PODER PÚBLICO E O TRATAMENTO DE DADOS PESSOAIS NO BRASIL

Regina Linden Ruaro[1],[2]

Resumo: O presente artigo tem como finalidade investigar as implicações do poder público no tratamento de dados pessoais no Brasil. No primeiro momento, será analisado o âmbito de incidência da lei de proteção de dados e a aplicação de seus conceitos básicos ao setor público. Em seguida serão analisadas como ocorre a interpretação das bases legais que autorizam o tratamento de dados pessoais em decorrência dos seus procedimentos e diretrizes legais com enfoque sobre sua eficácia. Em seguida, apresenta os requisitos e as formalidades a serem observados nas hipóteses de uso compartilhado de dados pessoais, com especial enfoque sobre data-analítica das pesquisas acerca do gerenciamento de dados pelo poder público. Ao final, dispõem acerca da necessidade de boas práticas pelos órgãos públicos com fim de garantir a proteção dos cidadãos perante o Estado super informado com enfoque na garantia dos direitos fundamentais.

Palavras-Chave: Proteção de dados pessoais; tratamento de dados pessoais; poder público; estado super informado.

PUBLIC AUTHORITIES AND THE PROCESSING OF PERSONAL DATA IN BRAZIL

[1] Pós-Doutora pela Universidad de San Pablo – CEU de Madrid (2016). Doutora em Direito pela Universidad Complutense de Madrid (1993). Professora Titular da Pontifícia Universidade Católica do Rio Grande do Sul – PUC-RS.

[2] O presente artigo contou com a colaboração do meu orientando de mestrando, bolsista CNPq, Bernardo Bonifácio Ferreira do Programa de Pós-Graduação em Direito da Pontifícia Universidade Católica do Rio Grande do Sul – PUCRS a quem agradeço pelo empenho.

Abstract*:* The purpose of this article is to investigate the implications for public authorities of processing personal data in Brazil. First, the scope of the data protection law and the application of its basic concepts to the public sector will be analyzed. This will be followed by an analysis of how the legal bases that authorize the processing of personal data are interpreted as a result of its legal procedures and guidelines, focusing on their effectiveness. It then presents the requirements and formalities to be observed in the event of shared use of personal data, with a special focus on the data analysis of research into data management by public authorities. Finally, they discuss the need for good practices by public bodies to guarantee the protection of citizens in the face of an over-informed state, focusing on ensuring fundamental rights.

Keywords: Personal data protection; personal data processing; public authorities; super-informed state.

CONSIDERAÇÕES INICIAIS

A sociedade moderna, também tida como sociedade da informação ou sociedade digital, necessita cada vez mais utilizar sistemas de tratamento de dados pessoais que se veem facilitados pelo uso de inteligência artificial. Se por um lado há inúmeras vantagens nesse tratamento pela capacidade na criação de big datas contendo as mais diversas informações sejam elas econômicas, de saúde, de pesquisas, de consumo ou tantas outras de forma organizada, por outro e no mais das vezes, deixa uma incógnita para os indivíduos no que se refere à falta de transparência.

Para além da existência e importância dos bancos de dados, hoje se compreende que o foco do Direito deve estar voltado

para as técnicas utilizadas no que se refere a tratamento de dados pessoais, independentemente de fazerem ou não parte daquele.[3] Acertadamente, um grande volume de dados mesmo que de forma organizada pode não representar um risco ao indivíduo, porém, pode significar que a equação entre o poder de quem tem a informação é inversamente proporcional ao controle que a pessoa sobre ela.

Nesse sentido, constata-se que o grande volume de dados tratados com o uso de tecnologia informatizada tem capacidades inimagináveis, sobretudo de fazer catalogação, combinações, permitindo que em fração de segundos perfis sejam criados e que suas ideias e ações podem ser manipuladas.

Se é presente a preocupação com a superinformação que detém hoje as chamadas big-techs e o uso que as mesmas fazem com os dados pessoais dos indivíduos, não menos preocupante é a existência de um Estado superinformado acerca de seus cidadãos. Essa realidade é que impulsionou a inclusão do Poder Público nas leis que regulam o direito à proteção de dados pessoais, como ocorre no Brasil.

O presente artigo é fruto da palestra proferida no evento comemorativo do 9º Aniversário da Revista Jurídica Luso-Brasileira, na Universidade de Lisboa em janeiro de 2024 e se insere na linha de pesquisa Direito, Tecnologia e Inovação do Programa de Pós-Graduação em Direito da PUCRS sendo fruto das pesquisas realizadas pelo Grupo Proteção de Dados no Estado Democrático de Direito.

1. ÂMBITO DE INCIDÊNCIA DA LEI DE PROTEÇÃO DE DADOS E A APLICAÇÃO DE SEUS CONCEITOS BÁSICOS AO SETOR PÚBLICO:

Primeiramente cabe esclarecer que a terminologia "Poder Público" é definida na Lei Geral de Proteção de Dados

[3] Cf. Stefano Rodotá. Tecnologie e diritti. Bolonha: Il Molino. 1995, p. 68.

Pessoais (LGPD - Lei 13.709/18) como sendo as pessoas jurídicas de direito público, remetendo o âmbito de aplicação das entidades contidas na Lei de Acesso à Informação (LAI – Lei 12.52711)[4].

Ao elucidar o âmbito de incidência da Lei Geral de Proteção de Dados, a Autoridade Nacional de Proteção de Dados Pessoais (ANPD) esclarece que estão incluídos órgãos ou entidades dos entes federativos (União, Estados, Distrito Federal e Municípios) e dos três Poderes (Executivo, Legislativo e Judiciário), inclusive das Cortes de Contas e do Ministério Público ademais dos serviços notariais e de registro as empresas públicas e as sociedades de economia mista que executem políticas públicas.

É importante destacar que a Lei Geral de Proteção de Dados é reconhecida como uma legislação baseada em princípios, visando proteger as interações que envolvem dados pessoais, com particular atenção aos direitos do titular desses dados[5]. Assim sendo, a administração pública terá sua atuação, preservando, sempre, o interesse coletivo e os direitos fundamentais.

Além disso, ao realizar uma análise detalhada, observa-se que os direitos fundamentais à proteção de dados pessoais, ao livre acesso, à transparência, à segurança, à prevenção e a não discriminação, estabelecidos na Lei Geral de Proteção de Dados, estão segundo o direito à privacidade (ainda que sejam direitos autônomos) conforme expresso no artigo 5º, inciso X da

[4] Art. 1º Esta Lei dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal.
Parágrafo único. Subordinam-se ao regime desta Lei:
I - os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público;
II - as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios.

[5] PINHEIRO, Patrícia Peck. *Proteção de dados pessoais*: comentários à Lei n. 13.709/2018 (LGPD). 2. ed. São Paulo: Saraiva, 2020.

Constituição Federal. Esses direitos podem ser vistos como extensões do direito à privacidade.[6]

Outrossim, o direito à proteção de dados pessoais está estabelecido não apenas como um direito humano, mas como um direito fundamental. Embora tenha suas raízes no direito à privacidade, sua importância é tal que evoluiu para um direito autônomo, sendo reconhecido tanto no âmbito do sistema global das Nações Unidas quanto no contexto legal europeu. Sua base legal está consubstanciada no artigo 5º, inciso LXXIX da Constituição Federal, promulgada através da Emenda Constitucional n.º 155 no ano de 2022[7].

Portanto, torna-se essencial que o tratamento de dados pessoais por pelo poder público esteja em concordância com os pressupostos de finalidade pública, persecução do interesse público e execução conforme as competências legais, bem como cumprimento de suas atribuições.

No que toca à execução das competências ou atribuições legais, cada ente público possui a sua "investidura legal" para praticar o ato e exercer uma função[8], uma vez que é investido de parte da autoridade soberana do Estado para desempenhar funções legais, de interesse público e administrativas, conforme estipulado pela legislação.

Dessa forma, as entidades públicas detêm prerrogativas para processar informações pessoais visando cumprir finalidades públicas voltadas para interesse público. No entanto, é crucial fornecer informações claras e detalhadas sobre a base legal, propósito, métodos e procedimentos para realizar tais atividades por meio de canais de acesso simplificado visando garantir evitar

---

[6] BRASIL, Lei n.º 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 07 mai. 2024.

[7] SARLET, Ingo Wolfgang. Fundamentos Constitucionais: o direito fundamental à proteção de dados. In: BIONI, Bruno [et al.]. (org.). Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2021. p. 21-59.

[8] CAVALCANTI., Themistocles Brandão. *Teoria dos atos administrativos*. São Paulo: Revista dos Tribunais, 1973. 345 p.

a constituição de discrepâncias na distribuição de informação entre o cidadão e o Poder Público. [9]

> *Nesse sentido, os órgãos públicos obtêm massivas quantidades de dados pessoais e dados pessoais sensíveis, em virtude da obrigatoriedade da entrega dessas informações pelos cidadãos. Afinal de contas, não é possível adquirir um imóvel ou veículo automotor, ser atendido em hospitais, emitir a Carteira Nacional de Habilitação e o Título de Eleitor, entre outras tantas hipóteses, sem que concedamos nossos dados pessoais. Deveria, assim, haver maior transparência nesses tratamentos, considerando a dicotomia "compulsoriedade" e "atendimento de políticas públicas".*[10]

Nessa linha, a Autoridade Nacional de Proteção de Dados foi estabelecida como a entidade responsável pela aplicação da Lei Geral de Proteção de Dados e pela criação de normas e diretrizes para controladores e operadores[11], desde a tomada decisões administrativas conclusivas sobre a interpretação da lei e suas próprias competências. Também possui aptidão para imposição de sanções administrativas na ocorrência de conflitos perante outras entidades e órgãos da administração pública no que tange a garantia da proteção de dados pessoais.[12]

Logo, perante a densidade massiva de dados tratados pelo setor público, a constituição de uniformização por parte da

---

[9] BOTELHO, M. C.; CAMARGO, E. P. do A. O Tratamento de dados pessoais pelo poder público na LGPD. *Revista Direitos Sociais e Políticas Públicas (UNIFAFIBE)*, *[S. l.]*, v. 9, n. 3, p. 549–580, 2022. DOI: 10.25245/rdspp.v9i3.1034. Disponível em: https://portal.unifafibe.com.br:443/revista/index.php/direitos-sociais-politicas-pub/article/view/1034. Acesso em: 9 maio. 2024.

[10] CRAVO, Daniela Copetti; CUNDA, Daniela Zago Gonçalves da; RAMOS, Rafael. *Lei Geral de Proteção de Dados e o Poder Público*. Porto Alegre: Tribunal de Contas do Estado do RGS, 2021. Disponível em: https://lproweb.procempa.com.br/pmpa/prefpoa/pgm/usu_doc/ebook_lgpd_e_poder_publico_23052021.pdf. Acesso em: 09 maio 2024.

[11] Controladores e operadores são os agentes de tratamento de dados pessoais segundo o 5º, inciso IX da LGPD.

[12] LANDERDAHL, Cristiane *et al*. *Tratamento de dados pessoais pelo Poder Público*. 2. ed. Brasília: Autoridade Nacional de Proteção de Dados, 2023. 52 p. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em: 08 maio 2024.

Autoridade Nacional de Proteção de Dados, em cumprimento de sua competência originária, sustenta a especificidade e uniformização no escopo da natureza dos dados e condução de auditorias sobre o tratamento de dados pessoais, assegurando a eficiência dos setores regulados.

Importante destacar que a consolidação destes procedimentos está no caráter preventivo da autarquia supramencionada com força para propulsionar transformações significativas na seara da proteção de dados para sociedade brasileira, sempre tendo mente, a necessidade de ampliação de conscientização, bem como, qualificação dos gestores e servidores públicos para promoção de diretrizes céleres e perenes nas ações promovidas pelos órgãos públicos.[13]

2. A ADEQUADA INTERPRETAÇÃO DAS BASES LEGAIS QUE AUTORIZAM O TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO:

Antes da realização do tratamento de dados pessoais pelo Poder Público é exigido a aprofundamento a fundamentação clara e objetiva acerca de sua base legal aplicável devendo ser feito consoante as hipóteses previstas no art. 7º (dados pessoais) ou no art. 11 (dados sensíveis) da Lei Geral de Proteção de Dados (LGPD).

Saliente-se que os dispositivos legais devem ser interpretados em conjunto e de forma sistemática, considerando-se também os critérios adicionais previstos no art. 23[14] da Lei Geral de

---

[13]. SARLET, Gabrielle Bezerra Sales; RODRIGUEZ, Daniel Piñeiro. A autoridade nacional de proteção de dados: elementos para uma estruturação independente e democrática na era da governança digital. *Direitos Fundamentais e Democracia*, [*s. l*], v. 27, p. 217-253, dez. 2022. Disponível em: https://revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/article/view/2285. Acesso em: 09 maio 2024.

[14] 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, com o objetivo de executar as

Proteção de Dados, para auxiliar na interpretação e aplicação prática das bases legais no âmbito do poder público. É sabido que a bases legais quando aplicada pelos agentes de tratamento do poder público tem enfrentado dificuldades e dúvidas nos âmbitos do consentimento, legítimo interesse, cumprimento de obrigação legal e execução de políticas públicas.

No que concerne ao consentimento, é necessário que ele seja obtido de forma livre, informada e inequívoca pelo titular dos dados, exigência esta que se redobra no caso de dados sensíveis, o consentimento deve ser específico e destacado para finalidades específicas.

No entanto, o consentimento pode não ser a base legal mais apropriada para o tratamento de dados pessoais pelo poder público, especialmente quando o tratamento é necessário para cumprir obrigações legais. Isso ocorre porque o poder público

---

competências legais ou cumprir as atribuições legais do serviço público, desde que: I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos;

II - (VETADO); e III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei. III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei; e (Redação dada pela Lei nº 13.853, de 2019)

IV - (VETADO). (Incluído pela Lei nº 13.853, de 2019).

§ 1º A autoridade nacional poderá dispor sobre as formas de publicidade das operações de tratamento. § 2º O disposto nesta Lei não dispensa as pessoas jurídicas mencionadas no caput deste artigo de instituir as autoridades de que trata a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) § 3º Os prazos e procedimentos para exercício dos direitos do titular perante o Poder Público observarão o disposto em legislação específica, em especial as disposições constantes da Lei nº 9.507, de 12 de novembro de 1997 (Lei do Habeas Data) , da Lei nº 9.784, de 29 de janeiro de 1999 (Lei Geral do Processo Administrativo) , e da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) .§ 4º Os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público, terão o mesmo tratamento dispensado às pessoas jurídicas referidas no caput deste artigo, nos termos desta Lei.§ 5º Os órgão notariais e de registro devem fornecer acesso aos dados por meio eletrônico para a administração pública, tendo em vista as finalidades de que trata o caput deste artigo.

exerce prerrogativas estatais típicas, o que pode criar um desequilíbrio de poder entre o àquele e o titular dos dados.

Sendo assim, o uso do consentimento pode ser aceito como fundamento legal em determinadas situações, desde que o tratamento não seja obrigatório e não esteja ligado ao exercício de funções típicas do poder público estatal.

Em caso de a base legal de tratamento adotada ser o consentimento, é crucial assegurar que o titular dos dados tenha a real capacidade de concordar ou recusar o tratamento de suas informações, sem restrições substanciais à sua posição jurídica ou à sua capacidade de exercer seus direitos fundamentais. Mais do que isso, o consentimento deve ser claro, específico e para determinada finalidade e seu termo deve conter uma linguagem capaz de ser entendida pelo titular dos dados pessoais.

No que se refere ao legítimo interesse como base legal, este permite o tratamento de dados pessoais quando necessário para atender às finalidades do controlador ou de terceiros, desde que os direitos e liberdades fundamentais do titular dos dados não se sobreponham. No contexto do poder público, sua aplicação é limitada, especialmente quando o tratamento é compulsório ou necessário para o cumprimento de obrigações legais hipótese esta que possui previsão legal.

Assim, todo decorrer de sua utilização deve ser precedido de uma avaliação da proporcionalidade entre os interesses do controlador ou de terceiros e os direitos e expectativas legítimas do titular dos dados. Portanto, é recomendado que os órgãos e entidades públicas evitem recorrer ao legítimo interesse como base legal, preferindo outras bases como execução de políticas públicas ou cumprimento de obrigação legal. Referente ao cumprimento de obrigação legal ou regulatória, permite o tratamento de dados pessoais pelo poder público para cumprimento de obrigações estabelecidas em leis, ou regulamentos. Essa é aplicada nas situações referentes as normas de conduta e organização. A primeira é caracterizada pela imposição de obrigações

de comportamento direto, com consequências legais em caso de não cumprimento. Já a segunda é estabelecida pela estrutura de órgãos e entidades, definindo suas competências e atribuições, sendo o tratamento de dados parte essencial do exercício dessas atribuições.

Assim sendo, a execução de políticas públicas permite que a administração pública trate dados necessários para executar políticas públicas previstas em leis, regulamentos ou outros instrumentos formais. Contudo, a definição exata de políticas públicas não é fornecida no Lei Geral de Proteção de Dados, mas a prática administrativa e os atos formais que instituem tais políticas devem ser considerados. Portanto, no caso do tratamento de dados sensíveis pelo poder público, a base legal é mais restrita e geralmente vinculada a políticas públicas executadas por órgãos públicos.

Destarte, o tratamento de dados pessoais pelo poder público deve sempre estar fundamentado em uma base legal específica, levando em consideração os interesses dos titulares dos dados e o cumprimento das obrigações legais e regulatórias.

3. OS REQUISITOS E AS FORMALIDADES A SEREM OBSERVADOS NAS HIPÓTESES DE USO COMPARTILHADO DE DADOS PESSOAIS;

O compartilhamento de dados pessoais é 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. Sua definição é compreendida como

> *comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicas 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"*[15].

O uso compartilhado de dados é um mecanismo extremamente relevante para a execução de atividades típicas e rotineiras do Poder Público, sendo reconhecida na Lei Geral de Proteção de Dados através do seu artigo 25, ao dispor que os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas 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.[16]

Assim sendo, 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*[17].

É importante observar que diante do novo contexto da sociedade digital é possível captar uma ampla diversidade de informações, por meio de diversas fontes, incluindo navegação online, registros em sites, dados de bancos de dados variados, bem

---

[15] FEDERAL, Governo. *Fique por dentro das palavras e termos-chave que dão suporte à Lei Geral de Proteção de Dados Pessoais*. 2020. Disponível em: https://www.serpro.gov.br/lgpd/menu/a-lgpd/glossario-lgpd. Acesso em: 09 maio 2024.

[16] FEDERAL, Supremo Tribunal. *STF valida compartilhamento de dados mediante requisitos*: o plenário também fixou restrições à atuação do comitê central de governança de dados.. O Plenário também fixou restrições à atuação do Comitê Central de Governança de Dados.. 2022. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=494227. Acesso em: 09 maio 2024.

[17] BRASIL. REPÚBLICA FEDERATIVA DO BRASIL. *Seção 1. Diário Oficial da União.* Brasília, p. 2-2. jun. 2023. Disponível em: https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=28/06/2023&jornal=515&pagina=2&totalArquivos=109. Acesso em: 09 maio 202.

como exigências acesso a serviços governamentais. Por exemplo, ao solicitar uma licença para conduzir veículo automotor no Brasil, os cidadãos fornecem uma série de dados pessoais, como nome, cadastro de pessoa física, endereço e informações biométricas. Isso inclui ocorrência da coleta de assinaturas digitais e físicas para identificação.[18]

Para isso, o compartilhamento de dados pessoais entre órgãos públicos possui pressupostos rigorosos em concordância com o art. 23, inciso I, da LGPD[19] ao qual garante a divulgação apropriada das circunstâncias em que cada instituição governamental compartilha ou obtém acesso a informações pessoais armazenadas em bancos de dados. Portanto, será exigido o fornecimento de 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.[20]

Ademais, a Lei Geral de Proteção de Dados estabelece a obrigatoriedade de coleta de consentimento do titular para comunicação ou compartilhamento de seus dados consoante as exceções respaldas nas hipóteses de dispensa de consentimento, execução de atividades de sua competência e nas demais

[18]CELLA, José Renato Gaziero; COPETTI, Rafael. Compartilhamento de dados pessoais e a administração pública brasileira. *Revista de Direito, Governança e Novas Tecnologias*, Maranhão, v. 3, n. 2, p. 39-58, dez. 2017. Disponível em: https://indexlaw.org/index.php/revistadgnt/article/view/2471/pdf. Acesso em: 08 maio 2024.

[19] 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, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:
I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos;

[20] BRASIL, Lei n.º 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 07 mai. 2024.

exceções tratadas no artigo 26, § 1º, da lei supramencionada.

Nesse sentido foi promulgado em 9 de outubro de 2019, o Decreto n.º 10.046, com o propósito de facilitar a troca de informações nos serviços públicos. Esta ação impulsionou a criação do Cadastro Base do Cidadão, uma plataforma consolidada que reúne dados de múltiplos bancos de dados do governo federal. Além disso, essa medida busca integrar informações de diferentes fontes do Poder Executivo com o intuito de estabelecer um sistema unificado de identificação do cidadão para a oferta de serviços públicos.[21]

A normativa estabelece três formas de compartilhar informações, eliminando a necessidade de convênios ou acordos para a troca de dados. Quando os dados não estão sujeitos a restrições ou confidencialidade, a partilha será aberta, envolvendo divulgação pública e disponibilização para qualquer interessado. Por outro lado, a abordagem restrita será aplicada para dados sujeitos a obrigações de confidencialidade, com o objetivo de facilitar a comunicação entre as entidades na execução de políticas públicas.

Por último, a abordagem específica refere-se a informações confidenciais, compartilhadas exclusivamente com órgãos designados. Nessa linha, a base integrada engloba informações básicas sobre os cidadãos brasileiros, como número de CPF, nome, data de nascimento, gênero, filiação, nacionalidade e naturalidade. Os órgãos do governo federal têm a possibilidade de requerer acesso a essa base e aos dados de identificação através da adesão ao sistema.[22]

Todavia, após a promulgação do Decreto supramencionado ações foram ajuizadas, respectivamente, pelo Conselho Federal da Ordem dos Advogados do Brasil e pelo Partido Socialista Brasileiro, que alegavam que o Decreto 10.046/2019 da

[21]BRASIL. *Decreto n.º 10.046, de 9 de outubro de 2019*. Brasília, 09 out. 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 09 maio 2024.
[22] BRASIL, ref.16.

Presidência da República, que dispõe sobre a governança desse compartilhamento de dados, geraria uma espécie de vigilância massiva e representaria controle inconstitucional do Estado, entre outras alegações.[23]

Nesse contexto, ocorreu o julgamento da Ação Direta de Inconstitucionalidade n.º 6.649, com relatoria do Ministro Gilmar Mendes do Supremo Tribunal Federal, no qual foi aprovado pelo pleno da corte, decidindo que para acessar o Cadastro Base do Cidadão devem ser observados rigorosos mecanismos de controle, condicionando o compartilhamento e processamento das informações pessoais à demonstração de propósitos legítimos, específicos e explícitos por parte dos órgãos e entidades do Poder Público.

> *[...] 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.*
> *[...] 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". [24]*
> *[...] A inclusão de novos dados na base integradora e a escolha*

[23] TRIBUNAL, Supremo Federal. *STF valida compartilhamento de dados mediante requisitos*. 2022. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=494227&ori=1. Acesso em: 09 maio 2024.
[24]JUSTIÇA, Supremo Tribunal de. *ADI 6649*. 2020. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=6079238. Acesso em: 09 maio 2024.

> *de bases temáticas que comporão o Cadastro Base do Cidadão devem ser precedidas de justificativas formais, prévias e minudentes, cabendo ainda a observância de medidas de segurança compatíveis com os princípios de proteção da Lei Geral de Proteção de Dados Pessoais, inclusive a criação de sistema eletrônico de registro de acesso, para fins de responsabilização em caso de abuso*[25].

Contudo, é essencial haver um limite ao compartilhamento de dados pessoais, especialmente quando isso compromete outros direitos relacionados à privacidade que carecem de receber proteção jurídica. Assim sendo, os procedimentos vão desde a coleta, armazenamento e tratamento de dados precisam de tutela jurídica. Afinal, trata-se de dados pessoais relativos à personalidade da pessoa, a aspectos da vida privada, e podem comprometer a imagem do indivíduo perante terceiros, sua moral e estrutura psíquica quando indevidamente utilizados ou tornados públicos.

Afinal, crescentemente o poder público tem solicitado dos indivíduos a divulgação constante de informações pessoais, carecendo da devida exploração sobre suas justificativas legais. Esse excessivo compartilhamento com outras entidades estatais traz como perigo manifesto a limitação da autodeterminação, que cada vez mais se intensifica. O armazenamento dos dados por instituições públicas não os torna de acesso público, pois eles continuam sendo de caráter pessoal.[26]

Esse entendimento está refletido pelo enfoque na construção de um governo digital pelo Estado brasileiro iniciado no ano de 2016, que propôs atender a todos os cidadãos, em todos os lugares e em diversos contextos socioeconômicos e culturais.

---

[25] JUSTIÇA, ref. 19.

[26] COELHO, Marcus Vinicius da Silva; SOUSA, Daiane Rodrigues de. Os impactos da lei de proteção de dados pessoais. *A (I)Responsabilidade do Poder Público no Compartilhamento de Informações e O Direito À Privacidade*, Rubiataba, p. 1-43, jun. 2022. Disponível em: http://repositorio.aee.edu.br/jspui/bitstream/aee/20154/1/2022%20-%20TCC%20-%20DAIANE%20RODRIGUES%20DE%20SOUSA.pdf. Acesso em: 09 maio 2024.

A estratégia está integrada com ações de todos os órgãos federais com o objetivo oferecer os serviços de melhor qualidade, mais simples, acessíveis e a um custo menor para o cidadão através do uso de tecnologia[27].

No ano final do ano de 2019, cerca de 53% dos serviços do governo federal já estavam disponíveis na versão digital, sendo que mais de 500 serviços públicos, de 28 órgãos diferentes, foram disponibilizados em canais digitais. Somado a isso, a redução de R$ 345 milhões nas despesas anuais do governo permite investimento suficiente para a construção de 156 novas Unidades de Pronto Atendimento (UPAs) na saúde ou 182 creches para educação de crianças[28].

Por outro lado, a disponibilização deste acesso simplificado ao governo, a qualquer momento de necessidade, eliminou aproximadamente 146 milhões de horas que o cidadão desperdiçava em deslocamento, filas e burocracia, todos os anos. Essa transformação proporciona ganhos de eficiência para a gestão pública, do qual permite que servidores sejam remanejados para outras áreas com maiores demanda do órgão e maior complexidade nas tarefas, tendo em vista que processos anteriormente complexos foram acelerados pelo uso da tecnologia. [29]

Tais ações demonstradas acima fizeram com que o Brasil atingisse a 2ª posição entre os países mais desenvolvidos do mundo em serviços públicos digitais pelo Banco Mundial[30]. Mesmo que o objetivo estabelecido durante a concepção do plano de execução do governo eletrônico fosse alcançar até o

[27]FEDERAL, Governo. *Estratégia de governo digital*. 2023. Disponível em: https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/EGD2020. Acesso em: 09 maio 2024.
[28]FEDERAL, ref. 22.
[29]FEDERAL, ref. 22.
[30]FEDERAL, Governo. *Brasil é reconhecido como segundo líder em governo digital do mundo*. 2023. Disponível em: https://www.gov.br/governodigital/pt-br/noticias/brasil-e-reconhecido-como-segundo-lider-em-governo-digital-no-mundo. Acesso em: 09 maio 2024.
[29] FEDERAL, ref. 22.

final de 2023 a disponibilidade digital de aproximadamente 5 mil serviços federais através da Plataforma GOV.BR, apenas 89% das iniciativas foram concluídas.[31].

A realidade do uso predominante de dados pelo Poder Público torna-se implacável, uma vez que, todas essas ações estão interconectadas com dados de mais de 203.062.512 de brasileiros[32], sendo 84% com acesso frequente à internet[33]. Embora o Estado procure fortalecer processos com o uso de dados, uma pesquisa da Kaspersky em colaboração com a consultoria Corpa revelou que o Brasil ocupa o primeiro lugar na lista de países com o maior número de pessoas que desconhecem seus direitos em relação à proteção de dados pessoais (20% dos entrevistados) – especificamente no contexto da Lei Geral de Proteção de Dados (LGPD) no Brasil. Além disso, somente metade dos participantes indicou estar ciente das consequências da lei para as organizações em que são empregados[34].

Nessa linha, a mesma pesquisa apontou que a principal causa de vazamento de informações pessoais continua sendo os ciberataques que, além de aumentar em volume, também evoluem continuamente. Por isso a cibersegurança tem uma importância tão grande na proteção de dados e prevenção de vazamentos.[35]

31

32SENADO. *IBGE divulga primeiros dados do Censo Demográfico de 2022*. 2022. Disponível em: https://www12.senado.leg.br/radio/1/noticia/2023/06/29/ibge-divulga-primeiros-dados-do-censo-demografico-de-2022#:~:text=O%20Instituto%20Brasileiro%20de%20Geografia,anterior%20da%20pesquisa%2C%20em%202010. Acesso em: 08 maio 2024.

33 SILVA, Victor Hugo; OTÁVIO, Murilo. *Acesso à internet cresce no Brasil e chega a 84% da população em 2023, diz pesquisa*. 2023. Disponível em: https://g1.globo.com/tecnologia/noticia/2023/11/16/acesso-a-internet-cresce-no-brasil-e-chega-a-84percent-da-populacao-em-2023-diz-pesquisa.ghtml. Acesso em: 09 maio 2024.

34 KASPERSKY. *Pesquisa da Kaspersky revela que 20% dos brasileiros não tem conhecimento sobre a LGPD*. 2023. Disponível em: https://www.kaspersky.com.br/about/press-releases/2024_pesquisa-da-kaspersky-revela-que-20-dos-brasileiros-nao-tem-conhecimento-sobre-a-lgpd. Acesso em: 10 maio 2024.

35 KASPERSKY, ref. 32..

Logo, denota-se a necessidade da transparência pelos órgãos do Poder Público sobre as bases legais para coleta, armazenamento, e a qualidade (dos dados pessoais|), bem como seu uso aumenta ainda mais essas preocupações, criando um ambiente em que os cidadãos podem se sentir coagidos a fornecer informações pessoais sem compreender plenamente os impactos e as garantias legais associadas a esses compartilhamentos.

Desse modo, a pesquisa da Tenable, empresa americana especializada em gerenciamento de exposição cibernética, apontou que 984,7 milhões de dados foram vazados no Brasil no ano passado. Isso representa 112 terabytes de informações expostas no país, volume que representa 43% dos 257 terabytes em todo o mundo, segundo o Relatório do Cenário de Ameaças feito pela companhia suprarreferida.[36]

A título exemplificativo, recentemente em 31 de janeiro de 2024, a Coordenação-Geral de Fiscalização (CGF) da Autoridade Nacional de Proteção de Dados (ANPD) apresentou quatro advertências à Secretaria de Estado de Educação do Distrito Federal (DF) devido às infrações dos artigos 37, 38 e 48 da Lei Geral de Proteção de Dados Pessoais (LGPD), com o artigo 5º do regulamento de fiscalização da autarquia federal. As sanções estabelecidas possuem força de advertências e não estabelecem medidas corretivas específicas para a secretaria[37].

O incidente com a Secretaria de Estado de Educação do Distrito Federal (SEEDF) foi julgado mediante processo administrativo[38] pela Autoridade Nacional de Proteção de Dados

[36]OTÁVIO, Chico. *Golpistas vazaram quase 1 bilhão de dados no Brasil em 2022. Quadrilhas montam painéis para vender na internet*. 2023. Disponível em: https://oglobo.globo.com/economia/defesa-do-consumidor/noticia/2023/06/dossies-com-dados-publicos-e-privados-municiam-golpes-eletronicos.ghtml. Acesso em: 10 maio 2024.

[37]INGIZZA, Carolina. *ANPD aplica sanções à secretaria de educação do DF por infrações à LGPD*. 2024. Disponível em: https://www.jota.info/executivo/anpd-aplica-sancoes-a-secretaria-de-educacao-do-df-por-infracoes-a-lgpd-31012024?non-beta=1. Acesso em: 10 maio 2024.

[38] BRASIL. Autoridade Nacional de Proteção de Dados. Nota Técnica Nº

(ANPD), como sendo constatado que a secretaria estava expondo indevidamente dados cadastrais e de saúde de cerca de 3.000 pessoas cadastradas no Programa Educação Precoce. Todo o problema ocorreu devido a uma falha de segurança no formulário de inscrição do programa.[39]

Contudo, mesmo após a formalização da ocorrência pela autarquia, a secretaria optou por não informar os titulares dos dados para evitar pânico exagerado e buscou resolver a questão de forma interna. Não obstante, mesmo diante da avaliação pela Coordenação de Tecnologia e Pesquisa da Autoridade Nacional de Proteção de Dados (ANPD) acerca da constatação de que o incidente de segurança era grave e que medidas apresentas eram insuficientes, sequer foi apresentado o relatório de impacto à proteção de dados da atividade afetada pelo incidente, registros de operações de tratamento de dados ou qualquer outro tipo de manifestação sobre a violação[40].

Já em 20 de setembro de 2023, a Justiça Federal[41] determinou que aproximadamente sejam indenizadas em R$ 15 mil reais cerca de 4 milhões de pessoas em razão do vazamento numeroso de dados ocorrido no ano de 2022. Os valores deverão ser pagos pela Caixa Econômica Federal, Empresa de Tecnologia e Informações da Previdência (Dataprev) e Autoridade Nacional de Proteção de Dados (ANPD), em razão da ação civil pública postulada pelo Instituto Brasileiro de Defesa da Proteção

57/2022/Cgf/Anpd nº 57/2022. Secretaria de Estado de Educação do Distrito Federal (SEEDF). Brasília, DF, 31 de janeiro de 2024. *Processo Sei/Anpd Nº 00261.001472/2021-41;*: Comunicação de Incidente de Segurança com Dados Pessoais. Brasília: Governo Federal, 31 jan. 2024. Disponível em: https://www.gov.br/anpd/pt-br/composicao-1/coordenacao-geral-de-fiscalizacao/pas-gdf-processo-publico.pdf. Acesso em: 26 maio 2024.

[39] INGIZZA, ref. 32.

[40] INGIZZA, ref. 32.

[41] BRASIL. Justiça Federal da 3ª Região - 1º Grau. Indenização Por Dano Moral, Indenização Por Dano Material, Lei Geral de Proteção de Dados (Lgpd), Lei Geral de Proteção de Dados (Lgpd) nº : 5028572-20.2022.4.03.6100. Decisão Judicial. São Paulo, 11 set. 2023. Disponível em: https://static.poder360.com.br/2023/09/decisaojustica-13set2023.pdf. Acesso em: 27 maio 2024.

de Dados Pessoais, Compliance e Segurança da Informação pela garantia dos direitos dos cidadãos prejudicados.[42]

Esse vazamento de dados armazenados alcançara majoritariamente os beneficiários do Auxílio Brasil, os quais, próximos às eleições presidenciais de 2022, passaram a ter possibilidade de disponibilizar uma parcela significativa de seus benefícios destinada para obtenção de crédito consignado. Logo, os dados pessoais vazados foram indevidamente adquiridos por agentes bancários terceirizados com fim de oferecer empréstimos e outros serviços financeiros.[43]

Dessa forma, o compartilhamento excessivo de dados entre entidades governamentais pode levar à criação de perfis detalhados dos cidadãos, aumentando a exposição de suas informações pessoais aos mais diversos tipos de agentes interessados no condicionamento de ações por meio de algorítmicos. A consequência direta de tais ações é a violação à autodeterminação dos indivíduos e o comprometimento de seus direitos a liberdade e privacidade.[44]

Na sociedade de vigilância, as tecnologias de coleta e análise de dados permitem que as autoridades governamentais e outras entidades monitorem e controlem os cidadãos em uma escala sem precedentes. Isso não apenas mina a privacidade e a liberdade individual, mas também cria um ambiente propício para abusos de poder e violações dos direitos fundamentais.

Conforme observado por Rodotà, o direito ao respeito

---

[42]FEDERAL, Ministério Público. *Justiça determina indenização de R$ 15 mil a cidadãos que tiveram dados pessoais vazados em 2022*. 2023. Disponível em: https://www.mpf.mp.br/sp/sala-de-imprensa/noticias-sp/justica-determina-indenizacao-de-r-15-mil-a-cidadaos-que-tiveram-dados-pessoais-vazados-em-2022. Acesso em: 10 maio 2024.

[43]FEDERAL, ref. 35.

[44] PAIVA, Marcella da Costa Moreira de; RAMADA, Paula Cristiane Pinto; PIRES, Telson. Sociedade da informação e vigilância. In: MARTINS, Plínio Lacerda *et al*. *Proteção de Dados*. Rio de Janeiro: Instituto de Direito Público e Privado, 2021. p. 85-98. Disponível em: http://ppgdin.uff.br/wp-content/uploads/sites/5/2021/03/Livro-Estudos-do-Grupo-de-Prote%C3%A7%C3%A3o-de-Dados-Pessoais-%E2%80%93-CNPQ.pdf. Acesso em: 10 maio 2024.

pela vida privada e familiar era predominantemente visto como um aspecto individualista. No entanto, dentro dessa proteção, a salvaguarda dos dados pessoais representa uma forma dinâmica de proteção que acompanha os dados em todos os seus movimentos. Isso implica em uma ampliação do escopo do direito à privacidade, resultando na especificação do direito à autodeterminação informativa. Este direito inclui a capacidade de manter controle sobre suas próprias informações e a liberdade para o titular escolher como configurar sua esfera particular.[45]

CONSIDERAÇÕES FINAIS

Após toda a abordagem realizada no presente artigo, percebe-se que o emprego da ética e de boas práticas que atendam a princípios no tratamento de dados pessoais são essenciais para garantir a proteção da privacidade dos indivíduos e para manter a confiança no poder público quando este maneja dados. Estas práticas são baseadas em princípios fundamentais que orientam a coleta, uso, armazenamento e compartilhamento de dados de maneira responsável devendo ser claro sobre suas práticas de tratamento de dados. Isso inclui informar aos indivíduos sobre quais dados estão sendo coletados, porque estão sendo coletados, como serão usados, com quem serão compartilhados e por quanto tempo serão armazenados, deve ainda adotar políticas de privacidade e avisos de coleta de dados escritos em linguagem clara e acessível, evitando jargões técnicos que possam confundir os usuários.

Ainda, quando a base legal de tratamento for o consentimento, os indivíduos devem receber informações suficientes para entender plenamente as implicações o quê que consentindo sendo que este deve ser obtido de forma voluntária, e os

[45] RODOTÀ, Stefano. *A vida na sociedade da vigilância* – a privacidade hoje. Organização, seleção e apresentação de Maria C. B. de Moraes. Trad. Danilo Doneda e Luciana C. Doneda. Rio de Janeiro: Renovar, 2008.

indivíduos devem ter a opção de revogá-lo a qualquer momento.

Outra prática importante é atender à minimização dos dados, ou seja, coletar apenas os dados pessoais que são estritamente necessários para cumprir a finalidade específica. A coleta excessiva de dados não só aumenta os riscos de privacidade, mas também é uma prática antiética. Praticar a retenção mínima de dados, eliminando-os de forma segura quando não forem mais necessários, bem como implementar medidas de segurança robustas para proteger os dados pessoais contra acessos não autorizados, perda, destruição ou alteração. Isso inclui o uso de tecnologias como criptografia, firewalls, e sistemas de detecção de intrusão, além de políticas internas de segurança da informação treinando os servidores sobre as melhores práticas de segurança e a importância da proteção de dados pessoais.

Garantir que os dados pessoais sejam acessíveis apenas por pessoas autorizadas e que têm uma necessidade legítima de acesso para desempenhar suas funções e evitar o compartilhamento de dados pessoais com terceiros, a menos que seja absolutamente necessário e que os terceiros estejam sujeitos às mesmas normas de privacidade e segurança.

O Poder público também deve ter responsabilidade e prestar contas do cumprimento das leis de proteção de dados e pelas práticas éticas de tratamento de dados. Isso inclui a designação de responsável pela proteção de dados e a realização de auditorias regulares para garantir a conformidade. Estabelecer canais para que os titulares de dados possam fazer perguntas, solicitar informações ou apresentar reclamações sobre o tratamento de seus dados e garantir que o tratamento de dados pessoais não resulte em discriminação ou injustiças[46]. Os dados não devem ser utilizados para fins que prejudiquem os direitos ou oportunidades dos indivíduos neste sentido é imperioso a

[46] O responsável por essas ações é o encarregado conforme o art. 5º, VIII - 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 (ANPD); (Redação dada pela Lei nº 13.853, de 2019).

implementação de medidas para detectar e corrigir quaisquer vieses ou práticas discriminatórias no tratamento de dados.

Respeitar e facilitar o exercício dos direitos dos titulares dos dados, como o direito de acesso, retificação, exclusão, restrição do tratamento, portabilidade e oposição. Prover mecanismos simples e eficientes para que os indivíduos possam exercer esses direitos. Realizar avaliações de impacto sobre a privacidade (Privacy Impact Assessments - PIAs) para identificar e mitigar riscos potenciais associados ao tratamento de dados pessoais, especialmente em novos projetos ou sistemas que envolvem grandes volumes de dados ou dados sensíveis.

Por fim, atentar para a ética na Inteligência Artificial e Big Data ao utilizar essas tecnologias avançadas, garantir que os algoritmos sejam transparentes e justos, evitando decisões automáticas que possam prejudicar os indivíduos sem supervisão humana adequada implementando práticas de governança de dados que assegurem o uso ético e responsável dessas tecnologias.

REFERÊNCIAS BIBLIOGRÁFICAS

BOTELHO, M. C.; CAMARGO, E. P. do A. O Tratamento de dados pessoais pelo poder público na LGPD. *Revista Direitos Sociais e Políticas Públicas (UNIFAFIBE)*, [S. l.], v. 9, n. 3, p. 549–580, 2022. DOI: 10.25245/rdspp.v9i3.1034. Disponível em: https://portal.unifafibe.com.br:443/revista/index.php/direitos-sociais-politicas-pub/article/view/1034. Acesso em: 9 maio. 2024.

BRASIL. Autoridade Nacional de Proteção de Dados. Nota Técnica Nº 57/2022/Cgf/Anpd nº 57/2022. Secretaria de Estado de Educação do Distrito Federal (SEEDF). Brasília,

DF, 31 de janeiro de 2024. *Processo Sei/Anpd Nº 00261.001472/2021-41*;: Comunicação de Incidente de Segurança com Dados Pessoais. Brasília: Governo Federal, 31 jan. 2024. Disponível em: https://www.gov.br/anpd/pt-br/composicao-1/coordenacao-geral-de-fiscalizacao/pas-gdf-processo-publico.pdf. Acesso em: 26 maio 2024.

BRASIL. Lei nº Lei N° 12.527, de 18 de novembro de 2001. Lei de Acesso A Informação. Brasília, DF: Governo Federal, 18 nov. 2001. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 27 maio 2024.

BRASIL, Lei n.º 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 07 mai. 2024.

BRASIL. *Decreto n.º 10.046, de 9 de outubro de 2019*. Brasília, 09 out. 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 09 maio 2024.

BRASIL. Justiça Federal da 3ª Região - 1º Grau. Indenização Por Dano Moral, Indenização Por Dano Material, Lei Geral de Proteção de Dados (Lgpd), Lei Geral de Proteção de Dados (Lgpd) nº : 5028572-20.2022.4.03.6100. Decisão Judicial. São Paulo, 11 set. 2023. Disponível em: https://static.poder360.com.br/2023/09/decisaojustica-13set2023.pdf. Acesso em: 27 maio 2024.

BRASIL. República Federativa do Brasil. *Seção 1. Diário Oficial da União.* Brasília, p. 2-2. jun. 2023. Disponível em: https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=28/06/2023&jornal=515&pagina=2&totalArquivos=109. Acesso em: 09 maio 202.

CAVALCANTI., Themistocles Brandão. *Teoria dos atos administrativos*. São Paulo: Revista dos Tribunais, 1973. 345

p.

CELLA, José Renato Gaziero; COPETTI, Rafael. Compartilhamento de dados pessoais e a administração pública brasileira. *Revista de Direito, Governança e Novas Tecnologias*, Maranhão, v. 3, n. 2, p. 39-58, dez. 2017. Disponível em: https://indexlaw.org/index.php/revistadgnt/article/view/2471/pdf. Acesso em: 08 maio 2024.

COELHO, Marcus Vinicius da Silva; SOUSA, Daiane Rodrigues de. Os impactos da lei de proteção de dados pessoais. *A (I)Responsabilidade do Poder Público no Compartilhamento de Informações e O Direito À Privacidade*, Rubiataba, p. 1-43, jun. 2022. Disponível em: http://repositorio.aee.edu.br/jspui/bitstream/aee/20154/1/2022%20-%20TCC%20-%20DAIANE%20RODRIGUES%20DE%20SOUSA.pdf. Acesso em: 09 maio 2024.

CRAVO, Daniela Copetti; CUNDA, Daniela Zago Gonçalves da; RAMOS, Rafael. Lei Geral de Proteção de Dados e o Poder Público. Porto Alegre: Tribunal de Contas do Estado do RGS, 2021. Disponível em: https://lproweb.procempa.com.br/pmpa/prefpoa/pgm/usu_doc/ebook_lgpd_e_poder_publico_23052021.pdf. Acesso em: 09 maio 2024.

FEDERAL, Governo. *Brasil é reconhecido como segundo líder em governo digital do mundo*. 2023. Disponível em: https://www.gov.br/governodigital/pt-br/noticias/brasil-e-reconhecido-como-segundo-lider-em-governo-digital-no-mundo. Acesso em: 09 maio 2024.

FEDERAL, Governo. *Estratégia de governo digital*. 2023. Disponível em: https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/EGD2020. Acesso em: 09 maio 2024.

FEDERAL, Governo. *Fique por dentro das palavras e termos-chave que dão suporte à Lei Geral de Proteção de Dados*

Pessoais. 2020. Disponível em: https://www.serpro.gov.br/lgpd/menu/a-lgpd/glossario-lgpd. Acesso em: 09 maio 2024.

FEDERAL, Ministério Público. *Justiça determina indenização de R$ 15 mil a cidadãos que tiveram dados pessoais vazados em 2022*. 2023. Disponível em: https://www.mpf.mp.br/sp/sala-de-imprensa/noticias-sp/justica-determina-indenizacao-de-r-15-mil-a-cidadaos-que-tiveram-dados-pessoais-vazados-em-2022. Acesso em: 10 maio 2024.

FEDERAL, Supremo Tribunal. *STF valida compartilhamento de dados mediante requisitos*: o plenário também fixou restrições à atuação do comitê central de governança de dados.. O Plenário também fixou restrições à atuação do Comitê Central de Governança de Dados.. 2022. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=494227. Acesso em: 09 maio 2024.

INGIZZA, Carolina. *ANPD aplica sanções à secretaria de educação do DF por infrações à LGPD*. 2024. Disponível em: https://www.jota.info/executivo/anpd-aplica-sancoes-a-secretaria-de-educacao-do-df-por-infracoes-a-lgpd-31012024?non-beta=1. Acesso em: 10 maio 2024.

JUSTIÇA, Supremo Tribunal de. *ADI 6649*. 2020. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=6079238. Acesso em: 09 maio 2024.

KASPERSKY. *Pesquisa da Kaspersky revela que 20% dos brasileiros não tem conhecimento sobre a LGPD*. 2023. Disponível em: https://www.kaspersky.com.br/about/press-releases/2024_pesquisa-da-kaspersky-revela-que-20-dos-brasileiros-nao-tem-conhecimento-sobre-a-lgpd. Acesso em: 10 maio 2024.

LANDERDAHL, Cristiane et al. *Tratamento de dados pessoais pelo Poder Público.* 2. ed. Brasília: Autoridade Nacional

de Proteção de Dados, 2023. 52 p. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em: 08 maio 2024.

OTÁVIO, Chico. *Golpistas vazaram quase 1 bilhão de dados no Brasil em 2022. Quadrilhas montam painéis para vender na internet*. 2023. Disponível em: https://oglobo.globo.com/economia/defesa-do-consumidor/noticia/2023/06/dossies-com-dados-publicos-e-privados-municiam-golpes-eletronicos.ghtml. Acesso em: 10 maio 2024.

PAIVA, Marcella da Costa Moreira de; RAMADA, Paula Cristiane Pinto; PIRES, Telson. Sociedade da informação e vigilância. In: MARTINS, Plínio Lacerda *et al*. *Proteção de Dados*. Rio de Janeiro: Instituto de Direito Público e Privado, 2021. p. 85-98. Disponível em: http://ppgdin.uff.br/wp-content/uploads/sites/5/2021/03/Livro-Estudos-do-Grupo-de-Prote%C3%A7%C3%A3o-de-Dados-Pessoais-%E2%80%93-CNPQ.pdf. Acesso em: 10 maio 2024.

PINHEIRO, Patrícia Peck. *Proteção de dados pessoais*: comentários à Lei n. 13.709/2018 (LGPD). 2. ed. São Paulo: Saraiva, 2020.

RODOTÀ, Stefano. *A vida na sociedade da vigilância* – a privacidade hoje. Organização, seleção e apresentação de Maria C. B. de Moraes. Trad. Danilo Doneda e Luciana C. Doneda.

RODOTÀ, Stefano. Stefano Rodotá. *Tecnologie e diritti*. Bologna: Il Molino. 1995.

SARLET, Gabrielle Bezerra Sales; RODRIGUEZ, Daniel Piñeiro. A autoridade nacional de proteção de dados: elementos para uma estruturação independente e democrática na era da governança digital. Direitos Fundamentais e Democracia, [s. l], v. 27, p. 217-253, dez. 2022.

Disponível em: https://revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/article/view/2285. Acesso em: 09 maio 2024.Rio de Janeiro: Renovar, 2008.

SARLET, Ingo Wolfgang. Fundamentos Constitucionais: o direito fundamental à proteção de dados. In: BIONI, Bruno [et al.]. (org.). Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2021. p. 21-59.

SENADO. *IBGE divulga primeiros dados do Censo Demográfico de 2022*. 2022. Disponível em: https://www12.senado.leg.br/radio/1/noticia/2023/06/29/ibge-divulga-primeiros-dados-do-censo-demografico-de-2022#:~:text=O%20Instituto%20Brasileiro%20de%20Geografia,anterior%20da%20pesquisa%2C%20em%202010. Acesso em: 08 maio 2024.

SILVA, Victor Hugo; OTÁVIO, Murilo. *Acesso à internet cresce no Brasil e chega a 84% da população em 2023, diz pesquisa*. 2023. Disponível em: https://g1.globo.com/tecnologia/noticia/2023/11/16/acesso-a-internet-cresce-no-brasil-e-chega-a-84percent-da-populacao-em-2023-diz-pesquisa.ghtml. Acesso em: 09 maio 2024.

TRIBUNAL, Supremo Federal. *STF valida compartilhamento de dados mediante requisitos*. 2022. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=494227&ori=1. Acesso em: 09 maio 2024.