptação e execução da LGPD, visando formar uma Política de Proteção de Dados Pessoais dentro de cada órgão específico, tendo como objetos dessa reorganização os dados da própria administração pública e os sistemas informatizados que armazenam tais informações. A nova lei de proteção de dados aborda conceitos que ainda dependem da efetivação dos gestores, em especial da criação de uma autoridade nacional de proteção de dados, e que cada ente federativo disponha de sua própria política de proteção de dados.

Um exemplo brasileiro de pioneirismo nesse tema é o Estado de Pernambuco, o primeiro a adotar uma política estadual de proteção de dados mediante decreto publicado em 7 de agosto de 2020. Essa política consiste em um conjunto de diretrizes, normas e ações para adaptação da LGPD no âmbito da administração pública estadual.

Nesse caso específico, as atividades ficam sob coordenação da Secretaria da Controladoria-Geral do Estado, visando todos os órgãos e entidades do executivo, onde cada um deles deverá seguir um plano quadrienal estratégico de proteção de dados pessoais, este que abarca as prioridades estaduais, as responsabilidades e papeis de cada órgão nessa atuação, os processos de gerenciamento de riscos, monitoramento das ações desenvolvidas e criação de um canal de atendimento ao titular (considerando as atividades desempenhadas pela Ouvidoria-geral do Estado), a produção de manuais de implementação de políticas e de outros modelos de documentos, entre outras ações que efetivam a LGPD.

Assim, entende-se que a os conceitos trazidos pela LGPD representam um avanço no que se refere à proteção de dados pessoais, em consonância com os marcos legais de outras nações. No momento, é relevante que todos os entes administrativos desenvolvam diretrizes, normas e ações para sua adaptação, visando a legitima efetivação de um direito a privacidade.

REFERÊNCIAS

CASTRO, Luiz Fernando Martins. **Proteção de dados pessoais:** panorama brasileiro e internacional. REVISTA CEJ (BRASÍLIA), Brasília-DF, v. 19, n.19, p. 40-45, 2002.

CAVALCANTE, P. L. R.; CUNHA, BRUNO QUEIROZ. É Preciso Inovar no Setor Público, Mas Por Quê? In: Pedro Cavalcante; Bruno Cunha; Marizaura Camões; Willber Severo. (Org.). Inovação no setor público: teoria, tendências e casos no Brasil. 1ed.Brasília: Instituto de Pesquisa Econômica Aplicada (Ipea) e Escola Nacional de Administração Pública (Enap), 2017, v. 1, p. 15-32.

Comitê Central de Governança de Dados. **Guia de Boas Práticas para implementação na Administração Pública Federal**: lei geral de proteção de dados (gpd). Brasília, 2020. 65 p. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-lgpd.pdf. Acesso em: 05 ago. 2020.

DIARIO DE PERNAMBUCO; **Governo de Pernambuco institui política de proteção de dados pessoais.** Diário de Pernambuco. Disponível em: <https://www.diariodepernambuco.com.br/noticia/economia/2020/08/governo-de-pernambuco-institui-politica-de-protecao-de-dados-pessoais.html>. Acesso em: 27 Nov. 2020.

DONEDA, Danilo. A proteção da privacidade e de dados pessoais no Brasil. **Observatório Itaú Cultural**, São Paulo, v. 16, n. 1, p. 136-150, jun. 2014. Semestral. Disponível em: https://issuu.com/itaucultural/docs/observatorio16. Acesso em: 05 ago. 2020.

DÓRIA, A. S., SANO, H., LIMA, J. P. de, e SILVA, A. F. S. B. S. (2017). Inovação no setor público: uma instituição pública de ensino sob a ótica dos servidores e colaboradores. Revista Do Serviço Público, 68(2). https://doi.org/10.21874/rsp.v68i2.1801

EXAME, Revista (ed.). O mundo sob vigilância:: veja cronologia do caso snowden. veja cronologia do caso Snowden. 2013. Disponível em: https://exame.com/tecnologia/o-mundo-sob-vigilancia-veja-cronologia-do-caso-snowden/. Acesso em: 09 ago. 2020.

G1(ed.). **Facebook eleva para 87 milhões o nº de usuários que tiveram dados explorados pela Cambridge Analytica**. 2018. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/facebook-eleva-para-87-milhoes-o-n-de-usuarios-que-tiveram-dados-explorados-pela-cambridge-analytica.ghtml. Acesso em: 10 ago. 2020.

OCDE. Manual de Oslo: Diretrizes para a coleta e interpretação de dados sobre inovação. 3. ed. FINEP, 2005. Disponível em: https://www.finep.gov.br/images/apoio-e-financiamento/manualoslo.pdf. Acesso em: 07 ago. 2020.

RODRIGO PUGLIESI LARA. **Os desafios da LGPD no setor público**. Consultor Jurídico. Disponível em: <https://www.conjur.com.br/2020-out-22/rodrigo-lara-desafios-lgpd-setor-publico>. Acesso em: 27 Nov. 2020.

ROSSO, ANGELA MARIA. LGPD e setor público: aspectos gerais e desafios - Migalhas. Uol.com.br. Disponível em: <https://migalhas.uol.com.br/depeso/300585/lgpd-e-setor-publico--aspectos-gerais-e-desafios>. Acesso em: 27 Nov. 2020.

SCHUMPETER, J. Theory of economic development. Cambridge: Harvard University Press, 1934.

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. 25. ed. São Paulo: Malheiros, 2005. 924 p.

TORMES, Diego. Accountability: o que significa?. 2017. Disponível em: https://www.politize.com.br/accountability-o-que-significa/. Acesso em: 08 ago. 2020.

VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação**: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. 297 f. Brasília, 2007.