CENTRO UNIVERSITÁRIO UNIDADE DE ENSINO SUPERIOR DOM BOSCO – UNDB
CURSO DE DIREITO

DAVI QUARESMA VALE PINHEIRO FIGUEIREDO

PROTEÇÃO DE DADOS PESSOAIS NO CONTEXTO DA ADMINISTRAÇÃO PÚBLICA: a responsabilidade civil da administração pública no tratamento de dados.

São Luís
2024

DAVI QUARESMA VALE PINHEIRO FIGUEIREDO

PROTEÇÃO DE DADOS PESSOAIS NO CONTEXTO DA ADMINISTRAÇÃO PÚBLICA: a responsabilidade civil da administração pública no tratamento de dados.

Monografia apresentada ao Curso de Graduação em Direito do Centro Universitário Unidade de Ensino Superior Dom Bosco como requisito parcial para obtenção do grau de Bacharel em Direito.

Orientadora: Profª Me Manuela Ithamar Lima

São Luís
2024

Dados Internacionais de Catalogação na Publicação (CIP)
Centro Universitário – UNDB / Biblioteca

Figueiredo, Davi Quaresma Vale Pinheiro

Proteção de dados pessoais no contexto da administração pública: a responsabilidade civil da administração pública no tratamento de dados. / Davi Quaresma Vale Pinheiro Figueiredo. __ São Luís, 2024.

66 f.

Orientador: Profa. Ma. Manuela Ithamar Lima

Monografia (Graduação em Direito) - Curso de Direito – Centro Universitário Unidade de Ensino Superior Dom Bosco – UNDB, 2024.

1. Dados pessoais. 2. Administração pública. 3. Responsabilidade civil. 4. LGPD. I. Título.

CDU 351.712.1:004.056.53

DAVI QUARESMA VALE PINHEIRO FIGUEIREDO

PROTEÇÃO DE DADOS PESSOAIS NO CONTEXTO DA ADMINISTRAÇÃO PÚBLICA: a responsabilidade civil da administração pública no tratamento de dados.

Monografia apresentada ao Curso de Graduação em Direito do Centro Universitário Unidade de Ensino Superior Dom Bosco como requisito parcial para obtenção do grau de Bacharel em Direito.

Aprovado em 25/11/2024

BANCA EXAMINADORA

_____

Profa. Orientadora Me. Manuela Ithamar Lima
Centro Universitário Unidade de Ensino Superior Dom Bosco

_____

Profa. Ma. Alyne Mendes Caldas
Centro Universitário Unidade de Ensino Superior Dom Bosco

_____

Adv. Esp. Fernando Vinicius Rezende Linhares
Membro Externo

A toda a minha família e amigos.

AGRADECIMENTOS

Primeiramente, agradeço ao meu Deus e a Nossa Senhora, por sempre me ajudarem a superar cada obstáculo que tive ao longo da minha formação acadêmica.

À minha mãe, Maria Quaresma, por ser o meu porto seguro, a minha maior fonte de inspiração e exemplo de vida. Sem a presença da minha mãe, eu nada seria.

Ao meu pai, Sócrates Figueiredo, e à minha mãe Geiza Barros, por serem tão especiais em minha vida, sempre me dando carinho e apoio.

Aos meus irmãos Jorge, Rômulo, Ramon, Ruan e à minha irmã Fernanda Tereza, por sempre me incentivarem em minhas decisões e me ajudarem a tornar cada sonho uma realidade.

À minha namorada, Ana Vitória, pelo apoio incondicional em todas as horas e por estar sempre ao meu lado em cada momento da minha vida.

A todos os meus amigos, por estarem sempre trilhando essa árdua caminhada ao meu lado.

Agradeço, de modo especial, à minha orientadora, a Professora Manuela Ithamar, por me guiar e me ensinar pacientemente na construção deste trabalho.

RESUMO

A Lei Geral de Proteção de Dados (LGPD) (Lei nº 13.709/2018) visa proteger os direitos dos cidadãos frente ao aumento da coleta de dados pessoais e, com a promulgação dessa lei, o tratamento de dados realizado pelo setor público passa a ser regido por princípios rigorosos e obrigações específicas. Dessa forma, torna-se intrínseco pautar que o problema maior do presente trabalho, foi questionar em que medida é concebida a responsabilidade civil da administração pública no tratamento de dados pessoais. Portanto, surge como hipótese para tal pergunta que o processamento de informações pessoais no contexto governamental deve ter finalidades claramente definidas e comunicadas, restringindo-se ao mínimo necessário para atender a esses objetivos. Vale evidenciar que em termos de responsabilidade, a LGPD exige que a Administração Pública implemente medidas de governança robustas para garantir a privacidade e a segurança dos dados. Logo, a responsabilidade civil do setor público pelo tratamento de dados segue um regime de responsabilidade objetiva, o que significa que, havendo dano ao titular dos dados, o poder público deverá indenizar a parte prejudicada, independentemente de dolo ou culpa. Este regime equilibra objetivamente o poder estatal, estabelecendo que, dado o poder superior e os recursos do Estado, este deve arcar com os danos decorrentes da sua atuação, o que é reforçado pelo princípio do risco administrativo. Esse princípio sustenta que o Estado assume o risco de prejuízos causados pelo tratamento inadequado dos dados, devendo reparar os danos, inclusive nos casos de falha de segurança ou uso indevido. Em razão disso, a justificativa do presente trabalho, é a grande importância de tratar sobre a proteção de dados na administração pública, visto que as entidades governamentais lidam com uma quantidade significativa de informações pessoais e de satisfação dos cidadãos. Dessa forma, a metodologia do presente trabalho é de cunho dedutivo, no qual fora analisado de forma geral a Lei Geral de Proteção de dados para se debruçar acerca da responsabilidade civil em matéria de dados pessoais, utilizando-se de técnicas de pesquisa bibliográfica e documental, tendo em vista que, para isso, fez-se a análise da jurisprudênciae da legislação abordada.

Palavras-chave: Dados Pessoais; administração pública; responsabilidade civil; LGPD.

ABSTRACT

The General Data Protection Law (LGPD) (Law No. 13,709/2018) aims to protect citizens' rights in the face of the increase in the collection of personal data and, with the enactment of this law, the processing of data carried out by the public sector is now governed by strict principles and specific obligations. Thus, it is intrinsic to state that the main problem of this work was to question to what extent the civil liability of the public administration in the processing of personal data is conceived. Therefore, the hypothesis for this question arises that the processing of personal information in the governmental context must have clearly defined and communicated purposes, restricted to the minimum necessary to meet these objectives. It is worth highlighting that in terms of responsibility, the LGPD requires the Public Administration to implement robust governance measures to guarantee data privacy and security. Therefore, the civil liability of the public sector for data processing follows a regime of objective liability, which means that, if there is harm to the data subject, the government must compensate the injured party, regardless of intent or fault. This regime objectively balances state power, establishing that, given the superior power and resources of the State, it must bear the damages resulting from its actions, which is reinforced by the principle of administrative risk. This principle maintains that the State assumes the risk of losses caused by inadequate data processing and must repair the damages, including in cases of security failure or misuse. Therefore, the justification for this work is the great importance of addressing data protection in public administration, since government entities deal with a significant amount of personal information and citizen satisfaction. Thus, the methodology of this work is deductive in nature, in which the General Data Protection Law was analyzed in general terms to address civil liability in matters of personal data, using bibliographic and documentary research techniques, considering that, for this purpose, the case law and legislation addressed were analyzed.

Keywords: Personal data; public administration; civil liability; LGPD.

SUMÁRIO

LISTA DE SIGLAS

ACP	Ação Civil Pública.
ADI	Ação Direta de Inconstitucionalidade.
ADPF	Arguição de Descumprimento de Preceito Fundamental.
ANPD	Autoridade Nacional de Proteção de Dados.
CDC	Código de Defesa do Consumidor.
CRFB	Constituição da República Federativa do Brasil.
DPO	Data Protection Officer.
GPDR	General Data Protection Regulation.
MPF	Ministério Público Federal.
RIPD	Relatório de Impacto à Proteção de Dados.
SES/SC	Secretaria de Estado da Saúde do Estado de Santa Catarina.
STF	Supremo Tribunal Federal.

1 INTRODUÇÃO

Diante da intensa necessidade da Administração Pública depender de dados pessoais para realizar diversas atividades administrativas, executar serviços e políticas públicas, torna-se intrínseca a essencialidade de dados e informações para administrar coisa pública. Logo, vale afirmar que tal assunto vem gerando uma série de balizas e posicionamentos dos tribunais superiores do Brasil, a exemplo do controle de constitucionalidade, em que se encontram as ADIn 6.387, 6.388, 6.389, 6.390 e 6.393 e os julgados do ano de 2022 ADI 6.649 e da ADPF 695 ou até mesmo a Ação Civil Pública nº 5028572-20.2022.4.03.6100.

Sendo assim, a Lei nº 13.709/2018, conhecida como a Lei Geral de Proteção de Dados (LGPD), vem a traçar para a administração uma série de requisitos e etapas ao longo do tratamento de dados, para uma estrutura adequada de governo aos administradores. Portanto, o tratamento deve vir respeitando a base legal e principiológica competente, para a garantia de direitos dos direitos do titular e adoção de boas práticas e adequada estrutura de governança.

Nesse contexto, surge a problematização do presente trabalho, onde se questiona em que medida é concebida a responsabilidade civil da Administração Pública no tratamento de dados pessoais. Tendo em vista tal questionamento, surge como hipótese, o fato da LGPD estabelecer que tanto o controlador quanto o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo. No caso da Administração Pública, essa responsabilidade é ainda mais acentuada por sua posição de poder e pela quantidade de dados pessoais que detém.

Vale afirmar que a responsabilidade civil da Administração Pública nesse contexto é objetiva, ou seja, independe da comprovação de dolo ou culpa. Basta que haja o dano e o nexo causal entre a conduta ilícita e o dano. Essa responsabilidade objetiva se justifica pela necessidade de garantir a efetividade da proteção de dados e incentivar a adoção de medidas de segurança adequadas. Vale elucidar que ainda há divergências doutrinárias sobre o regime da Responsabilidade civil da Administração Pública no tratamento de dados pessoais.

Dessa forma, quando se vem a falar sobre a responsabilidade civil da Administração Pública no tratamento de dados pessoais, elenca-se que a mesma surge como um dos mecanismos jurídicos essenciais para garantir que os direitos dos cidadãos sejam

preservados, em especial diante de eventuais falhas no tratamento dos dados. No entanto, a aplicação da responsabilidade civil no âmbito estatal enfrenta uma série de obstáculos, tais como a caracterização da culpa ou dolo no tratamento inadequado, a delimitação dos danos causados e a identificação dos responsáveis dentro da estrutura complexa da Administração Pública.

Logo, sem dúvida, o tratamento de dados pessoais deve observar uma devida e delimitada finalidade, cuja imperiosidade deve "ser assegurada também pelas pessoas jurídicas de direito público mediante o tratamento de dados pessoais de acordo com sua finalidade pública, na persecução do interesse público e com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público". (MOREIRA e VENTURINI, 2022).[1]

É nesse sentido que o artigo 23 da LGPD prevê um conjunto de requisitos ao dispor que o tratamento de dados pelo Poder Público deverá ser realizado em 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. (MOREIRA e VENTURINI, 2022).

Resta cristalino que, conforme ressaltado por Wimmer (2021), o princípio da finalidade permite o entendimento segundo o qual o Estado não poderia restar configurado como unidade informacional. Com efeito, alguns critérios devem ser observados quando do compartilhamento dos dados pessoais e daquilo que Wimmer (2021) define como uso secundário, que seria "a utilização de dados pessoais para finalidades distintas daquelas que justificaram originalmente a sua coleta" (mediante o compartilhamento entre órgãos e entidades da administração. É necessário, nessas hipóteses, que haja compatibilidade de finalidades e considerações às expectativas do titular; no caso de incompatibilidade, a fundamentação pelo compartilhamento pode advir de base legal ou de nova autorização expressa do titular. (MOREIRA e VENTURINI, 2022).

No que tange à justificativa da presente pesquisa, é válido afirmar que a proteção de dados é um direito de cada indivíduo baseado nas leis que determinam a referida proteção de dados. A interpretação da LGPD visa atender à privacidade sobre a coleta e tratamento de dados pessoais, sendo, portanto, uma lei a qual vem encontrar diversos desafios para atingir

---

1 Limites ao compartilhamento de dados pessoais pelo poder público. Disponível em conjur.com.br.

os objetivos e satisfazer uma lacuna normativa e principiológica em relação ao direito de proteção de dados.

Logo, é nítido que a proteção de dados na Administração Pública é um tópico de extrema importância, uma vez que as entidades governamentais lidam com uma quantidade significativa de informações pessoais e de satisfação dos cidadãos. A proteção de dados na administração envolve o tratamento adequado, a coleta, o armazenamento e o uso de informações pessoais, garantindo a privacidade e segurança dos dados.

Por isso, salienta-se, ainda, que as empresas públicas e as sociedades de economia mista quando atuarem em regime de concorrência, deverão respeitar o que dispõe a LGPD em relação às empresas privadas e em relação à questão do poder público. A LGPD disciplina que a governança dos dados e a estrutura do armazenamento dos dados quando referente ao poder público, deverão sempre ser pensados e estruturados da melhor forma a execução das políticas públicas e a persecução do interesse público. (CAPOBIANGO e DE VASCONCELOS, 2021)[2].

Dito isso**,** a metodologia do presente trabalho é de cunho dedutivo, no qual foi analisada de forma geral a Lei Geral de Proteção de Dados para se debruçar acerca da responsabilidade civil em matéria de dados pessoais. Logo, essa metodologia **"**[...] parte de princípios reconhecidos como verdadeiros e indiscutíveis e possibilita chegar a conclusões de maneira puramente formal, isto é, em virtude unicamente de sua lógica." (GIL, 2008, p. 9).

Juntamente à metodologia dedutiva, foram também utilizadas técnicas de pesquisa bibliográfica e documental, tendo em vista a análise de jurisprudência e da legislação abordada. Dessa forma, segundo afirma Gil (2002), do ponto de vista de seus objetivos, a pesquisa exploratória objetiva a maior familiaridade com o problema, tornando-o explícito, trazendo assim a facilidade na construção de hipóteses cujo tipo de pesquisa envolve também levantamento bibliográfico.

A organização da pesquisa distribui-se da seguinte maneira: o primeiro capítulo vem a analisar a Lei Geral de Proteção de Dados e sua aplicação na administração pública. Em seguida, debate-se sobre a responsabilidade civil da Administração Pública no tratamento de dados. E, por fim, discute-se a responsabilidade civil do poder público por vazamento de dados pessoais. Para isso, utilizou-se a Ação Civil Pública nº 5028572-20.2022.4.03.6100 como estudo de caso.

---

2 Como a LGPD se aplica à Administração Pública. Disponível em conjur.com.br.

2 A LEI GERAL DE PROTEÇÃO DE DADOS E SUA APLICAÇÃO NA ADMINISTRAÇÃO PÚBLICA.

É nítido que a administração pública exerce cotidianamente uma ampla gama de atividades administrativas, além de implementar políticas públicas em face do interesse público, sendo de grande importância a atuação da Administração Pública com base nas regras, leis e normas. Portanto, como afirma Freitas (2013), as políticas públicas não podem ser consideradas como "meros programas de governo, mas ações e pautas administrativas que precisam guardar vinculação com as prioridades constitucionais, imprimindo, de modo consciente, eficácia aos direitos fundamentais de todas as dimensões." (FREITAS, 2013, p. 456).

Portanto, para cumprir suas funções, o Estado demanda cada vez mais informações pessoais dos cidadãos, exigindo a exposição constante de dados sensíveis. A biometria, o reconhecimento facial e o cruzamento de dados bancários ilustram essa crescente coleta, que coloca em risco a privacidade individual e o controle dos cidadãos sobre suas próprias informações.

Visto isso, a Lei Geral de Proteção de Dados, vem a disciplinar sobre o tratamento e a proteção de dados pessoais pelas pessoas jurídicas de direito público (Capítulo IV, LGPD), mostrando que a Administração Pública não se torna alheia à realidade digital. Nesse sentido, a partir do artigo 23 da referida lei, determina-se 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. É dizer que deverão ser fornecidas informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução das atividades de tratamento de dados pessoais, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos, bem como deverá ser indicado um encarregado de dados. (ZILLOTO e PIRONTI, 2023).[3]

Portanto, os dados devem ser organizados em formatos padronizados e compatíveis entre si, permitindo o compartilhamento de informações entre diferentes órgãos públicos. Essa prática visa otimizar a prestação de serviços públicos, facilitar a tomada de decisões e promover

[3] *A LGPD e o tratamento de dados pela Administração Pública.* Disponível em conjur.com.br.

a transparência governamental. Essa relação jurídica existente entre o Poder Público e o indivíduo, titular de dados pessoais, contudo, caracteriza-se por uma natural assimetria, vez que o Estado possui amplos poderes para consecução de suas funções, realizando grande coleta e armazenamento de dados pessoais adquiridos para o desempenho de suas atividades ou como subproduto delas.(TASSO, 2019). Para Bioni, Silva e Martins (2022), considerando esse desequilíbrio entre as partes, "[...] uma das muitas formas de balancear esse desequilíbrio passa pela equalização do fluxo informacional [...], mediante regras mais protetivas que limitam ou balizam a atuação estatal, aumentando a transparência estatal para o cidadão." (BIONI, SILVA e MARTINS, 2022). [4]

Logo, a incorporação da LGPD à legislação que rege a Administração Pública exige que esta adote medidas mais rigorosas para proteger os dados pessoais dos cidadãos. A transparência e a segurança no tratamento desses dados devem ser prioridades, garantindo que os direitos individuais sejam respeitados sem comprometer a eficiência da gestão pública. Dessa forma, a participação da Administração Pública na lei é extremamente importante, como dispõe Garofano (2022) demonstrando essa importância em "[...] as prerrogativas e os poderes conferidos ao Estado para a consecução dos fins públicos; a relação assimétrica existente em relação aos indivíduos; a concentração de bancos de dados de cidadãos; a essencialidade desses dados para o exercício de atividades e políticas públicas; e a compulsoriedade da entrega de dados ao Estado". (GAROFANO, 2022, p.135).

Nesse contexto, o tratamento de dados pela Administração Pública, conforme a LGPD, deve garantir uma série de fatores, como a adequação do tratamento com as finalidades precípuas ou a garantia de [...]

> (i) procedimentos de proteção que levem em conta o risco do tratamento de dados pessoais, especialmente a partir da mudança de finalidade intrínseca a todo compartilhamento"; (ii) a necessidade do tratamento, limitando-o ao mínimo necessário; (iii) a qualidade dos dados, garantindo autodeterminação informada aos titulares e mecanismos efetivos para o exercício dos demais direitos; (iv) a segurança e a prevenção, mediante sistema de governança robusto, que permita a utilização de técnicas aptas a inibir o acesso escuso, eximindo os titulares de danos; (v) a não permissão de utilização dos dados para fins discriminatórios; (vi) a adoção de instrumentos de transparência e de accountability, que possibilitem o controle do fluxo dos dados pessoais pelo cidadão e pelos órgãos competentes; e (vii) a necessidade de realização

[4] *Intersecções e relações entre a Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação (LAI): análise contextual pela lente do direito de acesso.* Disponível em https://revista.cgu.gov.br/cadernos_CGU/article/view/504.

> de relatórios de impacto prévios ao compartilhamento de dados de alto risco. (MENDES, 2022).[5]

Em síntese, a Administração Pública, ao tratar dados pessoais, deve conciliar as exigências da LGPD com as normas que regem sua atuação. A proteção de dados não pode ser um obstáculo à transparência e ao controle social, especialmente em relação a informações de interesse público, como as relacionadas a licitações e contratos, que devem ser acessíveis, conforme previsto na Lei de Acesso à Informação e na Lei nº 14.133/2021 (Lei de Licitações e Contratos Administrativos).

2.1 O contexto histórico da criação da Lei Geral de Proteção de Dados e os impactos trazidos ao âmbito das políticas públicas.

Inicialmente, Quintiliano (2020), vem afirmar que o medo e a preocupação que os indivíduos nutrem em torno da sua privacidade, e da liberdade de exercer pleno controle sobre suas informações mais íntimas, bem como o direito de escolher como e para quem quer transmiti-las, vem a ser um dos fatores contribuintes para criação de lei que proteja o cidadão em relação às suas informações e dados pessoais.

Logo, tal preocupação generalizada atesta que o direito à proteção da privacidade é inerente ao direito à autodeterminação individual, constituindo-se, assim, a irradiação do princípio da dignidade humana. Não por outra razão, esse direito é reconhecido por diversas declarações de direitos fundamentais, especialmente a contemplada pelo artigo 5º da Constituição Federal de 1988 (CF-88). (QUINTILIANO, 2020).

Dessa forma, a Lei Geral de Proteção de Dados (LGPD) chegou ao cenário jurídico do Brasil com o propósito de unificar princípios que já faziam parte de diferentes leis nacionais, mas que ainda não estavam consolidados em um único estatuto legal. Seu objetivo principal era fornecer clareza em relação aos procedimentos de tomada de decisão em matéria de dados pessoais. Através dessa legislação, os cidadãos passaram a ter um arcabouço jurídico sólido que lhes concede o direito de solicitar informações sobre como seus dados pessoais estão sendo tratados, permitindo-lhes, assim, uma maior compreensão e controle sobre o uso dessas informações.

> Devido ao nível de intimidade presente nessas informações sensíveis, constata-se que seu tratamento inadequado, ou seja, sem o consentimento do

[5]*Democracia, poder informacional e vigilância*. Disponível em https://oglobo.globo.com/blogs/fumus-boniiuris/post/2022/08/laura-schertel-democracia-poder-informacional-e-vigilancia.ghtml.

> titular e com a inobservância das cautelas necessárias, pode gerar inúmeros danos, uma vez que tais informações podem ser utilizadas para promover a intolerância, o preconceito ou a discriminação, violando direitos e garantias fundamentais dos titulares (MACHADO, 2018).[6]

De acordo com Doneda (2020), "[...] tais regras apresentadas compõem um conjunto de medidas que passaram a ser encontradas em várias normas sobre a proteção de dados pessoais, às quais se passaram a referir como *Fair InformationPrinciples*". (Princípio da Informação Justa), constituindo-se em uma forma cuidadosa na hora de tratar os dados pessoais, refletindo sobre objetivos da administração dessas informações pelo consentimento e informações de dados. (DONEDA, 2020, p.100).

Tratando-se de uma evolução do reconhecimento do direito à proteção de dados pessoais, torna-se intrínseco abordar sobre a Declaração Universal de Direitos Humanos de 1948, que, em seu artigo 12º, aborda sobre o direito à privacidade:

> Artigo 12.º - Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito à proteção da lei. (DECLARAÇÃO UNIVERSAL DE DIREITOS HUMANOS).[7]

Ademais, o Pacto de San José da Costa Rica[8] e a Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais,[9] em seus artigos 11 e 8º, respectivamente, vem a abordar sobre a mesma temática.

---

[6]*LGPD e GDPR: uma análise comparativa entre as legislações.* Disponível em https.//www.linkedin.com/pulse/lgpd-e-gdpr-uma-análise-comparativa.

[7] Declaração Universal dos Direitos Humanos. Disponível em United Nations Regional Information Centre - https://unric.org/pt/declarac.

[8]O Pacto de São José é um tratado internacional que estabelece os direitos e as garantias fundamentais dos indivíduos, também conhecido como a Convenção Americana sobre Direitos Humanos. "*O que é o Pacto de São José: direitos humanos e suas garantias*."Disponível em https//reyabogado.com/BR/o-que-e-o-pacto-de-sao-jose/.

[9]A Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais (CEDH) é um tratado internacional que garante os direitos fundamentais, civis e políticos, não apenas aos cidadãos dos Estados-Membros do Conselho da Europa, mas também a qualquer pessoa singular ou coletiva que se encontre sob a sua jurisdição. Foi assinada em 4 de novembro de 1950, em Roma, e entrou em vigor em 1953.
Disponível emcruzvilaca.eu/PT/areas-de-pratica/Direitos-Fundamentais/subareas/Convencao-Europeia-para-Protecao-dos-Direitos-do-Homem-e-das-Liberdades-Fundamentais-CEDH/47/.

Vale elucidar que a Alemanha, marcada pelas experiências do nazismo, foi pioneira na proteção de dados, impulsionada pelos avanços tecnológicos da década de 1970. As primeiras leis nesse sentido surgiram por lá, inspirando a União Europeia a criar a Diretiva 95/46/CE. Já no âmbito da União Europeia, o direito à proteção de dados foi reforçado com a Diretiva 95/46/CE, de 1995,[10] a qual traz, em sua motivação preambular, todos os fundamentos e finalidades que justificam a adoção da proteção de dados, os quais se aplicam, em sua grande maioria, ao contexto brasileiro e de qualquer país que faça adesão aos princípios consagrados na Declaração Universal de Direitos Humanos (QUINTILIANO, 2020).

Essa diretriz, por sua vez, deu origem ao rigoroso GDPR,[11] que entrou em vigor em 2018, forçando gigantes da tecnologia como Facebook e Google a adaptarem suas práticas. O sucesso do GDPR serviu como modelo para outros países, incluindo o Brasil, que buscaram regulamentar a proteção de dados. Vale ressaltar, que a regulamentação da LGPD veio a alterar a Lei nº 12.965, de 23 de abril de 2014, conhecida como Marco Civil da Internet. A referida lei estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil, tendo como objetivo assegurar o exercício da cidadania nos meios digitais e definir diretrizes para a atuação da internet no país.

Ademais, indaga-se que, assim como qualquer outra norma jurídica, a LGPD é pautada em princípios, dentre eles, o mais importante, o princípio da finalidade,

> O primeiro dos princípios eleitos, e o mais importante que está previsto no inciso I do artigo 6º da referida Lei, emprega-se ao termo a "realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades" (MAIA, 2023, p.462-463).

---

[10]A Diretiva 95/46/CE é o texto de referência a nível europeu para a proteção de dados pessoais. Ela estabelece um quadro regulamentar que busca equilibrar a proteção da privacidade das pessoas com a livre circulação de dados pessoais dentro da União Europeia (UE). Disponível em Directive 95/46/EC of the European Parliament and of the Cou... (europa.eu).

[11] A General Data Protection Regulation (GDPR) é a norma europeia que regula a proteção de dados pessoais na Europa e que deu origem à Lei Geral de Proteção de Dados (LGPD) no Brasil. Essas normas possuem a finalidade de preservar a privacidade das pessoas. Disponível em https://www.aurum.com.br/blog/gdpr/.

Além desse, pode-se elucidar os princípios da adequação, necessidade, livre acesso, qualidade de dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas, princípios esses que devem ser observados durante o tratamento de dados pessoais.

Portanto, quando se pensa em um contexto de Administração Pública, a tarefa não se torna tão simples, haja vista a constante necessidade da administração pública de manusear dados e informações pessoais em consonância com preceitos e fundamentos da LGPD.

Dessa forma, em um contexto histórico, a Lei nº 13.709/2018 teve sua criação recente, e sua expansão no período pandêmico da Covid-19 e, como não poderia deixar de ser, a migração de serviços e de processos para o ambiente digital veio acompanhada por crescentes demandas de coleta, análise, compartilhamento e cruzamento de dados pessoais no âmbito do Poder Público. No caso do pagamento do auxílio emergencial, por exemplo, acórdão do Tribunal de Contas da União– TCU (2020) apontou para os riscos de inclusão e exclusão indevida de beneficiários, com identificação de seis fatores de risco: (i) baixa integração dos cadastros públicos; (ii) desatualização do Cadastro Único; (iii) dificuldade para identificação inequívoca em cadastros públicos; (iv) limitações para verificação de composição familiar; (v)limitações para verificação de vínculos de emprego e renda; e (vi)limitações para cadastramento de pessoas com menor acesso a serviços públicos. Para endereçar tais fragilidades, o acórdão apresentou diversas recomendações quanto ao aprimoramento do cruzamento de dados contidos em bases do Poder Público. (WIMMER, 2021).

2.2 Uma análise das mudanças necessárias na gestão de dados pela Administração Pública.

No presente trabalho já foi elencado que a LGPD representa um avanço significativo na legislação que regula a privacidade e a proteção de dados no Brasil, estabelecendo um sólido arcabouço legal para proteger os titulares de dados pessoais. No âmbito público, o cumprimento da LGPD não é apenas uma exigência legal, mas também uma oportunidade para reforçar as medidas de segurança da informação e salvaguardar os direitos fundamentais dos cidadãos, incluindo o direito à privacidade. Nesse contexto, é crucial analisar as disposições da LGPD à luz do artigo 37 da Constituição Federal, que delineia os princípios que regem a Administração Pública, e avaliar como esses princípios se relacionam com o direito à privacidade dos cidadãos.

O art. 37 da Constituição Federal estabelece os princípios que regem a Administração Pública, incluindo legalidade, impessoalidade, moralidade, publicidade e eficiência. Esses princípios são fundamentais para garantir a transparência e a accountability da Administração Pública direta ou indireta, promovendo a confiança dos cidadãos nas instituições públicas. No contexto da proteção de dados, esses princípios se alinham com os fundamentos epistemológicos da LGPD, que incluem a finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização. Ao adotar uma abordagem baseada nessas diretrizes, o Poder Público pode garantir que as informações dos cidadãos sejam tratadas de forma ética, transparente e segura, em conformidade com a legislação vigente e os direitos constitucionais. Além do mais, manterá e promoverá a conscientização entre a sociedade civil sobre a importância do conhecimento dos seus direitos, tornando a lei aplicável e com eficácia plena. A segurança da informação desempenha um papel crucial na proteção dos dados pessoais dos cidadãos. No âmbito da Administração Pública, é um imperativo categórico implementar medidas robustas de segurança cibernética para mitigar os riscos de violações de dados e garantir a integridade, confidencialidade e disponibilidade das informações, já que a *Res Pública* detém a obrigatoriedade legal de gerar tutela e fomentar discussão sobre a aplicação da lei." (CHECCHIA, 2024).[12]

Ademais, vale elencar que o direito à privacidade representa um dos princípios basilares dos direitos individuais e encontra-se tanto na Constituição Federal quanto na LGPD. Cabe ao Poder Público o compromisso de honrar e preservar esse direito, assegurando que as informações pessoais dos cidadãos sejam tratadas de maneira lícita, ética e segura.

Ao adotar medidas de segurança da informação em conformidade com a LGPD, o Poder Público não apenas cumpre suas obrigações legais, mas também reafirma seu compromisso com os princípios democráticos e os direitos constitucionais dos cidadãos. A proteção de dados e a privacidade devem ser consideradas como elementos essenciais da governança digital, promovendo a confiança e a legitimidade das instituições públicas. A segurança da informação na ótica da LGPD para o Poder Público não é apenas uma questão de conformidade legal, mas também uma questão de responsabilidade e ética. Ao adotar uma abordagem baseada nos princípios da Administração Pública e nos direitos constitucionais dos cidadãos, as entidades públicas podem fortalecer a proteção de dados e promover a confiança

[12]*Segurança da informação na ótica da LGPD para o Poder Público: Protegendo dados e respeitando os direitos constitucionais.* Disponível em https://www.migalhas.com.br/depeso/406158/seguranca-da-informacao-na-otica-da-lgpd-para-o-poder-publico/.

e a transparência na sociedade. A implementação eficaz de medidas de segurança da informação é essencial para garantir que o poder público cumpra seu papel de forma responsável e respeitosa com os direitos fundamentais dos cidadãos. (CHECCHIA, 2024).

Nesse contexto, o tratamento de dados pessoais por meio da Administração Pública deve vir subordinado à referida base legal e principiológica em garantia aos direitos dos portadores junto à adoção de boas práticas e adequada estrutura de governança. Ademais, a própria ANPD vem a tratar sobre a sua conceituação e relevância da proteção de dados, junto da elucidação principiológica para que ocorra o uso de dados pessoais pela Administração Pública da forma a mais correta possível.

O compartilhamento de dados pessoais é, portanto, a operação de tratamento pela qual órgãos e entidades públicos conferem permissão de acesso ou transferem uma base de dados pessoais a outro ente público ou a entidades privadas visando ao atendimento de uma finalidade pública. De forma mais específica, a LGPD utiliza o termo "uso compartilhado de dados", que é definido como a "comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados".[13]

O uso compartilhado de dados é um mecanismo relevante para a execução de atividades típicas e rotineiras do Poder Público, a exemplo de pagamento de servidores e prestação de serviços públicos. A LGPD reconhece essa relevância ao estabelecer, em seu art.25, que os dados devem ser mantidos "[...] em formato interoperável e estruturado para o uso compartilhado [...]," (ANPD, 2023), visando, entre outras finalidades, "[...] à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral." [...]. (ANPD, 2023).

Não obstante, assim como ocorre com as demais operações de tratamento, o uso compartilhado de dados pessoais deve ser realizado em conformidade com a LGPD, notadamente com os princípios, as bases legais, a garantia dos direitos dos titulares e outras regras específicas aplicáveis ao Poder Público. Além de conferir maior previsibilidade, transparência e segurança jurídica ao uso compartilhado de dados, a observância dessas disposições legais constitui peça-chave para a promoção de uma relação de confiança com os

[13] *Proteção de dados pessoais. Uso compartilhado de dados.* Disponível em https://lgpd/ufsc.br/glossario/.

titulares e para a adequada gestão de riscos pelos controladores, inclusive para evitar a ocorrência de abusos e desvios de finalidades. (ANPD, 2023).

Tendo em vista a intensa necessidade de compartilhamento de dados pessoais, a Administração Pública se vê na obrigação de sempre obedecer aos limites e possibilidades presentes nas diretrizes e princípios da LGPD. "De acordo com o princípio da finalidade (art.6º, i), o tratamento dos dados pessoais deve ser realizado para "propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades." (BRASIL, 2018). Adicionalmente, no âmbito do setor público, o tratamento de dados pessoais deve atender a uma "finalidade pública", conforme previsto no art. 23 da LGPD. (BRASIL, 2018). Portanto, o tratamento de dados pessoais pelo Poder Público deve estar sempre associado a uma finalidade pública, que seja: (i) legítima, isto é, lícita e compatível com o ordenamento jurídico, além de amparada em uma base legal, que autorize o tratamento; (ii) específica, de maneira que a partir da finalidade seja possível delimitar o escopo do tratamento e estabelecer as garantias necessárias para a proteção dos dados pessoais; (iii) explícita, isto é, expressa de uma maneira clara e precisa; e (iv) informada, isto é, disponibilizada em linguagem simples e de fácil compreensão e acesso ao titular dos dados". (ANPD, 2023).

Portanto, tais limites também se encontram presentes, no princípio da necessidade, onde o princípio da necessidade estabelece que o tratamento deve ser limitado ao "mínimo necessário para a realização de suas finalidades", abrangendo apenas os "dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados" (art. 6º, iii LGPD). (BRASIL, 2018). O princípio da necessidade impõe, portanto, que a coleta se atenha à menor quantidade possível de dados para o alcance da finalidade proposta. Da mesma forma, esse princípio desaconselha o próprio tratamento de dados pessoais quando a finalidade que se almeja pode ser atingida por outros meios menos gravosos ao titular de dados. (ANPD, 2023).

2.3 Análise das mudanças necessárias na gestão de dados pela Administração Pública adjacente ao estudo do Capítulo IV da LGPD em consonância com a ADI 6.649 e a ADPF 695.

A Lei Geral de Proteção de Dados (LGPD) representa um marco legislativo no Brasil, buscando salvaguardar a privacidade e a segurança dos dados pessoais dos cidadãos. Ao estabelecer diretrizes específicas para o tratamento dessas informações, a LGPD se aplica não apenas ao setor privado, mas também aos gestores públicos, englobando órgãos e entidades da Administração Pública. Assim, os administradores públicos são chamados a observar uma

série de obrigações e responsabilidades no que diz respeito à proteção dos dados pessoais sob sua guarda, em conformidade com as disposições da LGPD.

De acordo com a doutrina, o tratamento de dados pessoais deve seguir os princípios estabelecidos pela LGPD, como finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização. Assim, o administrador público deve garantir que a coleta, armazenamento e tratamento de dados pessoais estejam em conformidade com esses princípios e requisitos legais (MIRAGEM, 2021, p.24).

O consentimento do titular dos dados é um dos pilares da LGPD. Os administradores públicos devem obter o consentimento dos titulares antes de coletar e tratar seus dados pessoais, exceto em situações específicas previstas na lei, como no cumprimento de obrigações legais ou regulatórias e para a execução de políticas públicas (TARTUCE, 2021, p.15). A transparência e a informação são aspectos fundamentais na proteção de dados pessoais. Os administradores públicos devem garantir que os titulares dos dados estejam informados sobre a coleta e o tratamento de suas informações, proporcionando informações claras e acessíveis (NUNES, 2021, p. 14).

A segurança e proteção dos dados pessoais é uma responsabilidade essencial dos administradores públicos, que devem adotar medidas técnicas e administrativas para proteger as informações contra acessos não autorizados, perdas, destruição, alterações ou vazamentos (FARIAS, 2021, p. 31). Os administradores públicos também têm va responsabilidade de garantir que os titulares dos dados possam exercer seus direitos previstos na LGPD, como acesso, retificação, anonimização, bloqueio, eliminação, portabilidade, revogação do consentimento e oposição ao tratamento de seus dados pessoais (MIRAGEM, 2021, p.27).

Além disso, os órgãos e entidades da Administração Pública devem nomear um Encarregado de Proteção de Dados (DPO), responsável por supervisionar e orientar a conformidade com a LGPD (TARTUCE, 2021, p. 18). Por fim, a responsabilização e prestação de contas são princípios que exigem do administrador público a demonstração de conformidade com a LGPD, adotando medidas para assegurar a eficácia das normas de proteção de dados e prevenindo eventuais danos aos titulares dos dados (NUNES, 2021, p.16).

Portanto, no âmbito das prefeituras, é de suma importância a responsabilidade do gestor público para assegurar a proteção dos dados pessoais dos cidadãos e o pleno cumprimento da Lei Geral de Proteção de Dados (LGPD). As prefeituras são responsáveis pela gestão de uma vasta quantidade de informações pessoais dos cidadãos, englobando desde registros de identificação até dados relacionados a aspectos tributários, de saúde e educação.

Esses dados são coletados e processados com o intuito de viabilizar a prestação de serviços públicos, implementação de políticas e atendimento a obrigações legais.

A responsabilização do administrador público também abrange a cooperação com a Autoridade Nacional de Proteção de Dados (ANPD) e a adoção de medidas para prevenir e mitigar eventuais incidentes de segurança que possam levar a vazamentos de dados ou a outros danos aos titulares dos dados. Em caso de descumprimento das obrigações estabelecidas pela LGPD, o administrador público, incluindo aqueles que atuam em prefeituras, pode estar sujeito a sanções administrativas, como advertências, multas e bloqueio dos dados pessoais envolvidos na infração. Além disso, também pode haver responsabilização civil e penal em casos específicos. (FERRAREZI, 2023).

Outro impacto significativo é o mapeamento e gerenciamento de dados pessoais. As prefeituras devem identificar todos os processos e sistemas onde os dados pessoais são coletados, armazenados e processados, implementando políticas e práticas adequadas para garantir segurança, privacidade e conformidade com a LGPD. A transparência e o fornecimento de informações aos titulares também são impactos relevantes da LGPD. As prefeituras devem informar aos titulares dos dados sobre o tratamento de suas informações pessoais de forma clara e acessível, incluindo detalhes sobre a finalidade do tratamento, os direitos dos titulares, os prazos de armazenamento e os procedimentos para exercer esses direitos. (FERRAREZI, 2023).

A implementação dos princípios de proteção de dados desde a concepção e por padrão, conhecidos como "Privacy by Design" e "Privacy by Default", também deve ser incorporada pelas prefeituras em todos os seus projetos e sistemas que envolvam dados pessoais. Isso porque, inexistindo finalidade clara e adequação da coleta, i) o tratamento poderá ser considerado abusivo; ii) adequação do tratamento dos dados à sua finalidade (os dados coletados deverão ser utilizados apenas para as finalidades específicas devidamente informadas aos titulares); iii) privacy by default, ou privacidade por padrão, segundo o que o consentimento não é mais a única forma de legitimar o tratamento de dados, conforme se depreende da leitura do art. 7º da LGPD (SANTOS e TALIBA, 2018).

Por fim, a gestão de incidentes e violações de dados emerge como um aspecto crítico da LGPD. As prefeituras devem estabelecer procedimentos robustos para identificar, reportar e gerenciar incidentes de segurança relacionados a dados pessoais, comunicando à ANPD e aos titulares dos dados sobre quaisquer violações que possam representar riscos ou danos. Em resumo, a LGPD impõe uma série de obrigações e desafios para as prefeituras,

exigindo uma revisão substancial na forma como os dados pessoais são tratados, com o objetivo primordial de salvaguardar a privacidade e os direitos dos cidadãos.

A Lei Geral de Proteção de Dados (LGPD) estabelece uma série de obrigações e princípios para a proteção dos dados pessoais dos cidadãos, impactando significativamente o setor público, em especial, as prefeituras (MIRAGEM, 2021, p. 24). Nesse contexto, é imprescindível que as prefeituras adotem medidas adequadas para garantir a conformidade com a legislação, como a elaboração de um Relatório de Impacto à Proteção de Dados (RIPD).[14] ORIPD é um instrumento essencial para assegurar a conformidade com a LGPD no âmbito da Administração Pública, pois permite identificar, avaliar e mitigar os riscos associados ao tratamento de dados pessoais (NUNES, 2021, p. 14). Por meio do RIPD, as prefeituras podem adotar medidas apropriadas para resguardar a privacidade e os direitos dos cidadãos.

O Registro de Impacto à Proteção de Dados (RIPD) desempenha um papel crucial para as prefeituras, que atuam como controladoras de dados e lidam com um considerável volume de informações pessoais dos cidadãos. A elaboração e a manutenção contínua do RIPD permitem às prefeituras identificar, avaliar e mitigar os riscos associados ao tratamento de dados, garantindo a conformidade com a legislação vigente, como a LGPD, e a proteção da privacidade e dos direitos individuais.

O RIPD se configura como uma ferramenta essencial para analisar os riscos e os possíveis impactos à privacidade e aos direitos dos titulares dos dados, como vazamento de informações, discriminação ou uso inadequado dos dados. Além disso, possibilita que as prefeituras mantenham a conformidade com as normas de proteção de dados, evitando sanções e protegendo sua reputação.

Por meio do RIPD, as prefeituras têm a oportunidade de implementar medidas adequadas de mitigação e segurança para reduzir os riscos identificados, promovendo uma cultura de proteção de dados e privacidade em suas operações. O RIPD também contribui para a transparência e a comunicação eficaz com os cidadãos, esclarecendo-os sobre o tratamento de seus dados pessoais e garantindo o respeito aos seus direitos.

---

[14] O Relatório de Impacto à Proteção de Dados (RIPD) é a documentação que contém a descrição dos processos de tratamento de dados pessoais que podem gerar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos na LGPD e às liberdades civis e aos direitos fundamentais do titular de dados. Deve conter, ainda, as medidas, salvaguardas e mecanismos de mitigação de risco, nos termos dos artigos 5º, inciso XVII, e 38 da Lei nº 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em htpps:/www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd.

Ao estabelecer processos de monitoramento e revisão periódica do RIPD, as prefeituras podem garantir que as práticas de tratamento de dados permaneçam atualizadas e eficazes diante das mudanças na legislação, nos padrões tecnológicos e nas necessidades dos cidadãos.

Além disso, o RIPD pode contribuir para a capacitação e o treinamento dos profissionais das prefeituras, garantindo que todos estejam cientes de suas responsabilidades e obrigações relacionadas à proteção de dados pessoais.

A Lei Geral de Proteção de Dados (LGPD) no Brasil desempenha um papel crucial na reconfiguração das práticas das prefeituras e órgãos da administração pública municipal, uma vez que essas entidades lidam com uma ampla gama de dados pessoais dos cidadãos. Ao estabelecer um conjunto abrangente de normas e princípios, a LGPD impulsiona a salvaguarda da privacidade, a proteção dos direitos individuais e a promoção de uma cultura de responsabilidade e transparência no tratamento de informações pessoais. O Registro de Impacto à Proteção de Dados (RIPD) emerge como um instrumento vital nesse contexto, auxiliando as prefeituras a garantir a conformidade com as legislações de proteção de dados.

Ademais, vale elucidar que o capítulo IV da Lei Geral de Proteção de Dados trata diretamente do tratamento dos dados pessoais pelo Poder Público, em especial os artigos 23 e 26 do referido capítulo. Vejamos:

> Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, como objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:
>
> [...]
>
> Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art.6º desta Lei. (BRASIL, 2018).

Dessa forma, é importante destacar que, no contexto do tratamento de dados pelo Poder Público, a definição de uma finalidade, especificamente, é um requisito fundamental. Da mesma forma que ocorre em uma empresa privada, os órgãos públicos também devem designar um encarregado (DPO), cuja responsabilidade é gerenciar o tratamento de dados pessoais.

Ademais, a LGPD estabelece que a gestão e a estrutura de armazenamento de dados no âmbito do Poder Público devem ser estruturadas de modo a melhorar a execução de políticas públicas e a busca pelo interesse público. É incumbência do Poder Público garantir que o compartilhamento de dados e informações pessoais armazenados só ocorra quando houver prejuízos necessários para cumprir uma política pública ou prestar um serviço. Portanto, fica proibida a troca de dados e informações entre o Poder Público e empresas privadas sem um propósito claro e específico (em prol do interesse público ou da implementação de políticas públicas), sendo obrigatório o respeito contínuo pelos direitos dos titulares de dados, conforme é previsto no art.7º da LGPD.

Ainda vale elencar que, juntos, os principais fundamentos e princípios da LGPD, entre eles o da finalidade, foram utilizados em contexto pandêmico. No que tange, especificamente, ao Princípio da Finalidade, é possível observar, em tais manifestações, a ideia de que "os fins devem ser suficientemente específicos para excluir o tratamento posterior para finalidades não relacionadas com a gestão da crise sanitária da COVID-19 (por exemplo, fins comerciais ou de aplicação da lei)," e que "uma vez definido claramente o objetivo, será necessário assegurar que a utilização dos dados pessoais seja adequada, necessária e proporcionada" (WIMMER, 2021. p. 19). Assim, revela-se, claramente, a preocupação em compatibilizar o uso da tecnologia como ferramenta eficaz de resposta à pandemia com garantias de que esse aparato tecnológico de monitoramento, construído em um momento de excepcionalidade, não se perpetue após o fim da epidemia. (WIMMER, 2021).

Por outro lado, quando se trata das iniciativas voltadas para a aceleração da migração de serviços e de processos rotineiros de governo para o ambiente digital, fruto indireto da pandemia, observa-se que a discussão sobre o Princípio da Finalidade assume nuances distintas. De fato, os processos de transformação digital de serviços de governo são normalmente concebidos como caminhos sem volta. Assim, elementos como a limitação temporal do tratamento de dados pessoais ao período da pandemia e a utilização de tais dados apenas para a finalidade específica de gestão da crise sanitária, frisados em comunicações de autoridades de proteção de dados pessoais em diferentes países, podem ser colocados em questão, especialmente quando se verifica que os dados coletados e os compartilhamentos realizados podem eventualmente ser úteis para atingir outras finalidades públicas, distintas daquelas que justificaram o tratamento original. (WIMMER, 2021).

Ao seu lado, dispõe o Princípio da Necessidade:[15]

> [...] o princípio da necessidade dá-se pela limitação com uma objetividade, ou seja, a organização deve por obrigação legal utilizar apenas dados necessários para alcançar as suas finalidades. De acordo com Pestana (2020), essa expectativa ocorre pela necessidade da concretização de suas finalidades. Em regra, esse princípio trazido pela norma é o de realizar o tratamento apenas e tão somente quando e para o atingimento de determinada finalidade, pois a lei veda tratar dados que não se mostrem oportunos e relevantes à sua finalidade, como demonstram o artigo 5º, inciso xii e artigo 8º, § 4º. (KAMEDA e PAZELLO, p.7).

Nesse contexto, a LGPD estabelece regulamentações robustas, o que impõe à administração pública o cumprimento de diversos requisitos e procedimentos ao longo do ciclo de tratamento de dados, todos dentro de um quadro de governança bem estruturado. Consequentemente, o processamento de dados deve seguir as bases legais e princípios protegidos, garantindo os direitos dos titulares e adotando boas práticas e uma estrutura de governança adequada.

Dessa maneira, tais regulamentações robustas vem a auxiliar em conflitos atuais, como a exemplo da ADI 6.649 e a ADPF 695, votadas no ano de 2022, por maioria dos votos, pelo Supremo Tribunal Federal (STF), decidindo que órgãos e entidades públicas da Administração pública federal podem compartilhar dados pessoais entre si, sendo observado alguns critérios.

No julgamento, o voto decisivo coube ao relator, Ministro Gilmar Mendes, que defendeu a possibilidade de compartilhamento de dados, desde que sejam respeitados certos critérios. Vejamos trecho do acórdão da referida decisão:

> [...] 1. O compartilhamento de dados pessoais entre órgãos e entidades da Administração Pública, pressupõe: a) eleição de propósitos legítimos, específicos e explícitos para o tratamento de dados (art. 6º, inciso I, da Lei 13.709/2018); b) compatibilidade do tratamento com as finalidades informadas (art. 6º, inciso II); c) limitação do compartilhamento ao mínimo necessário para o atendimento da finalidade informada (art. 6º, inciso III); bem como o cumprimento integral dos requisitos, garantias e procedimentos estabelecidos na Lei Geral de Proteção de Dados, no que for compatível com o setor público.

---

[15] *E-Saúde e desafios à proteção da privacidade no Brasil.* Disponível em nupef.org.br/sites/default/files/downloads/artigo%20politics_esaude%20e%20privacidade.pdf.

> 2.O compartilhamento de dados pessoais entre órgãos públicos pressupõe rigorosa observância do art. 23, inciso I, da Lei 13.709/2018, que determina seja dada a devida publicidade às hipóteses em que cada entidade governamental compartilha ou tem acesso a banco 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.[...].

De acordo com a argumentação do voto do relator, o acesso a informações pessoais deve ter propósitos legítimos, específicos e claramente definidos, limitando-se às informações com restrições para atender ao interesse público. No entendimento do voto do relator, o compartilhamento de dados deve ser restrito ao mínimo essencial para cumprir a finalidade declarada, e deve aderir integralmente aos requisitos, garantias e procedimentos estabelecidos na Lei Geral de Proteção de Dados (LGPD), especialmente aqueles aplicáveis ao setor público.

Esses procedimentos incluem mecanismos rigorosos de controle de acesso ao Cadastro Base do Cidadão, a divulgação pública do compartilhamento de dados pessoais e o fornecimento de informações transparentes e atualizadas sobre uma base legal, específica e práticas envolvidas. No que diz respeito à inclusão de novos dados pessoais na base integrada, o ministro-relator enfatizou que deve ser precedida de uma justificativa formal, específica e prévia. O Comitê Central deve estabelecer medidas de segurança em conformidade com os princípios da LGPD, incluindo a criação de um sistema eletrônico de registro de acesso para fins de responsabilização em caso de uso indevido. O Tribunal também enfatizou que o compartilhamento de informações pessoais em atividades de inteligência deve obedecer a legislação específica e as condições previstas na decisão da ADI6529, que restringe o compartilhamento de dados do Sisbin, e deve estar alinhado com o interesse público, entre outras considerações.

Portanto, o compartilhamento de dados pessoais entre órgãos e entidades da administração pública deve ser adequado aos critérios presentes no julgado retratado, sendo assim de extrema importância o papel desempenhado pelo STF no que tange ao assunto, por considerar propósitos legais e específicos em compatibilidade com a finalidade e a limitação ao mínimo necessário.

3 RESPONSABILIDADE CIVIL DA ADMINISTRAÇÃO PÚBLICA NO TRATAMENTO DE DADOS.

Inicialmente é válido elucidar que a responsabilidade civil se baseia na necessidade de restaurar a situação anterior ao dano, buscando a recomposição da estabilidade jurídica que foi comprometida por um ato que infringe uma norma de conduta, seja por ação ou negligência. O objetivo da reparação é beneficiar não apenas a vítima diretamente prejudicada, mas também a sociedade como um todo, que tem suas expectativas de justiça atendidas. Nesse contexto, Venosa (2010) explica que os princípios da responsabilidade civil buscam restaurar um equilíbrio patrimonial e moral violado. Um prejuízo ou dano não reparado é um fator de inquietação social. Os ordenamentos contemporâneos buscam alargar cada vez mais o dever de indenizar, alcançando novos horizontes, a fim de que cada vez menos restem danos ressarcidos (VENOSA, 2010, p. 2).

Portanto, quando se vem a debater sobre a responsabilidade civil do Poder Público no tratamento de dados pessoais (sempre obter dados pessoais e não apenas dados), é nítido que a Lei Geral de Proteção de Dados Pessoais oferece um tratamento diferenciado ao Poder Público, visto que a LGPD vem adotar, como Poder Público, todos os entes previstos na Lei de Informação, sendo eles 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, e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios.

O tratamento de dados pessoais por pessoas jurídicas de direito público, é disposto no art. 23 da LGPD, observando-se:

> Art. 23 - O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, como objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público [...]. (BRASIL, 2018).

Logo, o artigo 23 da LGPD é fundamental para garantir que os órgãos públicos tratem os dados pessoais dos cidadãos de forma ética, transparente e responsável, respeitando os direitos fundamentais e contribuindo para a construção de uma sociedade mais justa e democrática. Desse modo, assim como as empresas privadas precisam ter uma finalidade objetiva para o tratamento do dado, o mesmo vale para o Poder Público, razão pela qual deve ser divulgada, em veículos de fácil acesso, a previsão legal, a finalidade, os procedimentos e

as práticas utilizadas para a execução do tratamento de dados pessoais, além disso, é necessária a indicação de um encarregado enquanto estiverem realizando essas operações. (MARINI, 2021).

Dessa forma, o Princípio da Finalidade presente no referido artigo, vem a fomentar que os dados pessoais devem ser coletados e tratados para finalidades específicas, explícitas e legítimas, informadas ao titular no momento da coleta. Na prática, os dados pessoais só podem ser coletados para uma finalidade determinada e clara, sendo que a empresa ou órgão público que coleta os dados deve informar o titular sobre a finalidade da coleta no momento em que os dados são fornecidos, sendo ressaltado que os dados coletados não podem ser utilizados para finalidades diferentes daquelas informadas ao titular, a menos que haja consentimento expresso do titular ou que a nova finalidade seja compatível com a original.

Com esses requisitos, verifica-se que a LGPD busca garantir não somente o Princípio da Finalidade, como também o da Transparência. Assim, é vedado ao Poder Público compartilhar os dados pessoais que têm acesso com entidades privadas. Excetua-se, porém, casos de execução descentralizada de atividade pública que exija a transferência, casos em que os dados forem de acesso público, quando houver previsão legal ou a transferência for respaldada em contratos, ou instrumentos congêneres; na hipótese da transferência objetivar exclusivamente a prevenção de fraudes, ou resguardar a segurança do titular dos dados, sendo vedado o tratamento para outras finalidades (art. 26, § 1º). (MARINI, 2021).

Logo, o Princípio da Transparência torna-se um dos pilares da Lei Geral de Proteção de Dados, garantindo aos titulares dos dados pessoais acesso a informações claras e precisas sobre como seus dados pessoais estão sendo tratados. Garantindo, em síntese, que os dados pessoais sejam tratados de forma ética e responsável. Diante disso, ao exigir que as empresas e órgãos públicos sejam transparentes sobre suas práticas, a LGPD empodera os titulares e contribui para a construção de uma sociedade mais justa e digital.

Após definidas as situações e os requisitos para o tratamento de dados pelo Poder Público, é importante destacar as exceções. A primeira delas diz respeito ao tratamento de dados pessoais sensíveis, que são dados pessoais que exigem um tratamento especial devido à sua natureza delicada e ao potencial de causar danos se tratados de forma inadequada, a exemplo de dados referentes à saúde, à opinião política ou convicção religiosa.

A lei protege situações que concernem exclusivamente a operações de tratamento de dados, isto é, aquelas “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" (art. 5º, X). Percebe-se pelo rol descritivo do que se entende por tratamento de dados, que inúmeras atividades que envolvem dados pessoais sofrerão a limitação e escrutínio da lei (MULHOLLAND, 2018).

Dessa forma, a LGPD deve vir a tratar tais dados a partir de um conjunto de regras específicas para garantir que esses dados sejam tratados de forma ética, transparente e segura.

Embora esses dados possam ser tratados e compartilhados pela Administração Pública para a execução de políticas públicas, sem a necessidade de consentimento, é imprescindível que a dispensa de consentimento seja tornada pública. Isso garante que os titulares dos dados sejam informados sobre a utilização de suas informações, como é visto no art. 11, § 2º da LGPD.

> Art. 11 - O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
>
> I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
>
> 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;
>
> § 2º Nos casos de aplicação do disposto nas alíneas "a" e "b" do inciso II do caput deste artigo pelos órgãos e pelas entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do caput do art. 23 desta Lei:

Dando ênfase às hipóteses de dispensa de consentimento no uso de dados pessoais o art. 7º da LGPD vem elucidá-los, como assim se observa:

> Art. 7º - O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
>
> I - mediante o fornecimento de consentimento pelo titular;
>
> II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
>
> III - 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;

> IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
>
> V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
>
> VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
>
> VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
>
> ~~VIII - para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;~~
>
> VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019).Vigência.
>
> IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
>
> X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Logo, em que pese a existência de dispensa de consentimento em determinadas hipóteses, o ideal é que seja dada ciência ao titular de dados sobre quais dados é necessária a coleta, como será o armazenamento, quais os tratamentos realizados, finalidades delimitadas, se haverá repasse dos dados à outra pessoa etc., sempre que possível. É claro que o controlador enquanto gestor dos dados também deve abster-se de impor burocracias e procedimentos desnecessários de consentimento do titular, atribuindo maior equilíbrio à relação jurídica estabelecida, seja ela consumerista, trabalhista ou qualquer outra que justifique o manuseio de dados pessoais. A intenção do consentimento trazido pela lei é proporcionar a proteção dos dados pessoais das pessoas físicas, impondo sanções e penalidades para motivar as empresas e demais pessoas que realizam o tratamento ao seu cumprimento. (MORAES, 2020).

Por fim, é relevante destacar as situações em que a Lei Geral de Proteção de Dados não se aplica, como nos casos de segurança pública, defesa nacional, segurança do Estado, ou em atividades relacionadas à investigação e repressão de crimes. Esses são casos de caráter estatal e que, pela sua não incidência, em que a administração pública se exime da

responsabilidade prevista na LGPD, porém deve respeitar todos os princípios constitucionais e previstos em demais legislações atinentes (ROSSO, 2019).

Dessa forma, em conclusão, a responsabilidade civil no tratamento de dados pelo Poder Público, à luz da Lei Geral de Proteção de Dados (LGPD), é um mecanismo essencial para garantir a segurança jurídica e a proteção dos direitos dos cidadãos. Embora o Poder Público tenha prerrogativas diferenciadas no tratamento de dados, como a dispensa de consentimento em certos casos, a exemplos do cumprimento de obrigação legal ou regulatória, pela administração pública, de políticas públicas previstas em lei ou regulamentos, estudos de órgãos de pesquisa, proteção da vida, tutela de saúde ou garantia de prevenção à fraude e à segurança do titular, se tornam exemplos desse caso.

De tal maneira, a administração pública deve sempre agir com transparência, informando os titulares sobre a utilização de seus dados e garantindo a finalidade pública dessas operações. Além disso, o compartilhamento de dados com entidades privadas é limitado, resguardando a proteção do titular, exceto em situações específicas previstas na lei. Assim, a LGPD busca equilibrar o interesse público e a proteção dos direitos individuais, reforçando a responsabilidade da administração pública em suas ações. Mesmo em casos de segurança pública ou defesa nacional, onde a LGPD não se aplica, o respeito aos princípios constitucionais e legais permanece indispensável, assegurando que os direitos fundamentais sejam preservados.

3.1 Regime da Responsabilidade Civil da Administração Pública em matéria de dados pessoais.

Como já elencado, os fundamentos legais da responsabilidade civil da administração pública em matéria de dados pessoais, decorrem prioritariamente da necessidade de proteger os direitos dos cidadãos em relação à privacidade e ao tratamento adequado de suas informações pessoais. No Brasil, tal responsabilidade é principalmente regida pela Constituição Federal, pela Lei Geral de Proteção de Dados (Lei nº 13.709/2018), pela Lei de Acesso à Informação (Lei nº 12.527/2011), além da própria base teológica que trata o assunto.

Inicialmente, é válido elencar que tanto a Constituição Federal, em seu art. 37, § 6º, quanto o Código Civil, em seu art. 43, tratam que a responsabilidade civil do estado é de regime objetivo. Nesse sentido, Carvalho Filho (2019), vem a ser claro ao explicar quais teorias fundamentaram a adoção do regime de responsabilidade civil objetiva pelo estado. O Estado tem maior poder e mais sensíveis prerrogativas do que o administrado. É realmente o sujeito jurídico, política e economicamente mais poderoso. O indivíduo, ao contrário, tem posição de

subordinação, mesmo que protegido por inúmeras normas do ordenamento jurídico. Sendo assim, não seria justo que, diante de prejuízos oriundos da atividade estatal, tivesse ele que se empenhar demasiadamente para conquistar o direito à reparação dos danos. Diante disso, passou-se a considerar que, por ser mais poderoso, o Estado teria que arcar com um risco natural decorrente de suas numerosas atividades: à maior quantidade de poderes haveria de corresponder um risco maior. Surge, então, a teoria do risco administrativo, como fundamento da responsabilidade objetiva do Estado. [...] (CARVALHO FILHO, 2019).

Carvalho Filho (2019) vem a ser claro, quando afirma que a Teoria do Risco Administrativo se torna um fundamento para o regime objetivo da responsabilidade do Estado. A Teoria do Risco Administrativo é um princípio fundamental do direito administrativo, que estabelece que o Estado é responsável pelos danos causados a terceiros no exercício de suas atividades, independentemente da existência de culpa por parte da administração pública. De acordo com essa teoria, o Estado assume o risco de eventuais danos decorrentes de suas atividades, e deve indenizar as vítimas por esses danos, mesmo que não tenha agido com culpa. Isso significa que o Estado deve arcar com os prejuízos causados a terceiros em decorrência das ações ou omissões da Administração Pública, inclusive em casos de danos causados por agentes públicos ou por coisas que estão sob sua guarda. (MACEDO VILELA, 2023).

Ademais, além da teoria do Risco Administrativo, constitui-se também como fundamento da responsabilidade objetiva do Estado, o Princípio da Repartição de Encargos. Portanto, que com o intuito de atenuar as dificuldades suportadas por aqueles prejudicados por condutas de agentes estatais, instituiu-se a responsabilidade objetiva do Estado. Nessa esfera, a teoria do Risco Administrativo e o Princípio da Repartição dos Encargos são mecanismos para garantir a justiça social e reduzir as disparidades entre o Poder Público e os cidadãos. (MARINI, 2021).

O Princípio da Repartição dos Encargos junto com a Teoria do Risco Administrativo funcionam como um alicerce da justiça social, como afirma Ancillotti (2024), alicerçada nos preceitos fundamentais da Constituição Federal, a responsabilidade objetiva do Estado estabelece o dever do Poder Público de indenizar danos causados a terceiros, independentemente da existência de culpa. Esse princípio, pedra angular da Teoria da Repartição dos Encargos sociais, visa garantir que os ônus decorrentes das intervenções estatais sejam distribuídos de forma justa e equilibrada por toda a sociedade, evitando que indivíduos ou grupos sejam desproporcionalmente prejudicados. (ANCILLOTTI, 2024).

Dessa forma, a responsabilização objetiva do Estado garante que, sempre que a Administração Pública cause um dano, seja por ação ou omissão, haja a obrigação de indenizar

os prejudicados, respondendo assim o Estado independente do ato que gerou prejuízo. Na mesma linha, expõe Ulhoa (2012):

> Não é relevante a questão da licitude ou ilicitude do ato causador do dano; a indenização será devida em qualquer hipótese pelo Estado. Note-se que, se houver ato ilícito (dolo ou culpa) por parte de seu agente, terá o Estado direito de regresso contra ele. Paga, então, ao prejudicado e recupera com o agente culpado o valor da indenização. [...] Para que o Estado se responsabilize objetivamente pelo dano, não se exige que o causador seja funcionário público efetivo ou comissionado. O preceito normativo menciona a responsabilidade das pessoas jurídicas de direito público pelos danos causados por seus agentes, conceito amplo que alcança toda e qualquer pessoa a serviço do Estado. Por outro lado, se o dano é provocado por quem não cumpre essa condição, o Estado não é responsabilizável. (ULHOA, 2012, p. 741).

Portanto, se a Administração Pública violar direitos individuais ao realizar o tratamento de dados, mesmo em situações não abrangidas pela LGPD, será responsável pelos danos causados, devendo indenizar os prejudicados, independentemente de culpa. Pinheiro (2018, p. 90), assevera que cabe à autoridade nacional garantir que medidas cabíveis e proporcionais sejam adotadas quando da violação do tratamento de dados pessoais nos órgãos públicos.

Por fim, no que tange aos fundamentos legais da responsabilidade civil da Administração Pública em matéria de dados pessoais, o art. 43 da LGPD vem a trazer aqueles que serão excluídos da responsabilidade civil dos agentes de tratamento, observando que:

> Art. 43 Os agentes de tratamento só não serão responsabilizados quando provarem:
>
> I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;
>
> II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou
>
> III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiros. (BRASIL, 2018).

Tais hipóteses podem também ser aplicadas à exclusão de responsabilidade do Poder Público, uma vez que rompem o nexo de causalidade, conforme diz Oliveira (2018), pois, de acordo com a Teoria do Risco Administrativo, adotada pelo art. 37, § 6.º, da CRFB, o

Estado pode se defender nas ações indenizatórias por meio do rompimento do nexo de causalidade, demonstrando que o dano suportado pela vítima não foi causado pela ação ou omissão administrativa. São causas excludentes do nexo causal: fato exclusivo da vítima, fato de terceiro e caso fortuito ou força maior. As causas excludentes decorrem da redação da referida norma constitucional que consagra a responsabilidade civil do Estado apenas pelos danos causados por seus agentes públicos, o que não ocorre nas hipóteses em que os danos são imputados à própria vítima, ao terceiro e aos eventos da natureza. Nessas situações não há ato ou fato administrativo que tenha causado o dano à vítima (OLIVEIRA, 2018, p. 797).

No que concerne à relação da responsabilidade civil com os Princípios da Necessidade e Finalidade, pode-se afirmar que há uma íntima ligação entre ambos, visto que, como já abordado, a Lei Geral de Proteção de Dados (LGPD) estabelece que os entes públicos têm o dever de tratar dados pessoais de forma lícita, leal e transparente, respeitando os direitos fundamentais de liberdade e privacidade. Além do mais, os Princípios da Necessidade e da Finalidade são pilares da LGPD e aplicam-se tanto à iniciativa privada quanto à Administração Pública.

Logo, se tratando do Princípio da Finalidade em relação à responsabilidade civil da Administração Pública, "[...] a violação dos princípios da necessidade e da finalidade especificamente no tratamento de dados pessoais resulta na responsabilidade civil do controlador, com base nos princípios gerais do Direito Civil, especialmente quando ocorre dano moral ou material ao titular dos dados" (SILVA, 2019, p. 142).

Ademais, a finalidade é o norte do tratamento de dados pessoais, sendo obrigatório o planejamento do objetivo antes de sua coleta. "Em caso de desvio, o controlador poderá ser responsabilizado civilmente, inclusive de forma objetiva, pelos danos causados ao titular" (GOMES, 2021, p. 95).

Dessa forma, a violação aos princípios da Necessidade e da Finalidade especificamente no tratamento de dados pessoais "[...] resulta na responsabilidade civil do controlador, com base nos princípios gerais do Direito Civil, especialmente quando ocorre dano moral ou material ao titular dos dados" (SILVA, 2019, p. 142). Nesse contexto, a responsabilidade civil da Administração Pública é acionada quando esses princípios e outros preceitos da LGPD são descumpridos, resultando em danos a terceiros, demonstrando a relação dos referidos princípios com a responsabilidade civil pública.

3.2 Responsabilidade Civil do controlador e do operador com base na LGPD.

Em síntese, a LGPD determina três figuras de agentes responsáveis pelo tratamento de dados, sendo eles o controlador, pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; o operador, pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador; e o encarregado, pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados. (MARINI, 2021).

É válido ressaltar que cada um desses agentes possui responsabilidades legais em relação aos titulares dos dados e à ANPD. Tanto o controlador quanto o operador tornam-se obrigados a manter registros das atividades de tratamento de dados pessoais realizadas, isso conforme está previsto no art. 36 da LGPD, observando-se que:

> Art. 36. As alterações nas garantias apresentadas como suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no inciso II do art. 33 desta Lei deverão ser comunicadas à autoridade nacional. (BRASIL, 2018).

Portanto, tal medida visa assegurar a transparência nas operações e permitir que a Autoridade Nacional de Proteção de Dados exerça seu controle. Ademais, a própria ANPD pode exigir que o controlador elabore um relatório de impacto à proteção de dados pessoais, incluindo dados sensíveis, para suas operações de tratamento, conforme o art. 37 da LGPD:

> Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse. (BRASIL, 2018).

Ademais, no que tange às obrigações, em especial as do controlador e do operador, é previsto no art.39 da LGPD, que:

> Art. 39. O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria. (BRASIL, 2018).

Portanto, segundo Pinheiro (2018), o artigo vem a estabelecer diretamente uma ligação entre a figura do controlador e a do operador, como se observa.

> "A regulamentação de proteção de dados pessoais tem o condão de estabelecer uma responsabilidade solidária do controlador para com o operador a partir do contrato entre eles, considerando que quem detém o consentimento do titular é o controlador e, portanto, continua a ser o que fica

> responsável pelo que ocorre no ciclo de vida dos dados pessoais na gestão e governança do negócio.” (PINHEIRO, 2018, p.98).

Dessa forma, quando se trata da questão da responsabilidade civil do controlador e do operador, elucida o art.42 da LGPD:

> Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.
> § 1º A fim de assegurar a efetiva indenização ao titular dos dados:
> I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;
> II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei (BRASIL, 2018).

Logo, a leitura do artigo revela que o operador e o controlador têm responsabilidades distintas em relação a eventuais danos causados. O operador só será responsabilizado de forma solidária quando não cumprir as obrigações legais ou desobedecer às instruções do controlador. Assim, qualquer violação cometida pelo controlador será motivo para sua responsabilização direta almejada pode ser atingida por outros meios menos gravosos ao titular de dados.

Por sua vez, os controladores dos dados sempre responderão pelo tratamento de dados. Isso ocorre, pois a LGPD em vários momentos estabelece obrigações específicas ao controlador, fazendo com que seja inviável a sua figura não estar envolvida no tratamento. A LGPD, ao adotar essas medidas, impossibilita que o operador se olvide de sua obrigação de tutelar os dados que estão em seu poder. (MARINI, 2021).

A responsabilidade solidária recai sobre o controlador e o operador quando o tratamento de dados for irregular. A irregularidade se configura no momento em que não se observa a legislação, não se adotando as medidas de segurança previstas, ou quando não se fornecer a segurança que o titular pode esperar, seja em relação ao modo pelo qual é realizado o tratamento; seja em relação ao resultado e os riscos ou as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado (art. 44). (MARINI, 2021).

No que se refere às vítimas, o *caput* do art. 42 utilizou o termo "outrem" para referir-se a elas, o que amplia o conceito de vítima para além do titular dos danos e se estende a qualquer pessoa que venha a sofrer um dano decorrente da violação da LGPD extensível até mesmo às pessoas jurídicas (BODIN MORAES e QUINELATO DE QUEIROZ, 2019).

Acrescenta-se que, como já pontuado no presente trabalho, o art. 43 da LGPD vem a detalhar sobre as possibilidades de que não haja responsabilidade dos agentes de tratamentos. Dessa maneira, de acordo com tais hipóteses, torna-se possível determinar o regime de responsabilidade civil adotado pela Lei Geral de Proteção de Dados.

Nessa linha, Bodin Moraes e Quinelato de Queiroz (2019) estabelecem que,

> [...] o sistema de responsabilidade civil da LGPD, previsto nos artigos 42 a 45, mostra-se especialíssimo, sendo talvez a principal novidade da lei, e reflete o disposto no inciso X do art. 6º da Lei que prevê o princípio da "responsabilização e prestação de contas, isto é, a demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas". (BODIN MORAES e QUINELATO DE QUEIROZ, 2019, p. 2). [16]

O legislador pretendeu não apenas mandar ressarcir, mas quer prevenir e evitar a ocorrência de danos. Assim, esta responsabilidade especial, à semelhança do que ocorre no Regulamento europeu, está articulada em torno de três noções fundamentais, que devem ser somadas: i) dano; ii) violação da legislação de proteção dos dados por parte do controlador e/ou operador e iii) reparação. Com efeito, o regime demanda que o dano seja resultante de violação da LGPD e que tenha sido causado por um agente de tratamento dos dados para então impor a obrigação de ressarcir a parte lesada. (BODIN MORAES e QUINELATO DE QUEIROZ, 2019).[17]

Dessa maneira, conforme apontado pelos autores, diante da necessidade de se comprovar, além do dano e autoria, a violação da legislação, entende-se que a LGPD adotou o regime de responsabilidade subjetiva. Entretanto, denota-se que não foi o regime comum e sim o regime de responsabilidade subjetiva com culpa presumida. (MARINI, 2021).

Como se observa, [...], no entanto, a responsabilidade subjetiva com presunção de culpa distingue-se, pois, nesse caso, porque a culpa deve estar presente como requisito,

---

[16] *LGPD: um novo regime de responsabilização civildito proativo*. Disponível em Editorial civilística.com || a. 8. n. 3. 2019 |.

[17] *LGPD: um novo regime de responsabilização civildito proativo*. Disponível em Editorial civilística.com || a. 8. n. 3. 2019 |.

havendo apenas uma inversão do ônus da prova. A culpa presumida refere-se à transgressão de um dever imposto por lei ou regulamento, razão pela qual a doutrina e a jurisprudência, por vezes, adotam o termo culpa contra a legalidade." (VENOSA, 2018, p. 487).

Portanto, ainda é necessário que haja a comprovação de culpa para configurar a responsabilidade. No entanto, ocorre uma flexibilização de produção de provas no processo. O § 2º do art. 42 da LGPD ao estabelecer que o juiz poderá inverter o ônus da prova a favor do titular dos dados, adota a culpa presumida, pois considera a hipossuficiência da vítima para produção de provas e presume que a causa do dano adveio de uma transgressão à Lei Geral de Proteção de Dados. (MARINI, 2021).

Outrossim, conforme preceitua o art. 45 [...] as hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente. Desse modo, em alguns casos de violação, a responsabilidade civil será aplicada de acordo com a legislação consumerista. (PINHEIRO, 2018).

Nesse contexto, em suma, a LGPD define três agentes responsáveis pelo tratamento de dados: o controlador, que toma as decisões; o operador que executa o tratamento em nome do controlador; e o encarregado, que atua como intermediário entre os agentes e a ANPD. A lei impõe a esses agentes a obrigação de manter registros das operações de tratamento e prevê a responsabilidade civil por danos causados no tratamento de dados. O controlador é sempre responsável, enquanto o operador responde solidariamente se descumprir obrigações legais ou instruções. A LGPD também adota um regime de responsabilidade subjetiva com presunção de culpa, facilitando a inversão do ônus da prova em favor do titular.

3.3. Divergências doutrinárias sobre o regime da Responsabilidade civil da Administração Pública no tratamento de dados pessoais.

A Lei Geral de Proteção de Dados, em seus artigos 42 a 45, vem a estabelecer regras referentes à responsabilidade civil dos agentes de tratamento de dados pessoais, trazendo à tona, um debate sobre o regime da responsabilidade civil da Administração Pública, sendo de um lado uma responsabilidade objetiva e, de outro lado, uma responsabilidade subjetiva. Tal discussão vem a envolver diferentes interpretações sobre a extensão da proteção de dados e o papel da Administração Pública.

Inicialmente, conforme exposto por Gisela Sampaio e Rose Meireles (2019),a LGPD adotou claramente a teoria subjetiva da responsabilidade civil, devendo haver a prova da conduta culposa do agente de tratamento na ocasião do dano, por sua vez fundamentada (i) na omissão na adoção de medidas de segurança para o tratamento adequado dos dados ("quando

não fornecer a segurança que o titular dele pode esperar,"); (ii) no descumprimento das obrigações impostas na lei ("em violação à legislação de proteção de dados pessoais" ou "quando deixar de observar a legislação"). (SAMPAIO e MEIRELES, 2019).[18]

As autoras indicam que o Capítulo VI da LGPD (artigos 46 a 54) - que trata de standards de conduta a serem seguidos pelos agentes de tratamento de dados para a segurança, sigilo, boas práticas e governança de dados - seria também o fundamento para o reconhecimento da responsabilidade subjetiva. Em complementação ao entendimento das autoras, na análise das excludentes de responsabilidade do artigo 43, da LGPD, o inciso II pareceria indicar a adoção de uma excludente tipicamente relacionada às hipóteses de responsabilidade civil subjetiva ao estatuir que só não serão responsabilizados se, ainda que exista o dano, não houver violação da legislação de proteção de dados. A violação da lei, para as autoras, seria elemento subjetivo da obrigação de indenizar e indicaria a conduta culposa do agente de tratamento de dados. Assim, não haverá obrigação de indenizar quando o agente de tratamento de dados tiver demonstrado que "[...] observou o standard esperado e, se o incidente ocorreu, não foi em razão de sua conduta culposa [...].” Em resumo, sustentam as autoras que a LGPD adota a teoria subjetiva da responsabilidade civil, calcada em duas "dicas" deixadas pelo legislador: (i) no artigo 42, quando o legislador faz menção a medidas de segurança; (ii) no art. 43, II, quando o legislador estabelece excludente de ilicitude referente ao cumprimento das normas da LGPD. (MULHOLLAND, 2020).

Ainda vale elencar que, no lado dos defensores da responsabilidade subjetiva, há aqueles que argumentam que se baseiam no fato de a estrutura da LGPD estar toda pautada na criação de deveres. De fato, não se justifica nem do ponto de vista lógico, nem do jurídico o legislador criar uma série de deveres de cuidado se não for para implantar um regime de responsabilidade subjetiva. Se o que se pretende é responsabilizar os agentes independentemente de culpa, seria ocioso criar deveres a serem seguidos, tampouco responsabilizá-los quando tiverem cumprido perfeitamente todos esses deveres. (FRAZÃO e CUEVA, 2022). apud

Entretanto, pode-se notar que em posição diversa estão Danilo Doneda e Laura Mendes (2018) *apud* (Mulholland, 2020) que consideram que a atividade de tratamento de dados encerra um risco intrínseco, na medida em que há uma potencialidade danosa considerável em caso de violação desses direitos, que se caracterizam por sua natureza de

[18]*Término do Tratamento de Dados.* Disponível em https://giselasampaio.com.br//wp-content/uploads/2021/12/23.-Termino-do-Tratamento-de-Dados.pdf.

direito personalíssimo e de direito fundamental. Partem os autores da constatação de que a legislação de proteção de dados tem como um dos seus principais fundamentos a diminuição de riscos de dano. Tanto é assim que a lei adota como princípio, no artigo 6º, III, o da necessidade que impõe a "limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados". Estas considerações a respeito da finalidade da lei e dos princípios por ela adotados (necessidade, minimização, responsabilidade e prestação de contas, dentre outros), levam os autores a concluir que o legislador optou por um regime de responsabilidade objetiva, vinculando o exercício da atividade de tratamento de dados pessoais a um risco inerente, potencialmente causador de danos a seus titulares. (MULHOLLAND, 2020).

Ainda vale elencar que, corroborando esse entendimento de uma responsabilidade civil objetiva, as doutrinas que apoiam tal lado usam, como argumento, as analogias da LGPD com o Código de Defesa do Consumidor. Portanto, de fato, a LGPD tem mesmo várias disposições inspiradas no Código de Defesa do Consumidor, a exemplo da possibilidade de o juiz inverter o ônus da prova (art. 42, § 2º, da LGPD). Além disso, o próprio texto do art. 43 da LGPD assemelha-se à redação do art. 12, § 3°, do Código de Defesa do Consumidor (e essa, por sua vez, é muito parecida com a do art. 14, § 3°, do Código de Defesa do Consumidor. (FRAZÃO e CUEVA, 2022).

De fato, há muitas semelhanças com o Código de Defesa do Consumidor, começando pelo *caput* do art. 43 da LGPD, que é bastante similar ao § 3° dos arts. 12 e 14 do CDC, pois ambos utilizam uma redação negativa ("só não serão responsáveis quando"). O inciso III do art. 43 da LGPD é quase idêntico ao inciso III, § 3°, do art. 12 do CDC, e o inciso I do art. 43 da LGPD parece claramente inspirado no inciso I, § 3°, do art. 12 do CDC. Portanto, a analogia com o Código de Defesa do Consumidor torna-se, portanto, compreensível, tanto mais se se considerar a assimetria informacional entre os titulares dos dados e os agentes de tratamento. Comparando-se os dois dispositivos (art. 43 da LGPD e art. 12 do Código de Defesa do Consumidor), a diferença fundamental encontra-se no inciso II, cuja análise será feita mais à frente, imprescindível para demonstrar a diversidade de regimes. A favor da responsabilidade objetiva, argumenta-se, ainda, que o escopo da LGPD foi limitar o tratamento dos dados para diminuir o risco de vazamentos, considerando que o próprio tratamento de dados, em si, apresenta "risco intrínseco aos seus titulares". (FRAZÃO e CUEVA, 2022).

Dessa maneira, voltando ao que tange sobre os artigos 42 a 45 da LGPD, que tratam diretamente sobre as regras referentes à responsabilidade civil dos agentes de tratamento de

dados pessoais, conclui-se, portanto, que, apesar do uso de expressões diversas em sua redação, tanto o artigo 42, quanto o artigo 44, da LGPD, adotam o fundamento da responsabilidade civil objetiva, impondo aos agentes de tratamento a obrigação de indenizar os danos causados aos titulares de dados, afastando destes o dever de comprovar a existência de conduta culposa por parte do controlador ou operador. Fundamenta esta conclusão o fato de que a atividade desenvolvida pelo agente de tratamento é evidentemente uma atividade que impõe riscos aos direitos dos titulares de dados, que, por sua vez, são intrínsecos, inerentes à própria atividade e resultam em danos a direito fundamental. Ademais, tais danos se caracterizam por serem quantitativamente elevados e qualitativamente graves, ao atingirem direitos difusos, o que, por si só, já justificaria a adoção da responsabilidade civil objetiva, tal como no caso dos danos ambientais e dos danos causados por acidentes de consumo. (MULHOLLAND, 2020).

Ainda se torna válido elencar uma terceira corrente de pensamento representada por Bodin Moraes e Quinelato de Queiroz (2019), na qual vêm a afirmar que a LGPD legitima a chamada teoria reativa ou proativa da responsabilidade civil. A teoria sugere uma perspectiva proativa sobre a responsabilidade civil, destacando a necessidade de que os agentes de tratamento de dados adotem medidas preventivas para evitar danos. A dúvida, nesse contexto, seria vista como uma última opção, reservada apenas para situações específicas em que as medidas preventivas. Dessa forma, para os autores "a proteção da intimidade por meio da mera não interferência na esfera individual dá lugar a uma abordagem positiva e proativa, garantindo ao titular pleno conhecimento das formas de tratamento, finalidade e destino de seus dados" (BODIN MORAES e QUINELATO DE QUEIROZ, 2019, p. 5).

A responsabilidade proativa está prevista no artigo 6º, inciso X, da Lei Geral de Proteção de Dados (LGPD) e refere-se ao princípio da responsabilização e prestação de contas. Esse princípio exige que os agentes envolvidos no tratamento de dados pessoais comprovem a eficácia das medidas adotadas para assegurar o cumprimento das normas de proteção de dados. Ou seja, além de implementar essas medidas, os responsáveis precisam demonstrar de forma clara que elas estão funcionando adequadamente. De acordo com Bodin de Moraes e Quinelato de Queiroz (2019), esse conceito enfatiza a necessidade de uma postura ativa na proteção de dados, antecipando-se a possíveis problemas e garantindo a transparência no processo de conformidade.

> Trata-se do conceito de ‘prestação de contas’. Esse novo sistema de responsabilidade, que vem sendo chamado de ‘responsabilização ativa’ ou ‘proativa’,14 encontra-se indicado no inciso X do art. 6º, que determina às empresas não ser suficiente cumprir os artigos da lei; será necessário também

> demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, a eficácia dessas medidas. Portanto, não descumprir a lei não é mais suficiente; é preciso 'proativamente' prevenir a ocorrência de danos. (BODIN MORAES e QUINELATO DE QUEIROZ, 2019, p. 5).

Portanto, Bodin Moraes e Quinelato de Queiroz (2019) argumentam que as ações necessárias não devem focar apenas nas peças de danos já causados, mas devem ir além, buscando também prevenir que esses danos aconteçam. "Ao contrário, é necessário ampliar sua abrangência para além do âmbito estritamente jurídico, buscando antecipar-se e prevenir a ocorrência dos danos." (LOPEZ, 2010, p. 1230).

Nesse contexto, as divergências doutrinárias refletem a busca por um equilíbrio entre garantir a proteção dos dados pessoais e evitar uma sobrecarga de responsabilidade à Administração Pública. Embora a responsabilidade objetiva seja predominante, há espaço para a aplicação da responsabilidade subjetiva em contextos específicos, conforme as nuances do caso e as particularidades da atividade administrativa.

4 RESPONSABILIDADE CIVIL DO PODER PÚBLICO POR VAZAMENTO DE DADOS PESSOAIS: UM ESTUDO DE CASO DA AÇÃO CIVIL PÚBLICA Nº 5028572-20.2022.4.03.6100.

Inicialmente, é válido apontar que a visão apresentada por Alvino Lima (1999), sobre a responsabilidade civil observa que:

> Partimos, como diz Ihering, do período em que o sentimento de paixão predomina no direito; a reação violenta perde de vista a culpabilidade, para alcançar tão somente a satisfação do dano e infligir um castigo ao autor do ato lesivo. Pena e reparação se confundem; responsabilidades penal e civil não se distinguem. A evolução operou-se, consequentemente, no sentido de se introduzir o elemento subjetivo da culpa e diferenciar a responsabilidade civil da penal. E muito embora não tivesse conseguido o direito romano libertar-se inteiramente da ideia da pena, no fixar a responsabilidade aquiliana, a verdade é que a ideia de delito privado, engendrando uma ação penal, viu o domínio da sua aplicação diminuir, à vista da admissão, cada vez mais crescente, de obrigações delituais, criando uma ação mista ou simplesmente reipersecutória. A função da pena transformou-se, tendo por fim indenizar, como nas ações reipersecutórias, embora o modo de calcular a pena ainda fosse inspirado na função primitiva da vingança; o caráter penal da ação da lei Aquília, no direito clássico, não passa de uma sobrevivência. (ALVINO LIMA, 1999, p. 26-27).

Logo, de forma análoga, a responsabilidade civil está profundamente enraizada na sociedade, sendo uma manifestação natural do conceito de justiça. O provérbio popular "olho por olho, dente por dente" reflete uma percepção moral estabelecida pela coletividade, sugerindo que o infrator deve ser responsabilizado de maneira proporcional ao dano causado, correspondendo à gravidade de suas ações. Portanto, conforme preponderado pelo Código Civil, a responsabilidade civil é o dever jurídico de reparação aos danos sofridos que sobrevieram de um ato ilícito praticado por outro, conforme expõe-se abaixo:

> Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo.(BRASIL, 2002).
>
> Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito. (BRASIL, 2002).
>
> Art. 187. Também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes (BRASIL, 2002).

Portanto, o Código Civil, em seu artigo 927, estabelece a obrigação de reparar o dano causado a outra pessoa em decorrência de um ato ilícito. Já os artigos 186 e 187 definem o que se caracteriza como "ato ilícito", abrangendo tanto os danos patrimoniais quanto os danos morais, que se referem a prejuízos que vão além dos financeiros, atingindo aspectos emocionais ou psicológicos.

Como já exposto, a responsabilidade civil é classificada em diferentes tipos, levando em consideração, primeiramente, a existência de culpa e, em seguida, a natureza da norma jurídica violada. Assim, o conceito de responsabilidade civil sugere que, quando alguém comete um ato ilícito, causando dano a outrem e violando uma norma legal, surge para o infrator a obrigação de indenizar a vítima, independentemente de ter agido com culpa ou intenção (dolo).

Portanto, voltando para o lado do vazamento de dados pessoais, é extremamente necessário debater que tal ato pode produzir uma série de prejuízos para todas as pessoas afetadas, de forma direta ou indiretamente. Pode-se exemplificar potenciais resultados dos vazamentos de dados pessoais como a fraude financeira, o roubo de identidade, violação da privacidade, prejuízos à saúde e/ou, até mesmo, assédio e perseguição, além de possíveis danos morais, sociais e materiais.

Dessa forma, resumidamente, pode-se expor que a responsabilidade civil do Poder Público por vazamento de dados pessoais é um tema de crescente relevância, especialmente após a promulgação da Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil. A LGPD estabelece normas para o tratamento de dados pessoais e impõe sanções administrativas e civis em caso de violação. No contexto da responsabilidade do poder público, o Estado pode ser responsabilizado com base no regime da responsabilidade objetiva, conforme o artigo 37, § 6º da Constituição Federal, que estabelece a obrigação de reparar danos causados por seus agentes, independentemente de dolo ou culpa.

Tal relevância e atualidade são expostas por meio da Ação Civil Pública nº 5028572-20.2022.4.03.6100, visto ser um exemplo concreto dessa aplicação da responsabilidade civil. Essa ação foi movida em razão de um vazamento de dados pessoais envolvendo uma entidade pública, com a alegação de que a negligência na segurança dos dados permitiu a divulgação indevida de informações sensíveis de cidadãos.

Em síntese, a ação envolveu o vazamento de dados pessoais de cidadãos em sistemas de uma instituição pública. A acusação argumenta que o órgão responsável pela gestão dos dados não implementou as medidas de segurança adequadas previstas pela LGPD, como

criptografia e controles de acesso. O vazamento expôs informações sensíveis, potencialmente sujeitando os titulares dos dados a fraudes e outros prejuízos.

Portanto, tal ação civil pública reflete a seriedade com que a LGPD está sendo aplicada no Brasil, tanto em âmbito privado quanto público. Decisões favoráveis aos titulares dos dados tendem a reforçar a necessidade de que órgãos públicos invistam mais em *compliance* de segurança da informação, alinhando suas práticas com os princípios da LGPD, como a segurança, a prevenção e a transparência.

4.1. Vazamento de dados pessoais e a responsabilidade civil do poder público.

Como já exposto no presente trabalho, o vazamento de dados pessoais pode resultar em uma ampla gama de consequências negativas para as pessoas afetadas, tanto de maneira direta quanto indireta. Entre os possíveis impactos estão fraudes financeiras, roubos de identidade, invasões de privacidade, consequências de saúde, além de assédio, perseguição e prejuízos morais, sociais e materiais. A fraude financeira, por exemplo, envolve o uso indevido de informações para a realização de operações ilícitas.

Inicialmente, no que tange à fraude financeira, trata-se de um crime que envolve o emprego de ações fraudulentas para obter benefícios financeiros de maneira ilícita, causando prejuízos a indivíduos, empresas ou instituições financeiras. O roubo de identidade é uma prática criminosa correlata, na qual informações pessoais de alguém são obtidas e utilizadas de forma indevida, com o propósito de cometer fraudes ou outros delitos financeiros em nome da vítima como afirma Silva e Almeida (2021), a apropriação indevida de dados pessoais permite que fraudadores simulam identidades para obtenção de benefícios financeiros ilícitos, prejudicando diretamente as vítimas, que prejudicam o comprometimento de sua estabilidade econômica". (SILVA e ALMEIDA, 2021).

Vale elencar que a violação de privacidade de dados pessoais, por sua vez, também é um crime previsto no ordenamento jurídico brasileiro. Como já demonstrado, a Lei Geral de Proteção de Dados (LGPD) (Lei nº 13.709/2018) define e regulamenta o tratamento de dados pessoais no Brasil. Uma vítima de vazamento de dados pode sofrer com prejuízos à saúde e bem-estar, além de assédio e/ou perseguição, incluindo possíveis danos à privacidade, discriminação e ameaças. (ULHÔA e NASCIMENTO, 2023).

Ademais, outros potenciais prejuízos à vítima de vazamento de dados pessoais são os danos morais, sociais e materiais. Citando um caso concreto recente, o Ministério Público Federal (MPF) determinou, em setembro de 2023, que cerca de 4.000.000 (quatro milhões) de pessoas fossem indenizadas em R$ 15.000,00 (quinze mil reais) cada, por terem sofrido um

vazamento massivo de dados pessoais no segundo semestre do ano anterior. “Esses dados violados pairam no registro e no banco de dados de incontáveis instituições, assim como em poder de terceiros que, facilmente, poderão fazer uso maléfico e fraudulento dessas informações, em franco prejuízo material, moral e social desses cidadãos”, comentou a procuradora da República Karen Louise Jeanette Kahn (MPF, 2023). (ULHÔA e NASCIMENTO, 2023).

Dessa forma, nota-se que os danos decorrentes de um vazamento de dados pessoais podem ser tanto materiais quanto morais. Danos materiais envolvem, por exemplo, a utilização fraudulenta de dados vazados para a prática de crimes financeiros, causando prejuízos patrimoniais diretamente às vítimas. Já os danos morais incluem o constrangimento e a violação do direito à privacidade dos cidadãos afetados. De acordo com Santos e Rodrigues (2020), o vazamento de dados sensíveis, como informações financeiras ou de saúde, pode causar danos irreparáveis à imagem e à segurança do titular dos dados, gerando um direito à indenização por danos morais, especialmente quando o órgão público falha em proteger essas informações. (SANTOS e RODRIGUES, 2020).

Vale ressaltar novamente que, no caso de um vazamento, além das obrigações de reparar os danos causados, o poder público tem o dever de adotar medidas preventivas para evitar a reprodução do evento. Isso inclui o fortalecimento dos sistemas de segurança, o treinamento de pessoal e a criação de políticas internas de proteção de dados. A LGPD, em seu artigo 6º, inciso X, também estabelece o princípio da responsabilização e prestação de contas que obriga os parâmetros de dados a demonstrar a eficácia das medidas de proteção inovadoras. Nesse contexto, Bodin Moraes e Quinelato de Queiroz (2019) afirmam que “o poder público deve adotar uma postura proativa na proteção dos dados que administra, utilizando tecnologia e protocolos robustos para evitar incidentes de segurança e demonstrar a conformidade com as normas de proteção de dados.” (BODIN MORAES e QUINELATO DE QUEIROZ, 2019

Em conclusão, em casos de vazamento de dados, o Estado tem a responsabilidade de adotar medidas preventivas e reativas para proteger os direitos dos titulares e mitigar os danos. A Administração Pública pode ser responsabilizada de forma objetiva, de acordo com o artigo 37 da Constituição Federal e o artigo 927 do Código Civil, o que dispensa a necessidade de comprovação de culpa. (CONJUR, 2021). Logo, o vazamento de dados pessoais geridos por órgãos públicos impõe uma série de responsabilidades ao Estado tanto pela necessidade de reparar os danos causados aos cidadãos quanto pela obrigação de prevenir novas falhas. A responsabilidade civil objetiva do Poder Público e as exigências da LGPD reforçam a

importância de uma governança eficaz de dados, que envolve tanto a segurança tecnológica quanto a transparência no tratamento das informações pessoais dos cidadãos.

4.2 O papel da ANPD na hipótese de vazamento de dados pessoais pelo poder público.

Introdutoriamente, conforme o artigo 55-A da LGPD, a ANPD, órgão autônomo vinculado à Presidência da República, detém a competência para exercer a regulação e a fiscalização da lei. Essa estrutura garante a independência técnica e decisória da autoridade, assegurando a efetividade da proteção de dados pessoais no país. Portanto, a ANPD é responsável por zelar pela proteção dos dados pessoais e garantir que tanto o setor privado quanto o público cumpram as disposições legais dispostas pela LGPD. No caso de vazamento de dados pessoais pelo Poder Público, a ANPD exerce suas funções de fiscalização, orientação e aplicação de avaliações.

O art. 55-J da LGPD, em especial os incisos I, III, IV e XI, vem a dialogar sobre a autoridade pode iniciar procedimentos administrativos para apurar as situações do incidente, verificar a conformidade dos agentes públicos com as medidas de proteção relevantes pela lei, e solicitar informações e documentos para verificar a ocorrência e a gravidade do vazamento, observa-se:

> Art. 55-J. Compete à ANPD:
>
> I - zelar pela proteção dos dados pessoais, nos termos da legislação;
>
> [...]
>
> III - elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade;
>
> IV - fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;
>
> [...]
>
> XI - solicitar, a qualquer momento, às entidades do poder público que realizem operações de tratamento de dados pessoais informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico

> complementar para garantir o cumprimento desta Lei. (BRASIL, 2018).

Portanto, segundo Nalin e Santarém (2020), a atuação da ANPD no setor público é de vital importância, especialmente na medida em que o Poder Público, para lidar com volumes significativos de dados sensíveis, precisa de maior controle e rigor na aplicação das normas de segurança de dados. (NALIM e SANTARÉM, 2020).

Dessa forma, a ANPD adota uma abordagem proativa, priorizando a orientação e a prevenção. A fiscalização e a aplicação de sanções são medidas complementares, utilizadas apenas em casos de descumprimento persistente da LGPD. Além disso, a ANPD desempenha um papel importante na disseminação de boas práticas e no esclarecimento de dúvidas sobre o tratamento de dados pessoais." (NALIM e SANTARÉM, 2020).

Vale ressaltar que, em caso de vazamento de dados, a ANPD tem o poder de aplicar medidas administrativas previstas no artigo 52 da LGPD. No entanto, o regime sancionatório aplicado ao poder público é mais flexível do que o setor privado, já que os prejuízos financeiros, como a aplicação de multas, não se aplicam diretamente aos órgãos públicos (BRASIL, 2018). Portanto, segundo Moraes (2020), "embora a ANPD não possa aplicar multas diretamente ao poder público, ela tem o dever de garantir que os órgãos que tratam dados pessoais adotem todas as medidas possíveis para corrigir falhas e prevenir novos vazamentos." (MORAES, 2020). A aplicação de avaliações pela ANPD visa, sobretudo, a correção de condutas e a adoção de medidas para a segurança dos dados tratados pelos entes públicos.

No mesmo viés, Ulhôa e Nascimento (2023), vem a acrescentar que as sanções que podem ser aplicadas pelo descumprimento da LGPD vão desde advertência até multa, que pode chegar a R$50 milhões por infração. Vale ressaltar que as sanções aplicadas pela ANPD são apenas e tão somente administrativas. Portanto, caso o órgão regulador identifique uma possível infração penal, o que constituiria crime, a mesma autoridade deve comunicar ao Poder Judiciário.

Nesse contexto, é válido analisar as decisões tomadas pela ANPD em casos práticos de vazamento de dados. Inicialmente, o Processo nº 00261.001886/2022-51, detalha um incidente que resultou no vazamento de dados pessoais da Secretaria de Estado de Saúde de Santa Catarina (SES/SC). No referido processo, houve um vazamento de dados da lista de espera do SUS em Santa Catarina, afetando cerca de 48 mil pessoas. Os dados vazados incluíam informações pessoais sensíveis como nome, CPF, endereço e dados médicos. Além disso, a SES/SC demorou a notificar a ANPD e os titulares dos dados sobre o incidente. As medidas de

segurança e as ações para mitigar os danos foram consideradas insuficientes pela ANPD, vindo a descumprir diversas determinações da ANPD, como a apresentação de um relatório de impacto à proteção de dados e a comunicação individual aos titulares afetados.

Dessa forma, no Relatório de Análise da Dosimetria de Sanções da SES/SC, nota-se que a ANPD vem a classificar as infrações cometidas pela SES/SC, sendo que a não apresentação do RIPD fora classificado como leve. Entretanto, o atraso na comunicação aos titulares, sistema inadequado e a não apresentação de documentos, foram classificados como infrações graves. Vale evidenciar que tais classificações são consideradas com base na natureza dos dados envolvidos, o impacto aos titulares e a falta de colaboração da SES/SC, não sendo sujeito a multa o órgão público, visto a sua natureza.

Entretanto, houve sanções aplicadas. Entre elas, a advertência para todas as infrações, considerando que a SES/SC já havia tomado medidas para corrigir as falhas e que a aplicação de multas não é permitida para órgãos públicos. Ademais, foram impostas medidas corretivas, como a manutenção de um aviso sobre o incidente no site da SES/SC por 90 dias e a comunicação individual aos titulares identificados.

Logo, é válido apresentar a conclusão do Processo nº 00261.001886/2022-51, visando analisar o enquadramento legal sofrido e as infrações cometidas pelo órgão público, conforme se observa:

> CONCLUSÃO:
>
> 8.1. Ante o exposto, considerando que o conjunto probatório dos autos demonstra que autoria e materialidade restam devidamente comprovadas nos autos, e que os fatos descritos correspondem às infrações tipificadas pelos enquadramentos indicados no ANPD - Auto de Infração 9 (SEI nº 3617432), conclui-se pelas seguintes recomendações:
>
> 8.1.1. Por violação ao art. 38 da LGPD, pela aplicação da sanção de ADVERTÊNCIA à SES/SC, sem a imposição de medida corretiva;
>
> 8.1.2. Por violação ao art. 48 da LGPD, pela aplicação da sanção de ADVERTÊNCIA à SES/SC, com imposição de medida corretiva, nos termos do [item 7.19] e do [item 7.20], conforme disposto no art. 52 da LGPD c/c o artigo 9º inciso II do Regulamento de Dosimetria e Aplicação de Sanções Administrativas;
>
> 8.1.3. Por violação ao art. 49 da LGPD, pela aplicação da sanção de ADVERTÊNCIA à SES/SC, sem a imposição de medida corretiva;

> 8.1.4. Por violação ao art. 5º do Regulamento de Fiscalização, pela aplicação da sanção de ADVERTÊNCIA à SES/SC, sem a imposição de medida corretiva;
>
> 8.2. Por fim, é importante salientar que a classificação das infrações, a definição das sanções (inclusos agravantes e atenuantes) e a adoção de medidas corretivas restringem-se às circunstâncias deste caso.

Dessa forma, as decisões da ANPD vieram a demonstrar de forma clara uma demonstração em aplicar o regime de responsabilidade civil da Administração Pública aos casos de violação da LGPD. A autoridade tem considerado a necessidade de responsabilizar os entes públicos pelos danos causados aos titulares de dados, inclusive quando a violação se deu por omissão ou negligência. Como já visto no presente trabalho, o regime de responsabilidade civil da Administração Pública objetiva é adotado em regra, em muitos dos casos, significando que a comprovação do dano e do nexo causal entre a conduta ilícita e o dano são suficientes para a responsabilização, dispensando a comprovação de culpa.

Ademais, a autoridade tem considerado a necessidade de responsabilizar os entes públicos pelos danos causados aos titulares de dados, inclusive quando a violação se deu por omissão ou negligência. Muitas das medidas da ANPD frente às suas decisões, como há o exemplo do caso exposto, vem a impor multas, determinar medidas corretivas para sanar as irregularidades encontradas e até mesmo responsabilizar individualmente os agentes públicos responsáveis pelas violações da LGPD.

Nesse contexto, o caso da SES/SC demonstra a importância da LGPD e a necessidade de que os órgãos públicos e as empresas cumpram as suas obrigações em relação à proteção de dados pessoais, provando assim que a ANPD tem um papel multifacetado nos casos de vazamento de dados relacionados ao poder público. Além de fiscalizar e investigar os incidentes, ela tem a função de orientar os órgãos públicos para garantir a conformidade com as normas da LGPD. A aplicação de avaliações visa tanto a garantia dos danos causados quanto à correção das falhas institucionais, reforçando a importância da adoção de medidas preventivas e proativas para a proteção de dados pessoais.

4.3 Análise da Ação Civil Pública nº 5028572-20.2022.4.03.6100.

A Ação Civil Pública nº 5028572-20.2022.4.03.6100 é uma ação movida pelo Instituto Brasileiro de Defesa da Proteção de Dados Pessoais, Compliance e Segurança da Informação Sigilo em face da União, Caixa Econômica Federal, Dataprev e a Autoridade

Nacional de Proteção de Dados (ANPD) devido a um suposto vazamento massivo de dados de beneficiários do Auxílio Brasil.

O Instituto narra, em síntese, que "como associação sem fins lucrativos, que trabalha em defesa da proteção de dados pessoais dos TITULARES DE DADOS, teve notícia, que, em 24.10.2022, houve o vazamento de dados em massa de mais de 4.000.000 (quatro milhões) de TITULARES DE DADOS, através de correspondentes bancários, contratados pelos RÉUS, que acessaram dados de beneficiários do AUXÍLIO BRASIL, programa governamental de renda mínima para pessoas mais pobres." (AÇÃO CIVIL PÚBLICA nº 5028572-20.2022.4.03.6100).

O vazamento ocorreu a partir de bancos de dados mantidos pela Caixa, União e Dataprev. A maioria das vítimas recebia o Auxílio Brasil e, às vésperas da eleição presidencial de 2022, passou a contar com larga porcentagem do benefício para a contratação de crédito consignado. Os dados pessoais divulgados ilegalmente acabaram nas mãos de correspondentes bancários, que utilizam as informações para o oferecimento dos empréstimos e de outros produtos financeiros. (AÇÃO CIVIL PÚBLICA nº 5028572-20.2022.4.03.6100).

Logo, para o MPF, o fato de o vazamento ocorrer em empresas e órgãos públicos aos quais milhões de brasileiros confiaram a proteção de seus dados torna o caso ainda mais grave. "Esses dados violados pairam no registro e no banco de dados de incontáveis instituições, assim como em poder de terceiros que, facilmente, poderão fazer uso maléfico e fraudulento dessas informações, em franco prejuízo material, moral e social desses cidadãos", destacou a procuradora da República Karen Louise Jeanette Kahn. (AÇÃO CIVIL PÚBLICA nº 5028572-20.2022.4.03.6100).

Portanto, vale ressaltar que a notificação dos titulares, a divulgação pública, a remoção dos dados da internet, a auditoria da ANPD, suspensão de créditos consignados, a indenização por danos morais, além de outras medidas, foram os pedidos pleiteados pelo réu. Ademais, no Relatório Processual do Juiz Federal Marco Aurélio de Mello Castrianni, é relatado que o pedido de tutela de urgência que visava medidas imediatas fora indeferido, além da apresentação das defesas das partes e o requerimento de perícia feito pelo Ministério Público Federal, visando a identificação da origem dos vazamentos.

Dessa forma, passado o relatório inicial, o Juiz Federal Marco Aurélio de Mello Castrianni, entendeu a completa legitimidade do Instituto para ajuizar a ação, considerando que a defesa da proteção de dados pessoais está dentro de seus objetivos estatutários, como se observa:

> O requisito essencial para a legitimidade da associação é o cumprimento do tempo mínimo de criação, a pertinência temática entre os objetivos da associação e o bem jurídico tutelado na ACP (AgInt nos EDcl no REsp n. 1.788.290/MS). Ao presente caso, resta evidenciado que os requisitos essenciais da associação autora estão preenchidos. Neste contexto, entendo que restou comprovada a legitimidade da associação autora, mesmo sem a autorização por assembleia, conforme entendimento jurisprudencial pátrio. (AÇÃO CIVIL PÚBLICA nº 5028572-20.2022.4.03.6100).

Restando-se clara a legitimidade para ajuizar a ação, o magistrado veio a indeferir as preliminares de ilegalidade ativa, nulidade da citação e impugnação do valor da causa. Além de indeferir também o pedido de perícia e antecipação de tutela, visto que o juiz veio a reconhecer e a considerar que as provas já existentes nos autos seriam suficientes para julgar o caso em questão, conforme se:

> No que atine à preliminar de inépcia da petição inicial e falta de interesse processual estas serão devidamente analisadas com o mérito. Indefiro o pedido de prova pericial requerido pelo Ministério Público Federal, uma vez que já estão presentes os elementos necessários à convicção do Juízo. Quanto ao pedido de antecipação de tutela, indefiro, tendo em vista a fundamentação exposta na decisão de ID 271367108. Em relação aos requerimentos de intimação das corrés solicitados pelo parquet federal, indefiro, uma vez que já estão presentes nos autos as provas para julgamento do feito. (AÇÃO CIVIL PÚBLICA nº 5028572-20.2022.4.03.6100).

Passado ao Mérito do processo, o Juiz Federal veio a julgar parcialmente procedente o pedido. O mesmo veio a argumentar sua decisão com base na própria LGPD, dando ênfase ao art. 2º e 42 da referida lei, onde o respeito à privacidade e à inviolabilidade da intimidade, da honra e imagem são disciplinados pela proteção de dados, e a responsabilidade civil que recai sobre o controlador ou o operador dos dados pessoais. Ademais, utilizou-se também dos artigos 3º e 22 da Lei nº 12.965/14 (Marco Civil da Internet), onde a proteção à privacidade e a proteção de dados pessoais são princípios intrínsecos do uso da internet no Brasil.

Portanto, com a devida base legal ao caso em questão, o magistrado considerou comprovado o vazamento de dados pessoais dos beneficiários do Auxílio Brasil, o que configura violação à LGPD. Assim, os réus foram considerados responsáveis pelo vazamento, devendo tomar as medidas necessárias para reparar os danos causados. Medidas estas pautadas

no fornecimento de registros de conexão e acesso aos dados vazados, disponibilização aos titulares de informações sobre seus dados e como eles foram utilizados, implementação de medidas de segurança para evitar novos vazamentos, comunicação aos titulares sobre o incidente e as medidas adotadas, elaboração de relatórios de impacto à proteção de dados e por fim o pagamento de indenização por danos morais individuais e coletivos no valor de R$ 15.000,00 para cada uma das 4 milhões de vítimas que tiveram seus dados vazados.

Vale salientar que o excelentíssimo Juiz Federal Marco Aurélio de Mello Castrianni veio a destacar a importância da proteção dos dados pessoais e a necessidade de responsabilizar os agentes que violem essa proteção. Logo, tal decisão vem a proteger os direitos dos titulares dos dados, garantindo que sejam informados sobre o vazamento e que tenham seus dados protegidos, além de servir como precedente para outros casos semelhantes, reforçando a importância da proteção de dados pessoais e a responsabilização dos agentes que violem a LGPD.

Dessa forma, é visto que a Ação Civil Pública nº 5028572-20.2022.4.03.6100 vem a se fundamentar diretamente com diversas teorias já abordadas no presente trabalho. A responsabilidade civil objetiva, onde a comprovação do dano e do nexo causal entre a conduta ilícita e o dano são suficientes para a responsabilização, dispensando a comprovação de culpa, como se tornaram presentes na referida ACP, visto que, no próprio mérito desenvolvido pelo Juiz Federal, a responsabilidade civil que recai sobre o controlador ou o operador dos dados pessoais se tornou suficiente para corroborar com a responsabilização direta da União, Caixa Econômica Federal, Dataprev e a Autoridade Nacional de Proteção de Dados (ANPD) com o vazamento massivo de dados de beneficiários do Auxílio Brasil.

Ademais, a Teoria do Risco Administrativo, onde cabe à administração pública o dever de indenizar os danos causados por seus serviços, independentemente de culpa, em razão do risco inerente às suas atividades pode auxiliar nas medidas tomadas pelo magistrado quanto à responsabilização dos órgãos públicos. Vale elencar que a Teoria do Risco Integral, na qual a administração pública assume a responsabilidade por todos os danos causados por seus serviços, independentemente de culpa ou do serviço ser essencial ou não, também corrobora com as medidas tomadas pelo magistrado no caso em questão.

Vale elencar, que a responsabilidade civil objetiva fora imposta na Ação Civil Pública nº 5028572-20.2022.4.03.6100, visto os fundamentos legais e natureza dos riscos envolvidos no tratamento de dados pessoais sensíveis, trazidos pelas teorias anteriormente elencadas. Afirma-se, que a fundamentação da adoção da responsabilidade civil objetiva teve como pilares Lei Geral de Proteção de Dados (LGPD), o Marco Civil da Internet e o Código

de Defesa do Consumidor (CDC), que consagram a proteção da privacidade e a segurança dos dados como direitos fundamentais, além do fato de serem pensamentos e jurisprudências devidamente consolidadas na legislação brasileira.

Ademais, como já debatido a Teoria do Risco Administrativo, reforçada pela Teoria do Risco Integral, avigoram a adoção da responsabilidade civil objetiva no caso em questão, na qual instituições que lidam com grandes volumes de dados pessoais devem implementar medidas preventivas adequadas, além do mais, o fato dos dados vazados terem sido usados por bancos correspondentes sem controle eficaz reforçou o entendimento de que houve falha no sistema de segurança, independentemente de dolo ou negligência. Portanto, vem se a questionar o motivo da na adoção das outras responsabilidades civis da administração pública na Ação Civil Pública nº 5028572-20.2022.4.03.6100

Dessa forma, em relação à não adoção da responsabilidade subjetiva da administração pública, se dá muito pelo fato da exigência de comprovação de dolo ou culpa no caso em questão, situação em que tal fato poderia dificultar o processo, tornando-o mais complexo e demorado, visto a necessidade de demonstrar negligência específica por parte dos réus. Ademais, o fato de já haver jurisprudência consolidada, fortificou o uso da responsabilidade objetiva ao caso em questão, além da própria natureza da LGPD adotar em sua maioria o regime de responsabilidade objetiva.

No que tange à responsabilidade proativa, pode-se notar pequenas nuances, visto a já previsão de medidas de prevenção e mitigação em parte da Lei Geral de Proteção de Dados. Dessa forma, aloca-se que a decisão busca não utilizar da responsabilidade subjetiva ou proativa na Ação Civil Pública nº 5028572-20.2022.4.03.6100 pela natureza da LGPD, pela especificidade do caso, pela busca por eficiência processual e pela jurisprudência consolidada, tendo a justiça que seguir uma linha que importasse avaliações claras e uma indenização coletiva e individual, além de medidas de reforço na segurança de dados, garantindo uma resposta mais ágil e prática ao dano já materializado.

Nesse contexto, a Ação Civil Pública nº 5028572-20.2022.4.03.6100 representa um passo importante para a proteção de dados pessoais no Brasil. A decisão nesse caso demonstra que a LGPD está sendo aplicada e que as empresas que não cumprirem a lei serão responsabilizadas.

5 CONCLUSÃO

Como exposto, o presente trabalho veio a questionar em que medida é concebida a responsabilidade civil da Administração Pública no tratamento de dados pessoais. Portanto, fora apresentado que, em geral, a responsabilidade civil da Administração Pública no tratamento de dados é objetiva, ou seja, independe da comprovação de dolo ou culpa, devendo haver apenas o dano e o nexo causal entre a conduta ilícita e o dano. Vale afirmar que há outras medidas que podem vir a conceber a responsabilidade civil da Administração Pública no tratamento de dados pessoais, sendo elas a responsabilidade subjetiva e responsabilidade proativa.

Dessa forma, em um contexto geral, o presente trabalho veio abordar a aplicação da Lei Geral de Proteção de Dados (LGPD) na Administração Pública, destacando a necessidade de transparência, segurança e proteção no tratamento de dados pessoais dos cidadãos. Conforme exposto, o Estado exerce vastas atividades administrativas e exige grande quantidade de dados pessoais para o desempenho de suas funções. A LGPD, especialmente o Capítulo IV, estabelecem que o tratamento de dados deve visar ao interesse público, executando competências legais e fornecendo informações claras sobre o uso desses dados pessoais de forma específica.

Ademais, fora ressaltado que o Poder Público, devido ao seu amplo alcance e poder, deve adotar práticas rigorosas para garantir que os dados sejam usados apenas para fins legítimos, específicos e informados aos titulares. Esse tratamento deve respeitar os princípios de minimização, qualidade dos dados, segurança e não discriminação. A Administração Pública também precisa garantir a interoperabilidade dos dados entre órgãos para melhorar a prestação de serviços e tomar decisões mais informadas.

Tratando-se de um contexto histórico, a criação da LGPD foi inspirada em normativas internacionais, como o GDPR da União Europeia, e visa consolidar os direitos de privacidade e proteção dos cidadãos. A lei exige a criação de estruturas e políticas específicas, como o Relatório de Impacto à Proteção de Dados (RIPD) e a nomeação de um Encarregado de Proteção de Dados (DPO), para supervisionar o cumprimento das diretrizes de proteção.

Por fim, o primeiro capítulo vem a debater sobre a decisão do Supremo Tribunal Federal (STF) nas ações ADI 6.649 e ADPF 695, reforçando a importância de critérios rigorosos para o compartilhamento de dados entre órgãos públicos. Este compartilhamento deve observar especificamente especificações, proporcionalidade e transparência, de forma a

mitigar riscos e proteger os direitos dos titulares, mantendo um equilíbrio entre o uso de dados e a privacidade individual.

Dessa forma, o segundo capítulo do presente trabalho vem a expor a LGPD, que estabelece um tratamento diferenciado para o Poder Público, que inclui órgãos da administração direta e indireta e define que o tratamento de dados pessoais deve ser realizado para fins públicos e legais. O artigo 23 da LGPD destaca a importância da finalidade e da transparência no tratamento de dados, exigindo que os órgãos informem aos titulares sobre a coleta e uso de seus dados.

Logo, os princípios da Finalidade e da Transparência são fundamentais. Os dados pessoais devem ser coletados para finalidades específicas e os titulares devem ser informados sobre como seus dados serão utilizados. O compartilhamento de dados com entidades privadas é restrito, exceto em situações específicas previstas na lei. Assim, vale evidenciar que a responsabilidade civil da Administração Pública é objetiva, ou seja, o Estado deve indenizar danos causados independentemente de culpa, fundamentada na teoria do risco administrativo. Isso implica que o Estado assume o risco de danos decorrentes de suas atividades.

Consequentemente, o presente trabalho vem a debater que a LGPD define três agentes: o controlador (quem decide sobre o tratamento), o operador (quem realiza o tratamento) e o encarregado (canal de comunicação). Ambos, controlador e operador, têm responsabilidades legais e podem ser responsabilizados solidariamente por danos causados no tratamento de dados. Vindo, por fim, discutir sobre divergências acerca do regime de responsabilidade civil, com algumas correntes defendendo a responsabilidade subjetiva, que exige prova de culpa, enquanto outras argumentam a favor da responsabilidade objetiva, dada a natureza arriscada do tratamento de dados. Há ainda a teoria proativa, que enfatiza a necessidade de medidas preventivas e a prestação de contas.

Por fim, o terceiro e último capítulo do presente trabalho vem abordar que a responsabilidade civil do Poder Público em casos de vazamento de dados pessoais, especialmente à luz da Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil. A responsabilidade civil é definida como a obrigação de reparar danos causados por atos ilícitos, conforme os artigos 927, 186 e 187 do Código Civil. O conceito é fundamentado na ideia de justiça e na necessidade de que o infrator seja responsabilizado proporcionalmente ao dano causado.

Logo, o vazamento de dados pessoais pode resultar em diversas consequências negativas, como fraudes financeiras, roubo de identidade, violação da privacidade e danos morais, sociais e materiais. A LGPD estabelece normas rigorosas para o tratamento de dados

pessoais e impõe sanções em caso de violação, permitindo que o Estado seja responsabilizado objetivamente, independentemente de culpa, conforme o artigo 37, § 6º da Constituição Federal.

Acrescenta-se que a Autoridade Nacional de Proteção de Dados (ANPD) desempenha um papel crucial na fiscalização e regulação da LGPD, podendo iniciar procedimentos administrativos em casos de vazamento. Embora não possa aplicar multas diretamente a órgãos públicos, a ANPD pode impor sanções administrativas e exigir medidas corretivas. Nesse contexto, um exemplo prático dessa responsabilidade é a Ação Civil Pública nº 5028572-20.2022.4.03.6100, movida em razão de um vazamento massivo de dados de beneficiários do Auxílio Brasil. O Instituto Brasileiro de Defesa da Proteção de Dados Pessoais alegou que mais de 4 milhões de dados foram expostos devido à negligência na segurança dos dados por parte de órgãos públicos, como a Caixa Econômica Federal e a Dataprev. O juiz reconheceu a legitimidade da ação e determinou que os réus tomassem medidas para reparar os danos, incluindo a indenização de R$ 15.000,00 para cada vítima.

Dessa forma, a presente monografia conclui que a responsabilidade civil do poder público em casos de vazamento de dados é um tema de crescente relevância, reforçando a importância de uma governança eficaz de dados e a necessidade de que órgãos públicos adotem medidas preventivas para proteger as informações pessoais dos cidadãos. A Ação Civil Pública mencionada exemplifica a aplicação da LGPD e a responsabilização dos órgãos públicos, destacando a importância da proteção de dados pessoais no Brasil.

REFERÊNCIAS

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS. Guia Orientativo: **Tratamento de dados pessoais pelo Poder Público**, Brasília, DF: ANPD, 2023. 52p. Disponível em:https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em 12 out. 2023.

ANCILLOTTI, Leon. **A Repartição dos Encargos Sociais e a Responsabilidade Objetiva do Estado no Brasil:** Um Olhar Crítico e Contemporâneo. Jusbrasil, Vitória, v. 1, n. 1, p. 1-4, mai./2024. Disponível em: https://www.jusbrasil.com.br/artigos/a-reparticao-dos-encargos-sociais-e-a-responsabilidade-objetiva-do-estado-no-brasil/2455754698#:~:text=Esse%20princ%C3%ADpio%2C%20pedra%20angular%20da,ou%20grupos%20sejam%20desproporcionalmente%20prejudicados. Acesso em 14 set. 2024.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS COORDENAÇÃO-GERAL DE FISCALIZAÇÃO COORDENAÇÃO DE FISCALIZAÇÃO. **Relatório de Instrução Nº 4/2023/FIS/CGF/ANPD**. Disponível em: file:///C:/Users/Ideapad/Downloads/ri-sesc-sc-00261001886202251-autos-publicos%20Secretaria%20de%20Estado%20da%20Sa%C3%BAde%20de%20Santa%20Catarina.pdf. Acesso em 06 out. 2024.

BIONI, Bruno Ricardo; SILVA, Paula Guedes F. da; MARTINS, Pedro Bastos L. **Intersecções e relações entre a Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação (LAI)**: análise contextual pela lente do direito de acesso. Coletânea de Artigos da Pós-graduação em Ouvidoria Pública, v. 1, 2022. Cadernos Técnicos da CGU/ Controladoria-Geral da União. Disponível em: <https://revista.cgu.gov.br/Cadernos_CGU/issue/view/39/46>. p. 11. Acesso em 06 out. 2024.

BRASIL**. Código Civil de 2002**. Disponível em: https://www.planalto.gov.br/civil_03/leis//2002/L10406compilada.htm>. Acesso em 11 out. 2024.

_____. **Lei nº 13.709, de 14 de agosto de 2018.** Diário Oficial da União de 15/08/2018. Brasília. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

_____. **Lei nº 12.527, de 18 denovembro de 2011**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em 14 set. 2024.

_____. **Constituição da República Federativa do Brasil de 1988.** Disponível em https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 07 nov. 2024.

CARVALHO, L. P.; OLIVEIRA, J. **Proteção de dados e humanidades digitais no Brasil:** caixas-pretas. Revista ScientiarumHistoria, v. 1, p. 9, 12 dez. 2019.

CASTRO, Rodrigo Pironti Aguirre de; ZILIOTTO, Mirela Miró. **Compliance nas contratações públicas**: exigência e critérios normativos. Belo Horizonte: Fórum, 2019.

COELHO, Fábio Ulhôa. **Curso de direito civil:** obrigações/responsabilidade civil. 5ª ed., São Paulo: Saraiva, 2012.

CONSULTOR JURÍDICO. **Como a LGPD se aplica à Administração Pública**. Disponível em: https://www.conjur.com.br/2021-out-04/opiniao-lgpd-aplica-administracao-publica. Acesso em 12 out. 2023.

_____. **Limites ao compartilhamento de dados pessoais pelo poder público**. Disponívelem:https://www.conjur.com.br/2022-out-02/publico-pragmatico-limites-compartilhamento-dados-poder-publico#_ftn5. Acesso em 11 out. 2023.

DONEDA, Danilo. **A proteção de Dados Pessoais como um Direito Fundamental**. Revista Espaço Jurídico, Joaçaba, v.12, n.2, p. 91-108, jul/dez.2011. Disponível em:https://dialnet.unirioja.es/descarga/articulo/4555153.pdf. Acesso em 12 out. 2023.

FARIAS, E. **Segurança da informação e proteção de dados:** uma análise à luz da LGPD. São Paulo: Revista de Direito Digital, 2021.

FERRAREZI, Thiago. LGPD e prefeituras:desafios e impactos na gestão de dados pessoais no setor público municipal/LGPD e prefeituras: **MIGALHAS**, São Paulo, v. 1, n. 1, p. 1-1, abr./2023. Disponível em: https://www.migalhas.com.br/depeso/385181/lgpd-e-prefeituras-desafios-e-impactos. Acesso em 07 nov. 2024.

FRAZÃO, Ana; CUEVA, Ricardo. 31**. Responsabilidade Civil dos Agentes de Tratamento de Dados** In: FRAZÃO, Ana; CUEVA, Ricardo. Compliance e Políticas de Proteção de Dados. São Paulo (SP): Editora Revista dos Tribunais. 2022. Disponível em:https://www.jusbrasil.com.br/doutrina/compliance-e-politicas-de-protecao-de dados/1506551345. Acesso em 15 set. 2024.

FREITAS, Juarez. O controle dos atos administrativos e os princípios fundamentais. 5. ed. rev. e ampl. São Paulo: Malheiros Editores, 2013. p. 456.

GAROFANO, Rafael R. **Limitação de finalidade no tratamento de dados pessoais pelo poder público:** controle de legalidade da reutilização para fins de interesse público. Tese de Doutorado. São Paulo: Faculdade de Direito, Universidade de São Paulo, 2022. p. 135.

GIL, Antônio Carlos. Como classificar as pesquisas? In:**Como elaborar projetos de pesquisa**. São Paulo:Atlas S.A., 2002. Cap.4, p. 41-44.Disponívelem:https://professores.faccat.br/moodle/pluginfile.php/13410/mod_resource/co

ntent/1/como_elaborar_projeto_de_pesquisa_-_antonio_carlos_gil.pdf. Acesso em 11 mar. 2021.

_____. **Métodos e técnicas de pesquisa social**. 6. ed. São Paulo: Atlas, 2008.

GOMES, R. M. V. **Teoria do risco administrativo:** responsabilidade objetiva da administração pública: Teoria do risco administrativo: responsabilidade objetiva da administração pública. Jusbrasil, Goiânia, v. 1, n. 1, p. 1-4, set./2023. Disponível em: https://www.jusbrasil.com.br/artigos/teoria-do-risco-administrativo-responsabilidade-objetiva-da-administracao-publica/1801715350. Acesso em 14 set. 2024.

GOMES, Lúcia. **Direito Digital e Responsabilidade Civil na Proteção de Dados**. Rio de Janeiro: Editora Digital, 2021.

GUEDES, Gisela Sampaio da Cruz; MEIRELES, Rose Melo Vencelau, **Término do tratamento de dados**, IN: Tepedino, Gustavo; Frazão, Ana; Oliva, Milena Donato. Lei Geral de Proteção de Dados Pessoais, Editora RT: São Paulo, 2019, p. 231.

KAMEDA, Koichi; PAZELLO, Magaly. **E-Saúde e desafios à proteção da privacidade no Brasil.**Disponívelemnupef.org.br/sites/default/files/downloads/artigo%20politics_esaude%20e%20privacidade.pdf. Acesso em 7 out 2024.

LIMA, Caio Cesar Carvalho; MONTEIRO, Renato Leite**. Panorama brasileiro sobre a proteção de dados pessoais:** discussão e análise comparada: novas práticas em informação e conhecimento, [S.l.], v. 2, n. 1, p. 60-76, ago. 2013. ISSN 2237-826X. Disponível em: <https://revistas.ufpr.br/atoz/article/view/41320>. Acesso em 06 abr. 2020.

LIMA, Alvino. **Culpa e Risco**. 2 ed. São Paulo: Revista dos Tribunais, 1999.

LOPEZ, Tereza Ancona. **Responsabilidade civil na sociedade do risco**. Revista da faculdade de direito da Universidade de São Paulo, v. 105, São Paulo, jan./dez. 2010. p. 1223-1234.

MACHADO, José Mauro Decoussau; SANTOS, Matheus Chucridos; PARANHOS, Mario Cosac Oliveira. **LGPD e GDPR:** uma Análise Comparativa entre as Legislações**.**

MAIA, Luciano Soares. **A privacidade e os princípios de proteção do indivíduo perante os bancos de dados pessoais**. Disponível na URL: http://www.publicadireito.com.br/conpedi/manaus/arquivos/anais/bh/luciano_soares_maia.pdf. Acesso em 12 out. 2023.

MARINI, Bruno**. Da responsabilidade civil do Poder Público e dos Agentes de Tratamentos de Dados no contexto da Lei Geral de Proteção de Dados:** Da responsabilidade civil do Poder Público e dos Agentes de Tratamentos de Dados no contexto

da Lei Geral de Proteção de Dados. Jusbrasil, Mato Grosso do Sul, v. 1, n. 1, p. 1-39, 2021. Disponível em: https://www.jusbrasil.com.br/artigos/da-responsabilidade-civil-do-poder-publico-e-dos-agentes-de-tratamentos-de-dados-no-contexto-da-lei-geral-de-protecao-de-dados. Acesso em 14 set. 2024.

MENDES, Laura Schertel; DONEDA, D. **Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018)**, o novo paradigma da proteção de dados no Brasil. REVISTA DE DIREITO DO CONSUMIDOR, v. 120, p. 555, 2018.

MENDES, Laura Schertel. **Democracia, poder informacional e vigilância**. O Globo, publicado em 13 ago. 2022. Disponível em: https://oglobo.globo.com/blogs/fumus-boni-iuris/post/2022/08/laura-schertel-democracia-poder-informacional-e-vigilancia.ghtml. Acesso em 24 out. 2024.

MIGALHAS. **LGPD e prefeituras:** desafios e impactos na gestão de dados pessoais no setorpúblico municipalDisponível em: https://www.migalhas.com.br/depeso/385181/lgpd-e-prefeituras-desafios-e-impactos. Acesso em 29 abr. 2024.

_____.**Segurança da informação na ótica da LGPD para o PoderPúblico:** Protegendo dados e respeitando os direitos constitucionaishttps://www.migalhas.com.br/depeso/406158/seguranca-da-informacao-na-otica-da-lgpd-para-o-poder-publico. Acesso em 29 abr. 2024. **Migalhas**, Rio de Janeiro, v. 1, n. 1, p. 1-6, jun./2020. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/329909/a-lgpd-e-o-fundamento-da-responsabilidade-civil-dos-agentes-de-tratamento-de-dados-pessoais--culpa-ou-risco. Acesso em 14 set. 2024.

MIRAGEM, B. **Lei Geral de Proteção de Dados e os impactos no setor público**. Porto Alegre: Revistade Direito Administrativo, 2021.

MORAES, Maria Celina Bodin; QUEIROZ, João Quinelato de. **Autodeterminação informativa e responsabilização proativa:** novos instrumentos de tutela da pessoa humana na LGDP. Cadernos Adenauer, Rio de Janeiro, f. 113-137, nº 3, out/ 2019. Disponível em: <https://www.kas.de/pt/web/brasilien/einzeltitel/-/content/proteçâo-de-dados-pessoais>. Acesso em 06 abr. 2020.

MORAES, Pauline Pacheco. **O consentimento previsto na LGPD**: o consentimento previsto na LGPD. **CONJUR**, São Paulo, v. 1, n. 1, p. 1-1, ago./2020. Disponível em: https://www.conjur.com.br/2020-out-25/pauline-moraes-consentimento-previsto-lgpd/. Acesso em 07 nov. 2024.

MORAIS, Alexandre; QUINELATO, Marcelo de Queiroz. **Direito digital e proteção de dados no Brasil** . São Paulo: Saraiva, 2019.

MULHOLLAND, Caitlin Sampaio. **Dados Pessoais Sensíveis e a Tutela de Direitos Fundamentais:** uma análise à luz da Lei Geral de Proteção de Dados(Lei nº 13.709/18):FDV, Rio de Janeiro, v. 1, n. 1, p. 1-22, ago./2018. Disponível em: https://sisbib.emnuvens.com.br/direitosegarantias/article/download/1603/pdf/. Acesso em 07 nov. 2024.

MULHOLLAND, Caitlin. **A LGPD e o fundamento da responsabilidade civil dos agentes de tratamento de dados pessoais: culpa ou risco: A LGPD e o fundamento da responsabilidade civil dos agentes de tratamento de dados pessoais: culpa ou risco.**MIGALHAS, Rio de Janeiro, v. 1, n. 1, p. 1-1, jun./2020. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/329909/a-lgpd-e-o-fundamento-da-responsabilidade-civil-dos-agentes-de-tratamento-de-dados-pessoais--culpa-ou-risco. Acesso em: 15 nov. 2024

NUNES, L.P. **A proteção de dados pessoais na administração pública e a Lei Geral de Proteção de Dados**. Revista Jurídica, v.1, n.1, p.1-20, 2021.

NALIN, Paulo; SANTARÉM, Ana Carolina. **A atuação da ANPD no setor público**. Revista de Direito Digital, 2020.

PINHEIRO, Patrícia Peck **Proteção de dados pessoais:** comentários à Lei n. 13.709/2018 (LGPD). São Paulo: Saraiva Educação, 2018.

PIRONTI, Rodrigo; ZILIOTTO, Mirela Miró. **O direito à autodeterminação informativa e a questão do consentimento no tratamento de dados pessoais pela AdministraçãoPública.***In*: PIRONTI, Rodrigo (Coord.). Lei Geral de Proteção de Dados no Setor Público. Belo Horizonte: Fórum, 2021, p. 423.

PJE - PROCESSO JUDICIAL ELETRÔNICO. **AÇÃO CIVIL PÚBLICA CÍVEL nº 5028572-20.2022.4.03.6100**. Disponível em: https://static.poder360.com.br/2023/09/decisaojustica-13set2023.pdf. Acesso em 06 out. 2024.

QUINTILIANO, Leonardo. **Contexto histórico e finalidade da Lei Geral de Proteção de Dados (LGPD):** Contexto histórico e finalidade da Lei Geral de Proteção de Dados (LGPD). IAPD, São Paulo, v. 1, n. 1, p. 1-1, jun./2020. Disponível em: https://www.jusbrasil.com.br/artigos/contexto-historico-e-finalidade-da-lei-geral-de-protecao-de-dados-lgpd/1203647706#:~:text=A%20LGPD%20%C3%A9%20fruto%20da,proemin%C3%AAncia%20no%20texto%20final%20aprovado.&text=A%20utiliza%C3%A7%C3%A3o%20da%20legisla%C3%A7%C3%A3o%20europeia,inclusive%2C%20mencion. Acesso em 07 nov. 2024.

ROSSO, Angela Maria. **LGPD e setor público:** aspectos gerais e desafios. Migalhas, 18 de abril de 2019. Disponível em: <https://www.migalhas.com.br/depeso/300585/lgpdesetor-público-aspectos-geraisedesafiosl>. Acesso em 14 set. 2024.

SANTOS, Camila; RODRIGUES, Pedro. **A responsabilidade civil do Estado pelo vazamento de dados pessoais e da LGPD**. Revista Brasileira de Direito Digital, 2020.
SANTOS, Fabíola Meira de Almeida; TALIBA, Rita. **Lei geral de proteção de dados no Brasil e os possíveis impactos.** Revista dos Tribunais, São Paulo, v. 998, p. 227-228, dez. 2018.

SILVA, L.A, e ALMEIDA, M.C. **Fraudes financeiras no ambiente digital**. Curitiba: Juruá, 2021**.**

SOUSA, Rafael. **Proteção de dados e privacidade:** Fundamentos e Princípios da LGPD. São Paulo: Editora Jurídica, 2020.

STF,**ADI 6.649; ADPF 695** (julgamento conjunto), rel.min. Gilmar Mendes, j.em 15 set. 2022. p. 30.

TARTUCE,F.**A. aplicação da Lei Geral de Proteção de Dados no âmbito da administração pública**. Revista de Direito e Políticas Públicas, v.5, n.1, p.50-68.

TASSO, Fernando Antonio. **Do tratamento de dados pessoais pelo Poder Público**. In. LGPD: Lei Geral de Proteção de Dados comentada. MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coords.). São Paulo: Thomson Reuters Brasil, 2019. p. 245.

UNICEF. **Declaração Universal dos Direitos Humanos**. Disponível em: https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos. Acesso em 7 nov. 2024.

VENOSA, Sílvio de Salvo. **Direito Civil:** Responsabilidade Civil. 10.ª ed., São Paulo: Atlas, 2010.

WIMMER, Miriam. **Limites e possibilidades para o uso secundário de dados pessoais no poder público:** lições da pandemia. In: Revista Brasileira de Políticas Públicas, Brasília, v.11, nº1, pp.123-143, abr. 2021.