PRESTAÇÃO DOS SERVIÇOS PÚBLICOS À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

PROVISION OF PUBLIC SERVICES UNDER THE GENERAL DATA PROTECTION LAW (LGPD)

Alison Cleiton Rodrigues[1]
Alan Pinheiro de Paula[2]

RESUMO

A Lei Geral de Proteção de Dados Pessoais (LGPD) foi estabelecida para promover a regulação do tratamento dos dados pessoais do indivíduo, seguindo princípios, deveres e direitos tanto do seu titular, quanto do usuário desses dados – pessoas físicas e jurídicas, além do poder público. O objetivo deste artigo é mostrar os conceitos, a aplicação e a abrangência dessa Lei, indicando os desafios para que possa ser aprimorada. Para explicar o alcance da LGPD é apresentado seu relacionamento com o serviço de administração pública. Em complemento, são comentados os aspectos do acesso aos dados pessoais e ambientes sensíveis no serviço público, com a utilização de referências de diversos autores para referir o modo de resposta do serviço público na solicitação de acesso de terceiros. A metodologia empregada neste trabalho é qualitativa, com base técnica na legislação em vigor, em publicações específicas sobre o tema.

Palavras-Chave: Proteção de Dados. Tratamento. Privacidade.

ABSTRACT

The General Law for the Protection of Personal Data (LGPD) was established to promote the regulation of the processing of the individual's personal data, following principles, duties and rights of both its owner and the user of such data - individuals and legal entities, in addition to power public. The purpose of this article is to show the concepts, application and scope of this Law, indicating the challenges for its improvement. To explain the scope of the LGPD, its relationship with the public

[1]Graduando em Direito, Universidade do Contestado (UNC). Campus Mafra. Santa Catarina. Brasil. E-mail: alisonpentatonixrodrigues@gmail.com
[2] Mestre em Ciência Jurídica pela UNIVALI. Especialista em Gestão de Segurança Pública pela Universidade de Santa Catarina (UNISUL). Professor de Direito da Universidade do Contestado (UnC). Santa Catarina. Brasil. E-mail: alanpinheirodepaula@gmail.com

administration service is presented. In addition, aspects of access to personal data and sensitive environments in the public service are discussed, using references from different authors to refer to the way in which the public service responds when requesting access from third parties. The methodology used in this work is qualitative, based on technical legislation in force, in specific publications on the subject.

Keywords: Data Protection. Treatment. Privacy.

1 INTRODUÇÃO

A Lei Geral de Proteção de Dados (LGPD), instituída pela Lei nº 13.709, de 14 de agosto de 2018 e alterada de forma parcial pela Lei nº 13.853, de 08 de julho de 2019, foi criada com a finalidade de proporcionar um regulamento para o tratamento dos dados de pessoas em relações comerciais de bens e serviços em território brasileiro.

Considerando os aspectos das relações comerciais no mundo atual, que levantam as preferências pessoais dos consumidores em suas decisões de compras, a LGPD é muito importante para preservar os dados pessoais dos indivíduos, unindo os processos de segurança com a disponibilidade de produtos e serviços personalizados, que representa a tendência atual da economia.

O problema a ser discutido é como o serviço oferecido pela administração pública federal pode ser analisado dentro dos princípios da LGPD.

Neste artigo são apresentados os aspectos gerais da LGPD e seus principais conceitos, bem como parte de sua trajetória, até se tornar lei.

Também é apresentada a relação entre a LGPD e o serviço público, pois a administração pública também tem obrigações na salvaguarda e proteção dos dados sob sua responsabilidade.

Finalmente é comentado o acesso aos dados pessoais e ambientes sensíveis no serviço público, com a utilização de referências de diversos autores para referir o modo de resposta do serviço público na solicitação de acesso terceiros.

A metodologia empregada no artigo é a qualitativa, com base técnica na legislação em vigor, em publicações específicas sobre o tema, em análises de setores do cotidiano do Brasil, para indicar os elementos fundamentais para a compreensão da importância da Lei Geral de Proteção de Dados (LGPD).

A pesquisa qualitativa, no âmbito das técnicas experimentais, pode utilizar várias técnicas à disposição, porém neste artigo será utilizada a técnica da teoria fundamentada que, a partir da busca de informações permite um desenvolvimento que enuncia e abrange o assunto em questão.

2 ASPECTOS GERAIS DA LGPD

A forte concorrência no mercado mundial e o rápido desenvolvimento tecnológico abriram caminho para várias questões sobre a segurança das informações corporativas e da pessoa natural, fazendo com que estas estejam expostas a ataques cibernéticos, com intenções diversas como apropriação de dados e a divulgação pública de assuntos sigilosos.

Somado a isto, várias empresas utilizavam incorretamente os dados de seus clientes, transferindo-os ou vendendo-os a outras empresas, sem que seja obtido o consentimento do(a) proprietário(a) dos dados (RAPOSO *et al*, 2019).

A LGPD é aplicável a pessoas físicas e jurídicas, além do poder público, nos limites do território brasileiro, no que se refere ao tratamento de dados de pessoas naturais, quando este tratamento ocorrer no Brasil e quando forem oferecidos bens e serviços para pessoas no Brasil (DONEDA, 2017).

De acordo com Soares (2020, p. 7), o tratamento de dados pessoais é:

> Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

O escopo da LGPD é salvaguardar a maneira como os dados pessoais devem ser tratados, incluindo o meio digital, em franco desenvolvimento nos dias de hoje. Para que os direitos essenciais de liberdade e do desenvolvimento do cidadão sejam preservados, o Decreto nº 10.474, de 26 de agosto de 2020, criou a Autoridade Nacional de Proteção de Dados (ANPD) (BRASIL, 2020).

A maioria dos artigos da LGPD está valendo desde setembro de 2020. Contudo, o que se refere à Autoridade Nacional de Proteção de Dados (ANPD) está em vigor desde o final de dezembro de 2018. A questão das punições de ordem

administrativa, constantes nos artigos de 52 a 54, começou a valer a partir de agosto de 2021, o que proporcionou, às empresas, principalmente, maior prazo para adaptação e evitarem exposição a punições (BRASIL, 2020).

A LGPD complementa direito consumerista expresso no Código de Proteção de Defesa do Consumidor, Lei nº 8078, de 11 de setembro de 1990, que, entre outros aspectos, previa disciplinar o tratamento de bancos de dados com a finalidade de análise de crédito, porém não se atendo às formas derivadas da coleta e do tratamento de dados. Estas formas foram definidas e tiveram regras sobre a proteção dos dados determinadas pelo Marco Civil da Internet (Lei nº 12.965, de 23 de abril de 2014), que regula o uso da internet no Brasil (MIRAGEM, 2019).

No que diz respeito aos registros, dados pessoais e às comunicações privadas, o Marco Civil da Internet, em seu art. 10, dispõe que:

> A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas (BRASIL, 2014, p. 3).

Um elemento fundamental da Lei Geral de Proteção de Dados é o consentimento da pessoa natural para que sua base de dados possa ser tratada. Contudo, o tratamento pode ser realizado sem que o indivíduo consinta, desde que este procedimento seja essencial para que uma obrigação de ordem legal seja cumprida, uma política pública (desde tenha previsão em lei) possa ser executada, na prevenção de fraudes contra o proprietário dos dados, no caso de proteção do crédito ou ainda no atendimento a uma legitimidade de interesse sem que haja risco aos direitos fundamentais da pessoa (SERPRO, s.d.).

Como ocorre como qualquer legislação, a LGPD tem também seus princípios, tais como: a finalidade, que determina que o tratamento de dados deve ser feito de acordo com uma finalidade clara, que deve ser informada ao titular dos dados, para que este autorize o processo; a adequação, que dispõe que o tratamento dos dados deve ser a maneira correta para que a finalidade informada ao titular seja atendida; a necessidade e minimização, que esclarece que devem ser usados apenas os dados que forem necessários para atingir a finalidade, dentro do menor prazo exequível.

Além destes princípios, outros que tratem do acesso, das garantias, da disponibilização e da segurança, estão inseridos na lei, que são: o livre acesso, que diz que ao titular deve ser disponibilizado o acesso gratuito e facilitado, abrangendo todos os pontos necessários para o tratamento de seus dados; a qualidade dos dados, que dispõe que ao titular deve ser dada a garantia de que os seus dados estão claros, corretos e aderentes à finalidade informada; a transparência, que o titular deve receber todas as informações necessárias sobre o modo como seus dados estão sendo tratados; a segurança, em que o agente responsável pelo tratamento dos dados deve utilizar todos os procedimentos técnicos e administrativos aplicáveis para a devida proteção de todas as informações sob sua responsabilidade, não permitindo acessos que não sejam autorizados (PINHEIRO, 2020).

Finalmente, aspectos relacionados à prevenção, ausência de discriminação e prestação de contas são igualmente importantes, vez que a prevenção diz respeito ao agente responsável pelo tratamento, que deve prover meios para que o titular não seja exposto a danos; a não discriminação, pois sob nenhuma hipótese os dados pessoais devem ser usados para finalidade de discriminação, uso ilegal ou caráter abusivo; e a responsabilização e prestação de contas, em que o agente responsável pelo tratamento dos dados deve estar apto a esclarecer que todos os procedimentos para a proteção destes dados são eficientes e estão de acordo com a LGPD (PINHEIRO, 2020).

Ainda que o assunto esteja atual devido à sua recente implantação, pode ser considerado que a LGPD teve sua história iniciada desde que o direito à privacidade foi formalizado, em 1890, passando pela oficialização dos Direitos Humanos pela Organização das Nações Unidas (ONU), em 1948, e por sucessivas etapas até chegar ao ponto de sua oficialização (SERPRO, 2021).

As empresas tiveram que enfrentar muitos desafios para chegar ao estágio atual, passando por adaptações necessárias que envolvessem as questões de armazenamento e acesso dos dados, treinamento das equipes, entendimento sobre os direitos dos proprietários dos dados, providenciar a contento os pedidos de informações recebidos e aderência aos conceitos de adaptabilidade e escalabilidade (DONEDA, 2017).

O modo de tratar dados pessoais por intermédio de empresas públicas deve estar em sintonia para o atendimento de sua finalidade pública, de acordo com o

interesse público, no cumprimento dos requisitos constantes na legislação em vigor e para que sejam cumpridos todos estes preceitos legais no âmbito público (SILVEIRA, 2012).

Tem grande relevância considerar que, a despeito da quantidade de empresas públicas detentoras de dados pessoais, o Serviço Federal de Processamento de Dados (Serpro) e a Empresa de Tecnologia e Informações da Previdência (Dataprev), tenham sido estruturados para aderir ao conceito de empresas públicas de destaque. Assim, continuam o desenvolvimento de sistemas para o serviço público, hospedam e processam diversas bases de dados de destaque para a Administração Pública Federal (DONEDA, 2017).

A seguir é apresentado o capítulo sobre a Lei Geral de Proteção de Dados e o serviço público.

3 LGPD E SERVIÇO PÚBLICO

São consideradas pessoas jurídicas de direito público, no âmbito da LGPD:

> Os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público;
> As autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios.
> Os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público, terão o mesmo tratamento dispensado às pessoas jurídicas de direito público.
> As empresas públicas e as sociedades de economia mista que atuam em regime de concorrência, sujeitas ao disposto no art. 173 da Constituição Federal, terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares. Porém, quando estiverem operacionalizando políticas públicas e no âmbito da execução delas, terão o mesmo tratamento dispensado aos órgãos e às entidades do Poder Público (PARANÁ, 2020, p. 19).

A Autoridade Nacional de Proteção de Dados (ANPD) pode, a qualquer tempo, emitir solicitação direcionada a órgãos públicos para que executem atividades de tratamento de dados pessoais, com informações direcionadas sobre o alcance e a natureza dos dados, bem como detalhamento do que foi executado, podendo gerar um parecer técnico como complemento à garantia de que a Lei Geral de Proteção de Dados estejam sendo cumprida (BRASIL, 2020).

Nos casos de infração à LGPD por órgãos públicos, a ANPD poderá enviar informe com medidas cabíveis para fazer cessar a violação, podendo ainda, de acordo com sua análise, pedir para que os agentes públicos orientem a execução de processos técnicos compatíveis com o modo legal de tratamento dos dados pessoais (CIRINO, 2020).

É fundamental o entendimento sobre a abrangência e a efetividade da LGPD no tocante ao poder público. Ainda que a lei tenha, no capítulo IV, artigos 23 a 30, preceitos de regulação do tratamento de dados pessoais deste setor, o assunto sempre foi tema de discussões e análises, sendo que sua exclusão chegou a ser sugerida (COTS; OLIVEIRA, 2019).

Em complemento a este ponto, a inserção de pontos no texto normativo, com claras manifestações de exceção relativas ao setor público, facilita a forma de tratar e compartilhar os dados pessoais e sensíveis pela administração pública federal (PINHEIRO, 2020).

Este tratamento diferenciado, ou privilegiado, está no inciso III do artigo 7º da Lei Geral de Proteção de Dados, que se refere às hipóteses de tratamento de dados pessoais:

> Pela administração pública, para o 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, observadas as disposições do Capítulo IV desta Lei (BRASIL, art. 7º, 2018).

Também no inciso II do artigo 11 do mesmo diploma, que dispõe sobre o tratamento de dados sensíveis, pode ser observado que:

> II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
> 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 (BRASIL, art. 11, 2018).

Como uma forma de compensação deste privilégio, a Lei atenua ou ameniza os termos de exceção, no parágrafo 2º do artigo 11, determina-se que na hipótese em que o consentimento é requerido, se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações (BRASIL, 2018).

Segue também a mesma compensação no artigo 23, que dispõe que o tratamento de dados pessoais pelas pessoas jurídicas de direito público deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:

> I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos;
> III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei (BRASIL, art. 23, 2018).

Ainda que não possa ser encarado como uma forma de autorização para que o setor público compartilhe de modo generalizado e indiscriminado os dados considerados sensíveis, não pode passar despercebido o fato de que controlar a publicidade da administração pública federal, assim como a maneira como é disponibilizada, nas páginas oficiais publicadas na internet, não é algo que possa ser classificado como claro, transparente e efetivo (FEIGELSON; SIQUEIRA, 2019).

Deste modo, concorrendo para a segurança da proteção dos dados de seus respectivos titulares, intenção existente na grande maioria dos países com leis similares, é que foi criada a ANPD, cuja criação tinha sido vetada na promulgação da LGPD, mas foi restaurada através da Medida Provisória (MP) nº 86917, pelo ex-presidente Michel Temer, em 28 de dezembro de 2018 (COTS; OLIVEIRA, 2019).

A disponibilidade de dados por intermédio da administração pública, sem dúvida, é um assunto carente de mais análises, pesquisas e melhoras, estando ligado ao relacionamento de confiança e credibilidade os órgãos públicos e à obrigatoriedade de ampla divulgação da gestão pública. Fica sempre possível fazer a pergunta: a administração pública é uma tutora confiável dos direitos individuais e das informações públicas dos cidadãos brasileiros? (MACKENZIE, 2019).

Para ser possível responder a esta pergunta, é preciso fazer a análise e a compreensão do modelo vigente de administração pública, no que tange à gestão, modo de tratar e disposição de dados pessoais e sensíveis, para que ver se existe o atendimento às recomendações de publicidade e transparência, mantendo intocada a privacidade. Como resultado preliminar desta análise não é difícil concluir que a gestão governamental pode ser considerada como ineficaz (RAPOSO *et al,* 2019).

Esta afirmação, ainda que, fruto de resultado preliminar, advém da observação de que a falta e a lentidão na adoção de uma legislação particular ao caso causam impacto negativo às políticas público-administrativas, com ausência de terminologia padrão, que seja precisa e não vaga, trazendo erros ao interpretar a administração pública (RAPOSO *et al*, 2019).

Existem diferenças no formato de gerir os dados entre os diversos órgãos públicos, com níveis de segurança de informação diferentes, podendo incorrer em situações contrárias à legalidade. Também não há transparência no tocante a sanções que são consequência de mau uso dos dados, que podem ser dificuldades oriundas da Lei de Acesso à Informação, para citar um exemplo (PINHEIRO, 2020).

Esta análise foi fomentada pela promulgação do Regulamento Geral de Proteção de Dados (RGPD) da União Europeia, em 25 de março de 2018, que trata da segurança dos dados da população da Comunidade Europeia, por intermédio de uma pessoa, de uma empresa ou de uma organização (MACKENZIE, 2019).

A imensa geração de dados no mundo digital, um fenômeno classificado como *Big Data*, se resume em ser possível obter mais informações tendo como ponto inicial uma variada quantidade de dados, o que possibilita dar origem a um relevante valor agregado de bens e serviços. Outro fenômeno, decorrente do *Big Data*, o *datafication*, traz o conceito de obter informações sobre tudo que possa existir (AMARAL, 2016).

Desta forma, tendo os dados e as informações se tornado ativos importantíssimos para as empresas da atualidade, segundo Mayer-Schonenberger e

Curier (2013), “dataficar um fenômeno é colocá-lo num formato quantificado de modo que possa ser tabulado e analisado”.

A vida particular, os aspectos privados e a própria intimidade dos indivíduos, assim, não ficaram a salvo do *Big Data* e do *datafication*, justamente por terem se transformado neste ativo valioso para as instituições de todo o mundo (BOTELHO, 2020).

Esses problemas são decorrentes de uma diversificação de questionamentos. Entre eles, reconhecer que é preciso existir uma política pública de proteção de dados pessoais no Brasil a falta, até meados de 2018, de um marco legal sobre o assunto, a terminologia difusa nas normas e regulamentos, a necessidade de atender aos conceitos de publicidade e a dificuldade de entendimento de conhecimento técnico em muitos setores, como na Tecnologia da Informação e na Comunicação (CHRISTIAN; GONÇALVES, 2019).

No mundo digital, o uso do *Big Data* pela administração pública traz questionamentos de ordem ética passíveis de observação. Desta forma, existe um certo embate entre a privacidade e o interesse público. Quanto à privacidade, o Decreto nº 8.789/16 trata do compartilhamento de bases de dados no ambiente das diversas instituições federais, sem que sejam necessárias celebrações de convênios ou acordo de cooperação, trouxe muita polêmica.

> O que acontece se informações pessoais que podem prejudicar ou causar discriminação (como de saúde ou previdência social) acabarem em bases de dados consultáveis por entes privados (como seguradoras)? Lembrando do polêmico caso em que o Tribunal Superior Eleitoral (TSE) permitiu que o Serasa tivesse acesso a sua base de dados, não dá para dizer que essa seja uma hipótese absurda. Se ela tivesse sido turbinada com outras informações, as consequências seriam ainda mais graves. O que dizer, também, de órgãos de investigação (como a Polícia Federal) criando perfis de potenciais criminosos a partir do cruzamento de dados sobre a saúde do indivíduo fornecidos pelo Ministério da Saúde, dados sobre escolaridade pelo Ministério da Educação e dados socioeconômicos pelos Ministérios das Cidades e do Desenvolvimento Social, por exemplo? Considerando o policiamento preditivo à base de big data que começa a ser implementado ao redor do mundo, não se pode descartar o seu uso aqui. A Polícia Federal já tem histórico de cruzar dados para otimizar o controle das alfândegas (ABREU, 2016, s.p.).

Como afirma Doneda (2012, p. 45), “qualquer dado pessoal e não somente o dado sensível é passível de, em determinadas circunstâncias, dar origem à discriminação ou ao controle, diminuindo as liberdades de escolha de uma pessoa”.

Mais que isso, segundo ele, “os efeitos geralmente atribuídos ao tratamento indiscriminado dos dados sensíveis também podem ocorrer quando da manipulação de dados”.

A questão do acesso a dados pessoais e sensíveis está distribuída em vários órgãos da administração pública e o próximo capítulo examina as observações feitas em pesquisas de diferentes autores a respeito da forma como a resposta a solicitações foram enviadas.

4 ACESSO AOS DADOS PESSOAIS E AMBIENTES SENSÍVEIS NO SERVIÇO PÚBLICO

Dentro do cenário para disponibilizar dados e ter a publicidade como regra a seguir e o sigilo a ser tratado como exceção, existe outra maneira de fornecer os dados pessoais e sensíveis através da administração pública, mas para agentes terceiros atuando como interessados. Nada mais é do que dispor os dados tendo como finalidade de pesquisa (MACKENZIE, 2019).

Assim, na questão de publicidade, o cotidiano da gestão pública da administração fica com grande teor de desafio o preparo e a integração das bases (com chaves comuns ou possibilitando cruzamentos), a classificação dos dados de acordo com o que agregam, a dificuldade para que os resultados das pesquisas pudessem ser controlados para que informações de dados pessoais não sejam objeto de revelação, a segurança e a tecnologia da informação, sem contar o planejamento, sempre requerido, ter o serviço priorizado e capacitar equipes que serão gestoras, bem como as interpretações complexas da lei (DONEDA, 2017).

Mesmo com os obstáculos, alguns setores da administração pública têm procurado, notadamente nos últimos dois anos, fomentar a execução de pesquisas usando os dados que estas coletaram, mesmo por agentes externos de pesquisas, para conseguir maior teor de transparência com base na Lei de Acesso à Informação, para que os meios de política pública melhorem (SERPRO, s.d.).

Um dos modos planejados pelos órgãos públicos para esse processo foi disponibilizar os dados, mesmo os pessoais ou os sensíveis, em plataformas classificadas e preparadas para serem seguras. Em cenário nacional, esse modelo de serviço tem sido executado por algumas instituições públicas e com níveis

diferenciados de segurança da informação. Destaque para o Instituto Brasileiro de Geografia e Estatística (IBGE), o Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (Inep) e o Instituto de Pesquisa Econômica Aplicada (Ipea) com relação ao acesso a bancos de dados típicos para cruzar informações que não estão disponibilizadas em micro dados públicos (CHRISTIAN; GONÇALVES, 2019).

Os maiores obstáculos na gestão desses serviços acontecem no tocante à permissão para manipular e cruzar bases de dados diferentes que incluem informação de origem socioeconômica; sobre a vida escolar do indivíduo; mercado de trabalho e programas sociais; informação sobre o tipo e o modelo de renda e característica demográficas. E, nesse cenário, a análise detalhada e minuciosa de um projeto de pesquisa submetido à análise quanto à possibilidade de acessar ambientes considerados seguros, assim como avaliar posteriormente os resultados obtidos podem apresentar erros quanto à segurança da informação (CIRINO, 2020).

Relevante destacar os serviços de acesso a ambientes seguros utilizados, no caso do IBGE e do Inep, como canais específicos de atendimento ao e-SIC, ou seja, caminhos indicados para o solicitante da informação. Em casos assim, pode ser considerado, para caso estatístico, que a devolutiva enviada pela administração pública conseguiu atender plena ou parcialmente o que foi pedido.

Além disso, os institutos citados usam a negação de pedido de acesso via e-SIC as razões a seguir: dados pessoais, informação sigilosa de acordo com legislação específica e informação sigilosa classificada de acordo com a Lei nº 12.527/2011, mostrando que a prestação do serviço de acesso ao ambiente seguro, nessas situações, não foi suficiente para atender as demandas (MACKENZIE, 2019).

A sala de acesso a dados restritos do IBGE, a partir da inauguração, em 2003, já tinha a preocupação na proteção de dados pessoais e sigilosos obtidos, procedendo à sua criptografia. O Serviço de Atendimento ao Pesquisador (SAP) foi criado em setembro de 2014, através da Portaria Inep nº 467. Ao contrário do IBGE, o modelo adotado anteriormente tinha como previsão a disponibilidade de bases de dados no modo em que se estavam, sem alterações, podendo ser acessadas, para finalidades institucionais e científicas, informações com sigilo ou pessoais, individuais, conseguidas pelo Instituto, sem a necessária anonimização (COSTA; OLIVERIA, 2019).

Depois de debates internos a respeito segurança e proteção dos dados pessoais e sensíveis, em 2017, a denominação do serviço foi alterada para Serviço de Acesso a Dados Protegidos (Sedap), através da Portaria nº 465. Com isso, novos critérios foram definidos e melhorados (SERPRO, s.d.).

Nos processos do SAP existia omissão quanto à possibilidade de utilização de bases de dados externas. Contudo, seu uso era aceito. No caso do Sedap, esse requisito foi melhorado, com a obrigatoriedade da autorização de uso e certificação de conteúdo de bases externas, emitida pela instituição que produzia os dados (MACKENZIE, 2019).

Além disso, o Inep pode não aceitar sua utilização se vislumbrar risco relacionado à exposição indevida de dados pessoais ou quebra de sigilo. Esse ponto é de muita importância porque, na dependência da pesquisa feita, tornasse possível cruzar dados que fazem com que a informação adquira sensibilidade, como no caso do cruzamento das bases sobre educação do Inep com a base da Relação Anual de Informações Sociais (RAIS), do Ministério do Trabalho; ou a do Cadastro Único para Programas Sociais, do Ministério do Desenvolvimento Social (MACKENZIE, 2019).

Finalmente, importante ressaltar que, pela disponibilidade de dados pessoais e sigilosos, o SAP/Sedap, primeiramente, também era usado como razão de resposta para pedidos direcionados ao Serviço de Informação ao Cidadão do Inep. O SIC-Inep informou que, de setembro de 2014, data da publicação da Portaria que criou o SAP, até maio de 2016, 35 pedidos tiveram resposta usando a justificativa de sua existência (FEIGELSON; SIQUEIRA 2019).

Através do sistema de buscas de pedidos e respostas do e-SIC há possibilidade de verificar o envio de perguntas de intenções diversas para o SAP/Sedap, como, por exemplo, que universidades têm mais cotistas (quantidade de cotas de raça) e quais são esses alunos (dados dos contatos); lista total das pessoas físicas que fizeram inscrição no ENEM a partir de 2011; informações divididas por ano (2011, 2012, 2014, 2015) e cursos, com o nome dos professores cadastrados pela instituição, a titulação e o regime de trabalho; alunos matriculados no ensino médio e superior em Joinville (SC), divididos por escola e curso, entre outros (MACKENZIE, 2019).

Desta forma é possível observar que os debates e análises sobre a proteção de dados pessoais e sensíveis no Instituto tiveram consequências em ações voltadas para a proteção destes recebem processos de melhoria contínua. Ainda que não se

tenha alcançado a possibilidade plena de acesso por parte de pesquisadores o acesso às bases de dados criadas pelo Inep, com a necessária dose de proteção aos dados pessoais e sensíveis, com vistas ao atendimento da orientação de publicidade total, uma eventual ilegalidade criada ao permitir um acesso de pesquisador a bases sem traços de identificação foi sanada (PARANÁ, 2020).

5 CONSIDERAÇÕES FINAIS

Este artigo apresentou informações importantes sobre um marco na questão de tratamento de dados pessoais do indivíduo: a Lei Geral de Proteção de Dados (LGPD).

Atendendo a uma consequência do avanço do mercado consumidor e na crescente necessidade de conhecer as preferências dos consumidores, a LGPD é de extrema importância na preservação dos dados da pessoa natural, sendo aplicável para pessoas físicas, jurídicas e para o poder público, no território nacional ou quando aqui for objetivo de oferecimento bens e serviços para pessoas daqui.

Esta lei tem como princípios básicos a finalidade da para a obtenção dos dados pessoais, a escolha, o livre acesso do titular dos dados, a segurança destas informações e a transparência de todo o processo de tratamento.

Antes da promulgação da LGPD, no Brasil foram instituídas legislações importantes para fundamentar a sua base, tais como a própria Constituição Federal, o Código de Defesa do Consumidor, a Lei do Cadastro Positivo, a Lei de Acesso à Informação e o Marco Civil da Internet.

O objetivo geral deste artigo foi mostrar os conceitos e a abrangência da Lei Geral de Proteção de Dados, bem como a mudança do cenário com o advento da LGPD, indicando onde a lei é ou não aplicada, além de comentar os desafios que precisam ser superados, foi foram plenamente alcançados, considerando o conteúdo proposto e apresentado, inclusive dentro da administração pública.

O problema proposto foi respondido com a análise da atuação de alguns órgãos da administração pública federal. A resposta traz o conceito de que o atendimento pode ser classificado como ineficaz dentro dos princípios da LGPD.

Com amparo em alguns artigos da lei, a administração pública recebe um tratamento diferenciado, com base na necessidade de atender às exigências de suas atividades legais.

Mesmo com a obrigação de utilizar seus *sites* para cumprir a determinação de publicidade, a fiscalização das atividades da administração pública no tratamento dos dados pessoais é de difícil execução, ainda mais pela pequena participação dos representantes do poder legislativo, que teriam mais acesso aos procedimentos necessários para um acompanhamento mais eficaz.

Este artigo tem importância para o mundo acadêmico pela análise da participação da administração pública federal dentro do contexto da LGPD, assunto ainda não explorado com maior intensidade, principalmente pelo fato de que apenas em agosto de 2021 os artigos relativos às sanções passaram a ter validade.

Uma análise sobre as atividades da administração federal e do poder legislativo dentro dos princípios da LGPD, representa uma excelente oportunidade para estudo futuro.

REFERÊNCIAS

ABREU, Jacqueline de Souza. **O compartilhamento de dados pessoais no Decreto nº 8.789/16:** um Frankenstein de dados brasileiro? 2016. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/o-compartilhamento-de-dados-pessoais-no-decreto-n-8-78916-um-frankenstein-de-dados-brasileiro-08072016. Acesso em: 24 ago. 2021.

AMARAL, Fernando. **Introdução à ciência de dados.** Rio de Janeiro: Alta Books, 2016.

BOTELHO, Marcos César. LGPD e a proteção ao tratamento de dados pessoais de crianças e adolescentes. **Revista Direitos Sociais e Políticas Públicas (UNIFAFIBE),** v.8, n.2, 2020.

BRASIL. Ministério da Defesa. **Lei Geral de Proteção de Dados**: LGPD. 3 de setembro de 2020. Disponível em: https://www.gov.br/defesa/pt-br/acesso-a-informacao/lei-geral-de-protecao-de-dados-pessoais-lgpd. Acesso em: 31 mar. 2021.

BRASIL. **Lei 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: DF, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709compilado.htm. Acesso em: 31 mar. 2021.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília: DF, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 31 mar. 2021.

CHRISTIAN, Agnes. GONÇALVES, Caio Felipe Martins. **Diferenças entre a LGPD e o Regulamento Geral de Proteção de Dados. Direito Novo**. 2019. Disponível em: https://direitonovo.com/justica/direito-digital/diferencas-entre-a-lgpd-e-o-regulamento-geral-de-protecao-de-dados/. Acesso em: 07 jun. 2021.

CIRINO, Luciana Gabriela. **Lei LGPD:** Programa de aplicação de dados pessoais. São Paulo: Itamarati Contábil, 2020.

COTS, Márcio; OLIVEIRA, Ricardo. **Lei geral de proteção de dados pessoais comentada**. 2. ed. São Paulo: Revista dos Tribunais, 2019.

DONEDA, Danilo. **Privacidade e proteção de dados pessoais**. Brasília: Tribunal de Contas da União, 2017.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, Joaçaba, v. 12, n. 2, p.91-108, jul/dez 2012. Disponível em: https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em: 28 out. 2021.

FEIGELSON, Bruno; SIQUEIRA, Antonio Henrique Albani (coords.). **Comentários à lei geral de proteção de dados:** Lei 13.709/2018. São Paulo: Revista dos Tribunais, 2019.

MACKENZIE. Universidade Mackenzie. **Compliance digital**. São Paulo: 2019 (*e-book*).

MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. **Big data:** como extrair volume, variedade, velocidade e valor da avalanche de informação cotidiana. Rio de Janeiro: Elsevier, 2013.

MIRAGEM, Bruno. A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o Direito do Consumidor. **Revista dos Tribunais**, v. 1009. Nov. 2019. Disponível em: https://brunomiragem.com.br/wp-content/uploads/2020/06/002-LGPD-e-o-direito-do-consumidor.pdf. Acesso em: 28 out. 2021.

PARANÁ. Controladoria Geral do Estado do Paraná. **LGPD:** Lei nº 13.709/2018, Lei Geral de Proteção de Dados. Paraná, 2020. Disponível em: https://www.cge.pr.gov.br/sites/default/arquivos_restritos/files/documento/2021-07/cartilha_LGPD.pdf. Acesso em: 31 mar. 2021.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais:** comentários à Lei nº 13.709/2018 (LGPD). 2.ed. São Paulo: Saraiva, 2020.

RAPOSO, Cláudio Filipe Lima; LIMA, Haniel Melo de; OLIVEIRA JÚNIOR, Waldecy Ferreira de; SILVA, Paola Aragão Ferreira; BARROS, Elaine de Souza. LGPD: Lei Geral de Proteção de Dados Pessoais em Tecnologia da Informação: Revisão Sistemática. **Race: Revista de Administração**, v.4, 2019.

SERPRO. **O que muda com a LGPD.** Disponível em: https://www.serpro.gov.br/lgpd/menu/a-lgpd/o-que-muda-com-a-lgpd. Acesso em: 30 mar. 2021.

SILVEIRA, Marco Antônio Karam. Lei de Acesso a Informações Públicas (Lei no 12.527/2011): democracia, república e transparência no Estado constitucional. **Revista Jurídica**: órgão nacional de doutrina, jurisprudência, legislação e crítica judiciária. São Paulo, v. 60, n. 416, p. 29-52, jun. 2012.

SOARES, Paulo Vinicius de Carvalho. **Lei geral de proteção de dados simplificada.** São Paulo: Lee Brock Camargo Advogados, 2020.

Artigo recebido em: 30/08/2021

Artigo aceito em: 11/11/2021

Artigo publicado em: 04/05/2022