REVISTA eixo
revistaeixo.ifb.edu.br

ISSN 2238-5630
Brasília-DF, v. 12, n. 2, maio-agosto de 2023

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD): O SETOR PÚBLICO E VAZAMENTOS DE DADOS PESSOAIS

GENERAL PERSONAL DATA PROTECTION LAW (LGPD): THE PUBLIC SECTOR AND PERSONAL DATA LEAKS

Delwin Edgar Huth Lemes[1]

RESUMO: Tendo em vista que, segundo recentes levantamentos realizados, a administração pública federal é o principal alvo de vazamentos de dados, pesquisa-se sobre a aplicabilidade da Lei Geral de Proteção de Dados Pessoais (LGPD) diante de vazamentos de dados pessoais sensíveis em posse de entidades públicas federais, com o objetivo de entender qual a aplicabilidade da lei em casos de incidentes dessa natureza em entidades federais. Para tanto, é necessário descrever a LGPD, identificar vazamentos de dados pessoais sensíveis e analisar a aplicabilidade desta lei. Realiza-se, então, uma pesquisa básica estratégica com objetivos descritivo e exploratório, utilizando uma abordagem qualitativa, por meio de método hipotético-dedutivo e com procedimentos de pesquisa bibliográfica e documental. Diante disso, verificou-se que há necessidade de sanções administrativas mais inflexíveis, bem como uma maior transparência em relação à sociedade, o que impõe a constatação de que a elaboração periódica de um Relatório de Impacto à Proteção de Dados seria imprescindível no controle da aplicação da lei no setor público.
Palavras-chave: Lei Geral de Proteção de Dados Pessoais; vazamentos de dados; setor público; aplicabilidade.

ABSTRACT: *Considering that, according to recent surveys carried out, the federal public administration is the main target of data leaks, research is carried out on the applicability of the General Law for the Protection of Personal Data (LGPD) in the face of leaks of sensitive personal data held by federal public entities, in order to understand the applicability of the law in case of incidents of this nature in federal entities. Therefore, it is necessary to describe the LGPD, identify leaks of sensitive personal data and analyze the applicability of this law. Then, a strategic basic research is carried out, with descriptive and exploratory objectives, qualitative approach, through a hypothetical-deductive method and through bibliographic and documentary research procedures. Therefore, it was found that there is a need for more inflexible administrative sanctions, as well as greater transparency towards society, which requires the observation that the periodic preparation of a Data Protection Impact Report would be essential to control the application. of law in the public sector.*
Keywords: General Personal Data Protection Law; Data Leaks; Public Sector; Applicability.

[1] Graduação em Gestão Pública
Lattes:http://lattes.cnpq.br/6671328493851386
ORCID:https://orcid.org/0000-0002-3622-4917
Email: delwinlemes@gmail.com

Recebido em: 21/07/2022
Aceito em: 15/05/2023

INTRODUÇÃO

Em agosto de 2018 foi sancionada a Lei n. º 13.709, chamada Lei Geral de Proteção de Dados Pessoais - LGPD. Essa norma visa o estabelecimento de novas e claras regras para o tratamento de dados pessoais em entidades públicas e privadas.

A proteção de dados está diretamente ligada à gestão na administração pública federal, de modo que o tratamento de dados pessoais seja mais eficiente, garantindo o direito à privacidade, além de práticas mais transparentes e seguras. No âmbito da administração pública, a má gestão desses dados interfere diretamente nos direitos fundamentais do cidadão, sendo a Lei Geral de Proteção de Dados Pessoais um importante instrumento na regulamentação e controle das atividades que os envolvam.

Segundo a Kaspersky, empresa líder global em segurança cibernética[1], o Brasil lidera a lista dos cinco países com maior índice de risco ao usuário, revelando que 1 (um) a cada 5 (cinco) brasileiros sofreram ataques *"phishing"* [2] no ano de 2020. Ademais, conforme noticiado pelo portal The Hack, em levantamento realizado pela Trend Micro, empresa de renome também na área de segurança cibernética, o setor público é o principal alvo de cibercriminosos no Brasil.

Desta forma, a partir de sua aprovação, foi visto que o não cumprimento das normas estabelecidas na lei implica em punição ao agente por meio de sanções administrativas. Portanto, a aplicabilidade da Lei Geral de Proteção de Dados Pessoais (BRASIL, 2018) diante de vazamentos de dados pessoais sensíveis em posse de entidades públicas federais é algo que necessita ser estudado.

Com a entrada em vigor da Lei n. º 13.709/18, em 1° de agosto de 2021, o não cumprimento das normas acarreta sanções administrativas. Portanto faz-se necessário questionar: qual a aplicabilidade da Lei Geral de Proteção de Dados Pessoais diante de vazamentos de dados sensíveis em posse de entidades públicas federais?

Nesta pesquisa, pretende-se primordialmente entender a aplicabilidade da LGPD ao identificar vazamentos de dados pessoais sensíveis em entidades públicas federais, a fim de assegurar que as sanções administrativas ocorram de modo a respeitar os direitos fundamentais do cidadão.

Sendo assim, descrever a LGPD é de suma importância para que se possa visualizar suas características e impactos na sociedade. Uma vez que, conforme diversas vezes noticiado nos últimos anos, vazamentos de dados pessoais sensíveis em posse de entidades públicas federais têm tomado grandes proporções, é necessário identificá-los. Por fim, o objetivo é avaliar a aplicabilidade dessa lei em entidades públicas federais.

Com o surto pandêmico em 2020, diversos procedimentos foram virtualizados e os debates sobre a Lei n. º 13.709/18 (BRASIL, 2018) intensificaram-se. Portanto, para chegar ao ponto focal desta pesquisa é necessário iniciar o trabalho com a conceituação da LGPD (BRASIL, 2018), bem como suas características, efeitos e abrangência. Intenciona-se também mostrar sua origem e inspirações, de modo que o leitor conquiste intimidade com o assunto.

Em um segundo momento, entende-se ser de grande importância identificar possíveis vazamentos de dados pessoais sensíveis que estejam sob a tutela da administração pública federal, expondo suas eventuais causas e consequências. Não se tem a ambição de analisá-los de maneira técnica e profunda, mas sim apresentá-lo de maneira concisa e clara. Além disso, serão relatados recentes vazamentos ocorridos na esfera pública recentemente.

Na parte final da pesquisa, é efetuada uma análise da aplicabilidade da Lei Geral de Proteção de Dados Pessoais em órgãos públicos, visando examinar sanções administrativas aplicáveis ao poder público e a eficácia dessas sanções na garantia dos direitos fundamentais do titular dos dados.

Em virtude dos fatos mencionados, parte-se da ideia de exigir a elaboração de um Relatório de Impacto à Proteção de Dados (RIPD) periodicamente, a fim de que seja mitigado ao máximo possíveis vazamentos de dados pessoais sensíveis no âmbito público federal. Com isso, realizou-se uma pesquisa básica estratégica com objetivos descritivos e exploratórios, abordagem qualitativa, por meio de método hipotético-dedutivo e utilizando-se procedimentos de pesquisa bibliográfica e documental.

Ao final, conclui-se que os objetivos foram atingidos, visto que a descrição da Lei Geral de Proteção de Dados Pessoais, a apresentação de vazamentos de dados originários no poder público, e a análise da aplicação da lei e suas sanções administrativas revelam que é relevante a concepção de um Relatório de Impacto à Proteção de Dados (RIPD) de forma periódica e obrigatória em entidades públicas federais que lidam com dados pessoais sensíveis, visando aprimorar a aplicabilidade da LGPD (BRASIL, 2018).

Assim sendo, a disposição do trabalho aprecia a materialização de um alicerce metodológico, onde a evolução do trabalho está balizada em partes bem definidas, sendo a primeira destinada ao referencial teórico, a segunda direcionada a progressão da coleta de

[1] "Ações voltadas para a segurança de operações, de forma a garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis. " Disponível em: <https://www.gov.br/anatel/pt-br/assuntos/seguranca-cibernetica>. Acesso em: 24 jul. 2021.

[2] "É um termo originado do inglês (fishing) que em computação se trata de um tipo de roubo de identidade online. Essa ação fraudulenta é caracterizada por tentativas de adquirir ilicitamente dados pessoais de outra pessoa, sejam senhas, dados financeiros, dados bancários, números de cartões de crédito ou simplesmente dados pessoais. " Disponível em: <https://canaltech.com.br/seguranca/O-que-e-Phishing/>. Acesso em: 25 jul. 2021.

ISSN 2238-5630
Brasília-DF, v. 12, n. 2, maio-agosto de 2023

dados e, abrangendo a argumentação e visualização das soluções, conforme adiante.

REFERENCIAL TEÓRICO

A Lei Geral de Proteção de Dados Pessoais

O Brasil não contava com uma legislação específica no que tange à proteção de dados, apenas com a Lei de Acesso à Informação (LAI) e o Marco Civil da Internet. No entanto, com a entrada em vigor do Regimento Geral de Proteção de Dados (RGPD) da União Europeia em 2018, novas regras foram implementadas visando regulamentar, entre outros aspectos, o compartilhamento de dados intra/internacionais. Com isso, o Brasil passou a não ser reconhecido como um país onde poderia haver transferências internacionais de dados com a União Europeia (UE).

Em um contexto de grandes inovações tecnológicas, incidentes a níveis mundiais, pressões externas e diante de possíveis danos que o mal tratamento de dados poderia ocasionar tanto para o setor público quanto para o privado, sancionou-se, então, após longos debates, a Lei Geral de Proteção de Dados Pessoais - LGPD (BRASIL, 2018). Esse cenário é evidenciado por Mendes e Doneda (2020, p. 471), quando afirmam que "a Lei brasileira é também a expressão da convergência internacional em torno de princípios básicos de proteção de dados no mundo, [...]".

A Lei Geral de Proteção de Dados - LGPD (BRASIL, 2018), sancionada em 2018, se inspira na lei Europeia (RGPD) e busca resguardar os dados pessoais de pessoas físicas e jurídicas, garantindo ao titular total controle e conhecimento de como seus dados estão sendo tratados e estabelecendo regras para toda a vida útil dos dados.

Desta forma, a partir da sanção desta lei, foi percebida a importância da mesma para o ordenamento jurídico brasileiro. De acordo com Mendes e Doneda (2020, p. 480), "a sanção da LGPD foi, certamente, um enorme avanço no marco normativo brasileiro".

Além disso, a Lei n. º 13.709/18 - LGPD (BRASIL, 2018) visa regulamentar, em sua totalidade, o tratamento de dados pessoais de brasileiros dentro e fora do Brasil e proteger os direitos fundamentais de liberdade e privacidade, conforme consta em seu artigo 1°. Vale ressaltar que essa se aplica a entes públicos e privados, abrangendo suas operações e o manuseio de dados pessoais.

Um importante pilar para a participação ativa do titular dos dados é o consentimento. Hoffmann-Riem (2020) destaca que a arbitrariedade desse requisito é fundamental para que o cidadão tenha o poder de decisão sobre como e para qual finalidade essas informações serão utilizadas, garantindo assim o seu direito de autodeterminação informativa. Assim, Mendes e Doneda (2020, p. 474) acrescentam:

> O estabelecimento de uma série de princípios de proteção de dados e de direitos do titular dos dados pela Lei procura garantir, por um lado, um arcabouço de instrumentos que proporcionem ao cidadão meios para o efetivo controle do uso de seus dados por terceiros.

Assim sendo, é evidente que a instituição de uma diretriz geral, no que compete ao tratamento de dados, promoveu uma maior proteção tanto para os indivíduos titulares dos dados quanto para entidades públicas e privadas. Por esse motivo, a norma busca expor pontos de vista mais atuais visando uma melhor aplicabilidade de seus princípios.

O tratamento de dados pessoais e sensíveis

Inicialmente, é necessário conceituar dados pessoais, que basicamente se referem à informação relacionada a pessoa natural identificada ou identificável, conforme consta no artigo 5°, da Lei n. º 13.709/18. A lei também trata de dados pessoais sensíveis que, ligados à pessoa natural, possuem caráter religioso, médico, político, racial, genético ou biométrico e vida sexual.

Por conseguinte, os dados pessoais sensíveis são atrelados a um alto potencial discriminatório, em razão da íntima relação deste com o seu titular. Logo, Mendes (2008) discorre sobre esse assunto ao afirmar que, esta determinação de dados ocorreu em razão da ideia de que o tratamento dos mesmos oferece ameaça à "personalidade individual".

Nesse sentido, também relata Bioni e Dias (2020), concluindo que, nos dias atuais, as pessoas são fortemente julgadas pelos seus dados, pois, a partir destes, é feita uma análise preconceituosa sem antes dar oportunidades às atividades reais do ser. Isso pode ocorrer ao fornecer dados a plataformas, órgãos públicos ou simples atividades de simulações de créditos, obtenção de seguros, entre outros.

Diante do exposto, a lei que normatiza a utilização e manutenção dos dados expressa firmemente a necessidade de sigilo dos mesmos, determinando que não será aceitável um cenário que ofereça condições aquém das estipuladas, desde a coleta de dados, passando pelo armazenamento até o descarte. Portanto, afirma Vieira (2007, p. 213):

> Por isso, qualquer espécie de tratamento que se ofereça a esses mesmos dados pelos órgãos públicos, tais como a coleta, armazenamento, alteração, recuperação, consulta, utilização e transmissão, requerer a adoção de procedimentos de segurança para

> evitar a interceptação e posterior utilização por terceiros não autorizados.

Ainda nesse contexto, Vieira (2007) relembra a necessidade de medidas restritivas a serem criadas para normatizar o compartilhamento de dados sensíveis entre entidades públicas. Essa regra é de extrema importância pois, muitas vezes, pelo simples fato de o dado já estar sob tutela do poder público, tem-se a falsa impressão de que podem ser livremente compartilhados. Contudo, esse fornecimento oferece grandes riscos à honra e à personalidade íntima do titular.

Tratamento de dados pessoais pelo poder público

Corroborando com a temática, vale elucidar conceitos pertinentes ao setor público, como *disclosure e accountability.* De modo a explicitar tais concepções, se contempla o exposto por Zorzal e Rodrigues (2015, p. 118):

> Quanto ao termo *disclosure*, não se tem uma tradução satisfatória para o português. Muitos o traduzem como divulgação, evidenciação, veiculação de informação. Gibbins, Richardson e Waterhouse (1990) definem *disclosure* como qualquer divulgação intencional de informação financeira, tanto quantitativa quanto qualitativa, obrigatória ou voluntária, difundida por canais formais ou informais.

Ainda, tratando de *accountability*, esta pode ser traduzida como um importante pilar do setor público, onde busca-se uma prestação de contas, de maneira que os entes envolvidos e interessados nas ações do poder público possam estar cientes e sejam capazes de compreender com clareza as informações prestadas, e não somente expor informações conflituosas e de difícil interpretação pela sociedade em geral. Segundo Zorzal e Rodrigues (2015), é necessário que o setor público, de maneira ampla, esteja focado em dar ao ente pagador de impostos as condições de visualizar as maneiras pelas quais os recursos estão sendo implementados e destinados.

Nesse sentido, o termo disclosure pode ainda ser disposto conforme o nível de divulgação, sendo: A divulgação denominada Adequada, aquela que reúne os meios básicos de exposição de informações de maneira clara; a divulgação Justa, a que se destina ao objetivo de dar o tratamento adequado, correto e democrático aos stakeholders; e por fim, a divulgação Completa onde é demonstrado em sua totalidade as evidências consideradas significativas, conforme elucidado por Hendriksen e Van Breda (1999, *apud* FABRE, BORNIA, BORGERT, 2021).

Salienta-se, portanto, a relevância da discussão sobre o tratamento e manuseio de dados pessoais em posse da administração pública, visto que não lhes faltam princípios norteadores para efetivamente executar o seu papel de maneira transparente para com a sociedade. Vale frisar que este trabalho não busca um maior aprofundamento nestes princípios, visa-se meramente apreciá-los a fim de enriquecer a discussão sobre o tratamento de dados por entes públicos.

Como discutido nos tópicos acima, o setor público possui um significativo papel no tratamento de dados pessoais. É de conhecimento geral que a Administração Pública é detentora de uma grande quantidade de dados pessoais, em sua maioria sensíveis, e, por isso, reafirma a necessidade de uma melhor forma de regulação desses dados, tanto pelo servidor quanto pelos sistemas utilizados.

Além disso, um dado ainda pode ser diretamente comprometido caso sofra alteração, pois isso pode gerar conflito entre a origem e os demais sistemas do poder público. Portanto, de acordo com Vieira (2007, p. 210), isso poderá acarretar em prejuízo ao indivíduo.

Logo, como afirma Hoffmann-Riem (2020, p. 435), a participação na proteção de dados deve ser de todos os envolvidos, contudo, é uma importante tarefa e deve ser tratada com seriedade pelos Estados. O autor aprofunda ainda mais, ao alegar que "o Estado é responsável por garantir a possibilidade de proteção da liberdade" (HOFFMANN-REIM, 2020, p. 450).

Ao falar de controle e regulação, a lei estabelece regras de estipulação destes, de modo a garantir a plena eficácia da aplicação da lei em toda a esfera pública e privada. A definição ficará a critério da Autoridade Nacional.

No que se refere a esta autoridade, foi criada, em 2018, a Autoridade Nacional de Proteção de Dados (ANPD), com o objetivo de aplicar e fiscalizar a LGPD (BRASIL, 2018). Desse modo, Mendes (2008, p. 14) previu essa necessidade ao afirmar que é de extrema importância a estipulação de um órgão administrativo capaz de tutelar a sociedade desde a aplicação dessas normas até ao auxílio do indivíduo que sofreu com o mau uso de seus dados.

A ANPD, institui a figura do controlador, operador e encarregado, onde o primeiro será responsável por tomar as decisões principais referentes ao tratamento de dados e definir sua respectiva finalidade. O segundo, por sua vez, desempenha o tratamento de dados em prol do controlador, conforme finalidade já estabelecida por este. Por fim, o encarregado é indicado pelo controlador, e deverá garantir a conformidade do tratamento de dados pessoais da entidade pública ou privada com a LGPD (BRASIL, 2018).

Uma das possibilidades da ANPD, é solicitar ao controlador um Relatório de Impacto à proteção de dados, de modo a fiscalizar

ISSN 2238-5630
Brasília-DF, v. 12, n. 2, maio-agosto de 2023

se a mesma está sendo devidamente aplicada, conforme destacam Mendes e Doneda (2020, p. 478):

> [...] sua competência vai desde a solicitação e análise de relatórios de impacto de privacidade, determinação de medidas para reverter efeitos de vazamentos de dados, disposição sobre padrões técnicos de segurança da informação até a autorização da transferência internacional de dados pessoais. Isso demonstra que o órgão não é um mero coadjuvante do sistema de proteção de dados: ao contrário, é o seu pilar de sustentação, [...].

Para tratar um pouco mais a respeito deste relatório, é interessante conceituá-lo. A lei apresenta o relatório como uma documentação detalhada, onde será relatada a descrição dos procedimentos de tratamento de dados que podem gerar riscos aos direitos fundamentais e também serão elencados os mecanismos utilizados para a contenção de riscos.

A ANPD poderá também aplicar sanções administrativas quando os agentes públicos ou privados de tratamento de dados cometerem infrações ou não cumprirem as normas previstas na LGPD (BRASIL, 2018). As sanções vão desde advertências com adoção de medidas corretivas, multas que podem chegar a 50 milhões por infração, até a proibição parcial ou total do exercício de suas atribuições ligadas ao tratamento de dados, conforme descrito no artigo 52 da lei.

Vazamento de dados

Em razão do que foi estudado anteriormente, percebe-se a necessidade de relatar também a respeito de vazamento de dados, que consiste no acesso, coleta e publicização de dados anteriormente privados e sigilosos, os quais podem pertencer a pessoas físicas ou jurídicas. Essa ação revela uma atitude criminosa feita no âmbito virtual, com o objetivo de obter vantagem indevida por meio das informações obtidas com esses dados.

Os vazamentos podem ser ocasionados, principalmente, pela exposição de senhas, furto de informações contidas em *sites* organizacionais, funcionários que repassam as informações a terceiros ou negligência no trato dos dados.

Desta forma, a LGPD (BRASIL, 2018) entra em vigor de modo a normatizar essa manutenção da proteção de dados, firmando regras e penalidades para o cumprimento ou não destas. Essa função é evidenciada por Doneda (2011, p. 98), ao reconhecer que "essas leis procuraram fortalecer a posição da pessoa em relação às entidades que coletam e processam seus dados".

Atualmente, observa-se que o vazamento de dados é um assunto cada vez mais discutido em meio a esfera pública, denotando assim sua importância. Desta forma, destaca Hoffmann-Riem (2020), ao comparar os dados com o petróleo, declarando seu alto valor econômico e a possibilidade de utilização diversificada de um dado ou conjunto deles, que podem beneficiar ou prejudicar a sociedade.

METODOLOGIA

Caracterização de pesquisa

O corrente trabalho é uma pesquisa com finalidade básica estratégica, objetivos descritivo e exploratório, elaborada pelo método hipotético-dedutivo, com abordagem qualitativa e executada através de levantamento bibliográfico e documental.

De acordo com a doutrina de Gil (2017, p. 18), "pesquisas voltadas à aquisição de novos conhecimentos direcionados a amplas áreas com vistas à solução de reconhecidos problemas práticos" classificam-se como básicas estratégicas.

Assim, o trabalho exposto visa apresentar uma cooperação para com a ciência, possibilitando mais entendimento por intermédio do teste da hipótese, que porventura possa configurar parcialmente a solução do problema, caracterizando-se como uma pesquisa básica estratégica.

No que diz respeito ao objetivo, repara-se que foi efetuado um levantamento bibliográfico, com o propósito de descrever o pensamento mais atual já catalogado pela ciência sobre a Lei Geral de Proteção de Dados - LGPD (BRASIL, 2018), que é o assunto central desta pesquisa.

Diante disso, é legítimo alegar que a parte inicial do texto se delimita na definição exposta por Duarte e Furtado (2014, l. 712), no momento que se afirma: "a pesquisa descritiva restringe-se a constatar o que já existe. Os acontecimentos (fenômenos) são narrados. Procura-se conhecer a natureza, as características, a composição e os processos que constituem o fenômeno".

Destarte, trata-se de uma pesquisa de abordagem qualitativa, o que é certificado pela perspectiva de Duarte e Furtado (2014) ao sustentar que "[...] entendemos essa denominação qualitativa e ou quantitativa não como uma tipologia de pesquisa, mas apenas uma explicitação da ênfase dada na pesquisa [...]".

Instrumento de coleta de dados

Preliminarmente, examinou-se a base teórica sobre a Lei Geral de Proteção de Dados - LGPD (BRASIL, 2018) e sua aplicação em entidades da administração pública federal, com a execução de fichamentos de obras doutrinárias e trabalhos acadêmicos atuais. Em um período delimitado entre 2018 e 2021, pesquisou-se em

repositórios públicos e *sites* governamentais acerca dos vazamentos de dados que serão citados neste estudo.

Além disso, foi efetuado um levantamento documental, no que tange às regras previstas na legislação vigente e à sua apreciação institucional, no viés do âmbito da jurisprudência dos Tribunais superiores.

O prosseguimento da pesquisa exigiu um pouco mais de cuidado, uma vez que ainda não foram elaboradas um grande número informações no ramo da ciência a respeito de vazamentos de dados pessoais sensíveis e a aplicabilidade da Lei Geral de Proteção de Dados - LGPD (BRASIL, 2018) quando esses estão em posse de entidades públicas federais brasileiras.

Por essa razão, o trabalho apresenta também cunho exploratório. Segundo Gil (2017, p. 18), "As pesquisas exploratórias têm como propósito proporcionar maior familiaridade com o problema, com vistas a torná-lo mais explícito ou a construir hipóteses".

Coleta e Análise dos dados

A seguir, desponta-se um texto dissertativo em que as informações são correlacionadas, a fim de que seja propiciado o teste da hipótese e, por consequência, levantada uma resposta para a questão.

Efetivamente, o estudo foi elaborado para produzir além do conhecimento simplesmente teórico, entretanto não esteve presente o desejo de expor uma aplicação que resolvesse decisivamente a situação problema.

Outrossim, a parte conseguinte da pesquisa aponta justamente esse objetivo, em outros termos, explanar o problema de melhor forma, denotando as características que acatem uma observação perante a teoria já disposta na primeira parte.

Ademais, a elaboração da pesquisa partiu da presunção de que, exigir a elaboração de um Relatório de Impacto à Proteção de Dados (RIPD) periodicamente, para assim mitigar ao máximo possíveis vazamentos de dados pessoais sensíveis na administração pública federal.

Marconi e Lakatos (2003, p. 96) ressaltam que "se a hipótese não supera os testes, estará falseada, refutada, e exige nova reformulação do problema e da hipótese, que, se superar os testes rigorosos, estará corroborada, confirmada provisoriamente.", no momento em que relatam o método hipotético-dedutivo.

Por conseguinte, verifica-se que o critério utilizado foi o hipotético-dedutivo, visando que o estudo decorreu de maneira concisa na coleta de dados que admitissem analisar o suposto ao final do trabalho. Destaca-se, contudo, que os dados foram coletados sem a utilização de ferramentas de precisão matemática ou estatística e foram sondados de forma avaliativa, decorrente do empenho racional de observação.

RESULTADOS E DISCUSSÃO

Em junho de 2019, o Ministério Público do Distrito Federal e Territórios (MPDFT) representou contra o Serviço Federal de Processamento de Dados (SERPRO) no Tribunal de Contas da União (TCU). A representação feita visa interromper o tratamento ilegal de dados pessoais de milhões de brasileiros, que estavam sendo comercializados por meio da plataforma DATAVALID.

A plataforma basicamente oferecia a validação de dados pessoais de cidadãos brasileiros, por meio do tratamento irregular de dados provenientes do Departamento Nacional de Trânsito (DENATRAN). Esses dados, contidos nas carteiras de habilitação (CNH), são pessoais e pessoais sensíveis.

O serviço oferecido pelo SERPRO limita-se em validar a identidade das pessoas através de sua biometria, ou seja, por meio de impressões digitais e reconhecimento facial. O DATAVALID era comercializado com entidades públicas e privadas.

Diante disso, a representação feita pelo Ministério Público do Distrito Federal e Territórios baseou-se, também, na recém sancionada Lei Geral de Proteção de Dados, que, mesmo ainda não vigorando, merecia ser devidamente observada.

Ainda mais, em 2020, o Superior Tribunal de Justiça (STJ) julgou mais de 500 (quinhentos) mil processos e, ao longo do ano, o número de processos tramitando no STJ se manteve na casa dos 200 mil, conforme exposto em seu relatório de gestão anual.

No dia 03 de novembro de 2020, a instituição sofreu o que o presidente do (STJ), Ministro Humberto Martins, descreveu como “o pior ataque cibernético já empreendido contra uma instituição pública brasileira, em termos de dimensão e complexidade”.

O ataque hacker ocorreu por meio de um vírus que infectou a rede de informática do tribunal resultando na retirada dos sistemas do STJ do ar como medida de precaução. Os dados da entidade foram criptografados, bloqueando o acesso a eles, comportamento típico de *ransomwares*, software malicioso (vírus) que “sequestra” os dados e costuma pedir pagamento para que sejam liberados.

O STJ comunicou que os sistemas de backup do órgão foram preservados e, em ação conjunta da Secretaria de Tecnologia da Informação e Comunicação (STI), do Comando de Defesa Cibernética do Exército brasileiro, da Polícia Federal, do SERPRO, bem como diversos servidores do quadro permanente do STJ, empresas privadas e fabricantes de tecnologia, trabalharam para reverter os dados, reverter os dados. Assim, no dia 18 de novembro, os sistemas de informática da Corte foram plenamente restabelecidos.

Outro importante episódio de vazamento de dados foi o ocorrido no Ministério da Saúde em dezembro de 2020. Segundo o que foi noticiado pelo veículo de comunicação Canaltech, aproximadamente 240 milhões de dados pessoais de brasileiros, incluindo

ISSN 2238-5630
Brasília-DF, v. 12, n. 2, maio-agosto de 2023

informações de pessoas falecidas, ficaram expostos por cerca de seis meses. A brecha teve origem no e-SUS Notifica, sistema de notificações da Covid-19.

A falha expôs dados pessoais, como CPF, nome completo, endereços e números de telefones. Entre as pessoas afetadas, encontravam-se o Presidente da República, o Presidente do Senado e da Câmara dos Deputados, Davi Alcolumbre e Rodrigo Maia, além de outros líderes do estado.

Essa falha consistia na exposição de credencias de acesso ao sistema, *login* e senha eram exibidos no código fonte do referido *site* de notificações. Com recursos disponíveis no próprio navegador e simples ferramentas gratuitas de criptografia simples disponíveis na internet, qualquer usuário poderia ter acesso às informações.

No final de novembro de 2020, houve outro vazamento de dados do Ministério da Saúde, em que cerca de 16 milhões de brasileiros com suspeita ou confirmação de Covid-19 tiveram seus dados expostos. A exposição dos dados ocorreu devido à publicação de senhas que davam acesso ao sistema do E-SUS-VE, sistema federal utilizado para notificar casos suspeitos ou confirmados com o quadro moderado da referida doença, e do SIVEP-GRIPE, também federal, onde se encontram os registros de todas as internações por Síndrome Respiratória Aguda Grave (SRAG).

As senhas foram publicadas por um funcionário do Hospital Albert Einstein no *site* GitHub. O funcionário teria acesso aos dados por estar trabalhando em um projeto que continha a pasta com as senhas. Segundo ele, teria sido de forma acidental. Informações de doenças pré-existentes, como diabetes, HIV, câncer, entre outras, são exemplos de dados pessoais sensíveis disponíveis através dessas senhas.

O fato foi informado pelo hospital ao Ministério da Saúde, o funcionário foi demitido, e as informações foram imediatamente removidas. O Ministério ressaltou que os dados não estavam facilmente acessíveis, uma vez que apenas o *login* e senha não eram suficientes para obter acesso ao banco de dados.

Diante dos incidentes de vazamentos de dados, o Conselho Nacional de Saúde (CNS), por meio de nota pública, pediu esclarecimentos ao Ministério da Saúde, de maneira urgente, "sobre os reais acontecimentos que motivaram a inegável falha de procedimentos de segurança de dados e informações em saúde da população brasileira ". A resposta ao CNS foi feita por meio de órgãos de controle interno.

Diante do que foi exposto, e dos incidentes elencados, não se objetivou exaurir os acontecimentos referentes aos vazamentos de dados, e sim descrevê-los acerca da discussão. Portanto, volta-se ao início da pesquisa, onde realizou-se um levantamento bibliográfico e documental, com uma abordagem qualitativa. Foi constatado que o Brasil ganhou meios legais e administrativos para se fazer uso dos dados pessoais dos brasileiros a partir da sanção da LGPD (BRASIL, 2018). Com isso, notou-se o inegável marco que esta lei representa para o país.

Ainda nesse sentido, foi observado que a Lei Geral de Proteção de Dados Pessoais (BRASIL, 2018) foi certeiramente elaborada, uma vez que, após a análise de alguns pontos, como fundamentos, órgãos reguladores, entre outros, foi possível observar que a aplicabilidade da lei garantirá o pleno funcionamento da máquina pública. Foi percebido também que, comparado aos padrões mundiais de proteção de dados, a LGPD (BRASIL, 2018) cumpre os requisitos necessários e, inclusive, foi muito influenciada pelas normas atribuídas à União Europeia.

É importante destacar a tamanha responsabilidade da Autoridade Nacional de Proteção de Dados (ANPD) como órgão regulador diante da LGPD (BRASIL, 2018), pois a lei estabelece claramente papéis e funções desta, garantindo assim a aplicabilidade da norma em entes públicos e privados. Observa-se a importância desta para o bom funcionamento da lei, tanto no cumprimento do seu dever de fiscalizar o tratamento de dados pessoais quanto na aplicação de sanções administrativas no caso da não observância à lei.

Com relação à análise das sanções administrativas, é importante salientar qual seria a aplicação da LGPD (BRASIL, 2018) quando houver infração e ou vazamentos de dados pessoais por órgãos públicos. Em seus artigos 31 e 32, é exposto que diante da infração cometida por entes públicos, cabe à ANPD estipular as medidas cabíveis para identificar e encerrar o incidente. Percebe-se a permissiva aplicabilidade da lei perante transgressões ocorridas na administração pública.

Entretanto, o Brasil encontra-se em busca de aprimoramento no que se refere à proteção de dados pessoais no setor público, pois, por falta de treinamento e/ou falta de equivalência e aplicabilidade entre os parâmetros legais já estabelecidos, ainda ocorrem diversos vazamentos de dados que comprometem direitos fundamentais do cidadão, como o direito à privacidade. Esses vazamentos são extremamente danosos, já que o indivíduo, por muitas vezes, fornece dados ao governo acreditando que estes estarão seguros, contudo, são vazados comprometendo sua particularidade.

Vazamentos de dados dificilmente serão extintos em uma sociedade cada vez mais tecnológica e dependente do tratamento de diversos tipos de informações. Para ocorrerem, não dependem somente da ingerência e falta de segurança da entidade vítima, porém é necessário tratá-los de maneira extremamente responsável, implementando meios para se proteger de possíveis ataques *hackers* e adotando medidas visando mitigar ao máximo os danos em eventuais vazamentos.

Desta forma, são necessárias políticas mais duras para o tratamento de dados, além de práticas mais transparentes e seguras. Assim, o cidadão terá plena consciência do fornecimento de seus

dados e também para que serão utilizados. Políticas estas que a LGPD (BRASIL, 2018) já traz em seu texto, porém é nítida a falta de implementação fiel desta em algumas entidades públicas, principalmente no que se refere à transparência e às medidas de respostas a incidentes.

No entanto, para estabelecer esse novo estilo de tratamento de dados, é necessário também o envolvimento de todas as partes, pois o cidadão precisa conhecer a norma, atentar-se aos dados que está fornecendo e aplicar práticas de segurança em sua vida. Em contrapartida, o Estado precisa garantir que suas instituições estejam capacitando funcionários, atualizando plataformas e adotando outras medidas para que assim seja criada uma cultura de proteção de dados.

Ademais, visando uma melhor aplicabilidade da Lei n. º 13.709/18, testou-se a hipótese de que a exigência de um Relatório de Impacto à Proteção de Dados (RIPD) periodicamente, e não apenas em casos em que a ANPD solicitaria ocasionalmente, ajudaria a conter o máximo possível de vazamentos de dados pessoais. Ainda, acredita-se que essa exigência é de grande valia para o processo de implementação de uma cultura de proteção de dados no setor público. Segundo Gomes (2019, p. 12):

> A ideia do relatório de impacto é refletir uma avaliação de impacto, hipótese foi confirmada, uma vez que, sua implementação acarretaria em mais transparência e controle sobre as atividades das entidades públicas que envolvam o tratamento de dados pessoais sensíveis.

O Relatório de Impacto à Proteção de Dados tem a função de revelar, averiguar, esquematizar e controlar o andamento dos procedimentos que buscam a plena implementação, por exemplo, de normativos e legislações, neste caso a LGPD (BRASIL, 2018) que visam o aprimoramento no tratamento de dados, olhando para os processos a serem realizados a fim de certificar o êxito no manuseio dos dados durante todo o seu ciclo de vida dentro da organização.

O empenho em conter incidentes faz com que o RIPD seja uma importante engrenagem que quando utilizado de forma correta e regularmente, pode-se obter os resultados almejados, como a preservação da privacidade do cidadão detentor dos dados.

A hipótese desta pesquisa é corroborada também conforme o elucidado por Souza (2021, p. 16), quando alega que "O treinamento constante das equipes responsáveis pela elaboração do RIPD é fundamental para que se incorpore corretamente as descobertas nos projetos em andamento, […] trazendo benefícios a proteção de privacidade".

A pesquisa partiu da seguinte pergunta: Qual a aplicabilidade da LGPD (BRASIL, 2018) diante de vazamentos de dados pessoais sensíveis em posse de entidades públicas federais? Então, após a coleta de dados e a análise das questões, concluiu-se que, atualmente, a aplicabilidade se caracteriza nos artigos 31 e 32 da lei, e esta é deficitária, visto que as sanções administrativas impostas sobre o setor público em casos de vazamentos encontram-se de maneira aquém do esperado.

Em suma, o estudo seguiu uma linha metodológica com abordagem qualitativa e finalidade básica estratégica, tendo objetivos descritivos e exploratórios. Além disso, utilizou-se o método hipotético-dedutivo, por meio de procedimentos de pesquisa bibliográfica e documental. Assim sendo, encontraram-se limitações, como a falta de transparência no reporte de incidentes ocorridos, além da dificuldade de se obter estudos práticos e quantitativos na área, visto que a LGPD (BRASIL, 2018) só começou a vigorar no Brasil apenas em agosto de 2021.

Diante disso, sugere-se que seja estudado o investimento necessário para se ter um nível adequado de recursos disponíveis para a administração pública federal realizar o tratamento de dados pessoais de maneira correspondente com as expectativas estabelecidas pela LGPD (BRASIL, 2018) no Brasil e internacionalmente. Além disso, quais seriam os meios para que se tenha uma comunicação verdadeiramente transparente em casos de vazamentos desses dados. Incentiva-se também a buscar averiguar o risco que a falta de atuação adequada da ANPD traria para o Estado e como isso afetaria a sociedade.

REFERÊNCIAS

BIONI, Bruno; DIAS, Daniel. **Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor**. civilistica. com, 2020, 9.3: 1-23. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/662/506>. Acesso em: 30 jul. 2021.

BRASIL. **Lei n° 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais. Brasília, DF: Presidência da República 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 20 jul. 2021.

Conselho da Justiça Federal. **Comunicado**. Disponível em: <https://www.cjf.jus.br/cjf/noticias/2020/11-novembro/comunicado>. Acesso em 05 ago. 2021.

Conselho Nacional de Saúde. **NOTA PÚBLICA: CNS pede explicações ao Ministério da Saúde sobre vazamento de dados de pacientes do SUS.** Disponível em: <http://www.conselho.saude.gov.br/ultimas-noticias-cns/1533-nota-publica-cns-pede-explica-

ISSN 2238-5630
Brasília-DF, v. 12, n. 2, maio-agosto de 2023

coes-ao-ministerio-da-saude-sobre-vazamento-de-dados-de-pacientes-do-sus>. Acesso em: 06 ago. 2021.

DEMARTINI, Felipe. **Nova falha no Ministério da Saúde expõe dados de 240 milhões de brasileiros.** Disponível em: <https://canaltech.com.br/seguranca/nova-falha-no-ministerio-da-saude-expoe-dados-de-240-milhoes-de-brasileiros-175578/>. Acesso em: 06 ago. 2021.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law [EJJL]**, [S. l.], v. 12, n. 2, p. 91–108, 2011. Disponível em: <https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315/658>. Acesso em: 30 jul. 2021.

DUARTE, S.V.; FURTADO, M.S.V. Trabalho de conclusão de curso (TCC) em ciências sociais aplicadas. São Paulo: **Saraiva, 2014. E-book Kindle.** Paginação irregular.

FABRE, Valkyrie Vieira; BORNIA, Antônio Cezar; BORGERT, Altair. Disclosure dos governos locais: nem tudo é transparente. **Revista Principia - Divulgação Científica e Tecnológica do IFPB**, João Pessoa, n. 54, p. 93-103, mar. 2021. ISSN 2447-9187. doi:http://dx.doi.org/10.18265/1517-0306a2021v1n54p93-103. Disponível em: <https://periodicos.ifpb.edu.br/index.php/principia/article/view/3376>. Acesso em: 14 jun. 2023.

FORATO, Fidel. **Vazamento de senhas do Ministério da Saúde expõe pacientes da COVID**, diz jornal. Disponível em: <https://canaltech.com.br/hacker/vazamento-de-senhas-do-ministerio-da-saude-expoe-pacientes-da-covid-diz-jornal-175307/>. Acesso em: 06 ago. 2021.

GIL, Antônio Carlos. **Como elaborar projetos de pesquisa**. 6. ed. São Paulo: Atlas, 2017.

GOMES, Maria Cecília Oliveira. Relatório de impacto à proteção de dados. Uma breve análise da sua definição e papel na LGPD. **Revista do Advogado**, São Paulo, 2019, 133: 6-15.

GONÇALVES, Tânia Carolina Nunes Machado. **Gestão de dados pessoais e sensíveis pela administração pública federal: Desafios, modelos e possíveis impactos com a nova lei**. Dissertação (Mestrado em Direito) - Centro Universitário de Brasília, Brasília, 2019. Disponível em: <https://repositorio.uniceub.br/jspui/bitstream/prefix/14499/1/61600099.pdf>. Acesso em: 10 jul. 2021.

HOFFMANN-RIEM, Wolfgang. BIG DATA E INTELIGÊNCIA ARTIFICIAL: desafios para o Direito. **REI - REVISTA ESTUDOS INSTITUCIONAIS**, [S. l.], v. 6, n. 2, p. 431–506, 2020. DOI: 10.21783/rei.v6i2.484. Disponível em: <https://www.estudosinstitucionais.com/REI/article/view/484>. Acesso em: 29 jul. 2021.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Fundamentos de metodologia científica**. 5. ed. São Paulo: Atlas, 2003.

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor**. vol. 120. ano 27. p. 469-483. São Paulo: Ed. RT, nov-dez. 2018. 2020. Disponível em: <https://revistadedireitodoconsumidor.emnuvens.com.br/rdc/article/view/1116>. Acesso em: 30 jul. 2021.

MENDES, Laura Schertel. **Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo**. Dissertação (Mestrado em Direito) - Universidade de Brasília, Brasília, 2008. Disponível em: <https://repositorio.unb.br/bitstream/10482/4782/1/DISSERTACAO%20LAURA.pdf>. Acesso em: 31 jul. 2021.

Ministério das Comunicações. **Segurança cibernética**. Disponível em: <https://www.gov.br/anatel/pt-br/assuntos/seguranca-cibernetica>. Acesso em: 24 jul. 2021.

Ministério Público do Distrito Federal e Territórios. **Representação**. Disponível em: <https://www.mpdft.mp.br/portal/pdf/comunicacao/junho_2019/Representacao_TCU_-_SERPRO_-_PGJ.pdf>. Acesso em: 04 ago. 2021.

NASCIMENTO, Anderson; YUGE, Claudio. **O que é Phishing**. Disponível em: <https://canaltech.com.br/seguranca/O-que-e-Phishing/>. Acesso em: 24 jul. 2021.

PETRY, Guilherme. **Governo é o principal alvo de ataques cibernéticos no brasil, revela pesquisa**. Disponível em: <https://thehack.com.br/governo-e-o-principal-alvo-de-ataques-ciberneticos-no-brasil-revela-pesquisa/>. Acesso em: 24 jul. 2021.

RODRIGUES, Renato. **Brasileiros são principais alvos de ataques phishing no mundo**. Disponível em: <https://www.kaspersky.com.br/blog/brasileiros-maiores-alvos-phishing-mundo/17045/>. Acesso em: 24 jul. 2021.

SOUZA, Thiago de Almeida. Um estudo da LGPD para nortear o desenvolvimento de novos sistemas e a manutenção de sistemas legados. Trabalho de conclusão de curso (Curso Superior de Tec-

nologia em Análise e Desenvolvimento de Sistemas) - **Faculdade de Tecnologia de São Paulo**, São Paulo, 2021.

Superior Tribunal de Justiça. **Comunicado da Presidência do STJ**. Disponível em: <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/19112020-Comunicado-da-Presidencia-do-STJ.aspx>. Acesso em: 05 ago. 2021.

Superior Tribunal de Justiça. **Comunicado da Presidência do STJ**. Disponível em: <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/18112020-Comunicado-da-Presidencia-do-STJ.aspx>. Acesso em: 05 ago. 2021.

Superior Tribunal de Justiça. **Relatório de Gestão do Exercício de 2020**. Disponível em: <https://transparencia.stj.jus.br/wp-content/uploads/Relatorio_gestao_2020.pdf>. Acesso em: 05 ago. 2021.

VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação.** Dissertação (Mestrado em Direito, Estado e Sociedade) - Universidade de Brasília, Brasília, 2007. Disponível em: <https://repositorio.unb.br/bitstream/10482/3358/1/2007_TatianaMaltaVieira.pdf>. Acesso em: 30 jul. 2021.

ZORZAL, Luiza; RODRIGUES, Georgete Medleg. Disclosure e transparência no setor público: uma análise da convergência dos princípios de governança. **Informação & Informação**, [S. l.], v. 20, n. 3, p. 113–146, 2015. DOI: 10.5433/1981-8920.2015v20n3p113. Disponível em:<https://ojs.uel.br/revistas/uel/index.php/informacao/article/view/19470>. Acesso em: 13 jun. 2023.