



PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS  
PRO-REITORIA DE GRADUAÇÃO  
ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO  
CURSO DE DIREITO  
NÚCLEO DE PRÁTICA JURÍDICA  
COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO

**OS LIMITES DO TRATAMENTO DE DADOS PELO PODER PÚBLICO:  
SERVIÇO PÚBLICO ONLINE, PORTAL GOV.BR E O CADASTRO BASE DO  
CIDADÃO (CBC)**

ORIENTANDA: MARIALUIZA FERREIRA LIMA

ORIENTADORA: PROF<sup>a</sup>. DR.<sup>a</sup> FERNANDA DA SILVA BORGES

GOIÂNIA-GO  
2023

MARIALUIZA FERREIRA LIMA

**OS LIMITES DO TRATAMENTO DE DADOS PELO PODER PÚBLICO:  
SERVIÇO PÚBLICO ONLINE, PORTAL GOV.BR E O CADASTRO BASE DO  
CIDADÃO (CBC)**

Artigo Científico apresentado à disciplina Trabalho de  
Curso II, da Escola de Direito, Negócios e  
Comunicação da Pontifícia Universidade Católica de  
Goiás Prof.<sup>a</sup> Orientadora: Dr.<sup>a</sup> Fernanda da Silva  
Borges

GOIÂNIA-GO  
2023

MARIALUIZA FERREIRA LIMA

**OS LIMITES DO TRATAMENTO DE DADOS PELO PODER PÚBLICO:  
SERVIÇO PÚBLICO ONLINE, PORTAL GOV.BR E O CADASTRO BASE DO  
CIDADÃO (CBC)**

Data da Defesa: 17 de maio de 2023.

BANCA EXAMINADORA

---

Orientador (a): Prof. (a): Dr.<sup>a</sup> Fernanda da Silva Borges Nota

---

Examinador (a) Convidado (a): Prof. (a): Me. Eliane Rodrigues Nunes Nota

**OS LIMITES DO TRATAMENTO DE DADOS PELO PODER PÚBLICO:  
SERVIÇO PÚBLICO ONLINE, PORTAL GOV.BR E O CADASTRO BASE DO  
CIDADÃO (CBC)**

Marialuiza Ferreira Lima<sup>1</sup>

O objetivo geral da pesquisa foi estudar quais são os limites do tratamento de dados pelo poder executivo federal no exercício da prestação de serviço público. Consequentemente, discutiu-se sobre a vulnerabilidade do cidadão enquanto consumidor necessário de serviços públicos. Sobretudo, diante das nuances que envolvem o governo digital. Nesse hiato, a pesquisa também vislumbra as diretrizes recepcionadas pela Lei Geral de Proteção de Dados (LGPD) no tocante ao exercício do tratamento de dados pelo poder público. A metodologia utilizada foi a pesquisa bibliográfica com abordagem qualitativa. Por fim, foi possível associar os limites do tratamento de dados à preservação dos direitos e garantias fundamentais inerentes à pessoa titular desses dados, como por exemplo a autodeterminação informativa.

**Palavras-chave:** Banco de dados. Tratamento de dados pessoais. LGPD. Princípios.

---

<sup>1</sup> Acadêmica do curso de Direito da Pontifícia Universidade de Goiás. Natural de Quirinópolis, Goiás. Iniciou a graduação no ano de 2019. Desde o primeiro ano da faculdade participou ativamente de atividades extracurriculares na Liga Acadêmica de Acessibilidade ao Direito (LAAD), como membro e, atualmente, Coordenadora de Pesquisa; na Bateria Universitária Primata como ritmista, Coordenadora de Ritmos e Regente; e, também, na Atlética Associação Clóvis Beviláqua (Atlética Primata), como atleta de basquetebol. Além disso, participou da Iniciação Científica da PUC-GO, cujo trabalho foi desenvolvido entre 2021-2022.

## INTRODUÇÃO

É possível notar o quanto a revolução da tecnologia digital-virtual tornou-se indispensável para a manutenção da vida em sociedade, como por exemplo, a comunicação pelas redes sociais, compra e venda online, serviços públicos digitais, fácil acesso à pesquisas e outras infinitudes de coisas que a internet é capaz de oferecer. Dessa forma, a sociedade evoluiu para um novo modelo de organização, em torno da informatização em massa, situação da qual emergem novos fatos sociais a serem discutidos pelas ciências jurídicas.

Nesse contexto, a migração dos sistemas de comunicação e prestação de serviços para o meio digital, intensificou a manutenção e o compartilhamento de dados de pessoais. Do mesmo modo, o poder público enquanto administrador dos interesses públicos adaptou-se às novas condições de gerenciamento de informações e serviços públicos, migrando para o meio digital.

Diante disso, a prestação de serviços públicos está vinculada ao tratamento de dados pessoais dos cidadãos por intermédio de sistemas digitais de banco de dados públicos. Nessa conjuntura, tendo em vista a vulnerabilidade dos dados pessoais perante a utilização de serviços prestados pelo Governo, urge a necessidade de se observar quais são os limites do tratamento de dados pelo poder público e suas nuances.

Assim sendo, a relevância social e jurídica da pesquisa diz respeito à atualidade do tema e da conveniência em promover o debate a fim de incentivar a difusão do conhecimento sobre as problemáticas que envolvem o tratamento de dados pessoais. Do mesmo modo, o objetivo geral da pesquisa é estudar quais são os limites do tratamento de dados pelo poder executivo federal no exercício da prestação de serviço público.

De forma complementar, são objetivos específicos: discutir a vulnerabilidade do cidadão enquanto consumidor necessário de serviços públicos; apresentar as nuances que envolvem o governo digital; e, discutir a inobservância do Cadastro Base do Cidadão (CBC) às determinações da Lei Geral de Proteção de Dados (LGPD).

A metodologia utilizada para o desenvolvimento do trabalho foi a pesquisa qualitativa, através do levantamento bibliográfico de doutrinas, artigos científicos, leis e jurisprudências todos a respeito da proteção de dados.

Com efeito, a estrutura das seções foi dividida de forma que o primeiro tópico dispõe inicialmente sobre o contexto da evolução das máquinas de computador e da internet. Assim, na sequência, o trabalho inicia as análises referentes ao tratamento de dados pessoais. Posteriormente, a segunda seção discute as nuances a respeito do Governo Digital desenvolvido

através do portal gov.br, como também, do aparato legislativo sobre a proteção de dados. Por fim, na terceira seção a discussão passa pela análise do Cadastro Base do Cidadão, com o escopo de exemplificar a quantidade de dados pessoais à disposição do poder público. E, por conseguinte, quais são os limites do tratamento de dados pessoais pelo poder público.

## **1 DISPOSIÇÕES GERAIS SOBRE O TRATAMENTO DE DADOS**

Antes de discorrer especificamente sobre o tratamento de dados pessoais pelo poder público do Brasil, é imprescindível fazer uma concisa retrospectiva histórica acerca da evolução das tecnologias que culminaram para a eclosão de uma sociedade da informação. Dessa forma será possível traçar uma linha de raciocínio que perpassa o início das tecnologias que possibilitaram a era digital e, conseqüentemente, fragilizaram a segurança pública ante o fornecimento de dados.

É possível conceituar a sociedade da informação como sendo um novo modelo de organização social em que a informação é elemento fundamental no desenvolvimento da economia e demais setores. Esse novo conceito de organização da sociedade existe como consequência da evolução tecnológica, a qual criou mecanismos capazes de processar e transmitir informações em quantidades e velocidades surpreendentes (BIONI, 2019).

O desenvolvimento da tecnologia atual, definida como digital, não foi uma ocorrência isolada. Em verdade, foi o resultado de um conjunto de macroinvenções que fomentaram microinvenções em variados setores da tecnologia, dentre eles, os de processamento, comunicação, armazenamento e o digital virtual.

Levando-se em consideração esse contexto de macroinvenções, a análise da evolução digital iniciará pelo segundo momento da Revolução Industrial, conforme descrição do autor Manuel Castells (1999). Esse período, já entre os séculos XVIII e XIX, foi definido pelo desenvolvimento da eletricidade, do motor de combustão interna, e pelo uso de produtos químicos. Esse último período marca o início das tecnologias de comunicação, através da difusão do telégrafo e a invenção do telefone.

Em meio a esse entusiasmo de avanços da tecnologia e da ciência, foi a partir do século XX que os Estados Unidos da América se tornou o país pioneiro no desenvolvimento das tecnologias baseadas em eletrônicos. A primeira invenção necessária para se destacar consiste nos avanços da microeletrônica, cuja ciência possibilitou o processamento, codificação e comunicação entre as máquinas. Somente após os estudos em microeletrônica que o primeiro computador foi desenvolvido, na cidade da Filadélfia (CASTELLS, 1999).

O sucesso das máquinas de computadores alcançou enorme sucesso em razão do processamento de dados. Logo após, com advento de microprocessadores o primeiro microcomputador de sucesso comercial foi idealizado pelos jovens Steve Wozniak e Steve Jobs. Mais adiante, o primeiro software para microcomputadores foi possível. Em meados do ano de 1970, dois jovens fundaram a Microsoft, Bill Gates e Paul Allen.

Essa capacidade exponencial de desenvolvimento e processamento de informações computadorizadas somente tornou-se possível em razão do concomitante avanço das telecomunicações de rádio, linhas telefônicas etc. Em outras palavras, a expansão dos meios de comunicação em massa foi o estopim para o surgimento da sociedade da informação, em razão da capacidade de gerar informações, armazená-las, recuperar, processar e transmiti-las.

Ainda nas últimas décadas do século XX, a criação e o desenvolvimento científico da Internet foram financiados por militares através da Agência de Projetos de Pesquisa Avançada (ARPA) do Departamento de Defesa dos EUA, com a finalidade de criar um sistema de comunicação invulnerável a ataques nucleares. A ARPANET, nome da primeira rede de computadores, era baseada na tecnologia de comunicação da troca de pacotes de dados, assim o sistema tornava a rede independente de centros de comando e controle, para que a mensagem alcançasse suas próprias rotas ao longo da rede, sendo programada para manter sentido coerente em qualquer ponto da rede (CASTELLS, 1999).

O patrocínio e governança da internet pelo poder público não se sustentou por muito tempo em razão das pressões comerciais. Logo, a internet foi privatizada e não contava com nenhuma autoridade supervisora, apenas coordenações técnicas.

Consequentemente, o desenvolvimento da internet acompanhava o progresso da tecnologia de inovação dos computadores, de modo sucessivo. Num primeiro momento a preocupação era em estabelecer da forma mais consistente a comunicação em larga escala num curto espaço de tempo. Em seguida, foi possível desenvolver a transferência direta de arquivos entre computadores, sem passar por um sistema principal.

A respeito da dimensão de possibilidades que a Internet foi e é capaz de oferecer, a autora Patrícia Peck Pinheiro (2021) faz uma definição muito pontual:

A Internet é mais que um simples meio de comunicação eletrônica, formada não apenas por uma rede mundial de computadores, mas, principalmente, por uma rede mundial de Indivíduos. Indivíduos com letra maiúscula, porque estão inseridos em um conceito mais amplo, que abrange uma individualização não só de pessoas físicas como também de empresas, instituições e governos. A Internet elimina definitivamente o conceito de corporação unidimensional, impessoal e massificada. Isso significa profunda mudança na forma como o Direito deve encarar as relações entre esses Indivíduos. (PECK, 2021, p. 31)

Ademais, o avanço da tecnologia eletrônica e digital, somado à rede de computadores (internet) e à disposição de um software, conseguiram revolucionar a capacidade de processamento, armazenamento e transmissão de um enorme contingente de dados e, conseqüentemente, de informações. Uma vez que, estão dispostos nas suas mais variadas formas, como por exemplo, arquivos de multimídia, documentos digitalizados, localização, reconhecimento facial e digital, biometria entre outros.

Portanto, essa revolução tecnológica é capaz de fragilizar a seara jurídica dos direitos inerentes ao cidadão, como também, a sua intimidade e personalidade. Assim sendo, a nova realidade da tecnologia enquanto provocadora de mudanças sociais e comportamentais é também jurídica, provocando o estudo do direito e das nuances que ameaçam a manutenção dos direitos da pessoa humana.

## 1.1 A EXPOSIÇÃO DOS DADOS PESSOAIS

Conforme exposto, a revolução tecnológica em conjunto com a sociedade da informação capacitou o intenso fluxo de informações. Em outras palavras, a globalização da informação alterou substancialmente o método como a prestação de serviços, comunicação e diversos outros setores da vida em sociedade se organizam, forçando a adaptação de todos a esse novo sistema.

De antemão, vale estabelecer a diferença entre os conceitos de informação e de dados. Embora anteriormente mencionados como sinônimos, possuem particularidades divergentes. Segundo Bruno Bioni (2019) dados são fatos brutos, um estado primitivo da informação, que organizados isoladamente não acrescem nenhum conhecimento, mas que, se de forma diversa forem processados e organizados em conjunto, podem possibilitar a extração de alguma informação.

Outro conceito importante é a respeito do que se trata os dados pessoais. A Lei Geral de Proteção de Dados Pessoais (LGPD) conceitua como sendo toda informação relacionada a uma pessoa identificada ou identificável, isto é, pode conter nome, idade, endereço, localização, número de IP, registros de bens móveis ou imóveis etc.

O desenvolvimento da informática, em conjunto com a tecnologia da informação, foi imprescindível para a criação de sistemas de bancos de dados, em que softwares automatizam o acesso e o processamento quantitativo e qualitativo de dados, capazes de extrair informações.

Como por exemplo a tecnologia do *Big Data*, a qual permite que um volume exorbitante de dados seja estruturado e analisado para uma gama indeterminada de finalidades.

Em conclusão, não se trata somente de dados ou de bancos de dados, mas, necessariamente, da dinâmica de um sistema de informação, que é o que permite a um manancial de fatos (dados) ser estruturado, organizado e gerenciado para produzir um conhecimento que possa ser revertido para tomada de uma decisão (e.g., direcionamento da ação publicitária). A tecnologia da informação (dos bits ao sistema de informação) permitiu agregar e acumular dados que revelam muitas informações sobre nós. (BIONI, 2019, p. 51)

A migração dessas tecnologias para os sistemas de gerenciamento de dados públicos é uma realidade, ou seja, as esferas do poder público armazenam diversos tipos de dados dos cidadãos, em bancos de dados públicos. Diante disso, é sobre o tratamento de dados gerenciados pelo poder executivo, enquanto responsável pela administração dos interesses públicos, que a pesquisa se debruçará.

Assim sendo, muito embora o termo “poder público” seja definido pela LGPD de forma a abranger 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, a pesquisa o utilizará para se referir tão somente às atribuições do poder executivo federal enquanto provedor de políticas públicas.

É nessa conjuntura, que a problemática dos limites do tratamento de dados pessoais começa a ser pensada. Haja vista que, dados pessoais dos cidadãos são fornecidos de forma espontânea e até mesmo compulsoriamente (dados de identificação pessoal, geolocalização, saúde, sexualidade, etc) por meio da prestação de serviços públicos.

A preocupação com a exposição de dados pessoais é relevante jurídica e socialmente porque são essenciais ao livre desenvolvimento da personalidade e até mesmo ao exercício da cidadania do indivíduo.

## 1.2. A ATUAÇÃO DO PODER EXECUTIVO ENQUANTO ADMINISTRADOR DOS INTERESSES PÚBLICOS

Conforme o site oficial do Governo Federal<sup>2</sup>, a prestação de serviços públicos possui desempenho digital sobre o percentual de 89%. Isto é, oitenta e nove por cento dos serviços públicos oferecidos pelo poder executivo federal já foi migrado para o meio digital. Dessa

---

<sup>2</sup> <https://www.gov.br/governodigital/pt-br/transformacao-digital/central-de-qualidade/painel-de-monitoramento-de-servicos-federais/#ancora-geral>

forma, o sistema digital de gerenciamento de informações e serviços públicos do governo utiliza-se do tratamento de dados pessoais, cujos fins precisam ser específicos e transparentes.

Desde o momento em que uma certidão de nascimento é emitida e passa a constar no Sistema Nacional de Informações de Registro Civil, brasileiras e brasileiros passam a ter informações pessoais coletadas e armazenadas em bancos de dados. Ao longo de sua vida, cada vez que você acessa um serviço público, preenche um cadastro em uma loja, usa aplicações ou interage em redes sociais, também gera e compartilha centenas de milhares de dados. (COALIZÃO DIREITOS NA REDE, 2019)

Muitos são os dados coletados pelo poder público, seja municipal, estadual ou federal. Entretanto, a base de dados do Governo Federal alcança um maior quantitativo de órgãos e conseqüentemente de cidadãos. A fim de ilustrar a diversidade e quantidade de dados coletados e mantidos pelo poder público federal, vale destacar alguns dados disponíveis em sítios eletrônicos dentro do site do gov.br.

Dentro das diversas ferramentas disponíveis no site do gov.br, é possível encontrar o Catálogo de Base de Dados (CBD)<sup>3</sup> e, ainda, o Portal Brasileiro de Dados Abertos<sup>4</sup> ambos são métodos de publicação e busca de dados públicos brutos em formatos abertos, isto é, acessíveis, utilizáveis, modificáveis e compartilháveis.

Do mesmo modo, podem ser entendidos como relatórios em que constam diferentes bases de dados custodiadas pela administração pública. Os formatos disponibilizados consistem em planilhas simples ou gráficos dinâmicos, com alguns exemplos de bases de dados, identificando a entidade responsável pelo tratamento e também a descrição sobre quais são os tipos de dados coletados.

Atualmente, a última atualização do CBD registra 304 (trezentos e quatro)<sup>5</sup> bases de dados, como por exemplo o Sistema Nacional de Informações de Registro Civil – SIRC, base de governo, mantida pelo INSS, que tem por finalidade captar, processar, arquivar e disponibilizar dados produzidos pelos cartórios de registro civil das pessoas naturais. Por outro lado, o Portal de Dados Abertos soma 5.291 (cinco mil duzentos e noventa e uma)<sup>6</sup> bases de dados abertas e monitoradas, sendo esse considerado o projeto central para a busca e acesso aos dados públicos no Brasil.

Vale destacar que esses exemplos representam a tentativa do Governo Brasileiro em se adaptar às exigências legais no que diz respeito à proteção, tratamento, acesso e transparência

---

<sup>3</sup> <https://www.gov.br/governodigital/pt-br/governanca-de-dados/catalogo-de-bases-de-dados>

<sup>4</sup> <https://www.gov.br/governodigital/pt-br/dados-abertos/portal-brasileiro-de-dados-abertos>

<sup>5</sup> <https://catalogodebases.sisp.gov.br/arquivos/lista-de-bases.pdf>

<sup>6</sup> <https://centralpaineis.cgu.gov.br/visualizar/dadosabertos>

de dados públicos custodiados pelo governo federal. Muito embora, o poder público tenha optado por organizar essas ferramentas sem a devida cautela para com a simplificação do acesso do cidadão, haja vista que suas finalidades seriam divulgar e facilitar o conhecimento público acerca dessas informações digitais.

Levando-se em consideração a infinidade de banco de dados ligados ao Governo Federal, a pesquisa se debruçará, majoritariamente, sobre aqueles coletados pelo Cadastro Base do Cidadão (CBC)<sup>7</sup> instituído pelo Decreto 10.046/2019. O qual foi instituído com vistas a unificar e melhorar as informações pessoais sobre o cidadão dentro dos sistemas do governo. Esse cadastro utiliza-se de dados pessoais fornecidos tanto de forma online, quanto por aqueles vinculados ao CPF (Cadastro de Pessoas Físicas), mantidos pela Receita Federal.

O artigo 18 do Decreto 10.046 estabelece um rol exemplificativo, de um mínimo de dados que compõem a base integradora do Cadastro Base do Cidadão, como por exemplo: número de inscrição no CPF, situação cadastral, nome completo, data de nascimento, sexo, filiação, naturalidade entre outros. Ainda no mesmo artigo, vale destacar que, o parágrafo segundo determina que essa base será acrescida de outros dados, provenientes de bases temáticas, resgatados através do número de CPF, como identificação inequívoca dos atributos biográficos, biométricos e cadastrais.

Ademais, o artigo 2º do mesmo Decreto considera como atributos biográficos dados de pessoa natural relativos a fatos da sua vida, como nome, data de nascimento etc; conceitua como atributos biométricos as características biológicas e comportamentais mensuráveis da pessoa natural, que podem ser coletadas para reconhecimento automatizado, tais como a palma da mão, as digitais dos dedos, a retina ou a íris dos olhos, o formato da face, a voz e a maneira de andar; em seguida também conceitua o que seriam os dados cadastrais, em que se estende a vários tipos de informações inerentes à identificação detalhada do cidadão.

Diante disso, é possível perceber que a essência desse conglomerado de dados públicos está intrinsecamente ligada à personalidade, intimidade e privacidade do indivíduo. Não obstante, as informações capazes de serem geradas a partir do tratamento desses dados atingem diretamente os direitos e garantias fundamentais da pessoa humana.

Nessas condições, considerando o processo de transformação digital, a atuação do poder público e o caráter personalíssimo dos dados mantidos, é imprescindível olhar para a problemática desse domínio. Além disso, questionar a observância do Governo Federal às

---

<sup>7</sup> <https://www.gov.br/governodigital/pt-br/governanca-de-dados/cadastro-base-do-cidadao-cbc>

diretrizes estabelecidas pela Lei Geral de Proteção de Dados, a fim de evitar o constrangimento dos direitos e das garantias individuais do cidadão.

## **2 A LGPD E A GOVERNANÇA DE DADOS PELA ADMINISTRAÇÃO PÚBLICA FEDERAL**

Muito se ouve dizer sobre a LGPD, Lei Geral de Proteção de Dados, entretanto, é válido discorrer, de forma breve, sobre as leis que a antecedem, a fim de demonstrar a evolução da preocupação com a proteção de dados. O aparato legislativo brasileiro anterior à LGPD demonstra a atenção do Estado em se adaptar às mudanças sociais, como também, às regulamentações jurídicas que devem amparar esse novo contexto social.

Sobretudo, a Constituição Federal da República Brasileira de 1988, trouxe grande respaldo aos direitos fundamentais da pessoa humana, razão pela qual a LGPD resgata alguns princípios inerentes às garantias fundamentais dispostos em sua grande maioria no artigo 5º do texto constitucional. Como por exemplo, a inviolabilidade da privacidade e intimidade (art. 5º, X), bem como, o sigilo das comunicações telefônicas e de dados (art. 5º, XII).

Ainda no que tange à tutela constitucional, vale destacar os incisos XIV e XXXIII do artigo 5º, os quais, respectivamente, asseguram o acesso à informação e o direito de todos em receber dos órgãos públicos informações de seu interesse particular ou interesse coletivo. Paralelo a isso, o inciso LXXII do mesmo artigo da CF, resguarda o instituto do *habeas data*, uma ação constitucional cuja finalidade é assegurar, àquele que dela se utilizar, o conhecimento, e a possibilidade de retificação, de informações relativas à sua pessoa. Informações essas que constam de registros ou banco de dados de entidades governamentais ou de caráter público.

Destaca-se que essas garantias constitucionais, muito embora não sejam reconhecidas como marco regulatório da proteção de dados, foram imprescindíveis para o desenvolvimento e delimitação do direito inequívoco à proteção de dados pessoais. Tanto é que, recentemente, em razão da intensificação das discussões acerca das nuances que envolvem a sociedade da informação, foi incluído no rol do art. 5º da CF, através da Emenda Constitucional nº 115 de 2022, o inciso LXXIX, o qual assegura, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.

A primeira lei a dar vistas à necessidade de se assegurar os dados dos indivíduos foi o Código de Direito do Consumidor (CDC), Lei nº 8.078/90, sancionado em 1990. Essa lei inaugurou uma seção para tratar sobre Bancos de Dados e Cadastros dos Consumidores, mais especificamente os artigos 43 e 44 do CDC. Tais artigos vão, resumidamente, enfatizar a

necessidade de empresas e órgãos públicos manterem a transparência de suas atividades, de forma que, resguarde o acesso do consumidor às informações inerentes a seus dados pessoais e de consumo. Além disso, também assegura que as respectivas fontes das informações devam ser públicas, como também, que essas empresas e órgãos mantenham os cadastros atualizados.

Na sequência, em 2011 foi sancionada a Lei de Acesso à Informação (LAI), Lei nº 12.527/11, a qual versa sobre a publicidade de informações pessoais e de interesse coletivo, à disposição dos órgãos públicos. Nesse diapasão, em seu art. 31, assevera que o tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais. Esse artigo conversa diretamente com aquelas garantias fundamentais previstas nos incisos XIV e XXXIII do artigo 5º da CF. Do mesmo modo, foi recepcionado pela LGPD como fundamento e princípio inerente ao exercício do tratamento de dados pessoais.

Pouco tempo depois, em 2014, foi sancionada a Lei nº 12.965/14, conhecida por Marco Civil da Internet. A referida lei estabeleceu princípios, garantias, direitos e deveres para o uso da internet no Brasil. É oportuno reiterar que dentre os fundamentos elencados está a preservação dos direitos humanos e desenvolvimento da personalidade. No mesmo sentido, o art. 3º elege a proteção da privacidade e dos dados pessoais como princípios específicos do uso da Internet. Ainda mais, essa mesma legislação prestigiou a inviolabilidade, a transparência no que diz respeito ao tratamento e o não fornecimento, de dados pessoais, a terceiros. Além disso, também vedou a guarda de dados pessoais que sejam excessivos à finalidade para a qual foi dado consentimento do titular. Conforme se discorrerá mais adiante, esses dispositivos destacados foram recepcionados pela LGPD como fundamentos e princípios para a observância da proteção de dados pessoais.

Por fim, em 2018 foi sancionada a Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/18, a qual vai incisivamente dispor sobre fundamentos, conceitos, princípios, direitos e deveres relacionados ao tratamento de dados pessoais. A LGPD foi sancionada diante da necessidade de unificar as diretrizes inerentes à proteção de dados no Brasil.

## 2.1. DIRETRIZES DA LGPD QUE REGULAMENTAM A GOVERNANÇA DE DADOS PELO PODER PÚBLICO FEDERAL

No primeiro tópico (item 1.2), foi apresentado, de forma breve, algumas das regulamentações dispostas do Decreto nº 10.046/2019, dentre as quais, além de instituir o Cadastro Base do Cidadão (CBC) também dispõe sobre a governança no compartilhamento de

dados no âmbito da administração pública federal, razão pela qual constituiu o Comitê Central de Governança de Dados.

Por oportuno, o inciso XV do artigo 3º do Decreto nº 10.046/2019 conceitua a governança de dados como sendo o exercício de autoridade e controle que permite o gerenciamento de dados sob as perspectivas do compartilhamento, da arquitetura, da segurança, da qualidade, da operação e de outros aspectos tecnológicos.

Resumidamente, a Administração Pública Federal detém a governança, qual seja, a máxima competência para regular e gerenciar as perspectivas sobre o compartilhamento, segurança e operação quanto ao tratamento de dados públicos. Diante disso, uma das finalidades da governança exercida pela Administração Pública Federal é promover a interoperabilidade das informações e a integração dos serviços públicos.

O conceito de interoperabilidade<sup>8</sup> pode ser encontrado no site do gov.br como sendo uma característica vinculada à capacidade de diversos sistemas operarem em conjunto (interoperar) com o objetivo de garantir a eficaz e eficiente comunicabilidade entre pessoas, organizações e sistemas computacionais, em prol da troca de informações. Nesse sentido, a interoperabilidade se traduz pelo compartilhamento de dados e informações entre diversas bases de dados.

Assim, o tratamento de dados ligados ao CBC, enquanto banco de dados pessoais regulada e mantida pelo poder público federal, faz parte da interoperabilidade exercida pela administração pública federal.

Nesse diapasão, todas as previsões legais mencionadas até então estão sujeitas às determinações contidas na Lei Geral de Proteção de Dados (Lei nº 13.709/2018), conforme expresso em seu artigo 1º, caput e parágrafo único. Os quais preceituam que a LGPD disporá sobre normais gerais de interesse nacional, as quais devem ser observadas por todos os Entes Federados, a respeito do tratamento de dados pessoais, inclusive nos meios digitais e por pessoa jurídica de direito público. Dessa maneira, o objetivo é proteger direitos e garantias fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade do indivíduo.

Sob o mesmo viés, o autor Cristiano Colombo (2022) reitera que a LGPD é a corporificação da disciplina sobre proteção de dados pessoais, no cenário nacional, tendo em vista a necessidade de uniformização da matéria. Isso posto, é criada a fim de evitar possíveis

---

<sup>8</sup> <https://www.gov.br/governodigital/pt-br/governanca-de-dados/interoperabilidade>

oscilações, em nível de proteção de dados, entre diferentes setores, inclusive no que diz respeito às atribuições do poder público.

Isso posto, esse tópico passa a discorrer sobre alguns dos fundamentos, conceitos e princípios trazidos pela LGPD, a serem aplicados sobre as atribuições do poder público quanto ao tratamento e proteção de dados pessoais, delimitando, assim, a sua competência.

No que tange ao art. 2º, a LGPD estabelece quais são os fundamentos da proteção de dados, dentre os quais se destacam para a pesquisa: I - o respeito à privacidade; II - a autodeterminação informativa; IV - a inviolabilidade da intimidade, da honra e da imagem; e VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. Todos os fundamentos elencados estão em consonância com os direitos e garantias fundamentais assegurados pelo texto constitucional.

Na sequência, a LGPD elenca um rol exemplificativo, em seu artigo 5º, de alguns dos conceitos imprescindíveis para a compreensão das nuances que envolvem a proteção de dados pessoais. Tanto esse artigo, quanto os demais, demonstram a finalidade da lei de instruir e divulgar conhecimento a todos os setores da vida em sociedade, como consequência da urgente necessidade em se discutir sobre dados pessoais enquanto produto da sociedade da informação.

Desse modo, é possível caracterizar a LGPD, de uma maneira geral, como uma norma de caráter principiológico (especialmente nos termos do artigo 6º) e de ordem técnica, tendo em vista a possibilidade de aferição, de forma auditável, e de controle quanto ao cumprimento da boa governança dos dados pessoais (...). Daí porque o artigo 5º da LGPD revela sua destacada importância, afinal, cumpre a função de especificação dos termos utilizados na norma, como, por exemplo, deixando expresso o que é considerado dado pessoal, (...). (BASAN, 2022, p. 102)

São alguns dos conceitos trazidos pela LGPD, no artigo 5º da lei, os quais servirão de base para essa pesquisa: (I) dado pessoal trata-se daquela informação relacionada a pessoa natural identificada ou identificável; (II) dado pessoal sensível é aquele que, quando vinculado a uma pessoa, diz respeito à origem racial ou étnica, convicção religiosa, opinião política, saúde, vida sexual, dado genético ou biométrico; (IV) banco de dados é o conjunto estruturado de dados pessoais, em suporte eletrônico ou físico, estabelecido em um ou em vários locais; (V) titular é a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento; (X) o tratamento, por sua vez, é toda operação realizada com dados pessoais como, por exemplo, a coleta, produção, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, controle da informação etc; (VI) o uso compartilhado de dados envolve a interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicas no cumprimento de suas competências legais;

Ademais, o artigo 6º da LGPD traz alguns dos princípios os quais as atividades de tratamento de dados pessoais deverão observar, entre eles estão: (I) a finalidade; (II) a adequação; (III) a necessidade; (IV) o livre acesso aos titulares; (V) a qualidade e atualização dos dados; (VI) a transparência; (VII) a segurança; (VIII) a prevenção de danos; (IX) a não discriminação; (X) e a responsabilização.

De forma suplementar, a LGPD separa um capítulo específico (Capítulo IV) para tratar a respeito do tratamento de dados pessoais pelo poder público. Logo no início, o artigo 23 delimita que o tratamento de dados pessoais, feito por pessoas jurídicas de direito público, deverá ser realizado estritamente ao 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.

Consoante ao uso compartilhado de dados pessoais pelo Poder Público, o artigo 26, caput, determina que devem ser atendidas as finalidades específicas de execução de políticas públicas, respeitados os princípios de proteção de dados pessoais dispostos no artigo 6º da LGPD.

A relação jurídica estabelecida entre o Poder Público e o indivíduo titular de dados pessoais é marcada pela assimetria de poder, seja em decorrência da natureza jurídica do ente estatal que atua com poder de império, dotado de poderes para a consecução de seus deveres, como pela circunstância objetiva de que o ente estatal detém grande quantidade de dados pessoais em seus bancos de dados, como insumo ou subproduto do desempenho de sua atividade. É inerente à atividade administrativa a gestão de uma série de bancos de dados potencialmente sensíveis, sendo que a coleta e tratamento desses dados é um ponto nevrálgico em termos de políticas públicas que tenham escala. (TASSO, 2020, p. 276 e 277)

Posto isso, a prestação do serviço público exercida pela administração pública federal, por intermédio da plataforma do gov.br, deve estar em completa consonância com as disposições previstas na LGPD. Não obstante a essas normas de dirigismo, o Cadastro Base do Cidadão é um exemplo mais próximo da vulnerabilidade dos direitos inerentes ao cidadão.

### **3 A PRESTAÇÃO DE SERVIÇO PÚBLICO PELO GOV.BR E OS LIMITES DO TRATAMENTO DE DADOS**

O portal do gov.br é um canal digital, instituído pelo Decreto nº 9.756 de 2019, cujo objetivo visa unificar todas as informações e serviços do Poder Executivo Federal, com a finalidade de facilitar o acesso do cidadão. O órgão responsável pela manutenção do portal

gov.br é o Ministério da Economia e sua gestão é feita pela Secretaria de Governo Digital (SGD)<sup>9</sup>.

O gov.br enquanto um projeto de unificação dos canais digitais do governo federal, é produto das iniciativas ao processo de transformação digital <sup>10</sup>do Brasil para se alcançar um Governo majoritariamente digital. O início desse processo consta dos anos 2000, por intermédio da Proposta de Política de Governo Eletrônico e em conjunto com o Comitê Executivo de Governo Eletrônico (CEGE).

Ainda que, a implementação de um governo eletrônico tenha desenvolvido diversas ações e projetos, foi possível concluir que a inclusão digital é elemento indissociável do governo eletrônico, como forma de contribuir com a manutenção do direito de cidadania. Assim, foi a partir do ano de 2015 que o paradigma do governo eletrônico evoluiu para “governo digital”, em detrimento do foco ter se tornado a acessibilidade e eficiência na oferta de serviços ao cidadão por meio das tecnologias digitais. Para que a estruturação dessa nova implementação fosse possível, foi estabelecida uma Estratégia de Governo Digital (EGD) cuja finalidade visava implementar programas e ações relacionadas ao processo de digitalização. Essa política esteve vigente entre os anos de 2016 a 2019, e passou por várias atualizações.

Em seguida, através do Decreto nº 10.332/2020 foi publicado novo documento que abrangesse as novas necessidades e capacidades para a Estratégia de Governo Digital, cuja vigência compreenderia o período de 2020 a 2022. O objetivo final desse planejamento é oferecer, de forma digital, a totalidade dos serviços públicos disponibilizados pela União, por intermédio da plataforma “gov.br”.

Conforme mencionado no capítulo anterior, no momento presente 89% dos serviços já foram migrados para o meio digital e totalizam 4.784 (quatro mil setecentos e oitenta e quatro) serviços disponibilizados por 217 (duzentos e dezessete) órgãos diferentes. Informações as quais são atualizadas com certa recorrência e podem ser encontradas no Painel de monitoramento de serviços federais no próprio portal do gov.br.

Nessa conjuntura, a prestação de serviço público enquanto atividade essencial inerente ao poder público, agora, é majoritariamente exercida através do portal gov.br, o qual unificou os canais digitais do governo.

O tratamento de dados pessoais é um aspecto da execução das políticas públicas que mereceu da LGPD regulamentação específica decorrente do reconhecimento de que a massificação das relações travadas entre o Estado e os cidadãos, marcada pela

---

<sup>9</sup> <https://www.gov.br/governodigital/pt-br/sisp/secretaria-de-governo-digital-sgd>

<sup>10</sup> <https://www.gov.br/governodigital/pt-br/estrategia-de-governanca-digital/do-eletronico-ao-digital>.

voracidade na coleta de dados, tratados de forma não padronizada e, tampouco, transparente, redundando no risco de o Estado violar direitos e garantias fundamentais do titular. (TASSO, 2020, p. 276)

Dessa forma, a governança de dados exercida pelo Poder Público, diante das nuances que envolvem prestação de serviço público, lida direta e intimamente com dados pessoais, por vezes sensíveis, fornecidos, voluntária e até mesmo compulsoriamente, pelos cidadãos. De maneira complementar, o Poder Público, no exercício de sua governança digital, instituiu o Cadastro Base do Cidadão (CBC) a fim de possibilitar a unificação de identificação do cidadão para otimizar a prestação de serviços públicos, utilizando-se da interoperabilidade.

Com efeito, a natureza da relação entre cidadão e Poder Público, diferentemente da relação com atores privados, é compulsória e se configura como pré-condição para o exercício da cidadania. O tratamento de dados pessoais pelo Estado é imprescindível para o desempenho de seu mandato constitucional. A questão a ser enfrentada, portanto, é de assegurar que no desempenho de suas missões, inclusive na dimensão de normatização, a atuação do Poder Público se dê de maneira a buscar a concordância prática entre princípios como os da eficiência, do interesse público e da publicidade, e os princípios constantes da LGPD, como os da finalidade, da adequação e da necessidade, orientados pela ideia de autodeterminação informativa do cidadão. (WIMMER, 2021, p. 433)

Assim sendo, a pesquisa passará a se debruçar sobre as disposições do CBC, caracterizado por sua extensa previsão de coleta de dados pessoais. Situação a qual gerou tamanha insegurança que alguns de seus artigos foram declarados inconstitucionais. Não obstante, é oportuno dar atenção a essa base integradora pois seu texto destoa dos princípios da finalidade e da adequação assegurados pela LGPD.

### 3.1 CADASTRO BASE DO CIDADÃO (CBC) INTIMAMENTE LIGADO À PRESTAÇÃO DE SERVIÇOS PÚBLICOS

Como já mencionado anteriormente, o CBC foi instituído pelo Decreto 10.046/2019, Capítulo IV, artigo 16 ao 20-A. A saber, atualmente 66 (sessenta e seis) órgãos já obtiveram acesso ao CBC<sup>11</sup>.

De acordo com o artigo 16 do Decreto, as finalidades do CBC estão voltadas para a criação de um (III) meio unificado de identificação do cidadão, (II e IV) manter a integridade das bases de dados em conjunto com a atualização cadastral unificada, (V) facilitar o compartilhamento de dados cadastrais do cidadão entre os órgãos da administração pública e

---

<sup>11</sup> [https://www.gov.br/governodigital/pt-br/governanca-de-dados/orgaos\\_acessam\\_cbc.pdf](https://www.gov.br/governodigital/pt-br/governanca-de-dados/orgaos_acessam_cbc.pdf)

(VI) realizar o cruzamento de informações das bases de dados cadastrais oficiais a partir do número de inscrição do cidadão no CPF; em prol de aprimorar a gestão de políticas públicas e prestação do serviço público.

Logo em seguida, o parágrafo único, do mesmo artigo, veda a utilização do CBC com o objetivo de realizar tratamentos de dados que visem mapear ou explorar comportamentos individuais ou coletivos dos cidadãos. No entanto, essa vedação é prevista apenas nos casos em que faltar o consentimento expresso, prévio e específico dos indivíduos afetados. Ou seja, é permitido esse tipo de tratamento de dados desde que o titular manifeste de forma expressa o seu consentimento para que seus dados sejam utilizados dessa forma.

Destaca-se aqui que, mapear e explorar comportamentos alcança direta e essencialmente o livre desenvolvimento da personalidade e a inviolabilidade da intimidade e imagem do cidadão. Isso ocorre porque a observação do comportamento dos indivíduos tem como cerne o exercício da vigilância (BIONI, 2020) e, ainda que a descrição da atividade seja em prol da prestação do serviço público ou elaboração de políticas públicas, o teor sensível desses dados pessoais exige maior transparência e adequação.

Diante disso, ainda que a previsão do tratamento de dados pessoais para mapear ou explorar comportamentos esteja vinculada ao consentimento expresso do cidadão, insurge aqui, a problemática de que apenas o consentimento não basta para garantir a autodeterminação informativa do titular.

Com relação ao exercício do tratamento de dados sensíveis, em consonância com o princípio da finalidade – propósitos específicos e explícitos – o consentimento prévio, expresso e específico do cidadão assegura a sua máxima participação dentro da dinâmica da proteção dos dados pessoais, baseada na aceção de que ele deveria acompanhar ou mesmo visualizar seus dados em todos os seus movimentos (BIONI, 2020).

Nesse sentido, não basta aceitar “com um clique” os termos de uso daquele serviço, mas sim, exige-se um procedimento detalhado acerca da interoperabilidade e respectivo tratamento desses dados. Isto é, a exigência conquanto à preservação da autodeterminação informativa do titular desses dados.

Na sequência, o artigo 17 do Decreto explica a estrutura do CBC, o qual será composto por uma base integradora, ou seja, central, e de bases temáticas, acessadas através dos componentes da interoperabilidade. Assim, o artigo 18 informa que a base integradora será, num primeiro momento, constituída de dados biográficos que constam da base temática do CPF, e em seguida, apresenta um rol mínimo de dados como por exemplo, número do CPF, nome completo, data de nascimento, sexo etc.

Além disso, o parágrafo segundo do artigo 18, reitera que a base integradora será acrescida de bases temáticas, através do número de CPF, para a consolidação de atributos biográficos, biométricos e cadastrais. No que diz respeito à dados biométricos, o artigo 2º do Decreto conceitua-os como “características biológicas e comportamentais mensuráveis da pessoa natural que podem ser coletadas para reconhecimento automatizado, tais como a palma da mão, as digitais dos dedos, a retina ou a íris dos olhos, o formato da face, a voz e a maneira de andar”.

Nesse ínterim, ainda que a LGPD traga previsão quanto ao compartilhamento de dados para a execução de políticas e serviços públicos, não há qualquer menção à possibilidade de se instituir uma base integradora. A dimensão dos dados previstos à serem incluídos ao CBC causam enorme insegurança jurídica uma vez que não há qualquer formalidade no que tange aos princípios assegurados pela LGPD, como por exemplo, à finalidade; adequação; necessidade; livre acesso dos titulares; transparência; e segurança.

Ademais, o Decreto também traz nomenclaturas alheias àquelas estabelecidas pela LGPD, como por exemplo, ao categorizar e prever o tratamento de dados cadastrais, biográficos e biométricos. Sendo que, esses últimos estão em dissonância com a íntima esfera da proteção dos direitos da personalidade, garantidos tanto pelo texto constitucional (art. 5º, X da CF) quanto pela LGPD, uma vez que se caracterizam como dados sensíveis.

Nessas circunstâncias, várias instituições de pesquisa fizeram denúncias a respeito do teor e das irregularidades do Decreto 10.046/2019, conseqüentemente, o Conselho Federal da Ordem dos Advogados do Brasil (CFOAB) ajuizou uma Ação Direta de Inconstitucionalidade (6649) questionando a constitucionalidade do compartilhamento de dados da Administração Pública Federal regulada pelo Decreto.

Posteriormente, a ADI 6649 foi julgada em 15 de setembro de 2022 e declarou inconstitucional o artigo 22 do Decreto, como também, conferiu interpretação, consoante ao compartilhamento de dados entre órgãos públicos, nos seguintes termos:

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. 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”. (ADI 6649, Tribunal Pleno, Relator Min. Gilmar Mendes, 2022)

Isso posto, é evidente que o Decreto 10.046/2019 não está em consonância com os termos da ADI 6649, nem mesmo com as diretrizes da LGPD, portanto, carece de urgente regularização com o escopo de manter-se em conformidade com as limitações do tratamento de dados exercido do poder público.

Vale ressaltar que, não obstante à ADI 6649 ter vislumbrado a inconstitucionalidade de um dispositivo, ainda restam inúmeras inseguranças no tocante às previsões de captação de dados pessoais a serem objeto da interoperabilidade entre os órgãos públicos.

### 3.2 OS LIMITES DO TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO

Em suma, os limites do tratamento de dados pessoais são justamente os direitos fundamentais inerentes ao cidadão, isto é, ao titular desses dados. Por essa razão a LGPD ao dispor sobre o tratamento de dados pessoais, recepcionou princípios oriundos do texto constitucional, como também, princípios derivados.

Nessas condições, há entre os princípios uma conexão sistemática capaz de traçar, de maneira coerente, quais são os limites do tratamento de dados pessoais pelo poder público. Como por exemplo a comunicabilidade entre os princípios da finalidade, adequação, necessidade e transparência em prol da liberdade, privacidade e do livre desenvolvimento da personalidade da pessoa natural.

Tanto é que, o princípio da finalidade estabelece que o motivo da coleta de dados deve ser compatível com o objetivo final do tratamento de dados. De forma tangente, o princípio da adequação assegura que o tratamento de dados pessoais somente pode ser realizado diante da compatibilidade com as finalidades informadas ao titular.

Isso ocorre porque, os dados pessoais enquanto expressão direta da personalidade do indivíduo, estarão sempre vinculados à identificação da pessoa natural, em razão da sua utilização ser capaz de refletir diretamente na vida de seu titular (VAINZOF, 2020). Posto isso, aos titulares é resguardado o princípio da qualidade dos dados, o qual garante a atualização de seus dados de acordo com a necessidade e nos limites da finalidade de seu tratamento.

Por oportuno, cabe resgatar a incoerência do texto legal do CBC (Decreto nº 10.046/19) uma vez que ao elencar um rol de finalidades que fundamentam a instituição da base de dados e, em seguida, prever um extenso quantitativo de dados de que se construirá, o faz de

maneira à não observar os limites do tratamento de dados pelo poder público. Dessa forma, a ampla previsão de dados sem qualquer relação com as finalidades específicas para seu tratamento, fortalece a hipervulnerabilidade do cidadão perante as instituições do poder público.

Ainda mais, a finalidade deve ser informada ao titular, uma vez que tem direito às informações sobre o tratamento de seus dados, nos termos dos princípios do livre acesso e transparência. A respeito da disponibilização dessas informações, deve ser realizada de forma clara, adequada e acessível.

Ao passo em que a finalidade for alcançada ou que os dados deixarem de ser necessários ou pertinentes, não mais haverá justificativa jurídica para a sua manutenção, culminando no dever de descarte em razão do término do tratamento.

Conforme já apontado anteriormente, tanto na análise dos objetivos da LGPD como em seus fundamentos, os mais variados dados pessoais coletados, se isoladamente vistos, dificilmente afetariam o titular, mas quando colocados em conjunto e processados por mecanismos altamente capacitados, formam um compilado da personalidade de cada pessoa, passando a representar, perante terceiros, inúmeras características (...). (VAINZOF, 2020, p. 138)

Nesse hiato, entre a finalidade e a adequação, soma-se, ainda, o princípio da necessidade, através do qual o tratamento de dados fica limitado ao mínimo necessário para se atingir a finalidade pretendida. Além disso, a necessidade também acarreta a análise da proporcionalidade do tratamento para com os riscos aos direitos fundamentais do titular, ou seja, à prevenção de danos ao titular.

Por fim, é possível interpretar que a conexão dos princípios entre si ao caracterizar quais são os limites do tratamento de dados pelo poder público, desemboca no propósito de preservar e manter a segurança dos direitos e garantias fundamentais do titular.

## CONCLUSÃO

Enfim, concluir sobre quais são os limites do tratamento de dados pessoais, exercido pelo poder público, a pesquisa perpassou de forma linear pelas nuances que envolvem a relação entre dados pessoais e o poder público.

Quais sejam, a evolução das tecnologias propulsoras da migração eletrônica de dados para a digital; a intensificação das trocas de dados e a consequente obtenção de informações; o indivíduo titular de dados e direitos condicionado à utilização do serviço público digital e ao compulsório compartilhamento de seus dados; o tratamento de dados inerentes ao exercício da prestação de serviço público; e, por fim, a regulamentação jurídica desse ecossistema.

A distribuição da pesquisa foi feita dessa forma para enfatizar a relevância do trabalho, uma vez que retrata uma situação a qual todos os cidadãos estão sujeitos e, por tratar-se de uma problemática recente que também implica termos técnicos, a discussão foi capaz de desencadear a curiosidade acerca do tema.

Assim, a pesquisa conseguiu discutir a vulnerabilidade do cidadão enquanto consumidor necessário de serviços públicos ao passo em que discorreu sobre o exercício dessa administração por intermédio do portal gov.br, inovação oriunda do Governo Digital.

Além disso, o trabalho também conseguiu demonstrar essa vulnerabilidade ao relacioná-la com o contingente de dados à disposição de bancos de dados mantidos pelo poder público, razão pela qual discutiu acerca do Cadastro Base do Cidadão (CBC) e sua discrepância para com as determinações legais estabelecidas pela LGPD.

Consequentemente, foi possível identificar quais são os limites do tratamento de dados exercido pelo poder público, os quais dizem respeito à observância dos princípios inerentes aos direitos e garantias fundamentais da pessoa titular de dados, alcançando-se, assim, o objetivo geral do trabalho.

Do mesmo modo, a pesquisa também confirmou a hipótese do projeto de trabalho, uma vez que a previsão dispunha sobre o Poder Público estar condicionado às regras atinentes ao tratamento de dados, elencadas pela LGPD, na persecução do interesse público e princípios como o da finalidade e transparência. Destaca-se que o trabalho também conseguiu estabelecer a correlação desses limites com a preservação do livre desenvolvimento da personalidade da pessoa titular através da autodeterminação informativa.

No que diz respeito à pergunta-problema da pesquisa, a qual questionou se o poder público estabelece um equilíbrio entre a proteção dos dados pessoais dos cidadãos e o tratamento desses dados, a resposta encontrada é não. O poder público não demonstra atuar em

equilíbrio, em razão de sua capacidade técnica em alcançar, manter e comunicar diversos bancos de dados. No entanto, foi possível extrair da pesquisa que existem tentativas de manter-se em consonância com esse equilíbrio, isto é, nos limites do tratamento desses dados.

Diante de todo o exposto, o trabalho é capaz de contribuir para o direcionamento de outras pesquisas que venham a discutir sobre alguma das possíveis vertentes da problemática consoante ao tratamento de dados pelo poder público.

## REFERÊNCIAS

- BASAN, Arthur Pinheiro. Art. 5º (pág. 99-117). In: **Comentários à lei geral de proteção de dados pessoais**. MARTINS, Guilherme. LONGHI, João Victor. JÚNIOR, José Luiz (coord.). Indaiatuba, SP: Editora Foco, 2022.
- BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Editora Forense Ltda, 2019.
- BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Editora Forense Ltda, 2020.
- BIONI, Bruno; GARROTE, Marina; MEIRA, Marina; PASCHOALINI, Nathan. **Entre a visibilidade e a exclusão: um mapeamento dos riscos da Identificação Civil Nacional e do uso de sua base de dados para a plataforma gov.br**. Associação Data Privacy Brasil de Pesquisa, 2022.
- BRASIL. Autoridade Nacional Proteção de Dados. **Guia Orientativo: Tratamento de Dados Pessoais pelo Poder Público** (janeiro/2022). Versão 1.0. Brasília, 2022.
- BRASIL. **Cadastro Base do Cidadão**. Governança de Dados, Cadastro Base do Cidadão – CBC. [Brasília]: Ministério da Gestão e da Inovação em Serviços Públicos. Disponível em: <https://www.gov.br/governodigital/pt-br/governanca-de-dados/cadastro-base-do-cidadao-cbc>. Acesso em: 03 de abril de 2023.
- BRASIL. **Catálogo de Bases de Dados**. [Brasília]: Ministério da Gestão e da Inovação em Serviços Públicos. Disponível em: <https://www.gov.br/governodigital/pt-br/governanca-de-dados/catalogo-de-bases-de-dados>. Acesso em: 03 de abril de 2023.
- BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 2020. Disponível em: <[https://www.planalto.gov.br/ccivil\\_03/constituicao/constituicaocompilado.htm](https://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm)>. Acesso em: 31 de março de 2023.
- BRASIL. **Decreto Nº 9.756, de 11 de abril de 2019**. Institui o portal único “gov.br” e dispõe sobre as regras de unificação dos canais digitais do Governo federal. Brasília, DF: Presidência da República, 2019. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_ato2019-2022/2019/decreto/D10046.htm](http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm)>. Acesso em: 03 de abril de 2023.
- BRASIL. **Decreto Nº 10.046, de 9 de outubro de 2019**. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Brasília, DF: Presidência da República, 2019. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_ato2019-2022/2019/decreto/D10046.htm](http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm)>. Acesso em: 31 de março de 2023.
- BRASIL. **Do Eletrônico ao Digital**. [Brasília]: Ministério da Gestão e da Inovação em Serviços Públicos, 27 de mar de 2023. Disponível em: <https://www.gov.br/governodigital/pt-br/estrategia-de-governanca-digital/do-eletronico-ao-digital>. Acesso em: 05 de abril de 2023

**BRASIL. Interoperabilidade.** Governo Digital, Governança de Dados. [Brasília]: Ministério da Gestão e da Inovação em Serviços Públicos. Disponível em: <https://www.gov.br/governodigital/pt-br/governanca-de-dados/interoperabilidade>. Acesso em: 03 de maio de 2023.

**BRASIL. Lei Nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2019. Disponível em: <[https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/113709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm)>. Acesso em: 31 de março de 2023.

**BRASIL. Lista de Bases do Catálogo de Bases de Dados.** [Brasília]: Ministério da Gestão e da Inovação em Serviços Públicos. Disponível em: <https://catalogodebases.sisp.gov.br/arquivos/lista-de-bases.pdf>. Acesso em: 03 de maio de 2023.

**BRASIL. Lista de Órgãos que Acessam o Cadastro Base do Cidadão.** [Brasília]: Ministério da Economia. Disponível em: [https://www.gov.br/governodigital/pt-br/governanca-de-dados/orgaos\\_acessam\\_cbc.pdf](https://www.gov.br/governodigital/pt-br/governanca-de-dados/orgaos_acessam_cbc.pdf). Acesso em: 03 de maio de 2023.

**BRASIL. O que é? Governança de dados** [Brasília]: Ministério da Gestão e da Inovação em Serviços Públicos. Disponível em: <https://www.gov.br/governodigital/pt-br/governanca-de-dados>. Acesso em: 03 de abril de 2023.

**BRASIL. Painel de Monitoramento de Dados Abertos.** [Brasília]: Ministério da Gestão e da Inovação em Serviços Públicos. Disponível em: <https://centralpaineis.cgu.gov.br/visualizar/dadosabertos> Acesso em: 03 de maio de 2023.

**BRASIL. Painel de Monitoramento de Serviços Federais.** Governo Digital, Transformação Digital, Central de Qualidade. [Brasília]: Ministério da Gestão e da Inovação em Serviços Públicos. Disponível em: <https://www.gov.br/governodigital/pt-br/transformacao-digital/central-de-qualidade/painel-de-monitoramento-de-servicos-federais/#ancora-geral>. Acesso em: 03 de maio de 2023.

**BRASIL. Portal Brasileiro de Dados Abertos.** Governo Digital, Dados Abertos. [Brasília]: Ministério da Gestão e da Inovação em Serviços Públicos. Disponível em: <https://www.gov.br/governodigital/pt-br/dados-abertos/portal-brasileiro-de-dados-abertos>. Acesso em: 03 de maio de 2023.

**BRASIL. Privacidade e Segurança da Informação.** [Brasília]: Ministério da Gestão e da Inovação em Serviços Públicos. Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protexao-de-dados>. Acesso em: 03 de abril de 2023.

**BRASIL. Secretaria de Governo Digital (SGD).** [Brasília]: Ministério da Gestão e da Inovação em Serviços Públicos. Disponível em: <https://www.gov.br/governodigital/pt-br/sisp/secretaria-de-governo-digital-sgd>. Acesso em: 03 de maio de 2023.

**BRASIL. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade (ADI) 6649.** 0111621-15.2020.1.00.0000. Requerente: Conselho Federal da Ordem dos Advogados do Brasil – CFOAB. Intimado: Presidente da República. Relator: Min. Gilmar Mendes, 15 de setembro de 2022. ATA Nº 27, de 15/09/2022. DJE nº 191, divulgado em 23/09/2022.

Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=6079238>. Acesso em: 06 de abril de 2023.

CASTELLS, Manuel. **A sociedade em rede**. 6. ed. (A era da informação: economia, sociedade e cultura, v.1.) São Paulo: Paz e Terra, 1999.

COALIZÃO DIREITOS NA REDE. **Nota da Coalizão Direitos na Rede sobre o Decreto nº 10.046/2019**. Brasília, 16 de outubro de 2019. Disponível em: <https://direitosnarede.org.br/2019/10/16/nota-da-coalizao-direitos-na-rede-sobre-o-decreto-no-100462019/>. Acesso em: 06 de abril de 2023.

COALIZÃO DIREITOS NA REDE. **Seus Dados São Você**. Porto Alegre, 2019. Disponível em: <https://direitosnarede.org.br/campanha/seus-dados-sao-voce/>. Acesso em: 13 de dezembro de 2022.

COLOMBO, Cristiano. Art. 2º (pág. 55-64). In: **Comentários à lei geral de proteção de dados pessoais**. MARTINS, Guilherme. LONGHI, João Victor. JÚNIOR, José Luiz (coord.). Indaiatuba, SP: Editora Foco, 2022.

LOTT, Yuri Monnerat. CIANCONI, Regina de Barros. **Vigilância e privacidade, no contexto do big data e dados pessoais: análise da produção da ciência da informação no Brasil**. Perspectivas em Ciência da Informação, v.23, n.4, p.117-132, out./dez. 2018. Disponível em: <https://www.scielo.br/j/pci/a/BXMsD73NL5dpYQWqGm8YrBN/?format=pdf&lang=pt>. Acesso em: 19 de setembro de 2022.

MACEDO, Nathália Brito de. **A proteção de dados pessoais em banco de dados públicos no atual contexto da sociedade da informação: reflexões sobre o tratamento de dados pessoais pelo poder público brasileiro**. 2022. 94f. Dissertação (Mestrado em Direito) - Centro de Ciências Sociais Aplicadas, Universidade Federal do Rio Grande do Norte, Natal, 2022. Disponível em: <https://repositorio.ufrn.br/handle/123456789/46857>. Acesso em: 19 de setembro de 2022.

PINHEIRO, Patricia Peck. **Direito digital**. 7. ed. São Paulo: Saraiva Educação, 2021.

SARLET, Ingo Wolfgang. Fundamentos Constitucionais: O Direito Fundamental à Proteção de Dados. (pág. 57-100). In: **Tratado de proteção de dados pessoais**. DONEDA, Danilo. SARLET, Ingo Wolfgang. MENDES, Laura Schertel. JUNIOR, Otavio Luiz (coord.). Rio de Janeiro: Forense, 2021. ISBN 978-85-309-9219-4.

TASSO, Fernando Antonio. Capítulo IV Do Tratamento de Dados Pessoais pelo Poder Público. Seção I Das regras. Art. 23 (pág. 276-295). In: **LGPD: Lei Geral de Proteção de Dados Comentada**. MALDONADO, Viviane. BLUM, Renato (coord.). 2. ed. rev., atual e ampl. São Paulo: Thomson Reuters Brasil, 2020.

TEIXEIRA, Tarcisio. **Direito Digital e Processo Eletrônico**. 6. ed. São Paulo: SaraivaJur, 2022.

VAINZOF, Rony. Capítulo I Disposições Preliminares. Art. 6º. In: **LGPD: Lei Geral de Proteção de Dados Comentada**. MALDONADO, Viviane. BLUM, Renato (coord.). 2. ed. rev., atual e ampl. São Paulo: Thomson Reuters Brasil, 2020.

VERGILI, Gabriela. ZANATTA, Rafael. **Os problemas do Cadastro Base do Cidadão e a ADI 6.649**. Data Privacy BR. Disponível em: <https://www.dataprivacybr.org/documentos/os-problemas-do-cadastro-base-do-cidadao-e-a-adi-6-649/>. Acesso em: 06 de abril de 2023.

WIMMER, Miriam. O Regime Jurídico do Tratamento de Dados Pessoais pelo Poder Público. (pág. 425-441). In: **Tratado de proteção de dados pessoais**. DONEDA, Danilo. SARLET, Ingo Wolfgang. MENDES, Laura Schertel. JUNIOR, Otavio Luiz (coord.). Rio de Janeiro: Forense, 2021. ISBN 978-85-309-9219-4.