UNIVERSIDADE FEDERAL DO ESTADO DO RIO DE JANEIRO – UNIRIO

CENTRO DE CIÊNCIAS JURÍDICAS E POLÍTICAS – CCJP

PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO – PPGD

Débora Alves Abrantes

TRATAMENTO DE DADOS PESSOAIS E POLÍTICA PÚBLICA DE ACESSO À INFORMAÇÃO: AÇÕES DO SERVIÇO DE INFORMAÇÃO AO CIDADÃO NA UNIVERSIDADE FEDERAL DO RIO DE JANEIRO

Rio de Janeiro

2024

UNIVERSIDADE FEDERAL DO ESTADO DO RIO DE JANEIRO – UNIRIO

CENTRO DE CIÊNCIAS JURÍDICAS E POLÍTICAS – CCJP

PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO – PPGD

Débora Alves Abrantes

TRATAMENTO DE DADOS PESSOAIS E POLÍTICA PÚBLICA DE ACESSO À INFORMAÇÃO: AÇÕES DO SERVIÇO DE INFORMAÇÃO AO CIDADÃO NA UNIVERSIDADE FEDERAL DO RIO DE JANEIRO

Dissertação apresentada ao Programa de Pós-Graduação *stricto sensu* em Direito (PPGD) na área de concentração Direito e Políticas Públicas na linha de pesquisa Direitos Humanos e Políticas Públicas como requisito parcial para a para obtenção do título de mestre.

Orientador: Prof. Dr. Leonardo Mattietto

Rio de Janeiro

2024

UNIVERSIDADE FEDERAL DO ESTADO DO RIO DE JANEIRO – UNIRIO

CENTRO DE CIÊNCIAS JURÍDICAS E POLÍTICAS – CCJP

PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO – PPGD

Débora Alves Abrantes

TRATAMENTO DE DADOS PESSOAIS E POLÍTICA PÚBLICA DE ACESSO À INFORMAÇÃO: AÇÕES DO SERVIÇO DE INFORMAÇÃO AO CIDADÃO NA UNIVERSIDADE FEDERAL DO RIO DE JANEIRO

Dissertação apresentada ao Programa de Pós-Graduação *stricto sensu* em Direito (PPGD) na área de concentração Direito e Políticas Públicas na linha de pesquisa Direitos Humanos e Políticas Públicas como requisito parcial para a para obtenção do título de mestre.

BANCA EXAMINADORA

_____

Prof. Dr. Leonardo Mattietto

_____

Prof. Dr. Oswaldo Lima

_____

Prof. Dr.ª Cristina Ayoub Riche

Rio de Janeiro

2024

FICHA CATALOGRÁFICA

AGRADECIMENTOS

A Jornada e os Encontros

Escrever uma dissertação é como atravessar uma longa estrada. No início, tudo parece planejado: mapas traçados, objetivos definidos. Mas logo descobrimos que o caminho é sinuoso, cheio de surpresas, desafios e, felizmente, encontros inesquecíveis.

Foi assim que, nessa caminhada, Deus esteve sempre presente. Nos momentos de incerteza, quando a exaustão pesava, era na fé que eu encontrava forças para continuar. Mais do que um destino, Ele foi meu abrigo em cada tempestade.

Minha família foi o alicerce firme. Houve dias de cansaço, noites mal dormidas, momentos de dúvida. Mas ali estavam eles, com palavras de incentivo, abraços silenciosos e aquele amor que não exige explicação. Sem eles, este caminho teria sido bem mais árduo.

E então, meu companheiro Vinicius Valentim. Parceiro de todas as horas, aquele que soube respeitar os silêncios e celebrar cada pequena vitória. Nos dias mais difíceis, um olhar bastava para me lembrar de que eu não estava sozinha.

No universo acadêmico, encontrei mestres eminentes. O professor Leonardo Mattietto foi mais que um orientador; foi um farol. Com paciência e precisão, me ajudou a transformar ideias soltas em um pensamento estruturado. Ao lado dele, aprendi a importância de enxergar além das palavras.

Cristina Ayuob Riche foi mais que professora, foi um exemplo de ser humano e de profissional excelente. Com seu apoio, sua generosidade e sua sabedoria, fez com que este percurso fosse mais leve e mais rico. Há mestres que ensinam dentro das salas de aula, outros que ensinam para a vida; ela faz parte do segundo grupo.

O professor Oswaldo Lima também esteve presente nessa jornada, trazendo reflexões instigantes e um olhar atento ao conhecimento. Suas contribuições foram fundamentais para o amadurecimento do meu pensamento e para que esta dissertação ganhasse ainda mais consistência.

Na Ouvidoria-Geral da UFRJ, onde trabalho desde 2019, tive a sorte de caminhar ao lado das professoras Cristina Ayoub Riche e Luzia Araújo. O compromisso com a escuta cidadã, a dedicação à transparência e ao serviço público foram uma inspiração diária. Trabalhar com alguém assim é lembrar, todos os dias, do verdadeiro propósito do que fazemos.

A UFRJ, por sua vez, é mais do que uma instituição para mim. Há 16 anos, é um espaço de crescimento, de desafios e de realização. Foi onde aprendi, ensinei e me transformei. E foi o lugar onde compreendi que servir ao público não é apenas uma função, mas uma missão.

Os que caminham ao lado

No início, imaginei que o mestrado fosse uma jornada solitária. Um caminho de leitura intensa, escrita silenciosa e reflexões individuais. Mas logo percebi que a estrada era cheia de vozes.

Havia as trocas antes das aulas, os olhares compartilhando a angústia dos prazos, as mensagens no grupo nos lembrando que ninguém estava sozinho. Havia as risadas depois de discussões acaloradas, que nos ajudavam a seguir adiante.

Minha turma de mestrado de 2023 foi mais do que um grupo de colegas. Foi um conjunto de trilhas que se cruzaram, formando uma rede de apoio, um espaço onde o conhecimento florescia e a amizade se fortalecia. Aprendi tanto com os professores quanto com vocês.

Cada encontro deixou sua marca, cada debate trouxe novas perspectivas, cada incentivo fez a caminhada parecer menos íngreme. Sei que, mesmo depois da última aula, carregamos algo uns dos outros.

A caminhada teria sido muito mais solitária sem vocês.

E há aqueles encontros que não acontecem no cotidiano, mas que deixam marcas profundas. O mestre Danilo Doneda foi um deles. Seu pensamento inovador sobre privacidade e proteção de dados foi a base da minha pesquisa, mas seu legado vai muito além dos livros e artigos. Ele abriu caminhos, e sua voz segue ecoando no tempo.

Ao fim dessa jornada, percebo que uma dissertação não se escreve sozinha. Ela é feita de histórias, trocas, aprendizados e, principalmente, das pessoas que encontramos pelo caminho.

A cada um que fez parte desta trajetória, meu mais sincero obrigada. Esta conquista também pertence a vocês.

"A Transparência deve ser diretamente proporcional ao poder. A privacidade deve ser inversamente proporcional ao poder. "

Danilo Doneda

RESUMO

O problema levantado nesta pesquisa remete ao seguinte questionamento: a Lei Geral de Proteção de Dados Pessoais (Lei Federal 13.709/2018) pode, ao mesmo tempo, ser uma ferramenta nas mãos do Estado para garantir o direito fundamental à privacidade, sem ser um obstáculo à política pública de acesso à informação?

Pretende-se demonstrar a hipótese de que a Lei Federal nº 13.709/2018 pode assegurar que dados pessoais sejam utilizados de forma transparente e com fins legítimos, ao mesmo tempo garantindo os direitos dos titulares, no momento da efetivação de políticas públicas de acesso à informação.

Para testar a hipótese mencionada, pretende-se analisar os pedidos de acesso à informação tratados pela UFRJ, de 2018 a 2023, antes e depois do advento da LGPD, por meio do sistema eletrônico de informações ao cidadão (e-SIC), integrado à Plataforma Fala.BR e desenvolvido pela Controladoria-Geral da União para a efetivação da política pública de acesso à informação. Busca-se, com esta análise, demonstrar como é realizado o tratamento e divulgação de dados pela IFE, considerando as Leis Federais 12.527/2011 (LAI), 13.709/2018 (LGPD) e outras normas brasileiras vigentes que tratem do mesmo objeto de pesquisa.

Para se validar a hipótese, busca-se entender os principais critérios e informações que conduziram à negativa de acesso por parte dos gestores responsáveis pelo tratamento das demandas, bem como a resposta da CGU após análise dos recursos encaminhados pelos cidadãos diante do indeferimento do pedido. Além dos dados coletados no e-SIC/CGU, almeja-se, através da análise da literatura jurídica, dos artigos científicos e do ordenamento jurídico brasileiro, avaliar a validade ou plausibilidade da hipótese aventada.

O desenvolvimento do trabalho está estruturado em três capítulos, em que se abordam o contexto e a importância da Política Pública de Acesso à Informação em um Estado Democrático de Direito, as principais inovações e repercussões da LGPD e o impacto desta lei no serviço de acesso à informação da Universidade Federal do Rio de Janeiro, adotando-se uma abordagem multidisciplinar, combinando método científico dedutivo, objetivo descritivo, exploratório e abordagem quantitativa e qualitativa.

Palavras-chave: Políticas Públicas; Direitos Humanos; Acesso à Informação; Privacidade; LGPD.

ABSTRACT

The problem raised in this research refers to the following question: can the General Personal Data Protection Law (Federal Law 13.709/2018) be a tool in the hands of the State to guarantee the fundamental right to privacy, without being an obstacle to the public policy of access to information?

The aim is to demonstrate the hypothesis that Federal Law 13.709/2018 can ensure that personal data is used transparently and for legitimate purposes, while at the same time guaranteeing the rights of the holders, at the time of the implementation of public policies of access to information.

To test the hypothesis, the aim is to analyze the requests for access to information processed by UFRJ, from 2018 to 2023, before and after the advent of the LGPD, through the electronic citizen information system (e-SIC), integrated with the Fala.BR Platform and developed by the Comptroller General of the Union for the implementation of the public policy of access to information. This analysis seeks to demonstrate how the IFE processes and discloses data, considering Federal Laws 12.527/2011 (LAI), 13.709/2018 (LGPD) and other current Brazilian regulations that address the same research subject.

To validate the hypothesis, we seek to understand the main criteria and information that led to the denial of access by the managers responsible for processing the demands, as well as the response of the CGU after analyzing the appeals submitted by citizens in response to the denial of the request. In addition to the data collected in e-SIC/CGU, we aim to assess the validity or plausibility of the hypothesis raised through the analysis of legal literature, scientific articles and the Brazilian legal system.

The development of the work is structured in three chapters, which address the context and importance of the Public Policy on Access to Information in a Democratic State of Law, the main innovations and repercussions of the LGPD and the impact of the LGPD on the information access service of the Federal University of Rio de Janeiro, adopting a multidisciplinary approach, combining deductive scientific method, descriptive, exploratory objective and quantitative and qualitative approach.

Keywords: Public Policies; Human Rights; Access to Information; Privacy; LGPD.

ABREVIATURAS E SIGLAS

ANPD - Autoridade Nacional de Proteção de Dados

CEDH - Convenção Europeia dos Direitos Humanos

CGU – Controladoria-Geral da União

CIS - Comunicados de Incidentes de Segurança

CNIL - Comissão Nacional de Informática e Liberdades Francesa

DPO - *Data Protection Officer* (Encarregado de Proteção de Dados)

e-Sic – Sistema Eletrônico de Informação ao Cidadão

FOIA - *Freedom of Information Act* (Lei de Transparência na Administração Pública Estadunidense)

GDPR – *General data protection regulation* (Regulamento Geral de Proteção de Dados Europeu)

GLBA – *Gramm-Leach-Bliley Act* (Lei de Proteção de Informações Financeiras Estadunidense)

HIPAA – *Health Insurance Portability and Accountability* (Lei de Proteção de Dados de Saúde e Informações Pessoais Estadunidense)

IFE – Instituição Federal de Ensino

LAI – Lei de acesso à Informação

LGPD – Lei Geral de Proteção de Dados Pessoais

LRF - Lei de Responsabilidade Fiscal

PHI – *Protected Health Information* (Informação de Saúde Protegidas Estadunidense)

UFRJ – Universidade Federal do Rio de Janeiro

SUMÁRIO

INTRODUÇÃO

O tratamento de dados pessoais e o acesso à informação são temas centrais no debate contemporâneo sobre direitos fundamentais, transparência governamental e proteção da privacidade. O avanço tecnológico e a digitalização de serviços públicos e privados têm gerado uma quantidade sem precedentes de dados, exigindo um equilíbrio delicado entre a proteção dos direitos individuais e o fomento à transparência e *accountability*[1]. Esse equilíbrio é especialmente importante no contexto de políticas públicas, em que a necessidade de acessar e tratar dados pessoais pode entrar em conflito com a obrigação de proteger a privacidade dos cidadãos.

Na era digital, dados pessoais se tornaram ativos valiosos, usados tanto por empresas para personalizar serviços quanto por governos para otimizar políticas públicas. Entretanto, o uso massivo e, por vezes, indiscriminado desses dados despertou preocupações sobre privacidade, segurança e o potencial de abuso por parte de atores estatais e privados. A sociedade, cada vez mais consciente dos riscos associados ao compartilhamento e uso inadequado de suas informações pessoais, exige maior controle sobre seus dados, ao mesmo tempo em que demanda transparência e responsabilidade das instituições públicas.

O desafio social reside na construção de uma cultura que valorize tanto a proteção da privacidade quanto a necessidade de acesso à informação como bases para a participação democrática e a proteção dos direitos individuais. A crescente preocupação com a privacidade e a proteção de dados evidencia que os cidadãos estão atentos às práticas de coleta e uso de seus dados, exigindo mais transparência e garantias de segurança. Ao mesmo tempo, o acesso à informação é visto como um direito essencial para a fiscalização da administração pública e para o exercício da cidadania.

No Brasil, a Lei Geral de Proteção de Dados Pessoais (LGPD), sancionada em 2018 e em vigor desde 2020, é um marco jurídico que estabelece diretrizes para o tratamento de dados pessoais, alinhando-se às tendências internacionais, como o Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia. A LGPD define princípios fundamentais, como a transparência, a finalidade e a segurança, que devem orientar o tratamento de dados em

[1] *Accountability* é um conceito amplamente utilizado nas ciências políticas, administração pública e gestão, que se refere à responsabilidade e à obrigação de prestação de contas de um cidadão, instituição ou governo em relação a suas ações, decisões e comportamentos. Em essência, significa que aqueles que exercem poder ou funções públicas devem ser transparentes em suas ações e responder por seus atos, especialmente quando afetam a coletividade.

qualquer contexto, público ou privado. Além disso, a lei estabelece direitos para os titulares dos dados, como o acesso, a retificação e a exclusão de suas informações.

Em paralelo, a Lei de Acesso à Informação (LAI), em vigor desde 2012, garante aos cidadãos o direito de obter informações de interesse público, promovendo a transparência e a *accountability* dos órgãos governamentais. A LAI é uma ferramenta poderosa para a fiscalização da administração pública, permitindo que qualquer pessoa solicite e obtenha informações sobre as atividades governamentais, desde que essas não estejam protegidas por sigilo legal ou não envolvam dados pessoais cuja divulgação possa comprometer a privacidade.

A coexistência dessas duas leis no ordenamento jurídico brasileiro cria um cenário em que o direito à privacidade e o direito ao acesso à informação precisam ser harmonizados. A LGPD e a LAI devem ser interpretadas de forma complementar, reconhecendo que, embora a proteção de dados pessoais seja essencial, há situações em que o interesse público pode justificar o acesso a informações que envolvem dados pessoais. Nesses casos, a anonimização ou pseudonimização de dados pode ser uma solução viável para garantir a transparência sem comprometer a privacidade.

No cenário internacional, o Regulamento Geral de Proteção de Dados (GDPR) é a principal referência em termos de proteção de dados, estabelecendo um padrão elevado para o tratamento de informações pessoais e impondo obrigações rigorosas às organizações que operam dentro da União Europeia ou que tratam dados de cidadãos europeus. O GDPR influenciou a legislação em vários países, incluindo o Brasil, que adotou muitos de seus princípios na elaboração da LGPD.

Nos Estados Unidos, a abordagem à proteção de dados é mais fragmentada, com leis específicas para diferentes setores, como na saúde, que conta com a Lei de Portabilidade e Responsabilidade de Provedores de Saúde (HIPAA/1996), em que determinadas informações sobre a saúde e os serviços de assistência médica de uma pessoa são classificadas como informações protegidas de saúde (PHI); na área finanças, a Lei de Modernização de Serviços Financeiros (GLBA/2019), que controla a forma como as instituições financeiras lidam com as informações privadas de cidadãos; e uma ênfase maior na transparência e no acesso à informação, refletida em leis como o *Freedom of Information Act* (FOIA/1966), que garante que qualquer pessoa ou organização, incluindo cidadãos não estadunidenses, possam acessar dados do governo dos Estados Unidos por meio de um pedido de informação.

O principal desafio enfrentado pelo Brasil e por outros países é a harmonização entre as políticas de proteção de dados e as políticas de acesso à informação. A aplicação da LGPD, no

Brasil, não deve obstruir a transparência governamental, mas sim ser integrada às práticas de gestão de informações públicas de forma a proteger a privacidade sem comprometer o acesso à informação. Da mesma forma, o uso de dados pessoais em políticas públicas deve ser feito de forma a garantir o cumprimento das finalidades legítimas do Estado, respeitando os princípios da necessidade e da minimização de dados.

As perspectivas para o futuro indicam uma crescente sofisticação nas práticas de tratamento de dados, com a utilização de técnicas avançadas de anonimização e de análise de dados que permitem a utilização de informações pessoais em políticas públicas sem comprometer a privacidade. Além disso, a educação e a conscientização sobre os direitos de proteção de dados e de acesso à informação são fundamentais para a construção de uma cultura de respeito aos direitos fundamentais, tanto por parte do Estado quanto da sociedade civil.

Nesse sentido, o estudo do tratamento dos dados pessoais, notadamente após o advento da Lei Federal nº 13.709/2018, é de extrema relevância social pois envolve questões como privacidade, segurança e ética. Com o aumento da coleta e uso de dados, compreender como essas informações são tratadas ajuda a proteger os direitos individuais e assegurar a privacidade, em um cenário em que a regra constitucional é o acesso à informação, como característica de um Estado Democrático de Direito.

O problema levantado nesta pesquisa remete ao seguinte questionamento: a Lei Geral de Proteção de Dados Pessoais (Lei Federal 13.709/2018) pode, ao mesmo tempo, ser uma ferramenta nas mãos do Estado para garantir o direito fundamental à privacidade, sem ser um obstáculo à política pública de acesso à informação?

A coexistência da Lei de Acesso à Informação (Lei nº 12.527/2011) e da Lei Geral de Proteção de Dados (Lei nº 13.709/2018) no ordenamento jurídico brasileiro impõe um desafio significativo para a administração pública. Como harmonizar os princípios de transparência e acesso à informação pública, promovidos pela LAI, com os direitos à privacidade e proteção de dados pessoais, assegurados pela LGPD, de forma a garantir uma administração pública eficiente e respeitosa dos direitos fundamentais? Eis o problema a ser analisado nesta pesquisa.

Pretende-se demonstrar a hipótese de que a Lei Federal nº 13.709/2018 pode assegurar que dados pessoais sejam utilizados de forma transparente e com fins legítimos, ao mesmo tempo garantindo os direitos dos titulares, no momento da efetivação de políticas públicas de acesso à informação. Para lidar com essa questão, é necessário encontrar um equilíbrio entre os princípios da proteção de dados e o direito à informação. Isso pode envolver a anonimização ou pseudonimização dos dados pessoais antes da divulgação, a obtenção de consentimento dos

titulares dos dados ou a aplicação de exceções previstas na LGPD e na LAI para situações específicas. Além disso, é importante que os órgãos públicos estejam cientes das suas obrigações legais sob ambas as leis e adotem medidas para garantir a conformidade com ambas.

Para testar a hipótese mencionada, foram analisados os pedidos de acesso à informação tratados pela UFRJ, no período de janeiro de 2018 a dezembro de 2023, através do sistema eletrônico de informações ao cidadão (e-SIC), integrado à Plataforma Fala.BR e desenvolvido pela Controladoria-Geral da União para a efetivação da política pública de acesso à informação. Buscou-se, com esta análise, demonstrar como é realizado o tratamento e divulgação de dados pela IFE, considerando as Leis Federais 12.527/2011 (LAI), 13.709/2018 (LGPD) e outras normas brasileiras vigentes que tratem do mesmo objeto de pesquisa.

Para se validar a hipótese de que a LGPD não é um obstáculo ao acesso à informação, foram estudados os principais critérios e informações que conduziram à negativa de acesso aos dados por parte dos gestores responsáveis pelo tratamento das demandas, bem como a resposta da CGU após análise dos recursos encaminhados pelos cidadãos diante do indeferimento do pedido.

Além dos dados coletados no e-SIC/CGU, almeja-se, por meio da análise da literatura jurídica, dos artigos científicos e do ordenamento jurídico brasileiro, avaliar a validade ou plausibilidade da hipótese aventada.

O trabalho está estruturado em três capítulos. No 1º capítulo, serão abordadas as delimitações e as intersecções jurídicas das políticas públicas de acesso à informação e proteção de dados pessoais. No 2º capítulo, será apresentada a tese da aparente oposição entre a LAI e a LGPD, a partir da perspectiva da hermenêutica jurídica e dos impactos da LGPD no contexto da política de acesso à informação. No 3º capítulo, será abordado o impacto da LGPD no serviço de acesso à informação da Universidade Federal do Rio de Janeiro.

A partir do estudo de casos concretos, ou seja, de demandas recebidas pelo Serviço do Informação ao Cidadão da UFRJ, e partindo da hipótese de convergência entre a LAI e a LGPD no fluxo de dados, pretende-se defender a ideia de que a lógica da Lei de Proteção de dados se fundamenta na garantia do tratamento adequado de dados e não no impedimento para o acesso à informação.

Considerando que o foco da pesquisa é a aparente assimetria de normas jurídicas, ou seja, entre a LGPD e a LAI, foi utilizada a seguinte metodologia: método científico dedutivo, por meio do qual foram formuladas hipóteses específicas ou proposições, testadas e examinadas com base em evidências relevantes para se chegar à hipótese de que a Lei Federal nº

13.709/2018 pode garantir o uso transparente e legítimo de dados pessoais ao mesmo tempo em que protege os direitos dos titulares durante a implementação das políticas públicas de acesso à informação.

Em relação ao objetivo, este foi descritivo e exploratório, cujo foco está em compreender o contexto jurídico da interpretação da LAI e da LGPD na prática dos casos concretos para gerar a hipótese inicial da pesquisa ou outras hipóteses mais específicas que possam ser investigadas posteriormente em estudos mais detalhados.

A pesquisa adota uma abordagem multidisciplinar, combinando métodos qualitativos e quantitativos. As etapas metodológicas qualitativas incluem uma revisão abrangente da literatura para contextualizar a LAI e a LGPD, as políticas governamentais e as discussões acadêmicas sobre o tema.

A pesquisa quantitativa contará com elaboração de procedimentos estruturados e formais para a coleta e análise de dados numéricos. Para tanto, utilizaremos o seguinte procedimento: (a) elaboração de uma base de dados a partir das demandas registradas no sistema de informação ao cidadão e encaminhadas à UFRJ, no período 2018 a 2023; (b) seleção, dentre a base de dados mencionada, de uma amostra representativa que proporcione a avaliação do atendimento da demanda nos termos da LAI e da LGPD; (c) análise de conjecturas (hipóteses) formuladas a partir das respostas concedidas pela UFRJ ao cidadão e, na esfera recursal, pela CGU; (d) elaboração de respostas provisórias aos problemas apresentados e submissão dessas respostas a um rigoroso processo de verificação, de modo a aceitá-las ou refutá-las, com fundamento na LAI e na LGPD.

O objetivo é conduzir uma pesquisa no campo do direito e das políticas públicas para analisar e compreender a Lei Federal 13.709/2018 (Lei Geral de Proteção de Dados Pessoais) e sua relevância para a formulação e implementação de políticas públicas relacionadas ao acesso à informação, levando em consideração os direitos da personalidade, o direito à privacidade e a dignidade humana.

Os resultados esperados contribuirão para os diversos atores sociais, o Estado brasileiro, as instituições públicas e privadas e a sociedade civil organizada ao apresentar pesquisas que abordem temas pertinentes da atualidade e propostas coerentes voltadas à aplicabilidade da LGPD nas políticas públicas de acesso à informação.

CAPÍTULO 1

POLÍTICA PÚBLICA DE ACESSO À INFORMAÇÃO E PROTEÇÃO DE DADOS PESSOAIS: DELIMITAÇÃO E INSTERSECÇÕES JURÍDICAS

A história pode ser vista como uma sucessão de mudanças desencadeadas pelo surgimento de novas tecnologias de informação e comunicação. Podemos descrevê-la em quatro etapas principais desse processo: a revolução agrícola, a revolução industrial, a revolução da gestão e a revolução da informação (Beniger, 1989).

A Revolução Agrícola marcou o início dos primeiros sistemas de informação, com as sociedades agrárias desenvolvendo métodos contábeis e registros para monitorar a produção de alimentos, o comércio e as transações econômicas. Isso incluiu sistemas simples de contagem, registros em tabuletas de argila e a invenção da escrita, que permitiu aos antigos povos registrar e compartilhar informações sobre plantio, colheita, armazenamento e comércio.

Civilizações antigas como Suméria, Egito, Grécia e Roma continuaram expandindo seus sistemas de informação com o avanço para sistemas escritos mais complexos, como cuneiformes e hieróglifos. Isso possibilitou o registro de leis, tratados comerciais, registros médicos e outras formas administrativas e culturais.

Da Idade Média ao Renascimento, os avanços na tecnologia de impressão ocorreram com a criação da prensa por Johannes Gutenberg no século XV. Isso resultou em uma maior disseminação de livros impressos e materiais escritos que ampliaram o acesso à informação e impulsionaram o progresso na educação, ciência e cultura.

A Revolução Industrial marcou o início de uma nova fase no desenvolvimento de sistemas de informação, trazendo consigo avanços em contabilidade, logística e gestão para lidar com as operações cada vez mais complexas das fábricas e empresas em expansão. Este período viu o surgimento de práticas contábeis duplas, da máquina de escrever, do telégrafo e dos sistemas de transporte e comunicação.

No século XX, com os avanços nas tecnologias de informação e comunicação, novas formas de sistemas informatizados surgiram, incluindo computadores, redes de comunicação e bancos de dados. Essa transformação revolucionou a maneira como as organizações armazenam, processam e transmitem informações, marcando o início da Era da Informação e da digitalização da sociedade. Na atual era da informação em constante evolução, tecnologias

como a Internet, computação em nuvem e inteligência artificial continuam a emergir. Essas mudanças têm alterado profundamente a maneira como as informações são produzidas, acessadas e compartilhadas; gerando oportunidades e desafios em praticamente todos os aspectos da vida humana.

A trajetória histórica dos sistemas de informação destaca a capacidade inovadora da humanidade para se adaptar às novas demandas sociais. Desde os primórdios dos sistemas contábeis e de escrita até as tecnologias digitais avançadas de hoje, os sistemas de informação desempenharam e continuam desempenhando um papel crucial na organização, comunicação e avanço da humanidade.

O cenário informacional da atualidade trouxe benefícios positivos, como a disseminação da Internet e da tecnologia da informação democratizando o acesso ao conhecimento, permitindo que mais pessoas alcancem uma vasta quantidade de informações e recursos educacionais, facilitando a comunicação instantânea entre cidadãos e grupos ao redor do mundo e a colaboração e compreensão intercultural. O contínuo avanço da tecnologia da informação impulsionou a inovação em diversos setores, como saúde, educação, negócios, entretenimento, melhorando a qualidade de vida, eficiência e produtividade das organizações, reduzindo custos e melhorando serviços. Além disso, pôde contribuir para aumentar a transparência de governos e empresas, promover responsabilidade e combater a corrupção.

Contudo, não se pode ignorar as consequências negativas do cenário informacional: a coleta massiva de dados pessoais levanta sérias preocupações sobre privacidade e segurança, assim como o risco de vigilância excessiva e uso indevido das informações.

Em um cenário onde a informação prevalece, é crucial promover o desenvolvimento de uma ética informacional sólida para maximizar os benefícios e minimizar os riscos. Isso inclui a implementação de políticas e práticas que incentivem o uso responsável das tecnologias de informação, protejam a privacidade e garantam um acesso equitativo a essas tecnologias. A sociedade deve ser vista como um ecossistema informativo, sendo que a sustentabilidade e a responsabilidade são fundamentais para um crescimento saudável e equilibrado.

No atual ambiente informativo em que estamos imersos, não podemos ignorar a interconexão entre sociedade da informação e sociedade em rede e mudanças profundas decorrentes do avanço das tecnologias de informação e comunicação.

A sociedade em rede é um modelo particular de organização social que surgiu na era da informação. Caracteriza-se pela utilização de redes de comunicação e informação como principais meios de coordenação e governança. Essas redes conectam pessoas, organizações e

instituições em diversos níveis, formando intricadas teias de interações e conexões. Nesse contexto, as estruturas hierárquicas tradicionais e os sistemas centralizados de poder dão lugar a redes descentralizadas e distribuídas, o que possibilita maior agilidade, flexibilidade e capacidade inovadora.

É evidente que a sociedade da informação fornece o suporte técnico e cultural necessário para o surgimento e evolução da sociedade em rede. A tecnologia da informação viabiliza a disseminação ampla de informações e contribui para a expansão e consolidação das redes em todos os aspectos da vida humana. Por sua vez, as redes de comunicação e informação facilitam a criação, compartilhamento e propagação de informações na sociedade da informação, promovendo uma maior interconexão e interdependência entre cidadãos e instituições.

O conceito de sociedade em rede refere-se a uma forma específica de organização social caracterizada pela presença dominante das redes de comunicação e informação. As redes representam as estruturas fundamentais que conectam pessoas, organizações e instituições em diferentes níveis para formar uma teia de interações e relacionamentos (Castells, 2013).

Na era da informação, as redes se tornaram o principal meio de organização social. Elas substituíram as hierarquias tradicionais e estruturas de poder centralizadas, tornando-se essenciais para coordenar e governar a sociedade atual. Uma característica marcante da sociedade em rede é sua fluidez e flexibilidade. Diferentemente das estruturas hierárquicas rígidas do passado, as redes se destacam pela capacidade de se adaptar e reconfigurar diante das mudanças nas condições sociais, econômicas e tecnológicas. Essa agilidade promove inovação em todos os aspectos da sociedade.

No entanto, a era da sociedade em rede também apresenta desafios e dilemas importantes, como a exclusão digital, a polarização social, a concentração de poder em mãos selecionadas e a perda de privacidade. Essas são questões cruciais que surgem com o avanço das redes na era da informação.

É essencial equilibrar os benefícios e desafios trazidos pela sociedade da informação para garantir que possamos aproveitar ao máximo as oportunidades oferecidas pela era digital, ao mesmo tempo em que lidamos com as questões e preocupações associadas a ela. Ao adotar uma política pública de tratamento de dados pessoais, considera-se o fato de que a privacidade em uma sociedade da informação é essencial para um ambiente digital inclusivo e responsável. Isso requer esforços contínuos de todas as partes interessadas: Governo, empresas públicas e privadas e sociedade civil.

1.1 Fundamentos Jurídicos da Política Pública de Transparência: Direito à Informação, Regulação, Democracia e Direitos Humanos

A política pública de transparência no Brasil possui uma base jurídica que reflete o compromisso do Estado com a promoção de uma gestão pública mais aberta, acessível e democrática. A Lei de Acesso à Informação (Lei n. 12.527/2011 - LAI) é o principal marco normativo que regulamenta o direito de acesso às informações públicas, assegurando o princípio da publicidade e a participação cidadã nos assuntos do Estado. Outro marco jurídico importante é a Lei Complementar n. 101/2000 (Lei de Responsabilidade Fiscal - LRF), que, em seu art. 48, exige que a transparência da gestão fiscal seja assegurada por meio da liberação de informações de execução orçamentária e financeira, reforçando a *accountability* do Estado perante a sociedade.

Contudo, para além de uma análise normativa, é fundamental compreender os fundamentos jurídicos dessa política pública no contexto das teorias de políticas públicas. Este capítulo examina os fundamentos jurídicos da transparência pública, contextualizando-os dentro do conceito de políticas públicas, com especial atenção ao papel regulatório do Estado e ao direito fundamental à informação, relacionando esses conceitos com os conceitos de Democracia e Direitos Humanos.

A definição de políticas públicas abarca as ações do Estado voltadas para a solução de problemas sociais, econômicos ou institucionais. Thomas Dye define política pública como o que o governo decide fazer ou não fazer, ressaltando que as escolhas governamentais se materializam em programas, normas e regulamentos que buscam atingir objetivos coletivos (Dye, 2016). Nesse sentido, a transparência pode ser vista como uma política pública que visa a democratização da informação e a promoção de uma gestão pública mais responsável e responsiva.

O processo de formulação e implementação de políticas públicas envolve múltiplos atores e etapas. No caso da transparência, atores como o legislativo, o executivo e a sociedade civil desempenham papéis cruciais na criação de um ambiente propício à participação democrática. A implementação da LAI, por exemplo, envolveu o desenvolvimento de portais de transparência, ouvidorias e sistemas de controle social, evidenciando a importância da estrutura institucional no sucesso dessa política.

Adicionalmente, a transparência pública pode ser analisada dentro das abordagens de políticas públicas focadas no processo de formulação. Segundo o modelo de ciclo de políticas

públicas (Secchi, 2022), a transparência se encontra na fase de implementação e avaliação, em que as ações governamentais são monitoradas e adaptadas conforme as necessidades da sociedade. A transparência fortalece o controle social, um mecanismo essencial para garantir que as políticas implementadas atinjam os resultados esperados. Pode-se considerar, também que a política pública de transparência se insere no conceito mais amplo de políticas públicas por seu caráter instrumental e normativo. O Estado, ao regulamentar o direito à informação, define regras que impactam diretamente na eficiência da gestão pública e na promoção de uma cultura de responsabilidade social. Trata-se, neste caso, de uma política pública que também é regulatória.

Bucci define políticas regulatórias como "marcos institucionais" que delimitam os direitos e deveres entre Estado e sociedade, contribuindo para a previsibilidade das ações estatais e o controle social (Bucci, 2017). Nesse contexto, a política pública de transparência pode ser vista como uma política regulatória que estabelece um novo regime de governança, no qual o acesso à informação pública é regulamentado, ao mesmo tempo em que são criados mecanismos de controle e participação social. Essa política não apenas define o que é permitido ou proibido dentro de uma área específica, mas também estabelecem os termos nos quais as relações sociais, econômicas e políticas se desenrolam. Em outras palavras, as políticas regulatórias são responsáveis por criar um arcabouço institucional que influencia profundamente o comportamento dos cidadãos e das organizações. Um marco regulatório eficaz proporciona previsibilidade, reduz incertezas e garante a coerência das ações estatais e privadas. Além disso, serve para equilibrar interesses públicos e privados, garantindo que os direitos fundamentais sejam protegidos em situações que envolvam riscos à coletividade.

A política pública de transparência, portanto, fundamentada no direito constitucional à informação e na Lei de Acesso à Informação, desempenha um papel central na democratização da gestão pública e na promoção da *accountability* estatal. Ao ser compreendida no contexto das teorias de políticas públicas, especialmente no modelo de políticas regulatórias, a transparência emerge como um marco institucional que redefine as relações entre o Estado e a sociedade. Com isso, o direito à informação deixa de ser apenas um direito passivo, tornando-se um instrumento ativo de participação cidadã e controle social. A política de transparência pública, ao alinhar-se aos conceitos de políticas públicas, demonstra sua importância como uma ferramenta de governança moderna e participativa, essencial para a construção de um Estado mais justo, eficiente e democrático. Logo, não podemos dissociar democracia de transparência pública, pois ambos os conceitos estão diretamente relacionados: não há democracia sem

transparência pública e acesso à informação; não há Estado Democrático onde o silêncio do cidadão se faz presente.

A democracia é, sob esta ótica, um sistema político em que todos nós temos voz e podemos expressar nossas opiniões. É um sistema no qual os cidadãos têm o poder de decidir como querem que as coisas sejam feitas e quem eles querem que os represente. Mas, para que isso funcione corretamente, é necessário que tenhamos acesso a informações confiáveis e atualizadas sobre o que está acontecendo no governo e o que nossos representantes estão fazendo. Assim, podemos tomar decisões informadas e influenciar as políticas de forma eficaz.

Sob esta óptica, o direito à informação é extremamente importante, pois ele permite que as pessoas tenham acesso às informações sobre o que os governos e os representantes eleitos estão fazendo. Isso é fundamental para uma democracia saudável, pois os cidadãos podem monitorar e avaliar o desempenho dessas autoridades. Além disso, ter acesso à informação também possibilita que as pessoas participem ativamente das questões políticas, contribuindo para o processo de tomada de decisão.

Mill (2016) discute a relação entre acesso à informação e democracia, argumentando que a liberdade de expressão e o livre acesso à informação são a base para o funcionamento saudável de uma sociedade democrática. Acredita que a livre troca de ideias e informações é essencial para o desenvolvimento individual e coletivo e que os cidadãos têm o direito inerente de procurar, receber e trocar informações e ideias sem interferência do governo ou da sociedade.

A diversidade de opiniões e perspectivas é muito importante para que a sociedade possa evoluir intelectual e moralmente. É por meio dessa diversidade que as pessoas têm a oportunidade de questionar suas próprias crenças, considerar novas ideias e buscar a verdade. Além disso, o acesso à informação é essencial para evitar que os governos exerçam um poder arbitrário sobre a população. Sem uma imprensa livre e a possibilidade de um debate aberto, os governos podem se tornar opressivos, suprimindo qualquer forma de discordância e limitando a liberdade de expressão. Portanto, a liberdade de imprensa e o direito à informação como mecanismos de controle do governo garante a sua responsabilização perante o povo e previne o abuso de poder.

Ao defender o acesso à informação, não se defende somente a liberdade individual, mas também os alicerces da democracia. Uma sociedade verdadeiramente democrática só pode existir quando os cidadãos são livres para procurar a verdade por si próprios, questionar a autoridade e participar ativamente no processo político.

Contudo, a democracia não se resume apenas ao sistema de votação ou à existência de instituições representativas; ela é, acima de tudo, um regime que exige a participação consciente e ativa dos cidadãos (Bobbio, 2009). Logo, o acesso à informação é crucial, pois possibilita que os eleitores compreendam as ações dos governantes, avaliem suas políticas e exerçam controle sobre os poderes constituídos. Sem uma base sólida de informações, os cidadãos não podem julgar adequadamente os candidatos ou os partidos, o que enfraquece o processo democrático.

Na Constituição Federal de 1988, a transparência pública envolve principalmente os princípios da administração pública e a garantia de acesso à informação, incluindo os princípios da legalidade, impessoalidade, moralidade, publicidade e eficiência. O princípio da publicidade está diretamente relacionado com a transparência e exige que as ações administrativas sejam abertas e públicas.

Outro ponto enfatizado pela Carta Magna é o direito de petição e o direito de obter informações. O direito de petição, previsto no artigo 5.º, inciso XXXIV, garante a todos o direito de apresentar pedidos às autoridades públicas para fazer valer direitos ou para se opor a práticas ilegais ou abusivas. Além disso, o inciso XXXIII, do mesmo artigo da Constituição, estipula o direito de obter informação, garantindo o acesso dos cidadãos à informação relacionada com a administração pública e mantendo a necessária confidencialidade nas circunstâncias previstas na lei.

Além da transparência pública, vários artigos da Constituição Federal de 1988 incluem referências à participação cidadã, refletindo a importância da participação popular no processo democrático. A Carta Magna prevê a realização de referendos, plebiscitos e iniciativas populares como ferramentas para a participação direta do povo na tomada de decisões políticas.

Embora não esteja explicitamente previsto na Constituição Federal, o orçamento participativo é uma prática adotada por muitas cidades no Brasil como forma de envolver os cidadãos na determinação das prioridades de investimentos e gastos públicos. Ainda, o artigo 204 da Constituição Federal prevê a participação da sociedade civil em conselhos e conferências que exercem o controle social sobre as políticas públicas. Embora este artigo trate especificamente de programas de assistência social, a participação da sociedade civil nos conselhos e reuniões que controlam as políticas públicas é uma prática muito mais ampla, abrangendo áreas tão diversas como saúde, educação, meio ambiente e muito mais. Estes espaços proporcionam oportunidades para os cidadãos participarem ativamente na formulação, implementação e monitorização de políticas públicas, contribuindo para uma governação mais democrática e inclusiva.

Apesar das disposições constitucionais, os desafios à transparência pública e à participação dos cidadãos no Brasil permanecem e refletem questões históricas, estruturais e culturais. Em um país com um histórico de corrupção e desigualdade, garantir a transparência nas ações governamentais e promover a participação ativa dos cidadãos são cruciais para fortalecer a democracia e promover o desenvolvimento sustentável.

Um dos desafios que enfrentamos é que, muitas vezes, o governo e a sociedade civil não são transparentes e não assumem responsabilidade. Isso significa que informações importantes são escondidas ou distorcidas, o que torna difícil para os cidadãos acessar dados sobre políticas públicas e como os recursos públicos estão sendo utilizados. Existem desigualdades no acesso à informação, com grupos marginalizados, como comunidades indígenas, quilombolas e pessoas de baixos rendimentos, que enfrentam maiores barreiras à participação ativa nos processos democráticos e exigem transparência governamental.

Outro desafio é a fragilidade das instituições responsáveis pelo controle e supervisão das autoridades públicas, tais como o Tribunal de Contas, a Controladoria-Geral da União, o Ministério Público, que muitas vezes enfrentam interferências políticas para desempenhar eficazmente as suas funções. A corrupção também representa uma barreira significativa à transparência e à participação dos cidadãos, minando a confiança nas instituições e dificultando a participação da sociedade civil. A falta de punição para os responsáveis por práticas corruptas perpetua o problema e dificulta a construção de uma cultura de integridade.

Todos esses desafios retratam um problema estrutural que vem de uma época em que o acesso à informação foi restringido e os direitos humanos desrespeitados. Durante os períodos de ditadura, os regimes autoritários implementaram uma série de medidas para censurar a imprensa, controlar o fluxo de informação e suprimir qualquer forma de discurso que pudesse desafiar a sua autoridade. O regime autoritário controlou os meios de comunicação, impôs censura prévia ao conteúdo noticioso e proibiu a publicação de notícias que pudessem questionar ou criticar o governo. Além disso, utilizou a propaganda como ferramenta para manipular a opinião pública, difundindo informações falsas ou distorcidas para promover as suas narrativas e justificar as suas ações.

Além da censura direta, os regimes autoritários recorreram à repressão e à intimidação para silenciar qualquer forma de dissidência ou oposição. Isto incluiu as detenções arbitrárias de jornalistas e ativistas, o encerramento de meios de comunicação independentes, a tortura e perseguição de críticos do regime e o uso da violência para reprimir protestos e manifestações.

Como resultado dessas medidas repressivas, o direito à informação foi gravemente comprometido durante a ditadura no Brasil, resultando num acesso limitado a informações precisas para os cidadãos. Isto criou um ambiente de medo e desconfiança, onde a liberdade de expressão foi suprimida e os cidadãos lutaram para buscar informações que pudessem desafiar a narrativa oficial do governo.

A abertura política no Brasil, iniciada na década de 1980, marcou um período de transição crucial da ditadura militar para a democracia. Este momento histórico trouxe consigo a necessidade urgente de restabelecer direitos civis fundamentais, entre os quais se destaca o acesso à informação. A luta pelo acesso à informação no Brasil pós-abertura política não só fortaleceu a democracia nascente, mas também impulsionou o desenvolvimento social, político e econômico do país.

Durante os anos de repressão militar, a censura foi uma prática comum, restringindo o fluxo de informações e suprimindo a liberdade de expressão. Com o fim do regime, a sociedade brasileira começou a demandar maior transparência e acesso irrestrito à informação, como forma de garantir a participação cidadã no processo democrático.

A promulgação da Constituição de 1988 foi um marco significativo nessa luta. O artigo 5º, inciso XXXIII, assegura que todos têm o direito de receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade. Este dispositivo constitucional foi um avanço importante, pois institucionalizou o direito ao acesso à informação como um direito fundamental do cidadão brasileiro. A Lei de Acesso à Informação (LAI), sancionada em 2011, representou um passo decisivo na consolidação desse direito e estabeleceu mecanismos claros e eficazes para que qualquer pessoa, física ou jurídica, possa solicitar e obter informações públicas de todos os níveis de governo. A lei trouxe maior transparência às ações governamentais, permitindo uma fiscalização mais rigorosa por parte da sociedade civil e dos meios de comunicação. A implementação da LAI também obrigou os órgãos públicos a adotarem práticas mais transparentes e a melhorarem a gestão de suas informações.

A luta pelo acesso à informação no Brasil pós-abertura política foi impulsionada por diversas organizações da sociedade civil, movimentos sociais e ativistas que se mobilizaram para garantir que este direito fosse efetivamente respeitado. Essas organizações frequentemente atuam como mediadoras entre os cidadãos e o governo, promovendo campanhas de conscientização e oferecendo suporte para que as pessoas saibam como solicitar informações públicas.

A transparência possibilitada pela abertura política e pela volta da democracia revelou inúmeros casos de corrupção, desvios de verbas públicas e abusos de poder. A possibilidade de acesso a dados públicos permitiu que jornalistas, pesquisadores e cidadãos em geral pudessem investigar e denunciar práticas ilícitas, promovendo maior responsabilidade e ética na administração pública. No entanto, a luta pelo acesso à informação no Brasil não está isenta de desafios. A resistência de alguns setores da administração pública em fornecer informações, a complexidade dos procedimentos e a falta de clareza na comunicação são obstáculos que ainda precisam ser superados. Além disso, a educação e a capacitação dos cidadãos para o uso efetivo das ferramentas disponíveis são aspectos essenciais para garantir que o direito à informação seja exercido plenamente.

Para Angélico (2012), o direito à informação vai muito além de ter acesso às decisões do governo e, portanto, vai muito além de uma democracia participativa. Para ele, o direito de acesso à informação é uma questão de direitos humanos, posto que é um instrumento para a promoção de direitos sociais, como acesso à educação, à saúde etc. Dessa forma, o direito à informação tem um valor instrumental para o acesso a outros direitos.

Quando se trata de ditadura, a transparência expõe torturas e crimes violentos, impede que a política de esquecimento e impunidade, que ainda permeiam a democracia brasileira, prosperem. O direito à informação estabelece o direito à verdade e pune os comportamentos abusivos, ilegais e corruptos. Não foi por acaso que a Lei de Acesso à Informação foi sancionada no mesmo dia em que se formalizou a criação da chamada Comissão da Verdade, com o objetivo de investigar abusos cometidos pelas forças do Estado brasileiro, entre 1946 e 1988. Dessa forma, o direito à informação, além das perspectivas de gestão e democracia, articula-se com a defesa dos direitos humanos e é um mecanismo importante contra a corrupção e a impunidade (Angélico, 2012).

O Art. XIX da Declaração Universal dos Direitos Humanos de 1948 afirma que toda pessoa tem direito à liberdade de opinião e expressão; este direito inclui a liberdade de, sem interferência, ter opiniões e de procurar, receber e transmitir informações e ideias por quaisquer meios e independentemente de fronteiras.

Como um dos pilares fundamentais na construção de sociedades democráticas e justas, este artigo assegura a todos os cidadãos o direito à liberdade de opinião e expressão, incluindo a liberdade de buscar, receber e disseminar informações e ideias por qualquer meio. Esse direito é crucial não apenas para o exercício da liberdade individual, mas também para a manutenção de um ambiente político transparente e responsável.

Na sociedade moderna, o Artigo XIX se manifesta como uma garantia essencial para que os cidadãos possam participar ativamente na vida pública, questionar autoridades, formar opiniões e, acima de tudo, exigir transparência dos governos. No Brasil, a materialização dos princípios do Artigo XIX ocorre, em grande parte, por meio da Lei de Acesso à Informação (Lei nº 12.527/2011): ambos buscam garantir que a informação circule livremente e que os governos sejam transparentes em suas ações. Ao assegurar o direito de acesso à informação, a lei brasileira reforça os princípios estabelecidos pela Declaração Universal dos Direitos Humanos, permitindo que os cidadãos exerçam plenamente sua liberdade de expressão e de informação.

Contudo há desafios na aplicação deste direito que reflete as tensões entre a proteção da liberdade de expressão e a necessidade de garantir outros direitos e interesses sociais.

Em muitos países, governos autoritários impõem restrições severas à liberdade de expressão, controlando a mídia e reprimindo dissidentes. Essas práticas minam a essência do Artigo XIX, suprimindo a livre circulação de informações e ideias. Com o advento das redes sociais e o fácil acesso à internet, a disseminação de desinformação se tornou um grande problema. O desafio é equilibrar o combate à desinformação sem comprometer a liberdade de expressão, evitando censuras arbitrárias.

Em nome da segurança nacional, muitos países implementam medidas que restringem o acesso à informação e monitoram comunicações, alegando a necessidade de prevenir o terrorismo. No entanto, essas práticas podem ser usadas para justificar violações do direito à liberdade de expressão. Há um debate contínuo sobre os limites da liberdade de expressão quando se trata de discursos que incitam ódio ou violência. Regulamentar esses discursos sem infringir o direito à livre expressão é um desafio complexo.

Outra questão é que grandes corporações de tecnologia, que controlam plataformas de mídia social e motores de busca, têm um enorme poder sobre o que pode ou não ser publicado. Isso levanta preocupações sobre censura privada e a concentração de poder na regulação do fluxo de informações. Em muitos países, especialmente em regiões em desenvolvimento, o acesso à internet e a outros meios de comunicação é limitado. Isso cria uma disparidade na capacidade das pessoas de exercerem seu direito à liberdade de expressão e informação. E a tentativa de regular o conteúdo na internet, para proteger outros direitos, como a privacidade ou a dignidade, levanta questões sobre a censura e a limitação da liberdade de expressão. Em alguns países, as leis nacionais entram em conflito com os princípios do Artigo XIX, seja por

meio de leis de difamação rigorosas, seja por políticas que criminalizam a expressão de certas opiniões.

Esses desafios destacam a complexidade de aplicar o Artigo XIX de maneira que proteja a liberdade de expressão, ao mesmo tempo em que considera outros interesses sociais e políticos legítimos. Encontrar o equilíbrio adequado entre a liberdade de expressão e outras prioridades sociais é uma das questões mais críticas enfrentadas pelas democracias modernas.

Na era digital, regulamentar o acesso à informação desempenha um papel fundamental na promoção da transparência, proteção da privacidade e defesa dos direitos humanos e democráticos. Embora a Internet e outras tecnologias digitais abram oportunidades sem precedentes para compartilhar informações e acessá-las, também apresentam consideráveis desafios que exigem intervenções regulatórias para mitigar seus impactos adversos. Isso implica em encontrar um equilíbrio entre a liberdade de expressão e a proteção contra conteúdos prejudiciais, além de lidar com a natureza global da Internet. É fundamental que os governos, empresas de tecnologia e organizações da sociedade civil colaborem na criação de diretrizes e normas que incentivem o acesso seguro, inclusivo e democrático à informação na era digital.

Fato é que os ambientes digitais não são neutros e as leis e políticas governamentais desempenham um papel crucial na definição da produção, distribuição e acesso à informação on-line. O código, ou seja, o software e a arquitetura digital, tem um impacto direto no comportamento on-line. As escolhas por determinadas informações no mundo digital refletem valores e interesses específicos nos sistemas computacionais e da Internet. Assim sendo, as leis combinadas com políticas governamentais têm uma influência significativa no acesso à informação na era digital (Lessig, 1999).

Um tópico debatido frequentemente que suscita controvérsia é a relevância da transparência e do controle democrático em relação às políticas sobre acesso à informação na era digital. De acordo com esse debate, é crucial limitar a influência indevida de interesses comerciais e econômicos nas decisões políticas através de regulamentações, garantindo uma participação mais ampla do público no processo regulatório. As leis e políticas relacionadas à informação devem representar os interesses e valores de toda a sociedade, não apenas os de grupos privilegiados ou poderosos.

A regulamentação do acesso à informação na era digital destaca a importância de políticas e leis que fomentem a liberdade de expressão, protejam dados pessoais sensíveis, garantam igualdade de acesso e transparência democrática, oferecendo conceitos valiosos sobre

como assegurar um acesso equitativo, seguro e justo. Isso é essencial em um mundo cada vez mais interligado.

Para Mattos (2017), o Estado regulador emerge como uma resposta às falhas do Estado interventor, que, nas décadas anteriores, mantinha uma participação direta nos setores produtivos da economia por meio de empresas estatais e políticas públicas centralizadas. O Estado regulador, ao contrário, atua principalmente por meio da criação de marcos regulatórios que visam ordenar o comportamento de agentes econômicos e sociais, delegando às agências reguladoras o papel de fiscalizar e implementar essas normas. A formação desse modelo está diretamente ligada ao processo de liberalização econômica e à globalização, que exigiram a adaptação das estruturas estatais para garantir um equilíbrio entre o funcionamento do mercado e a proteção de interesses públicos, como a defesa do consumidor, a proteção ambiental e a garantia de competição justa. As agências reguladoras, autônomas e especializadas, são criadas para supervisionar setores como telecomunicações, transporte, energia e saúde, atuando como mediadores entre o interesse privado e o interesse público.

A regulação, nesse contexto, passa a ser entendida como um processo técnico, que busca manter a previsibilidade e a estabilidade econômica, garantindo a segurança jurídica necessária para o investimento e a inovação. O Estado regulador, portanto, assume um papel de facilitador e fiscalizador, diferente do papel de operador que caracterizava o Estado interventor.

Lemos e Felice (2014) destacam a relevância da regulação do acesso à informação em sociedades conectadas em rede e possíveis medidas regulatórias legais. Eles discutem como a revolução digital está transformando a sociedade e o sistema jurídico, tornando essencial ajustar as leis para lidar com os desafios e oportunidades trazidos pela era da informação. As regras devem levar em conta questões como a proteção da privacidade, a liberdade de expressão na web, os direitos autorais no meio digital e o acesso às informações do governo. Ao lidar com a regulação do acesso à informação, é imprescindível adotar políticas que incentivem a transparência governamental e garantam aos cidadãos o direito de obter informações públicas. É crucial estabelecer uma legislação de transparência de dados que defina procedimentos claros para solicitar e receber dados do governo, juntamente com medidas para proteger a privacidade dos cidadãos e garantir a segurança das informações pessoais.

Importante destacar que o modelo do Estado regulador, especialmente no pós-Segunda Guerra Mundial, consolidou-se como um instrumento de controle sobre o mercado e de garantia

de direitos sociais. Inspirado por uma visão keynesiana[2], o Estado regulador intervia na economia para corrigir falhas de mercado, regular monopólios e assegurar a proteção dos consumidores e trabalhadores. A criação de agências reguladoras em áreas estratégicas, como telecomunicações, energia e transportes, reforçou esse papel.

Entre as principais características do Estado regulador estavam o controle direto, ou seja, Estado estabelecia regras claras e centralizadas para regular setores econômicos e sociais, com pouca margem para flexibilização ou adaptação pelos agentes regulados e monitorava de perto o cumprimento das normas e aplicava sanções em caso de violação. A intervenção regulatória visava garantir o bem-estar da sociedade, protegendo direitos sociais e limitando abusos de poder econômico.

Embora esse modelo tenha sido eficiente em muitos aspectos, ele começou a enfrentar críticas nas décadas seguintes. O crescente avanço tecnológico, a globalização e a complexidade das relações econômicas e sociais colocaram em xeque a capacidade do Estado de regular de forma eficiente todos os setores. Além disso, o aumento da burocracia e a falta de flexibilidade foram apontados como entraves ao desenvolvimento e à inovação.

O Estado pós-regulador, que emergiu a partir das últimas décadas do século XX, é uma resposta à incapacidade do Estado regulador de lidar com os desafios da modernidade. Em vez de atuar como um agente centralizador e controlador, o Estado pós-regulador se baseia na descentralização das funções regulatórias, na governança em rede e na colaboração com o setor privado e a sociedade civil.

Entre as principais características do Estado pós-regulador estão a descentralização e governança em rede, o Estado compartilha suas funções regulatórias com agências autônomas, o setor privado e organizações da sociedade civil. A regulação passa a ser um processo de coordenação entre diversos atores, e não mais uma ação unicamente estatal. O Estado pós-regulador incentiva a criação de mecanismos de autorregulação, especialmente em setores como o financeiro e o tecnológico, onde os próprios agentes econômicos criam códigos de conduta e mecanismos de controle. Diferente das normas rígidas do Estado regulador, o Estado pós-regulador busca criar marcos regulatórios que permitam adaptações e respostas rápidas às mudanças tecnológicas e de mercado. Nesse novo modelo de regulação estatal, o maior foco

[2] A visão keynesiana do Estado regulador é baseada na ideia de que o Estado deve desempenhar um papel ativo na economia para corrigir falhas de mercado, promover o pleno emprego e garantir o bem-estar social. Segundo Keynes, crises econômicas e desemprego são resultados de desequilíbrios na demanda agregada, que podem ser resolvidos por meio de políticas públicas, como investimento estatal, regulação de setores estratégicos e políticas monetárias e fiscais expansivas.

está no controle social e na transparência, que passam a ser elementos centrais da nova forma de governança. O Estado pós-regulador confia mais na vigilância social e na pressão pública para garantir o cumprimento das normas.

Na visão de Scott (2004), esse modelo de Estado não elimina o papel regulador, mas transforma a maneira como o governo interage com o mercado e a sociedade, promovendo novas formas de regulação através de redes de governança, autorregulação e colaboração interinstitucional. Nesse cenário, a política pública de transparência desempenha um papel fundamental, pois se torna o elo entre o Estado, o mercado e a sociedade civil, permitindo maior participação social e controle democrático.

O Estado pós-regulatório é caracterizado por três principais elementos (Scott, 2004):

a) Governança em rede: O Estado não atua sozinho, mas em colaboração com outros atores e instituições. A governança em rede implica em parcerias e cooperações, promovendo a regulação de forma menos hierárquica e mais horizontal;

b) Autorregulação: Setores do mercado passam a se autorregular, criando códigos de conduta e mecanismos próprios de fiscalização, com o Estado atuando como facilitador e garantidor de que essas normas estejam alinhadas aos interesses públicos;

c) Hibridização da regulação: A regulação se torna um processo híbrido, envolvendo múltiplas camadas e atores, com o Estado monitorando e avaliando resultados, mas não necessariamente implementando diretamente as políticas regulatórias;

O papel do Estado, portanto, se desloca de regulador direto para coordenador e incentivador de processos regulatórios mais dinâmicos e flexíveis.

Uma das principais características do Estado pós-regulatório, segundo Scott (2004), é a governança em rede. Nesse modelo, a transparência funciona como um mecanismo essencial para coordenar as interações entre os diferentes atores que compõem essa rede, como órgãos públicos, empresas privadas, ONGs e cidadãos. Ao permitir que todos esses atores tenham acesso às informações necessárias, a transparência fortalece a *accountability* coletiva e garante que as decisões regulatórias sejam monitoradas de forma ampla e compartilhada.

Além disso, a transparência favorece a legitimação do processo decisório, já que o acesso público às informações permite a participação direta e indireta da sociedade nas discussões sobre políticas públicas. No Brasil, essa participação é materializada por meio de

ferramentas como os portais de transparência e as audiências públicas, que criam oportunidades para que a sociedade civil influencie as decisões do governo e outros atores regulatórios.

A transição para esse novo modelo representa um deslocamento das responsabilidades do Estado para uma rede mais ampla de atores, o que torna o processo regulatório mais dinâmico e multifacetado. No entanto, essa descentralização também exige novos mecanismos de transparência e controle, uma vez que a multiplicidade de atores pode diluir as responsabilidades e dificultar a fiscalização. A descentralização e a governança em rede exigem que a informação esteja amplamente disponível e acessível, permitindo que a sociedade civil e os demais atores sociais possam acompanhar e fiscalizar as ações não apenas do Estado, mas também das empresas e organizações envolvidas.

Embora a política de transparência tenha avançado no contexto do Estado pós-regulador, ainda há desafios significativos a serem superados. A descentralização da regulação pode dificultar a coordenação das ações e a fiscalização, especialmente em setores onde o Estado tem menor controle direto. Além disso, a multiplicidade de atores envolvidos no processo regulatório torna a responsabilização mais difusa, o que pode enfraquecer a eficácia das políticas de transparência.

Outro desafio importante é a capacidade de acesso à informação pela sociedade. Embora a transparência pública seja um direito garantido por lei, nem todos os cidadãos possuem as mesmas ferramentas e conhecimentos para interpretar e utilizar as informações divulgadas. É necessário um investimento contínuo em educação e em sistemas de divulgação que sejam acessíveis e compreensíveis para todos os segmentos da sociedade.

Por outro lado, a transparência no Estado pós-regulador oferece uma oportunidade única para fortalecer a democracia e a participação social. Ao abrir os dados e tornar as informações públicas acessíveis, o Estado cria condições para que a sociedade civil atue como um parceiro no monitoramento das políticas públicas, contribuindo para a eficiência e legitimidade da governança.

1.2 Lei de Acesso à Informação Pública: Evolução, Princípios e Conceito de Informações Públicas e Pessoais

A evolução das políticas de acesso à informação no mundo e no Brasil teve uma trajetória importante, impulsionada pelo reconhecimento da importância da transparência e da

participação cidadã na governança democrática. Ao longo do tempo, vários movimentos políticos e sociais contribuíram para a consolidação deste direito fundamental.[3]

No cenário internacional, os movimentos pela transparência governamental e pelo acesso à informação intensificaram-se no século XX, à medida que cresciam as exigências de maior responsabilização e controle democrático do poder público. Um marco importante neste processo foi a aprovação da Lei de Liberdade de Informação de 1966 nos Estados Unidos, que estabeleceu os direitos dos cidadãos de aceder à informação detida pelo governo federal.

A Lei de Liberdade de Informação dos EUA (FOIA - *Freedom of Information Act*), promulgada em 1966, foi um marco histórico no aumento da transparência governamental e no fortalecimento da democracia. A legislação estabeleceu pela primeira vez o direito dos cidadãos dos EUA de acessar informações mantidas pelo governo federal.[4]

Nas décadas de 1950 e 1960, o governo dos EUA enfrentou críticas e questionamentos pela sua falta de transparência nas suas operações, particularmente no contexto da Guerra do Vietnã e do Movimento dos Direitos Civis. A Lei da Liberdade de Informação (FOIA) foi, portanto, promulgada em resposta a estas preocupações e foi concebida para garantir que os cidadãos tenham acesso à informação governamental de interesse público. A lei estabelece procedimentos e prazos claros para solicitação e divulgação de informações, estabelecendo que as agências governamentais devem divulgar os registros solicitados, sujeitos a certas exceções.

Estas exceções incluem informações classificadas por motivos de segurança nacional, informações relacionadas à privacidade pessoal, informações comerciais confidenciais e outras categorias específicas. No entanto, a lei exige que as agências interpretem as exceções de forma restrita e divulguem o máximo de informação possível.

Desde a sua promulgação, a FOIA tem sido uma ferramenta essencial para promover a transparência e a responsabilização no governo federal dos EUA. Milhares de pedidos de informação são apresentados todos os anos, abrangendo uma vasta gama de tópicos, desde políticas públicas e despesas governamentais até às atividades das agências de inteligência.[5]

[3] Para um estudo de direito comparativo sobre a liberdade de informação, ver o link https://www.gov.br/acessoainformacao/pt-br/central-de-conteudo/publicacoes/arquivos/liberdade-informacao-estudo-direito-comparado-unesco.pdf

[4] Para conhecer mais detalhes sobre a lei de liberdade de informação dos EUA, acesse os links https://www.foia.gov/ e https://edisciplinas.usp.br/pluginfile.php/1225286/mod_resource/content/3/FOIA.pdf.

[5] Para mais informações sobre o aumento de pedidos de informação, com base na FOIA, acesse o link https://www.poder360.com.br/internacional/governo-dos-eua-registra-recorde-de-pedidos-de-lai/

Além disso, a FOIA inspirou outros países em todo o mundo a aprovar leis de acesso à informação e a tornar-se um modelo para promover a transparência e a participação dos cidadãos na governação democrática. No entanto, apesar dos seus benefícios, a legislação tem enfrentado críticas e desafios ao longo dos anos, incluindo atrasos na resposta aos pedidos, utilização indevida de excepções e resistência por parte das agências governamentais.

Na Europa, as políticas de acesso à informação evoluíram gradualmente, impulsionadas por uma combinação de fatores históricos, políticos e sociais. Embora cada país europeu tenha as suas próprias abordagens e legislação específicas relativamente ao acesso à informação, certas tendências e influências comuns moldam o panorama em toda a Europa.

Em muitos países europeus, o movimento de transparência governamental e acesso à informação ganhou impulso no final do século XX. A queda do comunismo na Europa de Leste e o fortalecimento da integração europeia também desempenharam um papel importante neste processo, estimulando discussões sobre uma governação aberta e participativa.

Um marco importante na política europeia de acesso à informação foi a adoção da Convenção Europeia dos Direitos Humanos (CEDH) em 1950[6], que incluiu o direito à liberdade de expressão e informação como um dos direitos fundamentais protegidos pela Convenção.

Outro marco importante foi a promulgação do Regulamento Geral de Proteção de Dados (RGPD) pela UE, em 2016, e a sua implementação em 2018[7]. Embora o RGPD se concentre principalmente na proteção de dados pessoais, também promove a transparência e a responsabilização organizacional, estabelecendo regras claras para o processamento de dados e os direitos dos cidadãos de aceder às suas informações pessoais.

Além disso, alguns países europeus também promulgaram leis especiais de acesso à informação para proteger os direitos dos cidadãos de informação detida pelo governo. Por exemplo, o Reino Unido promulgou a Lei da Liberdade de Informação em 2000[8], enquanto a França aprovou uma lei semelhante em 1978, conhecida como Loi n° 78-17[9], que trata da tecnologia da informação, dos arquivos e das liberdades e promove a proteção da privacidade das pessoas, relacionada ao tratamento de dados pessoais.

[6] Para mais detalhes sobre a Convenção Europeia dos Direitos Humanos, ver link https://www.echr.coe.int/documents/d/echr/Convention_ENG

[7] Sobre a RGPD, ver o link https://eur-lex.europa.eu/PT/legal-content/summary/general-data-protection-regulation-gdpr.html

[8] Para ter acesso ao texto da lei, acesse o link https://www.legislation.gov.uk/ukpga/2000/36/contents

[9] Para acessar os artigos da lei, veja o link https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460

Desde então, outros países seguiram o exemplo, promulgando leis de acesso à informação para aumentar a transparência e a responsabilização do governo.

Avanços significativos também foram alcançados na evolução da política de acesso à informação no contexto brasileiro. O marco inicial foi a promulgação da Constituição Federal em 1988, que estabeleceu o princípio público como um dos fundamentos da administração pública. No entanto, o Brasil não promulgou leis específicas sobre acesso à informação até 2011, quando foi criada a lei 12.527/2011, conhecida como Lei de Acesso à Informação (LAI).

A Lei de Acesso à Informação[10] representa um avanço histórico na garantia dos direitos dos cidadãos de solicitar e receber informações das autoridades públicas, estabelecendo procedimentos e prazos claros para a divulgação das informações solicitadas. Desde então, a lei tornou-se uma ferramenta fundamental para promover a transparência na Administração Pública brasileira e a responsabilização no âmbito nacional.

Um dos principais impactos da LAI foi ampliar o escopo das leis de acesso à informação e como os cidadãos obtêm informações do governo. A lei estabelece procedimentos e prazos claros para que órgãos e entidades públicas forneçam informações de interesse público, facilitando a solicitação e obtenção de documentos e dados governamentais pelos cidadãos. Isto promove uma cultura de transparência e aumenta a responsabilização das autoridades públicas (Angélico, 2015).

Estruturalmente, a LAI define procedimentos e princípios para garantir o acesso dos cidadãos à informação pública. Abrange desde princípios orientadores até às agências responsáveis pela implementação, estabelecendo um quadro jurídico robusto para aumentar a transparência governamental.

De modo geral, pode-se definir a estrutura em:

a) Princípios básicos: O direito básico de obter informações, regras de publicidade e o princípio da divulgação proativa de informações. Esses princípios orientam a interpretação e aplicação da lei, garantindo que a transparência seja uma prioridade nas operações do país.

b) Definição e Escopo: A lei define o que se entende por informação pública e estipula que todos os órgãos e entidades públicas, inclusive os poderes Executivo, Legislativo e

[10] Para ter acesso ao texto da lei, veja o link https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm

Judiciário, devem cumprir suas disposições. Isto garante que a LAI cubra todas as áreas do governo e todas as informações pelas quais é responsável.

c) Procedimentos para Solicitação de Informações: A LAI estabeleceu procedimentos que os cidadãos devem seguir ao solicitar informações públicas. Isto inclui a forma de solicitação, prazos de resposta e possíveis restrições de acesso previstas na própria lei.

d) Responsabilidades dos órgãos públicos: A lei atribui responsabilidades específicas aos órgãos públicos na divulgação de informações públicas e no processamento de pedidos de informação. Isto inclui a criação de uma estrutura interna para tratar os pedidos, nomear autoridades de controle e garantir a transparência na gestão da informação.

e) Recursos e Sanções: A legislação prevê um mecanismo de recurso para os cidadãos cujos pedidos de informação sejam recusados ou não atendidos dentro de um prazo determinado. Além disso, a lei prevê sanções administrativas contra órgãos públicos que não cumpram as obrigações de transparência.

f) Divulgação proativa de informações: Uma das inovações da LAI é a obrigatoriedade de os órgãos públicos divulgarem proativamente informações de interesse público, mesmo sem solicitação prévia do cidadão. Isto ajuda a aumentar a transparência e facilita o acesso à informação governamental.

g) Órgãos de fiscalização e controle: A LAI prevê a criação de órgãos de fiscalização e controle, como a Controladoria-Geral da União (CGU) e a Ouvidoria Pública, responsáveis por fiscalizar a aplicação da lei e zelar pelo cumprimento de suas disposições.

Essa estrutura abrangente da LAI fornece uma base sólida para mais transparência governamental, participação cidadã e controle social no Brasil. Ao estabelecer procedimentos claros, responsabilidades claras e mecanismos de reclamação, a lei visa garantir que os cidadãos possam exercer eficazmente o seu direito fundamental de acesso à informação pública.

Contudo, Angélico (2015) sublinha a importância da implementação efetiva da LAI, destacando que a lei por si só não é suficiente. É necessário que haja uma mudança cultural dentro das instituições públicas, onde a transparência seja vista como um valor fundamental. Ele aponta que muitos órgãos públicos ainda enfrentam desafios na implementação plena da LAI, como a falta de capacitação dos servidores, resistência interna e a inexistência de sistemas adequados para a gestão da informação.

Além disso, a LAI não deve ser vista apenas como uma ferramenta de fiscalização, mas também como um instrumento de melhoria da gestão pública, pois a disponibilização proativa de informações pode levar a uma administração mais eficiente, à medida que os gestores públicos passam a utilizar dados e evidências para tomar decisões mais informadas. A transparência, portanto, não apenas fortalece a democracia, mas também contribui para a eficácia das políticas públicas e a responsabilização administrativa.

A responsabilização é, sob essa óptica, um princípio fundamental de qualquer sistema democrático e refere-se à obrigação das instituições públicas de serem responsabilizadas pelas suas ações e decisões. É um conceito que abrange transparência, responsabilidade e prestação de contas e é fundamental para garantir a integridade, eficácia e legitimidade das instituições governamentais.

A história da *accountability*, conceito que se refere à responsabilidade de cidadãos, organizações ou instituições na prestação de contas, tanto no cenário internacional quanto no Brasil, é marcada pelo seu desenvolvimento gradual ao longo do tempo, impulsionado por mudanças políticas, sociais e culturais. Nas sociedades antigas, embora a ideia de responsabilizar os governantes não fosse tão formalizada como é hoje, encontramos exemplos de responsabilização, como a prática de assembleias democráticas nas antigas repúblicas grega e romana (Alves, 2021).

Na Idade Média, as monarquias absolutas muitas vezes tinham pouca ou nenhuma responsabilidade para com os seus súditos. Durante o Iluminismo, surgiram ideias sobre o poder do povo e a necessidade de limitar o poder do Estado. Revoluções democráticas como a Revolução Americana e a Revolução Francesa fizeram da responsabilização um princípio fundamental da governança e consagraram-na em documentos como a Declaração dos Direitos do Homem e do Cidadão.

No século XX, com a ascensão de organizações internacionais como as Nações Unidas e a Organização dos Estados Americanos, a responsabilização tornou-se um tema central na governança global. Foram criados mecanismos como tratados internacionais, tribunais e órgãos de supervisão para responsabilizar os Estados-Membros por violações dos direitos humanos, crimes de guerra e corrupção.

No Brasil, o poder estava concentrado nas mãos da Coroa portuguesa durante o período colonial, de modo que a responsabilização era quase inexistente, com os governantes locais agindo em nome do rei e não prestando contas à população local.

Com a independência e a implantação do Império e a fundação da República Velha, o país viveu períodos de instabilidade política e autoritarismo, com pouca ou nenhuma responsabilização dos que estão no poder. O poder estava concentrado nas mãos das elites políticas e econômicas, resultando em falta de transparência e responsabilização no governo. Na ditadura, a censura violou os direitos humanos e os direitos fundamentais do cidadão e os ditadores não foram responsabilizados pelas atrocidades cometidas na época.

Com a redemocratização e a promulgação da Constituição de 1988, o Brasil obteve avanços significativos na promoção da responsabilização. A Carta Magna estabeleceu princípios básicos, como a divulgação de atos administrativos, o direito de acesso à informação e mecanismos de controle externo, e o fortalecimento da transparência e da responsabilização das instituições públicas.

Além da Constituição, o Brasil promulgou leis específicas para promover a responsabilização, como a Lei de Responsabilidade Fiscal (Lei Complementar nº 101/2000) e a Lei de Acesso à Informação (Lei nº 12.527/2011), que regulamenta a transparência e a responsabilização na administração pública, com sanções previstas na legislação.

O conceito de responsabilização não se limita à responsabilização por meio de sanções ou punições, mas também inclui a responsabilização por meio de explicações e justificativas para as ações tomadas. Esta abordagem permite uma compreensão mais ampla das relações de poder e responsabilidade em diferentes estruturas organizacionais. Existe a responsabilização horizontal, que ocorre entre intervenientes do mesmo nível, e a responsabilização vertical, que ocorre entre autoridades a diferentes níveis. Ambas as formas são essenciais para garantir a transparência e a responsabilização das instituições e prevenir o abuso de poder e a corrupção (Bovens, 2010).

A responsabilização é a ênfase na participação dos cidadãos e na sociedade civil como forças fundamentais que promovem a transparência e a cidadania. Não deve ser apenas responsabilidade das agências governamentais ou organizações privadas, mas deve ser um processo de envolvimento e diálogo contínuo com os cidadãos e as partes interessadas. Além disso, o papel das instituições formais e informais na promoção da responsabilização é essencial e os mecanismos de controle e supervisão, como o poder judicial, as agências de controle interno e as agências reguladoras são muito importantes.

No entanto, reconhecemos a necessidade de complementar estas instituições com mecanismos informais, como uma imprensa livre, uma sociedade civil organizada e redes sociais, que desempenham um papel vital na exposição de casos de corrupção e na exigência

de transparência e responsabilização. Na verdade, ainda há uma série de desafios para a implementação eficaz da responsabilização em diferentes áreas da sociedade. Um dos principais desafios é a resistência institucional à mudança, especialmente em organizações burocráticas e hierárquicas, onde as estruturas de poder estabelecidas podem dificultar a responsabilização e a transparência. A falta de uma cultura de responsabilização em muitas situações, em que a responsabilização não é valorizada ou incentivada, conduz a uma cultura de impunidade e falta de transparência. Isto é particularmente presente em países com um histórico de corrupção e autoritarismo, onde as instituições são frágeis e suscetíveis ao abuso de poder.

Contudo, apesar dos desafios, a implementação da LAI incentivou as instituições públicas brasileiras a melhorar os seus sistemas de gestão de informação, a fornecer dados de uma forma mais acessível e compreensível para o público, a tomar decisões mais informadas e a participar mais ativamente na vida política e social do país. país. nação.

Historicamente, a cultura burocrática no Brasil sempre foi marcada pelo sigilo e pela retenção de informações. Por outro lado, a Lei de Acesso à Informação trouxe impactos na cultura de abertura e transparência, o que já é um avanço civilizatório, que aproxima o Brasil dos padrões de governança dos países mais desenvolvidos e democráticos. Além de empoderar os cidadãos, fornecendo-lhes as ferramentas necessárias para participar de forma ativa e informada no processo político, a LAI é um mecanismo essencial para a melhoria da gestão pública, pois a transparência imposta pela lei obriga os gestores públicos a adotarem práticas mais eficientes e a buscarem constantemente a melhoria dos serviços prestados.

A possibilidade de os governantes serem constantemente avaliados pela sociedade cria um incentivo adicional para a busca de resultados concretos e positivos. E no contexto das políticas públicas, a LAI facilita a avaliação e o monitoramento das políticas implementadas. Com o acesso às informações, é possível analisar dados, verificar a execução de programas e projetos, e identificar áreas que necessitam de ajustes ou melhorias. Essa capacidade de monitoramento contínuo é fundamental para a adaptação e aprimoramento das políticas públicas.

Importante também destacar que o principal fundamento da LAI está na própria Constituição Federal, em particular nos artigos 5º, XXXIII, 37 e 216.

O artigo 5º, XXXIII, estabelece que "todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei". O artigo 37, por sua vez, impõe à administração pública os princípios da legalidade, impessoalidade, moralidade, publicidade e eficiência. A publicidade, aqui, se refere

à transparência dos atos públicos, essencial para o controle social. Já o artigo 216, no contexto da cultura, trata da gestão documental e da proteção dos documentos públicos como meios de acesso à informação.

Esses dispositivos constitucionais servem como alicerces para a LAI, que visa operacionalizar o direito à informação, detalhando como ele deve ser exercido e garantido. Ao estruturar a lei em torno desses princípios, o legislador buscou assegurar que o acesso à informação seja um instrumento efetivo de fortalecimento da democracia, permitindo que os cidadãos participem de forma mais ativa na vida pública e na fiscalização dos atos do governo.

A LAI está organizada em seis capítulos, que tratam de aspectos fundamentais como as disposições gerais, os procedimentos para solicitação de informações, as restrições de acesso, as responsabilidades dos agentes públicos e as disposições finais e transitórias.

O Capítulo I, que trata das disposições gerais, estabelece os princípios fundamentais da lei, reforçando que o acesso à informação é regra e o sigilo, exceção. Este capítulo define os conceitos essenciais, como "informação", "documento", "disponibilidade", "autenticidade", "integridade" e "primariedade", que orientam a aplicação da lei. Além disso, dispõe sobre a abrangência da LAI, que se aplica a todos os órgãos públicos dos três poderes, em todas as esferas de governo, incluindo administrações diretas e indiretas, e a entidades privadas sem fins lucrativos que recebem recursos públicos.

O Capítulo II, do Acesso à Informação e sua Divulgação, trata das formas de acesso à informação, estabelecendo que os órgãos públicos devem garantir a transparência ativa e passiva. A transparência ativa refere-se à obrigação de os órgãos públicos divulgarem, espontaneamente, informações de interesse coletivo, independentemente de solicitações. Isso inclui a publicação de dados em seus sítios eletrônicos, como despesas, receitas, licitações e contratos. A transparência passiva, por outro lado, envolve o atendimento às solicitações de informação feitas por qualquer cidadão. O Capítulo II define que o acesso à informação deve ser facilitado e gratuito, salvo os custos de reprodução de documentos. Os órgãos públicos têm o dever de responder às solicitações em até 20 dias, prorrogáveis por mais 10 dias mediante justificativa.

No Capítulo III, dos procedimentos de acesso à informação, a lei detalha os procedimentos para a solicitação de informações, prevendo que qualquer pessoa pode requerer informações de forma simples e sem a necessidade de justificar o pedido. Os órgãos públicos devem designar um Serviço de Informação ao Cidadão (SIC), responsável por receber,

processar e responder aos pedidos de informação. Este capítulo também estabelece o dever de orientação ao solicitante, caso a informação requerida não esteja claramente identificada.

Além disso, a lei prevê mecanismos para assegurar o direito de recurso, permitindo que o solicitante recorra a instâncias superiores dentro do órgão ou entidade caso a informação não seja fornecida ou o pedido seja negado.

O Capítulo IV trata das restrições de acesso à informação, estabelecendo que apenas em casos de sigilo, justificado por razões de segurança nacional, defesa, relações internacionais ou proteção à intimidade, vida privada, honra e imagem das pessoas, o acesso pode ser restringido. Este capítulo define os prazos de classificação das informações em ultrassecreta (25 anos), secreta (15 anos) e reservada (5 anos), além de prever a revisão periódica dessas classificações.

Este capítulo também garante que informações pessoais só podem ser divulgadas com o consentimento do titular ou em situações de interesse público devidamente justificadas, e protege informações cuja divulgação possa prejudicar investigações policiais, processos judiciais ou processos administrativos em andamento.

O Capítulo V estabelece as responsabilidades dos agentes públicos e das instituições no cumprimento da LAI. Estão previstas sanções administrativas para os servidores que negarem acesso à informação de forma injustificada, que destruírem documentos ou que agirem com dolo ou má-fé para ocultar informações. Este capítulo reforça o caráter vinculativo da lei, que impõe a obrigação de cumprimento a todos os agentes públicos.

O Capítulo VI traz as disposições finais e transitórias, incluindo prazos para que os órgãos públicos se adaptem às exigências da lei. Este capítulo também estabelece que a LAI prevalece sobre normas anteriores que sejam contrárias ao seu disposto.

Outro fundamento importante da estrutura da LAI é o equilíbrio entre o direito à informação e a necessidade de proteger outros direitos, como a privacidade, a segurança e a soberania nacional. A lei prevê exceções ao acesso à informação, como no caso de dados sigilosos, cuja divulgação possa comprometer a segurança do Estado ou a privacidade de cidadãos e define os tipos de informações que podem ser classificadas como públicas, pessoais ou sigilosas. Essa definição é importante para entender como funciona o acesso à informação de acordo com esta lei.

Importante destacar que a Lei de Acesso à Informação foi criada para regulamentar o direito constitucional de acesso à informação pública. Nesse contexto, a lei faz distinções claras

entre os conceitos de "informação pública" e "informações pessoais", estabelecendo regras específicas para o tratamento de cada um desses tipos de informações. Esses conceitos são essenciais para compreender como a transparência e a privacidade são equilibradas na aplicação desta lei.

Para Angélico (2012), a expressão “acesso à informação pública” trata da materialização do conceito de transparência. Em inglês, as leis que regulam a transparência pública são chamadas de “Freedom of Information Act” (FOIA). Pode-se inferir, portanto, que “liberdade de informação” (*freedom of information*) tenha sido traduzida ao português para “acesso à informação”, possivelmente para oferecer uma ideia de “livre acesso”, contudo há limites bem estabelecidos pela Lei de Acesso à Informação no Brasil.

Informação pública, de acordo com a lei Federal nº 12.527/2011, refere-se a qualquer dado, registro ou conhecimento produzido ou mantido pelos órgãos públicos que, por sua natureza, seja de interesse geral ou coletivo e não esteja sujeito a restrições de acesso por questões de sigilo ou proteção de dados pessoais. Isso inclui documentos, registros, relatórios, decisões administrativas, contratos, orçamentos, dados sobre licitações, despesas, entre outros, que são gerados ou mantidos pelas administrações públicas nas três esferas de governo (federal, estadual e municipal) e nos três poderes (Executivo, Legislativo e Judiciário).

A lei estabelece que a regra geral é a publicidade dessas informações, em consonância com o princípio da transparência, que é um dos pilares da administração pública. Isso significa que qualquer pessoa, independentemente de justificativa, pode solicitar acesso a informações públicas, e os órgãos governamentais têm o dever de disponibilizá-las, exceto nos casos previstos de sigilo.

Além da divulgação mediante solicitação, a LAI também impõe a obrigação de transparência ativa, ou seja, a divulgação espontânea de informações públicas relevantes, como receitas, despesas, auditorias, convênios, e demais dados que permitam o acompanhamento e fiscalização da gestão pública. Essa obrigação busca assegurar que a administração pública opere de forma aberta e responsiva, permitindo o controle social por parte dos cidadãos.

Por outro lado, a LAI também reconhece e protege o direito à privacidade, especialmente no que se refere ao tratamento de informações pessoais. Informações pessoais são definidas pela lei como dados relacionados à pessoa natural identificada ou identificável. Isso inclui informações como nome, endereço, documentos de identidade, registros financeiros, e qualquer outro dado que possa ser utilizado para identificar uma pessoa ou que se refira a aspectos de sua vida privada.

A proteção dessas informações é tratada com especial cuidado pela Lei Federal nº 12.527/2011, refletindo a importância do direito à privacidade. A lei estabelece que o acesso a informações pessoais depende, em regra, do consentimento do titular dos dados, exceto em situações previstas em lei, como para o cumprimento de uma obrigação legal, em casos de proteção de interesses vitais do titular, ou para a execução de políticas públicas. Além disso, define que as informações pessoais não podem ser divulgadas publicamente sem autorização, a menos que estejam relacionadas a uma pessoa cuja posição ou função pública implique maior transparência, como autoridades eleitas ou servidores em posições de destaque. Mesmo nesses casos, a divulgação deve se restringir ao necessário para atender ao interesse público.

Outro ponto relevante é que as informações pessoais podem ser acessadas pelo próprio titular a qualquer momento, e este tem o direito de solicitar correções ou atualizações, caso os dados estejam incorretos ou desatualizados. Esse direito é uma forma de garantir que os cidadãos mantenham o controle sobre suas próprias informações.

A LAI também aborda a situação em que informações públicas contêm dados pessoais. Nesses casos, a lei busca um equilíbrio entre a transparência e a privacidade. Quando a divulgação de informações públicas envolver dados pessoais, a lei recomenda que se busque a anonimização ou pseudonimização dos dados, de forma a proteger a identidade dos indivíduos, enquanto se mantém o acesso à informação de interesse público. Por exemplo, em casos de divulgação de listas de beneficiários de programas sociais, a informação sobre os valores recebidos pode ser considerada de interesse público, mas a exposição de detalhes pessoais dos beneficiários pode ser restrita para proteger sua privacidade. A lei, portanto, prevê mecanismos para que essa proteção seja efetiva, sem comprometer a transparência.

Desta forma, a Lei Federal nº 12.527/2011 estabelece um sistema que valoriza tanto o direito à informação pública quanto o direito à privacidade. Enquanto promove a ampla divulgação de dados e informações de interesse público para garantir a transparência e a participação cidadã, a LAI também assegura que as informações pessoais sejam tratadas com a devida confidencialidade e proteção. Esse equilíbrio é fundamental para a construção de uma administração pública que seja ao mesmo tempo aberta e respeitosa dos direitos individuais.

1.3 Evolução Histórica do Direito à Privacidade e a Política Pública de Proteção de Dados

O direito à privacidade, ou "right of privacy," é um dos conceitos mais fundamentais e debatidos no campo dos direitos individuais e das liberdades civis. Este direito protege a vida

privada dos cidadãos contra interferências não autorizadas, assegurando um espaço pessoal inviolável em que a pessoa pode tomar decisões e agir livre de vigilância ou intromissão.

O surgimento deste direito como um conceito jurídico reconhecido é relativamente recente, datando do final do século XIX. Uma das contribuições mais significativas para a formulação deste direito foi feita por Samuel D. Warren e Louis D. Brandeis, cujos esforços acadêmicos e jurídicos lançaram as bases para o reconhecimento e a proteção legal da privacidade nos Estados Unidos e, por consequência, influenciaram a evolução deste direito em diversas outras jurisdições.

O conceito de privacidade como um direito autônomo começou a ganhar forma em resposta às rápidas transformações sociais e tecnológicas do século XIX. Durante este período, a industrialização e a urbanização, juntamente com os avanços na tecnologia da informação, como a fotografia e a imprensa de massa, criaram ameaças à esfera privada dos indivíduos. Essas mudanças levaram a uma crescente preocupação com a capacidade de proteger informações pessoais e a integridade da vida privada contra invasões.

Antes do trabalho de Warren e Brandeis, as leis que protegiam a privacidade eram fragmentadas e limitadas. A proteção legal era geralmente oferecida através de outras áreas do direito, como a difamação, o direito contratual ou o direito de propriedade. Não havia uma doutrina unificada ou específica que reconhecesse a privacidade como um direito distinto e essencial. Neste contexto, a privacidade estava implicitamente protegida, mas a necessidade de um reconhecimento explícito e de uma defesa jurídica mais robusta tornou-se evidente à medida que novas ameaças emergiam.

Em 1890, Samuel D. Warren e Louis D. Brandeis publicaram um artigo intitulado "The Right to Privacy" na Harvard Law Review[11], que é amplamente considerado o ponto de partida para o desenvolvimento moderno do direito à privacidade. Neste artigo, argumentaram que o direito à privacidade deveria ser reconhecido como um direito legal autônomo, distinto de outros direitos existentes. Eles definiram a privacidade como o "direito de ser deixado em paz" ("the right to be let alone"), uma frase que se tornaria central para a compreensão do conceito.

Essa definição simples e poderosa reflete a compreensão de que os cidadãos têm o direito de controlar sua vida privada, livre de intrusões indesejadas por parte de terceiros, sejam eles outros indivíduos, empresas ou o governo.

[11] Para entender melhor o conceito de privacidade apresentado por Warren e Brandeis, leia o artigo: The right to privacy. Harvard Law Review, p. 123-220, 1890.

O "direito de ser deixado em paz" implica que cada pessoa deve ter a liberdade de escolher o que deseja compartilhar com o mundo e o que prefere manter em segredo ou restrito a um círculo íntimo. Esse direito se estende a vários aspectos da vida, incluindo: proteção contra intrusão física, ou seja, a pessoa tem o direito de estar em sua casa, ou em qualquer outro ambiente privado, sem ser perturbada por invasões físicas não autorizadas, como entrar na casa de alguém sem permissão; proteção contra intrusão em informação pessoal, que envolve a ideia de que as informações pessoais e íntimas não devem ser divulgadas ou exploradas sem o consentimento da pessoa. Isso inclui dados como correspondências, fotografias, e outras formas de comunicação que revelam detalhes sobre a vida privada; e proteção contra difamação e publicidade não autorizada, pois as pessoas têm o direito de controlar como sua imagem e identidade são apresentadas ao público. Isso significa que ninguém deve ser forçado a se tornar uma figura pública contra sua vontade, nem ter sua imagem ou nome usados comercialmente sem permissão.

Na época em que o artigo foi escrito, a sociedade americana estava enfrentando um rápido avanço tecnológico, com a proliferação de jornais sensacionalistas e a invenção da fotografia, que facilitavam a coleta e a disseminação de informações pessoais de maneira antes impensável. Warren e Brandeis observaram que essas mudanças estavam expondo a vida privada das pessoas a uma publicidade indesejada, o que poderia causar danos à dignidade, reputação e bem-estar emocional.

O "direito de ser deixado em paz", portanto, emerge como uma resposta a essas novas ameaças à esfera privada. É um direito que protege o indivíduo não apenas contra danos materiais ou físicos, mas também contra danos à sua psique e identidade pessoal, resultantes da exposição e intrusão indesejada. Ele reconhece que a privacidade é essencial para o desenvolvimento da personalidade, da autonomia e da liberdade pessoal.

Os autores basearam seu argumento no princípio de que as leis deveriam evoluir para responder às mudanças sociais e tecnológicas. Eles observaram que a jurisprudência americana até então se concentrava na proteção da propriedade e da reputação, mas não oferecia uma proteção adequada à privacidade pessoal. Para eles, a rápida expansão da tecnologia, especialmente a fotografia e a imprensa, tornava urgente a criação de um direito que protegesse os cidadãos contra a invasão indevida de sua vida privada.

O artigo é notável por sua antecipação de muitos dos desafios contemporâneos à privacidade. Eles discutiram como a tecnologia poderia permitir a coleta e a disseminação de informações pessoais de maneiras que ameaçavam a dignidade e a autonomia dos indivíduos,

reconheceram que o direito à privacidade precisava ser equilibrado com outros interesses sociais, como a liberdade de expressão, mas argumentaram que este equilíbrio deveria ser alcançado sem sacrificar a proteção adequada da privacidade individual.

O impacto dessas ideias foi profundo. Embora o argumento não tenha gerado imediatamente novas leis, ele teve uma influência significativa na forma como os tribunais americanos começaram a interpretar a privacidade. O conceito de privacidade como um direito autônomo gradualmente se infiltrou na jurisprudência americana e, eventualmente, foi reconhecido pela Suprema Corte dos Estados Unidos como um direito implícito na Constituição, particularmente em relação à proteção contra buscas e apreensões injustificadas e ao direito à intimidade pessoal.

No século XXI, as discussões sobre privacidade tornaram-se ainda mais complexas diante da expansão das tecnologias digitais e da coleta massiva de dados. Surge, nesta época, o conceito de privacidade na perspectiva do argumento “nada a esconder”, especialmente com o monitoramento e a coleta massiva de dados após os ataques de 11 de setembro de 2001, nos Estados Unidos. Foi nesse período que muitos países, em nome da segurança nacional, passaram a implementar políticas de vigilância em massa, o que levou ao aumento das discussões sobre o equilíbrio entre segurança e privacidade.

O uso do argumento “nada a esconder” é frequentemente atribuído a defensores de políticas de vigilância governamental, que buscavam justificar a intrusão nas vidas privadas dos cidadãos sob o pretexto de segurança pública. Embora não haja um único indivíduo que tenha formulado esse argumento de maneira formal, ele aparece repetidamente em discursos políticos e públicos que promovem a vigilância sob o pretexto de que “se você não está fazendo nada de errado, não tem por que se preocupar”.

Contudo, o argumento “nada a esconder” é uma tentativa de minimizar a relevância da privacidade, tratando-a como uma preocupação válida apenas para aqueles que têm algo a temer. De acordo com essa visão, a vigilância e a coleta de dados são justificáveis desde que não afetem diretamente quem não está envolvido em atividades ilegais.

Um dos estudiosos contemporâneos que mais se dedicou a explorar e refinar o entendimento moderno da privacidade é Daniel J. Solove, especialmente em seu ensaio "I’ve Got Nothing to Hide" and Other Misunderstandings of Privacy[12], em que ele desconstrói o argumento simplista de que, se alguém não tem nada a esconder, não deveria se preocupar com

[12] Para entender melhor o conceito de privacidade na frase “nada a esconder”, leia o ensaio I've Got Nothing to Hide' and Other Misunderstandings of Privacy. San Diego Law Review, Vol. 44, 2007.

invasões de privacidade. Neste texto, o conceito de privacidade, conforme explorado por Solove, vai além da tradicional visão de privacidade como mero sigilo, e aborda a complexidade das interações entre privacidade, vigilância e poder.

Solove (2007) inicia sua análise no ensaio ao abordar uma justificativa comum para minimizar a importância da privacidade: o argumento "nada a esconder". Este argumento postula que apenas aqueles que têm algo ilícito ou imoral a esconder devem temer a vigilância ou a coleta de dados. Essa visão simplista falha em reconhecer as várias dimensões da privacidade, e que a privacidade não se resume a esconder segredos, mas também envolve o controle sobre como as informações pessoais são usadas e disseminadas.

O argumento "nada a esconder", segundo Solove, desconsidera o fato de que todos possuem aspectos de sua vida que preferem manter privados, não por serem ilegais, mas por serem íntimos, pessoais ou simplesmente não destinados ao consumo público. A privacidade está intrinsecamente ligada à dignidade, à autonomia individual e ao controle sobre o próprio ambiente social.

Assim, propõe-se uma abordagem pluralista para a privacidade, argumentando que ela não pode ser reduzida a uma única definição ou categoria. Em vez disso, ele identifica várias "famílias de problemas" que se relacionam com a privacidade, como a vigilância, a coleta de dados, a disseminação de informações, a intrusão e a agregação de dados. Cada uma dessas categorias representa uma ameaça distinta à privacidade, que não pode ser completamente capturada por uma visão unidimensional de privacidade como sigilo.

Por exemplo, na era digital, a privacidade é muitas vezes ameaçada pela vigilância em massa e pela coleta de dados em larga escala por governos e corporações. E mesmo quando as informações coletadas não são particularmente sensíveis, a maneira como esses dados são agregados, processados e usados pode resultar em consequências prejudiciais, como discriminação, manipulação ou perda de autonomia.

Outro aspecto importante da evolução do conceito de privacidade, conforme discutido por Solove, é a relação entre privacidade e poder. Ele argumenta que a privacidade não é apenas sobre proteger informações pessoais, mas também sobre a distribuição do poder na sociedade. A coleta de dados e a vigilância conferem um poder desproporcional a governos e corporações, permitindo-lhes monitorar, influenciar e, em última instância, controlar o comportamento das pessoas.

O autor utiliza a metáfora do "panóptico", proposta originalmente por Jeremy Bentham[13]e popularizada por Michel Foucault, para ilustrar como a vigilância cria um estado constante de autocensura e conformidade. Em um ambiente de vigilância, mesmo que uma pessoa não tenha "nada a esconder", a simples possibilidade de estar sendo observada pode alterar seu comportamento, restringindo sua liberdade de ação e expressão.

O conceito de "panóptico" tem origens e interpretações distintas nas obras de Bentham (1791) e Foucault (1975), embora ambos utilizem o termo para discutir a vigilância e o controle.

Jeremy Bentham, filósofo e jurista inglês do século XVIII, é o criador original do conceito de panóptico. Ele idealizou o panóptico como um modelo arquitetônico para prisões, que permitiria a vigilância total dos prisioneiros por parte de um único vigia.

A estrutura do panóptico é circular, com uma torre de vigilância central que possui janelas voltadas para as celas dispostas em torno dela. As celas estão iluminadas, de modo que o vigia pode observar cada prisioneiro, mas os prisioneiros não podem ver o vigia. A ideia central é que, como os prisioneiros nunca sabem quando estão sendo observados, eles internalizam a vigilância e se disciplinam por conta própria, evitando comportamentos indesejados. Bentham acreditava que esse modelo seria eficaz não apenas em prisões, mas também em escolas, hospitais e fábricas, onde o controle e a disciplina eram necessários.

Michel Foucault, filósofo francês do século XX, retoma o conceito de panóptico em sua obra "Vigiar e Punir" (1975), mas com uma abordagem teórica e crítica mais ampla. Para Foucault, o panóptico de Bentham é uma metáfora poderosa para entender as sociedades modernas e o surgimento do que ele chama de "sociedade disciplinar".

Foucault (1975) argumenta que, no mundo moderno, a lógica do panóptico transcende a arquitetura das prisões e se espalha por diversas instituições sociais, como escolas, fábricas, hospitais e até mesmo a própria sociedade. Ele descreve como a vigilância se torna uma forma de poder que não precisa ser exercida continuamente, porque a possibilidade constante de ser

[13] O panóptico ou a casa de inspeção: contendo a idéia de um novo princípio de construção aplicável a qualquer sorte de estabelecimento, no qual pessoas de qualquer tipo necessitem ser mantidas sob inspeção; prisões, casas de indústria, casas de trabalho, casas para pobres, manufaturas, hospícios, com lazaretos, hospitais e escolas: em particular às casas penitenciárias.

observado leva os cidadãos a regular seu próprio comportamento. Assim, o panóptico é um modelo de poder que é eficiente precisamente porque é invisível e interiorizado pelas pessoas.[14]

Foucault utiliza o conceito para ilustrar como o poder nas sociedades modernas não é mais exercido apenas através da repressão direta, mas também através de técnicas sutis de vigilância e controle que levam as pessoas a se disciplinarem por si mesmas. Isso cria um ambiente onde a conformidade e a obediência são mantidas sem a necessidade de coerção física constante.

Enquanto Bentham (1791) via o panóptico como uma solução arquitetônica pragmática para a vigilância e o controle social, Foucault o transformou em uma metáfora para o funcionamento do poder nas sociedades modernas. O conceito, portanto, evolui de uma proposta de reforma penal para uma crítica mais ampla das dinâmicas de poder e controle na vida social contemporânea. Foucault critica a ideia de privacidade como uma proteção contra o controle social. Ele argumenta que a privacidade, na verdade, pode ser um efeito das práticas de controle, pois as técnicas modernas de vigilância e disciplina se escondem sob a superfície da vida privada. A ideia de privacidade pode, portanto, funcionar como uma fachada que oculta o poder sutil e difuso que atua sobre os indivíduos.

Já Solove utiliza a metáfora do panóptico em sua obra para ilustrar os desafios contemporâneos da privacidade, especialmente no contexto da vigilância e coleta de dados em massa.

Na era digital, o "vigia" no centro da torre pode ser entendido como as entidades que coletam e processam dados pessoais — como empresas de tecnologia, agências governamentais ou plataformas online. Assim como no panóptico de Bentham, onde os prisioneiros não sabem quando estão sendo observados, as pessoas na era digital não têm conhecimento sobre quando, como ou por quem seus dados estão sendo monitorados. Essa incerteza gera um efeito disciplinador, onde as pessoas podem moderar ou alterar seu comportamento por medo de

[14] Na punição analógica, o poder que pune se esconde. A frase "o poder que pune se esconde" de Michel Foucault, encontrada em sua obra "Vigiar e Punir" (1975), encapsula uma das principais ideias do filósofo sobre a natureza do poder e da punição nas sociedades modernas. Foucault examina como o poder não se manifesta apenas por meio de métodos diretos e visíveis, como o uso de força física, mas também por meio de mecanismos mais sutis e menos perceptíveis. A ideia de que "o poder que pune se esconde" sugere que a modernidade trouxe formas mais sofisticadas e menos perceptíveis de controle social. Em vez de uma presença constante e visível do poder punitivo, o controle é exercido através de práticas que se integram ao cotidiano das pessoas e que moldam seu comportamento de maneira mais discreta e eficaz.

serem observadas, mesmo que não tenham certeza de que estão sendo monitoradas em um determinado momento.

Como no panóptico original, a vigilância digital leva as pessoas a internalizarem o olhar do "vigia". A sensação de estar sob constante monitoramento pode levar à autocensura, reduzindo a liberdade de expressão e a criatividade, à medida que as pessoas tentam se conformar às expectativas percebidas de quem as observa. A metáfora do panóptico também destaca a perda de autonomia e controle sobre as informações pessoais. Na sociedade digital, as pessoas muitas vezes não têm controle sobre como seus dados são coletados, armazenados e utilizados, o que pode levar a consequências imprevistas e indesejadas, como discriminação ou manipulação.

Logo, a privacidade desempenha um papel crucial na proteção contra os efeitos negativos da vigilância panóptica. Não é apenas uma questão de impedir o acesso a informações pessoais, mas também de preservar a autonomia individual e a dignidade em face da vigilância. Regulamentações de proteção de dados, como as que garantem transparência, consentimento e controle sobre o uso de informações pessoais, são vistas como formas de mitigar o poder panóptico das instituições modernas.

Nesse contexto, é importante definir o que constitui uma invasão de privacidade. A mesma informação pode ser considerada privada ou pública dependendo das circunstâncias em que é coletada e usada. Por exemplo, uma foto tirada em um evento público pode ser aceitável para uso pessoal, mas sua disseminação online para um público amplo pode ser vista como uma invasão de privacidade, dependendo do contexto. Essa perspectiva contextual é fundamental para compreender as complexidades da privacidade no mundo moderno, onde as barreiras entre o público e o privado estão cada vez mais borradas pela tecnologia. Solove argumenta que a legislação e as políticas de privacidade precisam levar em conta essas nuances contextuais para serem eficazes na proteção dos direitos individuais.

Em uma abordagem pluralista e contextual deve-se entender a privacidade como um conjunto de interesses inter-relacionados que variam de acordo com o contexto e as circunstâncias, identificando diferentes tipos de ameaças e problemas que afetam a vida privada. A ideia de que a privacidade possa ser totalmente capturada por definições tradicionais, como "o direito de ser deixado em paz" ou "o controle sobre informações pessoais" deve, de acordo com Solove, ser completamente rejeitada.

Privacidade não envolve apenas o controle sobre a informação pessoal, mas também o contexto em que essa informação é coletada, usada e compartilhada. O conceito é sobre a

capacidade de gerenciar as próprias informações e sobre como o uso dessas informações pode impactar a dignidade, a liberdade e a autonomia da pessoa. Por exemplo, uma informação que é inofensiva em um contexto pode se tornar uma invasão de privacidade em outro. Isso demonstra que a privacidade não é uma questão de proteger apenas certos tipos de informações, mas também de considerar como, onde e por que essas informações são utilizadas.

Logo, a privacidade é uma questão complexa e contextual, que vai muito além do simples sigilo. Ela envolve a proteção contra uma variedade de ameaças que podem surgir em diferentes contextos e que afetam não apenas o controle sobre informações pessoais. Por exemplo, a monitorização constante das atividades de uma pessoa pode levar à perda de autonomia e à sensação de ser sempre observado, mesmo quando não há nada a esconder; a coleta extensiva e às vezes excessiva de informações pessoais, muitas vezes sem o consentimento explícito ou consciente do indivíduo, e que pode ser usada para fins inesperados ou prejudiciais; o uso de dados agregados para criar perfis, prever comportamentos ou tomar decisões automatizadas que podem afetar profundamente a vida das pessoas; a divulgação ou compartilhamento de informações pessoais, muitas vezes sem o controle ou conhecimento do indivíduo, o que pode levar à invasão de privacidade, constrangimento ou até mesmo discriminação.

O conceito de privacidade tem sido objeto de intensa discussão e evolução ao longo das últimas décadas, especialmente em resposta ao avanço das tecnologias digitais e à crescente coleta e uso de dados pessoais. Para Doneda (2021), o tema privacidade está diretamente relacionado à informação, especificamente aos dados pessoais. Para ele, nas últimas décadas, a privacidade passou a se relacionar com vários interesses e valores que acabaram por modificar substancialmente o seu conceito. Hoje, o Direito à Privacidade não mais se estrutura em torno do eixo “pessoa-informação-segredo”, mas sim no eixo “pessoa-informação- circulação-controle”.

Nesse contexto, a proteção da privacidade passou a estar relacionada à Teoria dos Direitos da Personalidade, como uma forma expansiva de proteger os dados pessoais.

Segundo Doneda (2021):

> Nessa mudança, a proteção da privacidade identifica-se e acompanha a consolidação da própria teoria dos direitos da personalidade e, em seus mais recentes desenvolvimentos, afasta a leitura segundo a qual sua utilização em nome de um individualismo exacerbado alimentou o medo de que eles se tornassem o direito dos egoístas privados. Algo, paradoxalmente, a proteção da privacidade na sociedade da informação, a partir da proteção de dados pessoais, avança sobre terrenos outrora

> improponíveis e nos induz a pensá-la como um elemento que, mais do que garantir o isolamento ou a tranquilidade, serve a proporcionar ao indivíduo os meios necessários à construção e consolidação de uma esfera privada própria, dentro de um paradigma de vida em relação e sob o signo da solidariedade – isto é, de forma que a tutela da privacidade cumpra um papel positivo para o potencial de comunicação e relacionamento do indivíduo. Tal função interessa à personalidade como um todo e ganha importância ainda maior quando fatores como a vida em relação e as escolhas pessoais entram em jogo – como nas relações privadas, na utilização de novas tecnologias, no caso da política e, paradoxalmente, na própria vida pública. (Doneda, 2021, p.194).

A teoria dos direitos da personalidade tem como base a ideia de que existem certos direitos inalienáveis e irrenunciáveis, que protegem a essência da pessoa humana. Esses direitos derivam do reconhecimento da dignidade humana como fundamento do ordenamento jurídico e buscam garantir a inviolabilidade da integridade física, moral e psíquica dos indivíduos. Entre os principais direitos da personalidade estão o direito à vida, à integridade física, à honra, ao nome, à imagem e, de forma crescente na modernidade, o direito à privacidade. Esses direitos são caracterizados pela sua indisponibilidade, o que significa que, mesmo que o titular deseje renunciá-los, o ordenamento jurídico impõe limitações, garantindo sua proteção mesmo contra a vontade do indivíduo, em prol de sua dignidade.

Importante salientar, também, que a cláusula geral de proteção da personalidade, prevista na Constituição brasileira, é indispensável para lidar com a complexidade da vida moderna e a multiplicidade de situações que não podem ser plenamente abarcadas por direitos subjetivos específicos. Devido à variabilidade dos tipos de situações que envolvem a proteção da pessoa, uma tutela baseada em direitos legais predeterminados é insuficiente para captar a totalidade das potencialidades e desafios da personalidade humana. Assim, apenas a técnica jurídica da cláusula geral, com sua abertura e flexibilidade, seria capaz de responder adequadamente às mudanças constantes e imprevisíveis da sociedade, como aquelas advindas das novas tecnologias da informação e comunicação e que, consequentemente, refletem na privacidade do cidadão.

De acordo com Mattietto (2017):

> A promoção constitucional da cláusula geral de proteção da pessoa deve-se à imprescindibilidade de, diante da multiplicidade da vida real e da complexidade do comportamento humano, ir além dos parcos direitos especiais da personalidade expressamente previstos na legislação civil brasileira.

> O conceito de personalidade, como valor ético fundamental e como expressão da humanidade, impõe uma estrutura jurídica compreensiva, não reducionista, aberta e maleável, sem a qual se esvazia boa parte de seu conteúdo. Mesmo que abrangentes, múltiplos ou variados sejam os tipos com que se pretenda assegurar a proteção da pessoa, uma tutela limitada a direitos subjetivos legalmente estabelecidos será sempre redutora das amplas potencialidades da personalidade humana. (Mattietto, 2017, p. 218 a 232)

A privacidade, dentro desse conjunto, aparece como um direito voltado para a preservação da esfera íntima e pessoal, assegurando ao indivíduo o controle sobre o acesso e a divulgação de informações sobre sua vida privada. A sua importância foi amplamente reconhecida na modernidade, especialmente com o desenvolvimento de teorias que analisam o impacto da invasão de privacidade nos direitos individuais e na liberdade pessoal.

Historicamente, o direito à privacidade não foi sempre reconhecido de forma explícita. No entanto, a partir do final do século XIX, com o famoso artigo de Samuel Warren e Louis Brandeis, “The Right to Privacy” (1890), o conceito começou a ser moldado como uma garantia essencial à dignidade humana, especialmente em face do crescente uso de novas tecnologias que ameaçavam expor aspectos da vida privada ao público.

Com o advento da era digital e o crescimento da internet, a privacidade tornou-se ainda mais vulnerável. O aumento exponencial do uso de dados pessoais para finalidades comerciais e governamentais gerou novas tensões em torno do controle e proteção da vida privada. Dessa forma, a privacidade passou a ser entendida não apenas como uma questão de sigilo ou isolamento, mas também como um direito ao controle sobre a própria informação, uma dimensão essencial da autodeterminação individual.

No âmbito da teoria dos direitos da personalidade, o direito à privacidade é essencial para garantir a autonomia e a liberdade do indivíduo e, como parte dos direitos da personalidade, possui um caráter absoluto e personalíssimo, ou seja, é um direito que se refere diretamente à condição humana e à necessidade de proteção da individualidade e dignidade. Sob esse aspecto, a privacidade envolve o controle sobre a exposição da vida pessoal, familiar e profissional, permitindo que o indivíduo decida o que deseja ou não compartilhar com terceiros. Essa proteção é fundamental para evitar danos à honra, à imagem e à reputação, que são elementos indissociáveis dos direitos da personalidade.

No contexto das sociedades digitais, onde grandes volumes de dados pessoais são coletados e processados por diversas entidades, a autodeterminação informativa[15] emerge como uma proteção crucial. A privacidade deve ser vista, portanto, como um direito de escolher como os dados pessoais são tratados, garantindo que as pessoas possam exercer controle sobre suas próprias informações em um ambiente onde a coleta e o processamento de dados são constantes e muitas vezes invisíveis.

Para Doneda (2021):

> A necessidade de funcionalização da proteção da privacidade fez, portanto, com que ela desse origem a uma disciplina de proteção de dados pessoais, que compreende em sua gênese pressupostos ontológicos muito similares aos da própria proteção da privacidade: pode-se dizer que a proteção de dados pessoais é a sua continuação por outros meios. Ao realizar essa continuidade, porém, a proteção de dados pessoais assume a tarefa de abordar uma série de interesses cuja magnitude aumenta consideravelmente na sociedade pós-industrial e acaba, por isso, assumindo uma série de características próprias, especialmente na forma de atrair os interesses que protege, mas também em referência a outros valores e direitos fundamentais. Daí a necessidade de superar a ordem conceitual pela qual o direito à privacidade era limitado por uma tutela de índole patrimonialista, e de estabelecer novos mecanismos e mesmo institutos para possibilitar a efetiva tutela dos interesses da pessoa. (Doneda, 2021, p. 194)

A conotação contemporânea da privacidade, especialmente no contexto da proteção de dados pessoais, revela uma transformação profunda no modo como o direito à privacidade é compreendido e exercido. A partir de uma visão individualista e restrita ao âmbito da vida privada, a privacidade passa a ser entendida como um conceito mais amplo e relacional, envolvendo a interseção de múltiplos direitos ligados à personalidade e às liberdades fundamentais da pessoa humana. Nesse novo paradigma, a privacidade é elevada a um estatuto normativo, englobando não apenas a proteção individual contra interferências indevidas, mas também as relações entre a personalidade e o mundo exterior, incluindo o impacto das novas tecnologias e o uso massivo de dados pessoais.

[15] A autodeterminação informativa é o direito de os cidadãos controlarem o uso de suas informações pessoais, decidindo quais dados podem ser coletados e compartilhados. Esse conceito surgiu na Alemanha em 1983, quando o Tribunal Constitucional Federal reconheceu esse direito em resposta à controvérsia sobre a coleta massiva de dados no censo populacional. A autodeterminação informativa é central em legislações como a LGPD e o GDPR, garantindo que o tratamento de dados seja transparente e baseado no consentimento. No contexto atual, esse direito é essencial para proteger a privacidade e a autonomia dos indivíduos em uma sociedade digitalizada. Para Doneda (2021), a autodeterminação informativa é uma subespécie do direito da personalidade e se relaciona diretamente com o direito de privacidade.

Historicamente concebida como o direito de estar só, a definição de privacidade focava na proteção de uma esfera íntima, longe de intromissões do Estado ou da sociedade. Entretanto, esse conceito se mostrou inadequado para lidar com os desafios impostos pelo avanço das tecnologias de informação e comunicação. Na contemporaneidade, especialmente com o desenvolvimento de tecnologias digitais e a coleta massiva de dados pessoais, a privacidade assume novas dimensões, que vai além da simples proteção de uma esfera íntima e envolve o direito de decidir quando, como e em que circunstâncias informações pessoais podem ser acessadas e utilizadas por terceiros.

Essa mudança reflete um deslocamento da privacidade como um direito isolado para um direito relacional, ou seja, um direito que se define na interação entre o indivíduo, o Estado, empresas e a sociedade. Nesse sentido, a privacidade deixa de ser apenas um direito individual e passa a ser compreendida como um direito que afeta a coletividade e o próprio funcionamento de sociedades democráticas.

1.4 Lei Geral de Proteção de Dados Pessoais: Evolução, Princípios e o processo de formulação da LGPD

A regulamentação de dados pessoais no mundo iniciou-se na Europa. A Alemanha foi o primeiro país a criar uma lei voltada para a proteção de dados, com a promulgação da Lei de Proteção de Dados de Hesse, em 1970. Este foi o primeiro marco regulatório destinado a proteger os cidadãos contra o uso indevido de suas informações por governos e empresas (Doneda, 2021).

A partir desta lei, seguiram-se outras determinações legislativas que Doneda define como gerações de leis de proteção de dados pessoais, que reflete as mudanças sociais, políticas e tecnológicas que exigiram respostas jurídicas mais sofisticadas para garantir a privacidade e os direitos dos cidadãos em relação aos seus dados.

A primeira geração das leis de proteção de dados pessoais surgiu em resposta ao crescimento dos bancos de dados e ao uso massivo de informações pessoais por governos e corporações. Um marco inicial foi o debate sobre a informatização dos registros de dados e a capacidade de coletar e armazenar informações em grande escala. Na Suécia, em 1973, elaborou-se o Estatuto para banco de dados, *Data Legen 279*, como resposta ao desenvolvimento dos bancos de dados automatizados. No ano seguinte, os Estados Unidos

aprovaram o *Privacy Act* (1974), que regulamentava o uso de informações pessoais pelas agências governamentais, exigindo maior transparência e controle por parte dos cidadãos. Nesse mesmo contexto, a Alemanha adotou legislações e debates que influenciaram o cenário global, abordando a coleta e o processamento de dados, sobretudo no contexto governamental e corporativo.

A primeira geração de leis, embora tenha sido inovadora ao enfrentar os desafios da coleta de dados em larga escala, foi limitada em seu alcance, focando principalmente no uso governamental de dados e na proteção contra abusos institucionais. As legislações da época tinham um caráter mais básico e reativo, com foco na regulamentação de bancos de dados e pouca ênfase no controle pessoal dos dados.

A segunda geração de leis de proteção de dados trouxe um avanço significativo. Em 1978, a França aprovou a sua Lei de Proteção de Dados (*Loi informatique et libertés*), que criou a Comissão Nacional de Informática e Liberdades (CNIL) para supervisionar o tratamento de dados pessoais. No mesmo período, países como Áustria, Portugal e Espanha introduziram proteções a dados pessoais em suas legislações e constituições, consolidando a privacidade como um direito fundamental.

Essa geração de leis foi marcada pela introdução de um enfoque mais centrado no indivíduo, reconhecendo o papel ativo dos cidadãos no controle sobre suas próprias informações. No entanto, as legislações ainda enfrentavam desafios relacionados à aplicação efetiva e à compreensão do desequilíbrio de poder entre os detentores de dados (empresas e governos) e os titulares (cidadãos).

Na década de 1980, surgiu a terceira geração de leis de proteção de dados, que buscou uma maior sofisticação na tutela dos dados pessoais, ao incorporar o princípio da autodeterminação informativa e expandir os direitos dos cidadãos em relação às suas informações pessoais. Essa geração foi impulsionada por decisões como a do Tribunal Constitucional Alemão e pela crescente conscientização da necessidade de mecanismos mais eficazes para proteger os cidadãos.

A decisão do Tribunal Constitucional Federal da Alemanha, em 1983, que consagrou o direito à autodeterminação informativa, marcou uma transformação no entendimento sobre a privacidade. Nesse julgamento, ficou estabelecido que cada pessoa tem o direito de controlar suas informações pessoais, o que estabeleceu um marco para a proteção de dados como um direito fundamental. As emendas às leis de proteção de dados na Alemanha e na Áustria, assim como a criação de novas legislações em países como Noruega e Finlândia, visaram expandir os

direitos de proteção de dados e garantir uma supervisão mais rigorosa. Essas leis centravam-se na figura do cidadão, buscando garantir que os cidadãos tivessem mecanismos claros e acessíveis para o controle e a correção de suas informações pessoais. A autodeterminação informativa foi consolidada como um direito fundamental, mas ainda permanecia acessível principalmente às elites e às minorias, o que indicava a necessidade de uma maior democratização desse direito.

O grande marco, no entanto, foi a adoção da Diretiva 95/46/CE pela União Europeia (UE), em 1995. Esta diretiva estabeleceu normas detalhadas para a coleta, o processamento e a transferência de dados pessoais dentro dos Estados-membros da União Europeia. A partir dela, diversos países europeus passaram a adotar legislações nacionais com base nas diretrizes estabelecidas pela UE. No entanto, à medida que as tecnologias evoluíam, essa diretiva se mostrou limitada em lidar com os novos desafios trazidos pela globalização e digitalização da economia.

A quarta geração de leis de proteção de dados, que emerge ao final do século XX e início do XXI, surge com o objetivo de superar as limitações do enfoque individualista das gerações anteriores. Essa geração reconhece que a simples autodeterminação informativa não era suficiente para lidar com o desequilíbrio estrutural entre os cidadãos e as entidades detentoras de grandes quantidades de dados.

As leis da quarta geração, como o Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia, buscam ampliar a proteção, incluindo instrumentos que elevam o padrão coletivo de proteção. A ênfase recai sobre a responsabilidade das organizações e a necessidade de proteger dados de forma proativa e colocam a privacidade como um aspecto central no desenvolvimento de sistemas e no tratamento de dados. Além disso, essa geração de leis aborda o desequilíbrio de poder, reconhecendo que as pessoas individualmente podem não ter o conhecimento, os recursos ou a influência necessária para proteger adequadamente seus dados. Por isso, as leis incorporam medidas coletivas de proteção e exigem das empresas e governos um nível maior de responsabilidade e transparência.

Em 2016, a UE substituiu a diretiva de 1995 pelo Regulamento Geral de Proteção de Dados (*General Data Protection Regulation, GDPR*). O GDPR entrou em vigor em 2018 e se tornou o principal marco regulatório de proteção de dados no mundo. Ele trouxe normas mais rígidas e detalhadas, aumentando os direitos dos cidadãos europeus e impondo maiores responsabilidades às empresas que lidam com dados pessoais. O GDPR também teve um impacto global, uma vez que sua aplicação extraterritorial exige que qualquer organização que

processe dados de cidadãos europeus esteja em conformidade com suas normas, independentemente de onde esteja sediada.

No Brasil, a proteção de dados pessoais avançou de forma mais gradual. Durante muito tempo, o país carecia de uma legislação geral sobre o tema. Antes da LGPD, a proteção de dados era abordada de maneira fragmentada em diversas normas, como o Habeas Data, o Código de Defesa do Consumidor (1990), a Lei do Cadastro Positivo (2011) e o Marco Civil da Internet (2014). Essas legislações abordavam a privacidade e a proteção de dados em contextos específicos, mas não ofereciam um regime geral e abrangente.

O Marco Civil da Internet, de 2014, foi um avanço importante, pois estabeleceu princípios e garantias para o uso da internet no Brasil, incluindo normas sobre a privacidade dos usuários. O Marco Civil tratava de forma específica da proteção de dados no ambiente digital, mas ainda não havia uma regulamentação ampla para todas as esferas de tratamento de dados pessoais.

A necessidade de uma legislação geral sobre proteção de dados tornou-se mais urgente após a aprovação do GDPR na Europa, que serviu de inspiração para a criação da Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil. O projeto de lei foi inicialmente apresentado como o PLC 53/2018 e foi sancionado em agosto de 2018, tornando-se a Lei nº 13.709/2018. A LGPD entrou em vigor em setembro de 2020, após algumas prorrogações devido à pandemia de COVID-19, e trouxe uma série de inovações, incluindo a definição de dados pessoais e dados sensíveis, a criação de bases legais para o tratamento de dados, o estabelecimento de direitos para os titulares de dados e a imposição de responsabilidades às empresas e organizações que tratam dados pessoais.

O processo de formulação da LGPD foi marcado pela colaboração entre diferentes setores da sociedade, incluindo especialistas, empresas, organizações civis e órgãos governamentais. Tal diversidade de vozes foi essencial na construção de um texto legal que, além de estabelecer a proteção dos dados como um direito fundamental, trouxe mecanismos de aplicação flexíveis, como a Autoridade Nacional de Proteção de Dados (ANPD). A criação dessa autoridade reguladora é um ponto de destaque na evolução da legislação brasileira, pois proporciona um acompanhamento técnico contínuo e a adaptação da LGPD às rápidas mudanças tecnológicas e sociais.

Elaborada com base em princípios fundamentais de proteção de dados pessoais (Doneda, 2021), garantindo o respeito à privacidade e aos direitos dos titulares de dados, a lei se baseia em diversos fundamentos, que podem ser destacados da seguinte maneira:

a) Respeito à Privacidade

O primeiro fundamento da LGPD é o respeito à privacidade do indivíduo. A proteção de dados é vista como uma extensão do direito à privacidade, consagrado no artigo 5º, inciso X, da Constituição Federal de 1988, que garante a inviolabilidade da intimidade e da vida privada. A LGPD reforça esse direito ao estabelecer que os dados pessoais não podem ser utilizados sem o consentimento do titular, salvo em exceções previstas na própria lei.

b) Autodeterminação Informativa

Um dos conceitos centrais da LGPD é o direito à autodeterminação informativa, que garante ao titular dos dados o controle sobre o uso de suas informações pessoais. Esse princípio, que também está presente no GDPR, permite que o titular tenha o poder de decisão sobre quais dados podem ser coletados, como serão utilizados e por quanto tempo serão armazenados.

d) Publicidade e Transparência

O princípio da publicidade e transparência é central para garantir que os titulares dos dados saibam como suas informações estão sendo tratadas. Segundo Doneda (2021), a transparência não se refere apenas ao direito de saber que os dados estão sendo processados, mas também à clareza e acessibilidade das informações fornecidas pelas organizações. Isso significa que as entidades que tratam dados pessoais (controladores) devem informar de maneira clara, precisa e acessível como os dados são coletados, armazenados, utilizados, compartilhados e protegidos.

e) Finalidade

O princípio da finalidade estabelece que os dados pessoais devem ser coletados e tratados para propósitos legítimos, específicos, explícitos e informados ao titular. Esse princípio proíbe o tratamento de dados para finalidades não previamente comunicadas ou incompatíveis com aquelas que motivaram a coleta inicial.

f) Livre Acesso

O princípio do livre acesso assegura ao titular o direito de consultar de forma gratuita e facilitada todas as informações relacionadas ao tratamento de seus dados. Doneda (2021) destaca que esse princípio é fundamental para que o titular tenha uma visão completa e contínua de como suas informações estão sendo tratadas, incluindo os dados que foram coletados, as finalidades para as quais estão sendo utilizados e a duração do tratamento. O livre acesso é um componente indispensável da autodeterminação informativa, pois permite que o titular exerça um controle efetivo sobre seus dados. Isso é especialmente importante para garantir a transparência e a responsabilização das organizações no tratamento de dados.

g) Segurança Física e Lógica

O princípio da segurança diz respeito à adoção de medidas técnicas e administrativas para proteger os dados pessoais de acessos não autorizados, situações acidentais ou ilícitas, destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. Esse princípio abrange tanto a segurança física (proteção de locais e sistemas onde os dados são armazenados) quanto a segurança lógica (proteção dos sistemas de tecnologia da informação).

h) Liberdade e Autonomia

A liberdade e a autonomia do titular são outros fundamentos cruciais da LGPD. A lei visa proteger os indivíduos de práticas abusivas de tratamento de dados, que possam restringir suas escolhas ou gerar discriminações. Nesse sentido, a LGPD não apenas garante o consentimento informado, mas também estabelece limites para o uso de dados em situações de vulnerabilidade.

i) Desenvolvimento Econômico e Inovação

A LGPD também reconhece o papel fundamental dos dados pessoais no desenvolvimento econômico e na inovação tecnológica. O tratamento adequado dos dados pessoais é visto como uma maneira de fomentar o crescimento econômico, promovendo um ambiente de confiança entre empresas e consumidores. Ao mesmo tempo, a lei impõe normas que evitam o uso abusivo dos dados e garantem a competitividade das empresas brasileiras no mercado global

j) Direitos Humanos e Dignidade da Pessoa Humana

Outro fundamento essencial da LGPD é a proteção dos direitos humanos e a garantia da dignidade da pessoa humana. A LGPD foi concebida para evitar abusos no tratamento de dados que possam violar os direitos fundamentais, como o direito à liberdade, à privacidade, à igualdade e à não discriminação.

A estrutura da lei foi desenhada para abordar os diversos aspectos relacionados à coleta, uso, armazenamento e compartilhamento de dados pessoais, oferecendo um arcabouço para a proteção dos direitos fundamentais. Composta por dez capítulos que delineiam os princípios, direitos, obrigações e sanções relacionados ao tratamento de dados pessoais no Brasil, desempenha um papel fundamental na proteção da privacidade.

Os capítulos iniciais da LGPD estabelecem os princípios que orientam toda a legislação, incluindo a finalidade, adequação, necessidade, transparência e segurança. Esses princípios são fundamentais para garantir que o tratamento de dados pessoais seja realizado de forma ética e transparente, com o propósito claro e em conformidade com a lei. Ao exigir que os dados sejam coletados e tratados apenas para finalidades específicas e legítimas, a lei protege a privacidade, evitando a coleta excessiva ou inadequada de informações.

Um dos aspectos centrais da LGPD é a concessão de direitos específicos aos titulares dos dados. O Capítulo III detalha esses direitos, como o acesso, correção, exclusão, portabilidade e revogação do consentimento. Esses direitos são instrumentos fundamentais para que os cidadãos possam exercer controle sobre seus dados pessoais, permitindo-lhes gerenciar como suas informações são utilizadas e garantindo a possibilidade de corrigir ou excluir dados inapropriados. Ao fornecer esses mecanismos de controle, a LGPD fortalece a privacidade dos titulares, assegurando que suas informações pessoais sejam tratadas de acordo com suas expectativas e direitos.

O Capítulo IV define as responsabilidades dos controladores e operadores de dados, estabelecendo obrigações claras para garantir a conformidade com a LGPD. A introdução da figura do encarregado (*Data Protection Officer - DPO*) é uma medida importante para assegurar que as organizações mantenham um alto padrão de proteção de dados. O encarregado atua como um ponto de contato entre o titular dos dados, a organização e a Autoridade Nacional de Proteção de Dados (ANPD), facilitando a comunicação e a resolução de questões relacionadas à privacidade. Essa estrutura de responsabilidades reforça a necessidade de uma governança adequada em torno da proteção de dados pessoais, essencial para a preservação da privacidade.

A LGPD dedica um capítulo inteiro à segurança dos dados pessoais, exigindo que os agentes de tratamento adotem medidas técnicas e administrativas para proteger as informações contra acessos não autorizados e outros riscos. A segurança é um componente crítico para a proteção da privacidade, pois violações de dados podem expor informações sensíveis e causar danos irreparáveis aos cidadãos. Além disso, a promoção de boas práticas e a criação de programas de governança em privacidade, conforme incentivado pela LGPD, ajudam as organizações a manterem um ambiente seguro e em conformidade com os princípios da lei.

Os capítulos que tratam da fiscalização e das sanções são essenciais para garantir que as disposições da LGPD sejam efetivamente aplicadas. A Autoridade Nacional de Proteção de Dados (ANPD) desempenha um papel central na supervisão do cumprimento da lei, podendo aplicar sanções que variam de advertências a multas significativas. A existência de sanções rigorosas é fundamental para dissuadir práticas inadequadas de tratamento de dados e para assegurar que as organizações levem a sério a proteção da privacidade. A fiscalização eficaz por parte da ANPD é, portanto, uma garantia de que os direitos dos titulares devem ser protegidos e que as organizações serão responsabilizadas por qualquer violação à LGPD.

Assim como a LAI, um dos princípios fundamentais da LGPD é a transparência, que exige que os órgãos públicos informem claramente aos titulares sobre como seus dados serão utilizados. A administração pública deve assegurar que os titulares tenham acesso a informações sobre as finalidades do tratamento, as bases legais, os compartilhamentos realizados e as medidas de segurança adotadas. Além disso, a LGPD, assim como a LAI, permite que os cidadãos tenham acesso aos seus dados, sempre que solicitados.

Em relação à divulgação dos dados a terceiros, no contexto da transparência, a LGPD permite a divulgação de dados pessoais pela administração pública em situações em que a publicidade seja necessária para garantir a transparência das atividades governamentais. No entanto, essa divulgação deve ser limitada aos dados estritamente necessários para o cumprimento de suas funções, respeitando a privacidade dos cidadãos e evitando a exposição ilegal e desnecessária de informações pessoais.

Para entender este princípio, é importante analisar o conceito de dados pessoais. Doneda (2021) aborda o conceito de dados pessoais com uma visão que combina a análise técnica e jurídica com uma perspectiva voltada para a proteção dos direitos fundamentais da pessoa humana. Ele define dados pessoais como qualquer informação que possa, direta ou indiretamente, identificar uma pessoa física. Essa definição alinha-se com a concepção adotada

pela Lei Geral de Proteção de Dados Pessoais (LGPD), em que dados pessoais são definidos como "informação relacionada a pessoa natural identificada ou identificável".

A definição de dados pessoais vai além da simples identificação direta, como nome ou número de identificação. Ela também inclui informações que, quando combinadas com outros dados, podem levar à identificação de uma pessoa. Esse entendimento é crucial no contexto moderno, em que grandes volumes de dados são coletados e processados, muitas vezes permitindo a identificação do cidadão a partir de padrões de comportamento, dados de localização, entre outros. Além disso, Doneda (2021) enfatiza a importância de considerar o contexto no qual os dados são utilizados. Ele argumenta que a identificação de uma pessoa depende não apenas dos dados em si, mas também das tecnologias e dos métodos disponíveis para processá-los. Dessa forma, o conceito de dados pessoais é dinâmico e pode evoluir conforme novas tecnologias e práticas de tratamento de dados se desenvolvem.

Um exemplo prático que ilustra a visão de Doneda sobre a identificação de uma pessoa depender não apenas dos dados em si, mas também das tecnologias e dos métodos disponíveis para processá-los, pode ser encontrado no uso de dados de localização coletados por dispositivos móveis.

Imagine que uma empresa colete dados de localização de usuários de smartphones em uma cidade grande, sem coletar diretamente informações como nome, número de telefone ou endereço. Isoladamente, os dados de localização podem não parecer suficientes para identificar uma pessoa específica. No entanto, com o uso de tecnologias avançadas de análise de dados e métodos de cruzamento de informações, é possível identificar padrões de comportamento que revelem a identidade do cidadão: se os dados de localização mostram que um dispositivo móvel frequenta um determinado endereço residencial todas as noites e se move para o mesmo local de trabalho todos os dias etc. Esses padrões podem ser cruzados com informações disponíveis publicamente, como registros de propriedade ou dados de redes sociais. A combinação dessas informações pode permitir que a empresa identifique o titular dos dados, mesmo sem ter coletado diretamente seu nome ou outras informações de identificação tradicional.

Esse exemplo demonstra a importância da abordagem de Doneda, que considera o contexto tecnológico e metodológico na definição de dados pessoais. O avanço das tecnologias de análise de dados permite que informações que, à primeira vista, não pareçam identificáveis, possam, na prática, levar à identificação de cidadãos. Assim, a proteção dos dados pessoais deve levar em conta não apenas os dados brutos, mas também a capacidade das tecnologias de extraírem informações que possam comprometer a privacidade.

Nesse contexto, importante diferenciar o acesso de cidadãos aos seus próprios dados, o que, na lei, é sempre permitido, e o acesso a dados pessoais de cidadãos por terceiros. Neste último caso, importante destacar os dispositivos legais que delimitam este acesso, considerando o direito à privacidade e o conceito de dados pessoais.

Embora o consentimento seja uma das principais bases legais para o tratamento e divulgação de dados pessoais, e talvez o mais importante, a LGPD estabelece outras bases legais que permitem o tratamento, incluindo a divulgação, sem a necessidade de obter o consentimento do titular. As principais situações em que isso é permitido incluem:

a) Cumprimento de Obrigação Legal ou Regulatória

Se a divulgação dos dados pessoais for necessária para o cumprimento de uma obrigação imposta por lei ou regulamento, a empresa ou entidade pode compartilhar esses dados com terceiros sem o consentimento do titular. Isso se aplica, por exemplo, ao compartilhamento de dados com órgãos governamentais para fins de fiscalização, tributação, ou cumprimento de ordens judiciais.

b) Execução de Políticas Públicas

A administração pública pode compartilhar dados pessoais com terceiros sem o consentimento do titular quando esse compartilhamento for necessário para a execução de políticas públicas previstas em leis, regulamentos ou em convênios, contratos e similares. Nesse caso, o tratamento deve sempre respeitar o interesse público e os princípios da necessidade e da minimização dos dados.

c) Estudos realizados por Órgão de Pesquisa

Os dados pessoais podem ser divulgados a terceiros sem consentimento quando forem utilizados para a realização de estudos por órgãos de pesquisa, desde que garantida, sempre que possível, a anonimização dos dados pessoais (ou seja, a retirada de elementos que permitam a identificação direta ou indireta dos titulares).

d) Execução de Contrato

Quando a divulgação dos dados for necessária para a execução de um contrato no qual o titular dos dados é parte, ou para procedimentos preliminares relacionados ao contrato, não é necessário obter o consentimento do titular. Isso é comum em situações em que uma empresa precisa compartilhar dados com fornecedores ou prestadores de serviço para cumprir obrigações contratuais.

e) Exercício Regular de Direitos em Processos Judiciais, Administrativos ou Arbitrais

A LGPD permite a divulgação de dados pessoais sem consentimento quando for necessário para o exercício regular de direitos em processos judiciais, administrativos ou arbitrais. Por exemplo, uma empresa pode compartilhar dados com advogados ou tribunais para a defesa de seus interesses legais.

f) Proteção da Vida ou da Incolumidade Física do Titular ou de Terceiros

Em emergências, em que a divulgação dos dados seja necessária para proteger a vida ou a incolumidade física do titular dos dados ou de terceiros, a LGPD permite o compartilhamento sem a necessidade de consentimento.

g) Tutela da Saúde

A divulgação dos dados pessoais é permitida sem consentimento em procedimentos realizados por profissionais de saúde, serviços de saúde ou autoridades sanitárias, desde que estejam atuando para garantir a saúde pública, como no caso de emergências sanitárias.

h) Legítimo Interesse

A LGPD também permite a divulgação de dados pessoais com base no legítimo interesse do controlador ou de terceiros, desde que esse interesse seja legítimo e que os direitos e liberdades fundamentais do titular não prevaleçam. Nesses casos, é necessário realizar uma avaliação cuidadosa para garantir que a divulgação seja justificável e proporcional.

Importante destacar que a tutela dos dados pessoais é orientada por uma série de fundamentos que legitimam o tratamento de dados, sendo o consentimento um dos mais

importantes. Embora não seja o único, o consentimento é frequentemente visto como a forma mais direta de manifestação da vontade do titular, conferindo a ele um controle explícito sobre o uso de suas informações.

O consentimento na LGPD é definido como a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados para uma finalidade específica. Essa definição carrega uma natureza contratual e voluntária, pois envolve o exercício da vontade do titular em autorizar ou não o uso de suas informações. No entanto, o consentimento não é meramente um acordo formal; ele deve ser obtido de forma transparente e em condições que garantam a liberdade de escolha do titular.

A natureza jurídica do consentimento é dupla: ele é, ao mesmo tempo, um ato de manifestação de vontade e um instrumento de legitimidade para o tratamento de dados. Como ato jurídico, o consentimento é submetido aos requisitos de validade e pode ser contestado se não for obtido de acordo com os princípios estabelecidos pela LGPD, como a clareza das informações e a ausência de coerção. Além disso, o consentimento não deve ser tratado como um “cheque em branco”. Ele deve ser específico quanto às finalidades para as quais os dados serão usados e limitado a essas finalidades, respeitando o princípio da necessidade. Assim, o consentimento deve ser obtido para usos determinados, e qualquer mudança nas finalidades ou condições de tratamento deve ser informada ao titular, que pode, então, decidir sobre seu aceite ou recusa.

Um dos aspectos centrais da funcionalidade do consentimento na LGPD é sua revogabilidade. O titular dos dados tem o direito de, a qualquer momento, revogar o consentimento dado anteriormente para o tratamento de seus dados. A revogação do consentimento deve ser um processo tão simples quanto o ato de fornecê-lo, e não pode ser submetida a obstáculos ou complicações que dificultem o exercício desse direito.

A revogabilidade está relacionada à autodeterminação informativa, um conceito amplamente defendido por Doneda (2021), que sugere que o titular deve ter o controle contínuo sobre o uso de suas informações pessoais. Esse controle envolve a possibilidade de mudar de ideia sobre o uso de seus dados, conforme as circunstâncias ou as suas preferências. Entretanto, a revogação do consentimento não invalida os tratamentos realizados anteriormente com base no consentimento dado de forma válida e legítima. Na prática, a revogabilidade exige que as organizações estejam preparadas para cessar o tratamento de dados quando o consentimento for retirado, exceto em casos em que existam outros fundamentos legais para continuar o

processamento. A LGPD prevê que, mesmo após a revogação, os dados tratados anteriormente não podem ser utilizados de forma incompatível com os direitos do titular.

Nesse sentido, destaca-se a funcionalização do consentimento que, na LGPD, refere-se ao papel pragmático que ele desempenha na regulação do tratamento de dados pessoais. Não é apenas uma formalidade, mas um mecanismo que confere ao titular poder sobre o tratamento de seus dados. Deve ser informado, ou seja, o titular deve compreender as implicações do tratamento de seus dados e as finalidades específicas envolvidas, e deve ser transparente, sem ambiguidades ou práticas enganosas.

A funcionalização também implica que o consentimento deve ser adequado à realidade do tratamento de dados. A lei prevê que, em certos casos, como no tratamento de dados sensíveis ou de crianças, o consentimento deve ser reforçado com requisitos adicionais, como a autorização dos pais ou responsáveis no caso de menores de idade. Isso demonstra que o consentimento, como mecanismo de tutela dos dados pessoais, deve ser moldado às circunstâncias específicas, garantindo a proteção proporcional ao risco do tratamento. Contudo, embora o consentimento seja uma base legítima para o tratamento de dados, ele não deve ser o único fundamento utilizado para justificar o processamento de informações pessoais. Em situações em que o consentimento possa ser ineficaz ou impraticável, outros fundamentos legais podem ser aplicados, como a execução de contrato ou o cumprimento de obrigação legal, sempre observando os direitos dos titulares.

No campo dos direitos humanos, observa-se, do exposto, que a lei geral de proteção de dados pessoais no Brasil introduz um novo paradigma regulatório que transcende a mera proteção de dados. Para Doneda (2021), a proteção de dados está diretamente relacionada à privacidade, que, por sua vez, está relacionada à honra e aos valores do homem em cada sociedade e, dentro de cada uma, aos diversos grupos sociais.

A necessidade de se criar uma normativa legal que proteja os dados é, na verdade, a necessidade de se buscar um conteúdo comum para o direito à privacidade que satisfaça a diversas sociedades em função da evolução tecnológica e do fluxo de informações nos últimos anos. Interessante notar que a evolução das legislações, mencionada de maneira resumida neste texto, permite estabelecer alguns critérios para a evolução do próprio conceito de privacidade, que certamente não representa o viés patrimonialista do direito de propriedade, mas vai muito além disso. Também não se trata da questão de “não ter nada a esconder”, ideia equivocada de transparência de quem não tem nada a perder, que, na verdade, é uma forma de controle social

que anula a individualidade, cerceia a autonomia privada e inviabiliza o livre desenvolvimento da personalidade humana.

No contexto atual, as leis de proteção de dados devem refletir o conceito de privacidade com posição de destaque da proteção humana, mas não somente como escudo contra o Estado, mas como elemento indutor da autonomia, da cidadania e da própria atividade política em sentido amplo e dos direitos da liberdade (Doneda, 2021).

CAPÍTULO 2

A LGPD PODE IMPEDIR O ACESSO À INFORMAÇÃO? ANÁLISE DO TRATAMENTO DE DADOS PESSOAIS E A POLÍTICA PÚBLICA DE TRANSPARÊNCIA

A Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação (LAI) tratam de temas que podem parecer contraditórios, o que tem gerado controvérsias quanto à sua aplicação conjunta. A LGPD foca na proteção dos dados pessoais, garantindo que as informações individuais sejam tratadas com cuidado e segurança, enquanto a LAI visa garantir o acesso a informações públicas, promovendo transparência e controle social.

As principais controvérsias surgem nos seguintes pontos: a LAI promove o direito de acesso a informações públicas, o que muitas vezes incluem dados pessoais. No entanto, a LGPD impõe restrições ao tratamento de dados pessoais, especialmente quando afeta a privacidade; a LGPD categoriza certos dados como "sensíveis", o que exige um tratamento ainda mais rigoroso.

Quando essas informações são requeridas sob a LAI, pode haver dúvidas sobre o que pode ou não ser divulgado, já que a necessidade de proteção é mais elevada. A LGPD permite o tratamento de dados pessoais para o cumprimento de obrigações legais, mas há discussões sobre até que ponto a divulgação de dados pessoais pela LAI pode ser justificada pelo "interesse público" sem infringir a proteção de dados. Há dificuldade em definir claramente os limites entre esses interesses; a LGPD exige uma base legal clara para o tratamento de dados pessoais, como o consentimento do titular ou o cumprimento de obrigação legal. Na aplicação da LAI, o fornecimento de informações, especialmente dados pessoais, pode ser feito sem consentimento, o que levanta questões sobre a compatibilidade entre as legislações.

Para equilibrar os direitos, uma solução frequentemente adotada é a anonimização dos dados, permitindo que informações sejam divulgadas sem expor diretamente os cidadãos. No entanto, a implementação eficaz dessa medida é complexa e ainda gera debates sobre sua real eficácia.

Essas controvérsias refletem a dificuldade de equilibrar a necessidade de transparência e o direito à privacidade, ambos fundamentais em um Estado democrático. A interpretação dessas normas em casos concretos é o que vem trazendo desafios para sua aplicação harmônica.

O desafio está em conciliar esses direitos: como divulgar informações de interesse público sem violar a privacidade? Este, portanto, é o problema jurídico a ser analisado neste capítulo.

2.1 A Aparente Oposição entre a LAI e a LGPD: Uma análise sob a Perspectiva da Hermenêutica Jurídica

A LAI foi criada com o objetivo de promover a transparência governamental, assegurando o direito dos cidadãos de solicitarem informações relativas às atividades do Estado. Por outro lado, a Lei Geral de Proteção de Dados (LGPD), promulgada em 2018, veio para regulamentar o tratamento de dados pessoais no Brasil, tanto no setor público quanto no privado, estabelecendo princípios e regras para a proteção da privacidade.

O principal ponto de aparente oposição entre a LAI e a LGPD surge quando um pedido de acesso à informação pública envolve dados pessoais, como, por exemplo, solicitações sobre salários de servidores públicos ou contratos de licitação que incluem informações sobre empresas e seus representantes. Nesses casos, a LAI defende o interesse público na divulgação dessas informações, enquanto a LGPD defende a privacidade dos envolvidos.

Importante destacar que quando se solicitam informações sobre salários ou benefícios de servidores públicos, esses dados são, ao mesmo tempo, informações de interesse público, mas também dados pessoais protegidos pela LGPD. No caso de divulgação de informações sobre contratos e licitações públicas, a LAI defende que esses dados devem ser amplamente acessíveis à população, pois envolvem o uso de recursos públicos. No entanto, a LGPD protege os dados pessoais de cidadãos e empresas envolvidas nesses processos, exigindo que informações como endereços, números de documentos e outros dados sensíveis sejam resguardados. O que fazer, então, nesses casos?

A solução para esse aparente conflito está, muitas vezes, na interpretação cuidadosa de ambas as leis, visando à harmonização de seus objetivos. A própria LGPD, em seu artigo 7º, inciso II, prevê que o tratamento de dados pessoais é permitido quando necessário para o cumprimento de obrigações legais ou regulatórias, o que inclui o dever de transparência previsto na LAI. Dessa forma, a divulgação de informações públicas que incluam dados pessoais pode ser feita desde que se observe o princípio da minimização de dados, ou seja, divulgando-se apenas o estritamente necessário para atender ao interesse público.

Embora a aparente oposição entre a LAI e a LGPD possa gerar incertezas na aplicação das duas normas, existe um consenso de que elas podem e devem ser aplicadas de maneira

complementar. O desafio está em encontrar o equilíbrio entre a transparência e a proteção da privacidade, o que requer uma interpretação criteriosa dos casos concretos e a adoção de medidas que protejam os dados pessoais sem comprometer o direito de acesso à informação.

Um dos mecanismos que pode ser utilizado para resolver esses conflitos é a anonimização dos dados pessoais, que consiste em remover ou alterar dados que possam identificar diretamente a pessoa, preservando assim sua privacidade. Dessa forma, é possível atender aos pedidos de acesso à informação, divulgando dados de interesse público sem comprometer a privacidade dos envolvidos. Além disso, a transparência ativa prevista na LAI pode ser utilizada como uma estratégia para minimizar os conflitos com a LGPD. A transparência ativa envolve a divulgação proativa de informações por parte dos órgãos públicos, sem que seja necessário um pedido formal por parte do cidadão. Nesses casos, é possível que os órgãos públicos divulguem informações de interesse público de forma generalizada, já adotando medidas para garantir a proteção de dados pessoais sensíveis.

Apesar dos mecanismos existentes para a harmonização entre a LAI e a LGPD, desafios permanecem. A falta de clareza em alguns aspectos da legislação e a interpretação variada por diferentes órgãos públicos são fatores que dificultam a aplicação uniforme das leis. Além disso, a resistência institucional em algumas esferas do governo e a falta de capacitação dos servidores públicos responsáveis pelo tratamento de dados também são entraves significativos.

Destaca-se que a doutrina jurídica oferece diversos entendimentos sobre a oposição entre normas, especialmente quando se trata de leis que aparentemente possuem objetivos conflitantes. A discussão sobre esse tema envolve princípios da hermenêutica jurídica, com técnicas de interpretação e a aplicação de normas com base em princípios como proporcionalidade, razoabilidade e hierarquia normativa.

A hermenêutica jurídica é fundamental para a compreensão e aplicação do direito. Originada da filosofia e da teoria da interpretação, ela se dedica ao estudo das técnicas e métodos de interpretação das normas jurídicas. Em um sistema legal, a hermenêutica jurídica visa oferecer um entendimento profundo e coerente das leis, promovendo uma aplicação que respeite o espírito e a letra das normas.

A palavra "hermenêutica" deriva do termo grego "hermeneuein", que significa "interpretar" ou "explicar". Portanto, a hermenêutica jurídica refere-se ao estudo e à prática da interpretação das normas jurídicas. Inicialmente desenvolvida na filosofia, a hermenêutica busca compreender textos e discursos em suas dimensões mais profundas. No direito,

concentra-se na interpretação das leis e regulamentos para garantir que sejam aplicadas de forma justa e eficaz.

Historicamente, a hermenêutica jurídica evoluiu a partir dos trabalhos de filósofos e teóricos da interpretação, como Friedrich Schleiermacher e Wilhelm Dilthey, que influenciaram a forma como os textos legais são analisados e compreendidos. Esses pensadores introduziram conceitos fundamentais que ainda são relevantes na interpretação jurídica contemporânea.

Para Dilthey (1944), a hermenêutica ocupa um lugar central na compreensão das chamadas ciências do espírito, como a história, a sociologia, a filosofia e a psicologia. Não se limita à interpretação de textos, como era tradicionalmente concebida, mas se amplia para abarcar a interpretação das manifestações sensíveis da vida humana e suas objetivações culturais. Ele propõe que o conhecimento das ciências do espírito difere radicalmente das ciências naturais, pois estas últimas buscam explicações causais e objetivas, enquanto as ciências do espírito buscam compreensão. Essa compreensão só é possível porque o ser humano, ao investigar fenômenos históricos e culturais, está lidando com expressões da vida humana — ou seja, com sentidos que têm origem na experiência subjetiva de outros seres humanos.

A hermenêutica, nesse contexto, é o método que permite ao estudioso reconstruir esses sentidos e entender a realidade do espírito humano em sua historicidade. Dilthey (1944) considera que a hermenêutica vai além da mera decodificação: ela permite que o intérprete reviva os processos históricos e espirituais que geraram as objetivações culturais. Por meio da interpretação, o estudioso do espírito não apenas observa o produto de uma criação (um livro, uma instituição, uma norma), mas vivencia o processo criativo que deu origem a esse mundo espiritual. Esse processo de recriação possibilita ao intérprete acessar o mundo histórico de uma forma profunda e relacional, colocando-se no lugar do outro, buscando entender as condições de vida e os valores que nortearam as ações humanas ao longo da história. Portanto, nesse sentido, a hermenêutica não é apenas um método técnico de interpretação de textos, mas um processo de compreensão humana fundamental para as ciências do espírito. Ela possibilita o acesso ao mundo subjetivo e cultural, permitindo que o estudioso viva o processo de criação espiritual em sua forma histórica.

Schleiermacher (1977) ampliou o escopo da hermenêutica, elevando-a de uma técnica restrita ao estudo de textos bíblicos ou jurídicos a uma teoria geral da interpretação aplicável a todas as formas de comunicação humana. Sua concepção da hermenêutica vai além das simples regras metodológicas, sendo uma reflexão filosófica mais abrangente sobre a compreensão e o

processo de interpretação. Ele propõe que todo ato de compreensão envolve uma interação entre duas esferas: a dimensão gramatical e a dimensão psicológica. A dimensão gramatical refere-se à interpretação do texto em seu contexto linguístico, ou seja, à análise das palavras, frases e estruturas linguísticas. No entanto, a compreensão plena de um texto não pode ser alcançada apenas pela análise da linguagem em si; é necessário entrar na dimensão psicológica, que envolve a tentativa de entender as intenções e o pensamento do autor por trás do texto. Sob este viés, a interpretação é um processo bidimensional: de um lado, a interpretação gramatical analisa o uso da linguagem comum, que serve como base para a comunicação; do outro, a interpretação psicológica busca reconstituir o contexto subjetivo do autor, levando em conta suas motivações, experiências e intenções ao produzir o texto. Essa abordagem exige que o intérprete se aproxime do estado mental do autor para captar os significados mais profundos e implícitos que podem estar presentes na obra.

Uma das principais inovações da hermenêutica de Schleiermacher é sua ideia de que a interpretação nunca é mecânica ou puramente objetiva. Pelo contrário, o processo de compreensão envolve uma forma de círculo hermenêutico, no qual o intérprete deve constantemente ir e vir entre o todo e as partes do texto para construir uma interpretação coerente. O intérprete, ao mesmo tempo que analisa as partes do texto (frases, palavras), deve considerar o texto como um todo, e vice-versa. Essa relação circular é fundamental porque permite que a compreensão se dê de forma progressiva, com o intérprete ajustando continuamente sua interpretação à medida que vai adquirindo maior familiaridade com o texto e com a perspectiva do autor.

A hermenêutica jurídica desempenha um papel crucial na aplicação do direito por várias razões. Ao aplicar métodos hermenêuticos, os intérpretes das normas podem alcançar uma compreensão clara e coerente das leis. Isso é fundamental para garantir que as decisões judiciais e administrativas sejam baseadas em interpretações consistentes e fundamentadas. Em casos de normas aparentes ou reais contradições, a hermenêutica jurídica ajuda a encontrar soluções que respeitem o equilíbrio entre diferentes normas e princípios. Essa capacidade de harmonizar normas conflitantes é essencial para a aplicação justa do direito.

Outro ponto a ser destacado é que a hermenêutica jurídica estabelece que quando há uma oposição aparente entre duas leis, a solução não deve ser imediata pela anulação de uma delas. Pelo contrário, a doutrina jurídica defende que normas conflitantes podem coexistir, desde que sejam interpretadas de maneira que se respeite ao máximo seus objetivos e fundamentos. Na presença de um aparente conflito entre duas normas, deve-se buscar uma

interpretação que permita a harmonização dessas normas. Isso significa encontrar um ponto de equilíbrio em que ambas possam ser aplicadas, ainda que com algumas restrições. No caso da Lei de Acesso à Informação (LAI) e da Lei Geral de Proteção de Dados (LGPD), esse princípio sugere que tanto a transparência quanto a privacidade devem ser preservadas, e que os casos de conflito devem ser analisados individualmente para determinar qual direito prevalece.

Nesse contexto, importante destacar a doutrina de Ingo Wolfgang Sarlet, especialmente no que se refere à proteção e à aplicação dos direitos fundamentais. Um dos temas centrais de sua obra é a questão da ponderação de normas e princípios nos casos concretos, que, segundo ele, é uma tarefa essencial, mas que requer critérios claros para assegurar a legitimidade e a efetividade do ordenamento jurídico.

Sarlet (2019) defende que a ponderação de leis e princípios deve ocorrer quando direitos fundamentais ou normas entram em aparente conflito em um caso concreto, sendo necessário buscar um equilíbrio que respeite as características e os limites de cada um. Segundo Sarlet, esse processo de ponderação não deve ser arbitrário ou pautado apenas pela intuição do intérprete, mas sim fundamentado em critérios objetivos e racionais que preservem a hierarquia e a harmonia do sistema jurídico.

O autor enfatiza que a ponderação exige uma análise cuidadosa das circunstâncias do caso concreto, levando em consideração elementos como a intensidade da restrição de cada direito, a proporcionalidade da medida adotada e o impacto prático da decisão. Ele afirma que os direitos fundamentais, embora sejam aplicáveis de maneira direta e imediata, não possuem caráter absoluto, devendo ser interpretados em conformidade com o princípio da unidade da Constituição. Argumenta, ainda, que a ponderação não deve ser vista como uma flexibilização desmedida das normas, mas como um instrumento para a concretização dos valores constitucionais em um sistema jurídico baseado na dignidade da pessoa humana. Para ele, o objetivo final da ponderação é garantir a máxima efetividade possível dos direitos fundamentais, mesmo em situações de tensão entre eles.

Um aspecto importante de sua posição é a ênfase na fundamentação da decisão judicial que resulta da ponderação. Ele defende que o julgador deve explicitar os critérios adotados, os valores priorizados e os motivos que levaram à decisão, de modo a assegurar a transparência e a legitimidade da atuação judicial. Assim, para Sarlet (2019), a ponderação é um mecanismo indispensável na aplicação do direito em casos concretos, desde que conduzida de forma rigorosa e orientada pelos princípios constitucionais. Essa abordagem busca alcançar um

equilíbrio justo e racional entre os direitos e as normas, promovendo a unidade e a coerência do sistema jurídico brasileiro.

Outro autor que merece destaque no que tange à ponderação das leis nos casos concretos é Gustavo Binembojm. Segundo Binenbojm (2014), a ponderação é uma técnica de interpretação que se torna imprescindível em situações em que há colisão entre normas ou princípios constitucionais, especialmente em um sistema jurídico como o brasileiro, que adota a Constituição como fundamento de validade de todo o ordenamento. Ele destaca que os princípios constitucionais possuem caráter normativo e aplicabilidade direta, mas sua natureza aberta e a pluralidade de valores protegidos pela Constituição frequentemente geram tensões. Nesse contexto, a ponderação se apresenta como um método para equilibrar os valores e interesses em conflito, buscando a máxima concretização dos direitos fundamentais.

O autor reconhece que a ponderação deve obedecer ao princípio da proporcionalidade, que é composta por três subprincípios: adequação, necessidade e proporcionalidade em sentido estrito. Esse último, em especial, requer que o intérprete avalie o peso relativo dos direitos ou normas em colisão, com base nas circunstâncias concretas do caso, e adote a solução que cause o menor sacrifício possível aos valores envolvidos. A ponderação, embora necessária, deve ser conduzida com rigor metodológico para evitar arbitrariedades e garantir a legitimidade das decisões judiciais. Ele ressalta que o processo decisório deve ser fundamentado em argumentos racionais, objetivos e transparentes, de modo que o julgador explicite as razões que levaram à prevalência de um princípio ou norma sobre outro. A fundamentação clara e detalhada é essencial para assegurar a previsibilidade e a confiança no sistema jurídico.

Além disso, Binenbojm (2014) destaca que a ponderação não é um processo de relativização indiscriminada dos direitos, mas sim um mecanismo para assegurar a máxima efetividade da Constituição. O objetivo da ponderação é realizar um diálogo entre os valores constitucionais, promovendo a concretização simultânea, na medida do possível, de direitos aparentemente conflitantes.

Diretamente relacionado à ponderação entre os princípios constitucionais está o princípio da proporcionalidade, que é usado para resolver conflitos entre normas constitucionais ou infraconstitucionais. Esse princípio envolve uma análise criteriosa, destacando-se as seguintes fases:

a) Adequação: Verifica-se se a aplicação de uma das normas é adequada para alcançar o objetivo visado, sem causar um prejuízo desnecessário à outra.

b) Necessidade: Avalia-se se a restrição de um direito (como a privacidade ou a transparência) é necessária para proteger o outro.

c) Proporcionalidade em sentido estrito: Ponderam-se os impactos da aplicação de uma norma sobre a outra, buscando um equilíbrio que respeite ao máximo ambos os direitos.

No caso da LAI e da LGPD, a doutrina sugere que a aparente oposição deve ser solucionada com base no princípio da proporcionalidade, de forma que se considere o interesse público em divulgar informações e, ao mesmo tempo, se proteja a privacidade dos dados pessoais. Esse princípio leva em conta o interesse público envolvido, como no caso de informações sobre a gestão de recursos públicos, e pondera os riscos à privacidade.

Outro ponto importante é a oposição entre princípios constitucionais, como o princípio da publicidade, constante no art. 37 da Constituição Federal, e o direito à privacidade, tratado no art. 5º, inciso X. A publicidade rege a transparência dos atos da administração pública, enquanto a privacidade protege os direitos fundamentais. Esses princípios não são absolutos e podem ser relativizados dependendo do contexto. A aplicação de um princípio deve respeitar os limites impostos por outros direitos fundamentais. Assim, a hermenêutica propõe que esses princípios sejam aplicados de maneira proporcional e ponderada, conforme as circunstâncias de cada caso.

A doutrina jurídica também analisa conflitos de normas com base na hierarquia normativa. Quando uma lei infraconstitucional, como a LAI ou a LGPD, parece colidir com outra, a doutrina propõe que o julgador avalie as normas à luz da Constituição Federal. A Constituição estabelece a supremacia dos direitos fundamentais, e os julgadores devem aplicar as leis de maneira que esses direitos sejam respeitados.

Nesse contexto, o Supremo Tribunal Federal (STF) tem o papel de guardião da Constituição e frequentemente é chamado para resolver tais conflitos. Em decisões recentes, o STF tem reiterado a importância da ponderação entre a publicidade e a proteção de dados, entendendo que a privacidade, ainda que fundamental, pode ceder em face de um interesse público preponderante.

Em muitos casos, a solução para os conflitos aparentes entre leis pode ser encontrada não apenas na interpretação judicial, mas também na atuação de órgãos fiscalizadores e reguladores. No caso da LAI e da LGPD, a Controladoria-Geral da União (CGU) e a Autoridade Nacional de Proteção de Dados (ANPD) desempenham um papel essencial na resolução de conflitos práticos entre as duas leis. A CGU, responsável pela aplicação da LAI, e a ANPD, criada para regulamentar a LGPD, trabalham na formulação de diretrizes e orientações que ajudam a mitigar conflitos e orientar a aplicação das normas. Esses órgãos devem atuar de maneira coordenada para garantir que os direitos de acesso à informação e à privacidade sejam aplicados de forma equilibrada.

Logo, a aparente oposição entre leis não é algo intransponível, mas sim como um desafio interpretativo a ser solucionado por meio de princípios da hermenêutica, como a proporcionalidade, razoabilidade e harmonização. No caso da LAI e da LGPD, a doutrina aponta que o aparente conflito entre transparência e privacidade pode ser gerido por meio de uma interpretação que respeite o contexto de cada situação, equilibrando a necessidade de divulgação de informações com a proteção dos dados pessoais.

Importante destacar que diante de um caso de acesso à informação, a decisão do gestor é um processo que envolve a seguinte pergunta: a informação requerida contém dados pessoais identificados ou identificáveis? Se sim, devem-se analisar leis, decisões administrativas, judiciais e enunciados da CGU que determinam a divulgação e divulgar conforme o que está determinado.

Por outro lado, se a informação solicitada contém dados pessoais de pessoas identificadas ou identificáveis e não há leis, decisões judiciais, administrativas nem enunciados da CGU que determinem a divulgação da informação, o que o gestor deve fazer?

Em primeiro lugar, à luz da hermenêutica jurídica, deve-se analisar os riscos e benefícios da transparência desses dados. Há perguntas que podem ajudar nessa análise, como por exemplo: esta informação possibilitará a transparência pública e benefício coletivo, sem afetar a privacidade das pessoas? O acesso aos dados gerará conhecimento para a sociedade e participação nas decisões políticas, e não gerará risco à segurança do Estado ou do cidadão? A divulgação dos dados proporcionará a efetivação de políticas públicas, sem causar constrangimento a uma ou mais pessoas? Essas perguntas certamente ajudarão o gestor a entender se pode ou não divulgar a informação e, neste caso, quando o benefício de divulgar os

dados se sobrepor ao risco de sua divulgação, pois esta não afetará a segurança do Estado ou de um cidadão, nem afetará a sua privacidade, o acesso aos dados deve ser deferido.[16]

Vejamos um exemplo da análise de um caso específico, como a divulgação da carteira de vacinação de uma autoridade pública. Considerando que este documento contém dados pessoais, necessário avaliar se a divulgação, neste caso, é permitida. A legislação em vigor determina que as informações sobre a saúde de uma pessoa não devem ser divulgadas. Sendo assim, a divulgação da carteira de vacinação de uma autoridade pública é proibida?

Importante destacar que a lei não trata especificamente da carteira de vacinação, no entanto, a interpretação restrita de que este documento contém dados pessoais pode levar o gestor a indeferir o acesso ao documento. Neste caso, faz-se necessário analisar os impactos que essa divulgação proporciona.

De acordo com o relatório do Transparência Brasil[17], em uma situação normal, o impacto positivo da divulgação seria baixo, porém, em um contexto mais crítico, como o de uma pandemia, a informação proporcionará múltiplas utilidades, pois representará para a população a importância de se vacinar, especialmente se o exemplo dado é de uma autoridade pública, cuja atribuição é, também, promover políticas de acesso à saúde e vacinação.

Por outro lado, qual o risco de se divulgar a carteira de vacinação de uma autoridade pública? Esta divulgação pode gerar constrangimento, caso a autoridade não tenha tomado as vacinas indicadas, por exemplo. E isso pode afetar a intimidade e privacidade da pessoa.

O que fazer neste caso? Parece estarmos diante de um possível conflito entre o direito de acesso à informação e a proteção de dados pessoais sensíveis. Convém, portanto, recorrer à hermenêutica jurídica, e à luz do princípio da proporcionalidade, avaliar os benefícios e riscos na divulgação desses dados.

Ora, em um contexto normal, sem pandemia, por exemplo, o benefício da divulgação não supera o risco de se divulgar um dado pessoal sensível, contudo, em um contexto de emergência em saúde púbica, a carteira de vacinação pode ser divulgada, com limitações, ou seja, somente as informações do período em que a pessoa esteve na gestão de um cargo público,

[16] O Guia LAI e LGPD: Como Equilibrar?, do Transparência Brasil, traz um conteúdo importante que se propõe a ajudar servidores da Administração Pública na decisão sobre divulgar ou não informações pessoais produzidas e armazenadas pelo Pode Público.

[17] Para mais detalhes, veja o link https://www.transparencia.org.br/downloads/publicacoes/guialailgpdcomoequilibrar.pdf?utm_source=blogtb&utm_medium=link&utm_campaign=lai-lgpd

pois o benefício da divulgação seria alto, sem violar outros dados pessoais sensíveis constantes no documento.

Um outro exemplo apresentado pelo relatório do Transparência Brasil é o caso prático de não divulgação dos dados, como o que ocorre em decisão do judiciário pela compra de um medicamento para um paciente específico, em que se solicitam as informações sobre o procedimento de compra deste medicamento. Importante destacar que na compra de um medicamento pela Administração Pública, os documentos incluem a identificação e o diagnóstico da pessoa que vai receber o remédio. Portanto, divulgar o processo de compra, seja por dispensa de licitação ou outro ato administrativo, implica em divulgar os dados do paciente, gerando constrangimento e nenhum benefício à sociedade. Logo, deve-se perguntar qual é o benefício de se divulga a identificação e o diagnóstico do paciente?

Neste caso específico, o impacto positivo é baixo e o risco é alto. A decisão, portanto, envolve esta análise e o balanço benefício e risco, à luz dos princípios da razoabilidade e proporcionalidade. Assim, na divulgação do gasto público com o medicamento, devem ser anonimizados os dados pessoais sensíveis.

A partir desses casos, pode-se concluir a importância da hermenêutica jurídica no tocante às decisões que envolvem política pública de transparência e tratamento de dados pessoais. Essa análise não é tão simples quanto parece para alguns que, de forma equivocada, indeferem todos os pedidos que contêm dados pessoais sensíveis, gerando um problema que envolve um suposto conflito de leis. Por isso, a interpretação da lei, o conhecimento das decisões judiciais e administrativas, bem como a análise do caso concreto à luz dos princípios constitucionais e avaliação dos riscos e benefícios, concederão ao gestor público diretrizes e fundamentos para a decisão mais adequada.

2.2. Impactos da LGPD na Transparência Governamental: Análise das Restrições Impostas no Contexto da LAI

A Lei de Acesso à Informação entrou em vigor há mais de uma década e, nessa época, não havia uma lei de tratamento de dados pessoais, bem como não havia na legislação brasileira uma definição clara sobre dados pessoais. A LAI trouxe essa definição em seu artigo 31 ao afirmar que as informações pessoais são aquelas relativas à intimidade, vida privada, honra e

imagem e, portanto, o tratamento dessas informações deve ser feito de forma transparente e com respeito a honra e imagem das pessoas, bem como às liberdades e garantias fundamentais.

A Lei Geral de Proteção de Dados, que entrou em vigor em 2020, veio para apresentar uma definição mais detalhada sobre a definição de dado pessoal, dado pessoal sensível e dado anonimizado, além de definir, no seu artigo 7º, os requisitos para o tratamento de dados pessoais. Doneda (2021) afirma que a LGPD é um complemento à LAI no que tange à expansão da definição do que é um dado pessoal. Isso é, portanto, um impedimento àqueles que tentam colocar informação pública na categoria de sigilo.

Contudo, na prática, o que tem ocorrido é o inverso: gestores públicos, sob o argumento de a informação conter dados pessoais, nos termos da LGPD, restringem o acesso à informação pública. Este é um dos principais desafios para a Administração Pública: a negativa de acesso a dados púbicos quando envolvem dados pessoais.

Um exemplo prático dessa negativa, ocorrida em 2020, mostra um cidadão que solicitou, com base na LAI, a lista completa de servidores públicos federais e seus respectivos salários. O governo federal, em resposta, limitou a divulgação de informações detalhadas, alegando que a divulgação de certos dados seria uma violação da privacidade dos servidores, conforme estabelecido pela LGPD. A controvérsia foi levada à Justiça, que acabou por determinar que, em nome do princípio da transparência pública, o salário dos servidores deveria ser divulgado, uma vez que o uso de recursos públicos justifica o interesse coletivo. No entanto, o caso ilustra o embate entre o direito de acesso à informação e a proteção da privacidade prevista na LGPD, que impôs restrições à divulgação de outros dados pessoais, como CPF e endereço.[18]

Embora a lei permita a divulgação de dados públicos com a devida proteção da privacidade, a administração pública tem, em alguns casos, interpretado a LGPD de forma a restringir o acesso a esses dados. Isso ocorre especialmente em contextos em que a divulgação poderia incluir dados pessoais ou informações que, embora relevantes para a transparência, são classificadas como sensíveis.

Alguns órgãos públicos têm utilizado a Lei Geral de Proteção de Dados Pessoais para justificar a classificação de documentos administrativos como sigilosos, com base na proteção de dados pessoais. Por exemplo, dados sobre contratos administrativos que contenham informações pessoais podem ser classificados como sigilosos, mesmo quando a lei permite a

[18] Para saber mais detalhes sobre o caso, acesse o link https://fiquemsabendo.com.br/transparencia/lgpd-lai

divulgação com a devida anonimização. Gestores podem adotar uma interpretação excessivamente cautelosa da LGPD para proteger dados pessoais, levando à não divulgação de informações que poderiam ser divulgadas em formato anonimizado ou agregado. Essa abordagem cautelosa pode levar a uma redução na transparência sobre atividades governamentais. Informações detalhadas sobre gastos públicos e aquisições podem ser restringidas sob a alegação de proteção de dados pessoais, mesmo que a transparência sobre esses gastos seja crucial para a fiscalização e controle social.

A Controladoria-Geral da União (CGU), responsável por administrar o sistema de acesso à informação na Administração Pública, analisou alguns temas relacionados à utilização indevida da restrição de acesso a informações pessoais com fundamento na LGPD, bem como no Art. 31 da LAI.[19] Conclui-se que, em alguns casos o acesso à informação é negado com base em restrição aos dados pessoais e sigilosos.

Um caso a ser destacado é o pedido de acesso aos procedimentos administrativos disciplinares de agentes públicos, que muitas vezes é negado sob a alegação de conter dados pessoais (LGPD) e sensíveis; em alguns casos, o administrador público define como dados sigilosos, nos termos da LAI.

De acordo com a CGU, a negativa de acesso à informação aos processos deve ser adotada com cautela pois, o órgão de controle entende que os Processos Administrativos Disciplinares (PAD) que ainda estejam em curso, possuem acesso restrito a terceiros. Uma vez concluído o PAD, ou seja, com a edição de seu julgamento, deixa de subsistir a situação que justifica a negativa de acesso a seu conteúdo.

Contudo, convém ressaltar que não há restrição de acesso ao acusado e ao se procurador em qualquer fase processual. Isso porque a Lei no 8.112/1990 estabelece que o inquérito administrativo deverá obedecer ao princípio do contraditório, assegurada ao acusado ampla defesa, com a utilização dos meios e recursos admitidos em direito, logo, a consulta ao procedimento administrativo é indispensável para tutela de direito fundamental, o que vai ao encontro do disposto no artigo 21 da Lei nº 12.527/2011.

A Administração Pública, portanto, não pode utilizar indiscriminadamente a LGPD ou a LAI para restringir o acesso a procedimentos administrativos disciplinares, após a edição de seu julgamento, como ocorreu, por exemplo, nos processos de números 60143.002645/2021-17, 60143.002709/2021-80, 60143.002750/2021-56, 60143.002216/2021-40 e

[19] Para mais informações, verificar o Parecer sobre Acesso à Informação, da CGU, constante no link https://repositorio.cgu.gov.br/bitstream/1/73916/3/Parecer_Acesso_Informação_2023.pdf

60143.002675/2021-23[20]. De acordo com a legislação mencionada, corroborada no entendimento da CGU, admite-se apenas a restrição de acesso às informações que ensejarem a divulgação de dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Outro caso importante a ser destacado pela CGU é o acesso a informações pessoais de agentes públicos agindo nessa condição. O entendimento que prevalece é que o acesso a informações relativas ao exercício de atividades governamentais por ocupante de cargo, posto, graduação, função e emprego público, incluindo programas, projetos, serviços, políticas, ações, decisões e processos administrativos, deve ser permitido, sob o fundamento de que, desta forma, a sociedade pode mesurar a eficácia, a eficiência e a efetividade dos atos administrativos realizados pelo servidor público, representante do Estado. Além disso, entende a CGU que a divulgação desses dados não prejudica a intimidade, a vida privada, a honra e a imagem do servidor, pois sua formação, inclusive, é importante para o cumprimento de sua missão institucional.

A princípio, por exemplo, não se deve considerar que documentos relativos à participação de agentes públicos em reuniões oficiais, atos de nomeação de servidores para cargos e funções públicas, a identidade de servidores públicos responsáveis pela produção de documentos, bem como pela organização e o desenvolvimento de políticas, ações e projetos desenvolvidos ou financiados pelo Estado sejam considerados de acesso restrito com fundamento na LGPD e na LAI, pois não se referem a assuntos de natureza particular.

Contudo, ressalta a CGU que eventuais registros realizados em documentos de natureza pública, caso divulgados, podem criar situações de constrangimento e, inclusive, riscos à integridade física de agentes públicos, especialmente aqueles que atuam em atividades ostensivas de segurança pública. Nesses casos, a divulgação da informação pessoal deve ser verificada no caso concreto, de maneira que seja avaliada a existência de risco razoável à integridade física do agente público e o contexto em que a informação foi produzida. Não devem ter seu acesso restrito, contudo, as informações capazes de identificar agentes públicos responsáveis pelo cometimento de condutas ilícitas, respeitadas as garantias e os direitos fundamentais aplicáveis ao caso concreto.

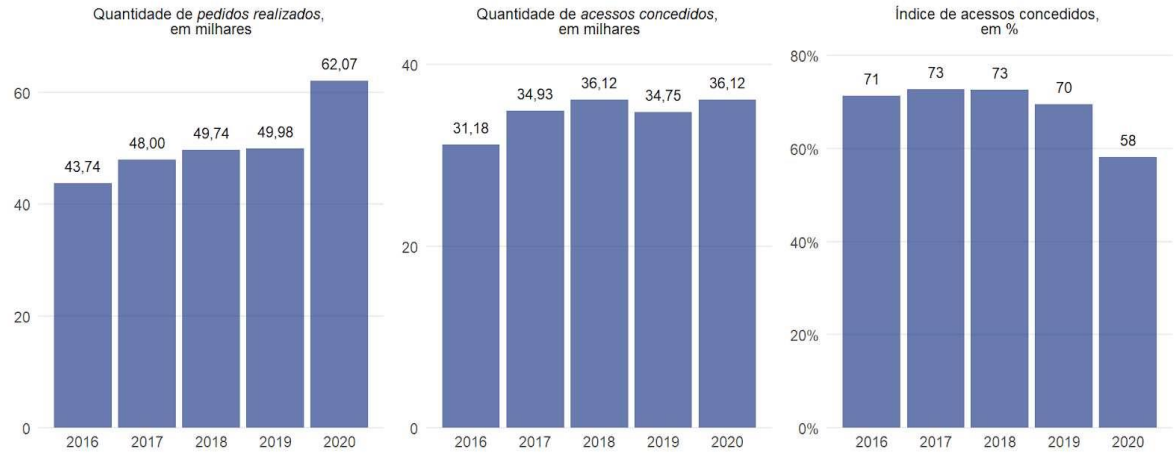
[20] Veja detalhes dos processos no link https://repositorio.cgu.gov.br/bitstream/1/73916/3/Parecer_Acesso_Informação_2023.pdf

Sendo assim, é importante destacar que, nos casos em que o acesso à informação é impedido pelo gestor sob uma interpretação restritiva e equivocada da LGPD e, inclusive, da LAI, estamos diante de uma decisão arbitrária que pode, sim, impedir a realização de uma política pública de transparência, essencial ao Estado Democrático de Direito. Imprescindível, portanto, a análise do caso concreto, à luz da legislação em vigor que trata essencialmente do acesso à informação e da Proteção de Dados Pessoais.

Interessante notar que as negativas de acesso já aconteciam antes mesmo da LGPD entrar em vigor, segundo dados do Relatório da Transparência Brasil, e aumentou com o advento da LGPD.[21]

No período de 2019 a 2020, no governo do presidente Jair Bolsonaro, o cenário de negativas de acesso à informação foi o maior desde que a LAI entrou em vigor, em 2011. Muitos casos apresentavam o argumento de "pedido genérico" e "desproporcional"; outros eram negados sob a hipótese de haver dados pessoais.

Em 2020, com a entrada em vigor da LGPD, houve uma redução significativa de acesso à informação. Dados do relatório indicam que a taxa de acessos concedidos no ano mencionado foi de 58% e a médias dos anos anteriores (2016, 2017, 2018 e 2019) foi de 71,8%. O governo Bolsonaro apresentou menor índice de acessos concedidos em comparação com os governos Temer e Dilma.



Fonte:https://www.transparencia.org.br/downloads/publicacoes/Negativas_de_acesso_a_informacao_pioram_sob_governo_Bolsonaro.pdf

[21] Para mais informações sobre os dados mencionados, acesse o link https://www.transparencia.org.br/downloads/publicacoes/Negativas_de_acesso_a_informacao_pioram_sob_governo_Bolsonaro.pdf

Apesar de os motivos para a negativa serem vários, o que chamou a atenção foi o aumento do uso de negativas com base em "dados pessoais", 20% dos pedidos negados, ou seja, quatro vezes mais do que nos governos Dilma e Temer.

Contudo, o aumento das negativas de acesso não quer dizer exatamente que o problema está na LGPD, muito menos que haja um conflito entre esta lei e a LAI. O cenário aponta para a necessidade de que as regras sejam devidamente interpretadas e cumpridas, com soluções para cada caso concreto. O problema, muitas vezes, está vinculado a falhas na implementação efetiva das políticas públicas de transparência e acesso à informação. A LGPD, por sua vez, foca na proteção de dados pessoais e não aborda diretamente as questões de transparência e acesso à informação. Assim, a ausência de acesso pode ser mais uma questão de falta de mecanismos eficazes e de implementação das leis de acesso à informação do que um problema inerente à LGPD.

Outro ponto abordado é o potencial conflito entre direitos, como o direito à privacidade (assegurado pela LGPD) e o direito ao acesso à informação (garantido por outras legislações e normas, como a Lei de Acesso à Informação - LAI). Doneda (2021) argumenta que é necessário encontrar um equilíbrio entre esses direitos, e as questões de negativa de acesso muitas vezes surgem da dificuldade em harmonizar esses interesses.

A negativa de acesso à informação também pode refletir deficiências institucionais e práticas administrativas, como a falta de clareza nas normas, a resistência à transparência e a ausência de processos bem definidos para garantir o acesso à informação. Esses problemas são mais relacionados à cultura organizacional e à gestão pública do que à LGPD em si. A aplicação da LGPD e a interpretação de suas disposições podem influenciar como as informações são acessadas e compartilhadas. No entanto, as questões de negativa de acesso muitas vezes estão mais ligadas à interpretação e aplicação das normas de acesso à informação e à gestão dos dados dentro das organizações do que aos princípios estabelecidos pela LGPD.

A interação entre a LAI e a LGPD representa, portanto, um desafio para a proteção de dados e a transparência pública. Desde que entraram em vigor, novas possibilidade e discussões sobre a aplicação dessas leis surgiram, especialmente em relação às negativas de acesso à informação. Assim, novas possibilidades de interpretação, restrições e embates vão continuar acontecendo.

O desafio nesses casos é como as autoridades públicas vão tratar as questões controversas, especialmente a Autoridade Nacional de Proteção de Dados, para que a política de transparência pública não seja prejudicada em função do uso e interpretação inadequada da LGPD.

2.3 Desafios da CGU nos Casos de Restrição Indevida de Acesso à Informação

A Lei nº 12.527/2011, conhecida como Lei de Acesso à Informação (LAI), foi criada com o objetivo de regular o acesso a informações públicas no Brasil, assegurando que qualquer cidadão possa ter acesso a dados de interesse coletivo ou geral, sem a necessidade de apresentar justificativas. No entanto, a efetivação desse direito depende da capacidade de os órgãos e entidades públicas de implementar as diretrizes da lei de forma eficiente e transparente. Nesse contexto, a Controladoria-Geral da União (CGU) surge como o principal órgão responsável pela coordenação, regulamentação e monitoramento da aplicação da LAI no âmbito da administração pública federal.

Dentre suas competências e atribuições legais, a CGU é responsável por editar normas complementares e diretrizes para a correta implementação da LAI em todo o âmbito da administração pública federal. Como órgão de controle interno do Poder Executivo, a CGU tem o papel de garantir que os ministérios, autarquias e outras entidades federais adotem práticas que assegurem a disponibilização de informações de interesse público, conforme exigido pela LAI. Sua função normativa inclui a elaboração de regulamentos e manuais que orientam os órgãos públicos sobre como lidar com pedidos de informação, além de determinar os procedimentos necessários para garantir a transparência proativa, ou seja, a disponibilização automática de informações públicas, sem a necessidade de solicitação.

A CGU também desenvolve políticas e iniciativas para uniformizar o tratamento das solicitações de acesso à informação, promovendo um sistema integrado e coerente de transparência. Além disso, gerencia o e-SIC (Sistema Eletrônico do Serviço de Informações ao Cidadão), uma plataforma digital por meio da qual os cidadãos podem solicitar informações a órgãos federais. O sistema facilita a interação entre o governo e a sociedade, permitindo a rastreabilidade e o controle das demandas de acesso à informação, bem como a garantia de cumprimento dos prazos estabelecidos pela LAI.

Como órgão de controle do Poder Executivo, a CGU exerce uma função fiscalizatória importante no cumprimento da LAI. Uma de suas atribuições é monitorar e avaliar a implementação da lei nos órgãos e entidades da administração pública federal, realizando auditorias e inspeções para verificar se as instituições estão cumprindo as exigências de transparência ativa e passiva (respostas a solicitações de informação), além de analisar a qualidade e o prazo de respostas fornecidas aos cidadãos.

Quando são identificados casos de descumprimento da LAI, a CGU possui competência sancionadora, podendo impor penalidades administrativas a agentes públicos ou entidades que desrespeitam as disposições da lei. Ainda, tem a responsabilidade de investigar denúncias de violação ao direito de acesso à informação e de aplicar medidas corretivas, quando necessário. As penalidades podem variar desde advertências até sanções mais severas, como a responsabilização por improbidade administrativa, caso a negativa de acesso à informação seja considerada uma violação grave da lei.

Um aspecto relevante do papel fiscalizador da CGU é seu compromisso com a promoção da integridade e do combate à corrupção. Ao garantir que informações sobre o uso de recursos públicos sejam amplamente acessíveis, a Controladoria-Geral da União promove um ambiente em que a sociedade civil pode exercer controle social e denunciar práticas ilícitas, contribuindo diretamente para a responsabilização de agentes públicos. Além disso, desempenha um papel fundamental na promoção da transparência e na fiscalização da administração pública no Brasil, conforme estabelecido pela Lei de Acesso à Informação (LAI).

No entanto, a aplicação prática da LAI enfrenta diversos desafios, especialmente no que diz respeito à restrição indevida do acesso à informação, com base na LGPD. Um dos principais desafios da CGU é garantir a correta interpretação e aplicação da LAI em consonância com a Lei Geral de Proteção de Dados Pessoais.

Muitas vezes, as restrições ao acesso à informação são baseadas em interpretações incorretas ou excessivas dos limites estabelecidos pela lei. Isso pode ocorrer devido à falta de clareza nas normas internas dos órgãos públicos ou à resistência à transparência. A CGU precisa enfrentar a dificuldade de uniformizar a aplicação da LAI em um contexto em que a interpretação das normas pode variar significativamente entre diferentes entidades.

Outro desafio é a resistência de alguns órgãos e entidades públicas em divulgar informações. Essa resistência pode advir de uma cultura de sigilo, receio de exposição de informações comprometedoras ou simplesmente falta de familiaridade com a LAI. A CGU enfrenta o desafio de promover uma mudança cultural e estrutural em órgãos públicos que ainda têm uma postura avessa à transparência.

A coexistência da LAI com a Lei Geral de Proteção de Dados (LGPD) adiciona complexidade à gestão de pedidos de acesso à informação. A necessidade de proteger dados pessoais pode levar a conflitos sobre quais informações podem ser divulgadas. A CGU deve lidar com a complexidade de equilibrar a transparência com a proteção de dados pessoais,

evitando restrições indevidas que possam ser justificadas sob a LGPD, mas que não se sustentam quando analisadas à luz da LAI.

No Parecer sobre Acesso à Informação[22] elaborado pelo órgão de controle, destaca-se o objeto de direito de acesso à informação, ou seja, a informação pública. Um dos desafios é saber exatamente o que é informação pública e que tipos de requerimentos podem ser objeto de acesso informação.

> Pode-se ser considerada uma informação pública, do ponto de vista da sua produção e custódia, aquela contida em registros ou documentos, produzidos ou acumulados por seus órgãos ou entidades, recolhidos ou não a arquivos públicos, bem como a informação produzida ou custodiada por pessoa física ou entidade privada decorrente de qualquer vínculo com seus órgãos ou entidades, mesmo que esse vínculo já tenha cessado.
>
> Do ponto de vista substantivo, a informação pública é aquela que versa sobre atividades exercidas pelos órgãos e entidades, inclusive as relativas à sua política, organização e serviços; que é pertinente à administração do patrimônio público, utilização de recursos públicos, licitação, contratos administrativos; bem como a informação relativa à implementação, acompanhamento e resultados dos programas, projetos e ações dos órgãos e entidades públicas, bem como metas e indicadores propostos e ao resultado de inspeções, auditorias, prestações e tomadas de contas realizadas pelos órgãos de controle interno e externo, incluindo prestações de contas relativas a exercícios anteriores.
>
> (https://repositorio.cgu.gov.br/bitstream/1/73916/3/Parecer_Acesso_Informação_2023.pdf)

Essa definição é importante do ponto de vista interpretativo dos casos concretos, notadamente quando se solicitam documentos com informações públicas, de livre acesso, e outras de acesso restrito. O desafio, portanto, consiste em trabalhar com a harmonia entre o acesso à informação e a restrição devida de determinadas informações. Para a CGU, importante, neste ponto, acionar o art. 7º, § 2o da Lei n. 12.527/2011, que dispõe que "quando não for autorizado acesso integral à informação por ser ela parcialmente sigilosa, é assegurado o acesso à parte não sigilosa por meio de certidão, extrato ou cópia com ocultação da parte sob sigilo."

Porém, o desafio vai muito além: analisar adequadamente o regime de restrições ao direito de acesso à informação, cuja natureza é relativa, pois o seu grau de proteção não se estende a todo o seu escopo e a transparência pública depende da interação entre o direito de

[22] O referido Parecer foi elaborado para atender ao despacho presidencial de 1º de janeiro de 2023. Para ver mais detalhes, acesse o link https://repositorio.cgu.gov.br/bitstream/1/73916/3/Parecer_Acesso_Informação_2023.pdf

acesso à informação e as limitações impostas ao seu exercício. Logo, a LAI, além de regulamentar o acesso à informação pública, também disciplina o regime de proteção às informações custodiadas pelo Estado.[23]

Para a CGU, esse regime de restrições deve ser interpretado com muito cuidado e sempre de maneira restritiva, pois a regra é o acesso à informação. Por isso, o interesse público deve ser preponderante nas decisões de divulgação de dados e na publicidade das ações do governo; o sigilo, portanto, é exceção, nos termos do art. 5º da Constituição Federal.

> A restrição de acesso deve limitar-se, dentro do possível, apenas às partes legalmente protegidas do documento solicitado, nos termos do §2o do artigo 7o da LAI, segundo o qual "quando não for autorizado acesso integral à informação por ser ela parcialmente sigilosa, é assegurado o acesso à parte não sigilosa por meio de certidão, extrato ou cópia com ocultação da parte sob sigilo". Trata-se da aplicação do princípio da máxima divulgação, em que a transparência deve ser percebida como regra geral e, o sigilo, como exceção. Garante-se, assim, a devida transparência a documentos de interesse público, ao mesmo tempo em que se resguardam informações sigilosas e pessoais, nos termos do artigo 6o, inciso III da Lei de Acesso à Informação.
>
> A Lei de Acesso à informação, desse modo, dispõe três bases legais que, quando devidamente comprovadas, autorizam a restrição de acesso a informações produzidas ou custodiadas por órgãos e entidades públicas, em razão da sua natureza sensível: informações classificadas (art. 23), informações restritas devido à existência de sigilo legal específico (art. 22), e informações pessoais relativas à intimidade, à vida privada, à honra e à imagem de terceiras pessoas (art. 31). (https://repositorio.cgu.gov.br/bitstream/1/73916/3/Parecer_Acesso_Informação_2023.pdf)

Importante destacar que a LAI já tratava do acesso a informações pessoais quando a LGPD entrou em vigor. Conforme o inciso IV do artigo 4° da Lei n° 12.527/2011, é aquela relacionada à pessoa natural identificada ou identificável. Entende-se por pessoa natural a pessoa física, ou seja, o indivíduo.

Contudo, a LAI, conforme o artigo 31, não protege todas as informações pessoais, mas somente aquelas com potencial de afetar os direitos da personalidade, conforme os definidos no artigo 5º, inciso X, da Constituição Federal, a saber: a intimidade, a vida privada, a honra e a imagem das pessoas.

[23] Veja mais detalhes sobre o regime de proteção às informações no link https://repositorio.cgu.gov.br/bitstream/1/73916/3/Parecer_Acesso_Informação_2023.pdf

> No núcleo desse conjunto de dados, estaria o que se denominou, com amparo na doutrina existente, a informação pessoal sensível. Ou seja, aquela informação que viola o direito de autodeterminação da imagem ou que possa levar a que terceiros adotem ações discriminatórias contra o titular daquele dado. Dessa forma, a restrição ao direito à intimidade e à vida privada apenas se justifica quando necessária para assegurar a proteção de outros direitos fundamentais ou bens constitucionais relevantes, de modo que é, em geral, no conflito com outros direitos que se pode, em cada caso, avaliar a legitimidade constitucional da restrição.
>
> (https://repositorio.cgu.gov.br/bitstream/1/73916/3/Parecer_Acesso_Informação_2023.pdf)

Nesse contexto, o desafio da CGU é construir entendimentos, a serem aplicados na Administração Pública, que reforçam a tese legal de que a negativa de acesso a informações pessoais ocorre quando a divulgação cause danos aos direitos de personalidade do titular das informações. Logo, em havendo a possibilidade de divulgação de dados pessoais de terceiros pela Administração, deve-se observar os princípios da razoabilidade e proporcionalidade, bem como a existência de interesse público relevante na sua divulgação.

Para exemplificar este entendimento, convém trazer ao texto um recente julgado da CGU, que analisou um pedido de informação negado pelo órgão público. Tal pedido envolvia acesso a telegramas enviados pelo Itamaraty a um brasileiro morto sob a proteção da autoridade estrangeira. Apesar de o documento conter informações pessoais, a CGU decidiu por sua divulgação, considerando que a divulgação das circunstâncias da morte do brasileiro poderia contribuir para a devida apuração e responsabilização dos culpados, devolvendo ao falecido parte de sua dignidade.[24]

Portanto, o desafio consiste em desconstruir a ideia equivocada de que a existência de qualquer dado pessoal deve ser objeto de restrição. A LAI identifica restrições apenas a informações sensíveis que prejudiquem a intimidade, honra e imagem do seu titular. Assim, reforça-se as diretrizes do artigo 31, da Lei Federal nº 12.527/2011, de 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 fundamentais. Tais diretrizes corroboram com o fundamento da LGPD, que não pode servir como fundamento para a negativa de acesso à informação pública que contenha dados pessoais, pelo mesmo

[24] Veja mais detalhes no link Brasil. Controladoria-Geral da União. Recurso de acesso à informação n. 09002.001968/2022-21, julgado em 17/01/2023.

entendimento de que a restrição deve considerar os dados relativos à intimidade, vida privada, honra e imagem das pessoas.

2.4 O Papel da Autoridade Nacional de Proteção de Dados na Política Pública de Tratamento de Dados Pessoais

A Lei Geral de Proteção de Dados (LGPD) estabelece um marco regulatório para a proteção de dados pessoais no Brasil. Um dos pilares dessa legislação é a criação da Autoridade Nacional de Proteção de Dados Pessoais (ANPD), órgão responsável por supervisionar, regulamentar e garantir o cumprimento das disposições da LGPD.

A ANPD, autarquia de natureza especial, vinculada ao Ministério da Justiça e Segurança Pública, tem por objetivo assegurar a aplicação uniforme e eficaz das normas de proteção de dados pessoais no Brasil.[25]

Composta por um Conselho Diretor, todos nomeados pelo Presidente da República, a estrutura organizacional da ANPD também abrange a Presidência, a Secretaria e a Corregedoria, além de comitês técnicos e consultivos que auxiliam na formulação de políticas e na supervisão das atividades da autoridade. Possui autonomia administrativa, financeira e técnica, o que lhe confere independência na execução de suas funções. Essa autonomia é essencial para garantir que a ANPD possa atuar de forma imparcial e eficaz, sem interferências políticas ou pressões externas.[26]

A ANPD desempenha diversas funções e competências fundamentais para a implementação e supervisão da LGPD:

- Elabora e divulga regulamentações e diretrizes que detalham a aplicação da LGPD. Essas normas orientam organizações e entidades sobre como cumprir as exigências da lei, incluindo aspectos como consentimento, direitos dos titulares e medidas de segurança;

- Fiscaliza e monitora o cumprimento da LGPD pelas organizações públicas e privadas. Isso inclui a análise de práticas de tratamento de dados, a realização de auditorias e a verificação de conformidade com as disposições legais. A ANPD também pode instaurar investigações e processos administrativos para apurar irregularidades e aplicar sanções;

- Promove a educação e a conscientização sobre proteção de dados pessoais. Isso envolve a realização de campanhas de sensibilização, a oferta de treinamentos e a publicação de

[25] De acordo com a Lei nº 14.460, de 25 de outubro de 2022.
[26] Nos termos do Decreto nº 10.474, de 26 de agosto de 2020.

materiais informativos para orientar tanto os responsáveis pelo tratamento de dados quanto os titulares sobre seus direitos e deveres.

- Recebe e trata de reclamações de titulares de dados pessoais que se sintam prejudicados pelo tratamento de seus dados. A autoridade atua na mediação e resolução de conflitos, buscando soluções que garantam o respeito aos direitos dos titulares e a correção de práticas inadequadas.[27]

O papel da ANPD também é um desafio que envolve a correta interpretação e aplicação da Lei Federal nº 13.709/2018, a LGPD. Por isso, busca orientar os agentes sobre o tema de Políticas Públicas de tratamento de dados pessoais, por meio de regulamentações e publicações.

As políticas públicas de tratamento de dados emergem em um cenário no qual a informação se tornou um dos principais ativos de sociedades contemporâneas, principalmente com o avanço das tecnologias digitais. Em face da crescente importância dos dados e seu uso para diversos fins, desde marketing até governança pública, as políticas públicas desempenham um papel essencial na regulação dessas atividades, garantindo a proteção de direitos fundamentais, como a privacidade, e o uso responsável das informações.

Entende-se por políticas públicas de tratamento de dados o conjunto de diretrizes, normas e regulamentações implementadas por governos e entidades estatais com o objetivo de regular como os dados pessoais são coletados, processados e armazenados por organizações públicas e privadas. Essas políticas são elaboradas com base em legislações nacionais e internacionais que visam a proteção dos cidadãos contra abusos relacionados ao uso de suas informações, como a Lei Geral de Proteção de Dados (LGPD) no Brasil e o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia.

Importante esclarecer que a regulação do tratamento de dados visa, em essência, a proteção da privacidade e o controle dos cidadãos sobre suas informações pessoais. Esse controle é fundamental para garantir que os dados sejam utilizados de maneira justa e transparente, evitando abusos como discriminação, violação de direitos e até manipulação de comportamento.

O papel da ANPD é, essencialmente, garantir a implementação da política de tratamento de dados, que apresenta tanto desafios quanto oportunidades para os governos e a sociedade. O mapa estratégico da ANPD para o período de 2024 a 2027 inclui resultados a serem alcançados em prol da sociedade, tais como: impulsionar a pesquisa, o desenvolvimento e a inovação na

[27] Nos termos da Lei nº 13.709, de 14 de agosto de 2018.

área de proteção de dados pessoais; promover a cidadania para o exercício do direito à proteção de dados pessoais; ampliar a prevenção, a detecção e a repressão às infrações à LGPD e estabelecer um ambiente regulatório confiável, participativo e inovador no Brasil. A visão da ANPD é, por meio dessas políticas públicas, promover um ambiente seguro para o exercício do direito à proteção de dados pessoais.

Em novembro de 2023, a ANPD divulgou um relatório com o resultado do trabalho realizado nos últimos três anos (2021 a 2023), em que a Autoridade afirma que os desafios se multiplicam, mas, apesar disso, vem se posicionando em debates caros à sociedade, como regulação de plataformas digitais e regulamentação da inteligência artificial no Brasil. [28]

A atuação orientativa da ANPD nesses três anos foi marcada, principalmente, pela publicação dos guias orientativos. Dentre eles, destacam-se: o Guia Orientativo para Definição dos Agentes de Tratamento de Dados Pessoais e Encarregado[29]; Cartilhas Segurança para Internet [30]; Guia Como Proteger seus Dados Pessoais[31]; Guia orientativo Tratamento de dados pessoais pelo Poder Público[32]; Guia orientativo da aplicação da LGPD por agentes de tratamento no contexto eleitoral[33]; Enunciado sobre hipóteses legais aplicáveis ao tratamento de dados pessoais de crianças e adolescentes[34], e Guia orientativo Tratamento de dados pessoais para fins acadêmicos e para a realização de estudos e pesquisas[35]

No âmbito de sua atuação fiscalizatória, a ANPD desenvolveu ações de monitoramento, orientação, atuação preventiva e atuação repressiva, com o objetivo de identificar práticas inadequadas, riscos potenciais e garantir que os agentes de tratamento de dados pessoais estejam em conformidade com as obrigações legais estabelecidas pela LGPD.

A partir desse monitoramento, até agosto de 2023, a Autoridade de Proteção de Dados recebeu 237 (duzentos e trinta e sete) Comunicados de Incidentes de Segurança (CIS), que estão

[28] Veja mais informações sobre o balanço dos anos de 2021 a 2023 no link https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/anpd_balanco_tres_anos.pdf

[29] Mais detalhes estão no link https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_agentes_de_tratamento_e_encarregado___defeso_eleitoral.pdf

[30] Mais informações estão no link https://www.gov.br/anpd/pt-br/assuntos/noticias/cert-br-em-parceria-com-a-anpd-publica-dois-novos-fasciculos-da-cartilha-de-seguranca-para-a-internet

[31] Informações detalhadas sobre o tema estão no link https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-do-consumidor_como-proteger-seus-dados-pessoais-final.pdf

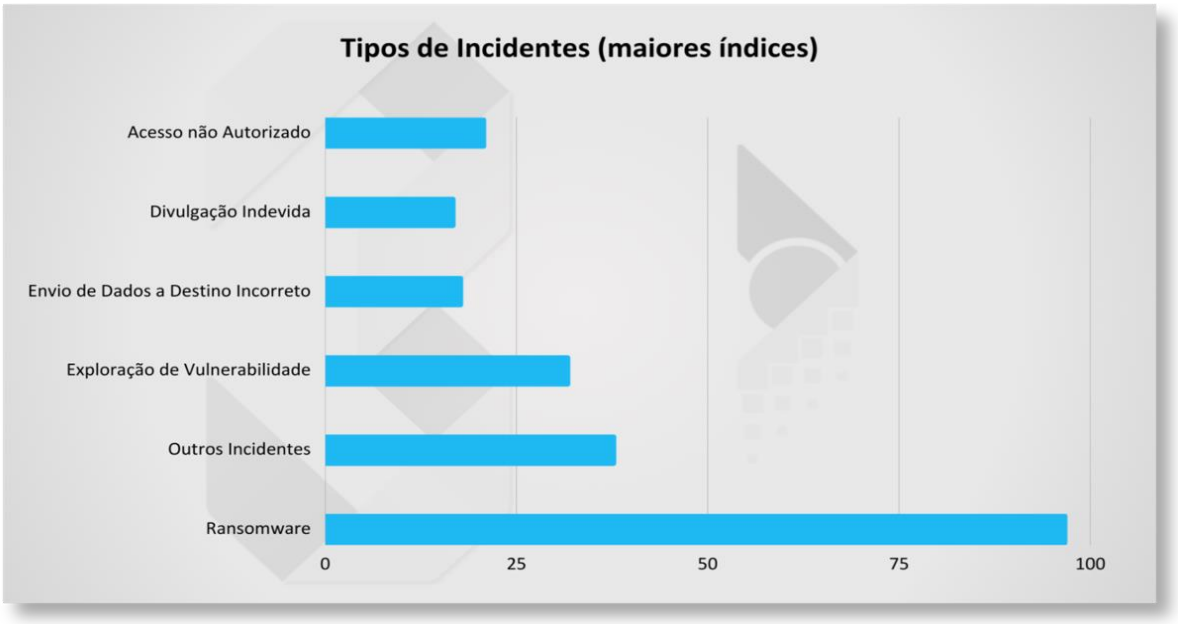
[32] Detalhes podem ser conferidos no link https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf

[33] Informações mais detalhadas sobre o tema estão no link https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_lgpd_final.pdf

[34] Veja mais informações no link https://www.in.gov.br/en/web/dou/-/enunciado-cd/anpd-n-1-de-22-de-maio-de-2023-485306934

[35] Mais detalhes sobre o tema estão no link https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/web-guia-anpd-tratamento-de-dados-para-fins-academicos.pdf

sob análise. Os tipos de casos foram separados por quantidade e divulgados no quadro a seguir[36], constante no relatório de atuação da ANPD.[37]



A partir dos tipos de incidentes, a ANPD analisa a efetivação adequada da política pública de tratamento de dados, corrigindo erros por meio de uma regulação que a Autoridade define como responsiva, baseada em um diálogo com os agentes regulados. Os dados sobre processos de fiscalização são constantemente atualizados e mantidos em transparência ativa[38].

A ANPD define incidente de segurança como um evento adverso confirmado que comprometa a confidencialidade, integridade ou disponibilidade de dados pessoais. Pode decorrer de ações voluntárias ou acidentais que resultem em divulgação, alteração, perda ou acesso não autorizado a dados pessoais, independentemente do meio em que estão armazenados. Na hipótese de o incidente ser capaz de causar risco ou dano relevante aos titulares, nos termos do art. 48 da Lei Geral de Proteção de Dados, o controlador deverá comunicar à autoridade nacional e ao titular da sua ocorrência. Seguem alguns quadros com números de incidentes de segurança apresentados em relatório pela ANPD[39].

[36] https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/anpd_balanco_tres_anos.pdf

[37] Ransomware é um tipo de malware que criptografa os arquivos de um computador ou sistema, tornando-os inacessíveis ao usuário. Em alguns casos, é cobrado um valor para que seja fornecida uma senha para descriptografar os arquivos.

[38] Ver dados no link https://www.gov.br/anpd/pt-br/composicao-1/coordenacao-geral-de-fiscalizacao

[39] https://www.gov.br/anpd/pt-br/composicao-1/coordenacao-geral-de-fiscalizacao

Comunicados de incidente de segurança recebidos pela ANPD

Ano	Comunicados no Ano	Acumulado desde 2021
2021	186	186
2022	275	461
2023	352	813
2024 (junho)	152	965

Tipo de Incidente (2023)	Quantidade de Comunicados
Sequestro de Dados (*ransomware*) sem transferência de informações	69
Sequestro de dados (*ransomware*) com transferência e/ou publicação de informações	65
Exploração de vulnerabilidade em sistemas de informação	54
Acesso não autorizado a sistemas de informação	35
Divulgação indevida de dados pessoais	25
Roubo de credenciais / Engenharia Social	24

Envio de dados a destinatário incorreto	23
Outro tipo de incidente não cibernético	13
Perda/roubo de documentos ou dispositivos eletrônicos	11
Publicação não intencional de dados pessoais	10
Outro tipo de incidente cibernético	8
Falha em sistema de informação (*software*)	8
Alteração/exclusão não autorizada de dados pessoais	2
Vírus de Computador / Malware	2
Descarte incorreto de documentos ou dispositivos eletrônicos	1
Violação de credencial por força bruta	1
Negação de Serviço (DoS)	1
Total Geral	**352**

Tipo de Incidente (junho/2024)	**Quantidade de Comunicados**
Sequestro de Dados (*ransomware*) sem transferência de informações	29
Roubo de credenciais / Engenharia Social	22
Acesso não autorizado a sistemas de informação	19
Outro tipo de incidente não cibernético	18
Sequestro de dados (*ransomware*) com transferência e/ou publicação de informações	15
Divulgação indevida de dados pessoais	12
Exploração de vulnerabilidade em sistemas de informação	11
Envio de dados a destinatário incorreto	9
Publicação não intencional de dados pessoais	9
Falha em sistema de informação (*software*)	3
Navegação de serviço (DoS)	2
Falha em equipamento (*hardware*)	1

Violação de credencial por força bruta	1
Perda/roubo de documentos ou dispositivos eletrônicos	1
Total Geral	**152**

Além de receber comunicados de incidentes de segurança no tratamento de dados pessoais, a ANPD recebe requerimentos e denúncias. Os requerimentos são classificados de acordo com sua natureza, podendo ser petições de titular ou denúncias. A petição de titular é um instrumento utilizado pelo titular de dados pessoais para exercer seus direitos em relação ao tratamento de seus dados. Já a denúncia consiste em uma comunicação feita por qualquer pessoa, natural ou jurídica, sobre uma suposta infração cometida contra a legislação de proteção de dados pessoais brasileira.[40]

Seguem números de requerimentos e denúncias recebidos pela ANPD, no período de 2021 a junho de 2024[41]

Requerimentos recebidos pela ANPD

Ano	Requerimentos no Ano	Acumulado desde 2021
2021	769	769
2022	1.045	1.814
2023	1.138	2.952
2024 (junho)	615	3.567

[40] A partir de 08/07/2024 o envio de requerimentos à ANPD (Denúncias e Petições) deve ser realizado por meio do preenchimento de formulário disponível na página do serviço https://www.gov.br/pt-br/servicos/abrir-requerimento-relacionado-a-lgpd

[41] Mais dados estão no link https://www.gov.br/anpd/pt-br/composicao-1/coordenacao-geral-de-fiscalizacao

Importante também destacar o papel da ANPD no incentivo da participação da sociedade na edição de regulamentos e normas, sempre precedida de audiência pública e de consulta pública, conforme preceitua a Lei Geral de Proteção de Dados Pessoais – LGPD, em seu art. 55-J, §2º. [42]

Outro instrumento de participação social muito utilizado pela ANPD são as Tomadas de Subsídios, em que a ANPD levanta quesitos relacionados a determinada temática e os submete a amplo debate social, para que seja possível obter opiniões das mais variadas matizes a respeito de determinada questão a ser regulamentada. Destacam-se alguns quesitos: Regulamento de Dosimetria e Aplicação de Sanções Administrativa; Processo de Fiscalização e do Processo Administrativo Sancionador; Comunicação de incidentes e especificação do prazo de notificação; Transferência Internacional de Dados Pessoais; Relatório de impacto à proteção de dados pessoais; Uso de dados pessoais para fins acadêmicos e para a realização de estudos por órgãos de pesquisa e Estudo Preliminar sobre Hipóteses Legais de Tratamento de Dados Pessoais - Legítimo Interesse[43]

A participação da sociedade é importante para a política pública de tratamento de dados. Por isso, o Conselho Nacional de Proteção de Dados Pessoais e Privacidade, Conselho Consultivo da ANPD, tem representantes do setor público, membros do setor produtivo, da sociedade civil e da academia.

Além do Conselho Consultivo, a Ouvidoria também é um canal importante de interação com a sociedade. Por meio de sua Ouvidoria, a ANPD já atendeu aproximadamente 7 mil demandas da sociedade, com os seguintes temas: Ações de Fiscalização; Sanções Administrativas; Comunicação de Incidente de Segurança e Exercícios de Direitos. Temas relevantes que contribuem para a eficácia da política pública de tratamento de dados no Brasil.

Em seu último relatório[44], a ANPD enfatizou o seu papel fundamental como autoridade garantidora do direito à proteção de dados pessoais. Destacou os desafios que tem pela frente e convidou a sociedade a participar das audiências e consultas públicas. Para a Autoridade Nacional de Proteção de Dados, o conhecimento da LGPD é importante para a construção de

[42] As Consultas Públicas da ANPD são realizadas por meio da Plataforma Participa Mais Brasil, https://www.gov.br/participamaisbrasil/.

[43] Veja tabela detalhada no link https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/anpd_balanco_tres_anos.pdf.

[44] https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/anpd_balanco_tres_anos.pdf.

um ambiente seguro para o tratamento de dados pessoais e para a proteção dos direitos da personalidade, consagrados no artigo 5º da Constituição Federal.

CAPÍTULO 3

TRANSPARÊNCIA E LEGITIMIDADE: A LGPD COMO ALIADA À POLÍTICA PÚBLICA DE ACESSO À INFORMAÇÃO NA UFRJ

A Universidade Federal do Rio de Janeiro (UFRJ), fundada em 1920, é uma das mais importantes instituições de ensino superior e pesquisa do Brasil e da América Latina. Ao longo de sua história, a UFRJ consolidou-se como um centro de excelência acadêmica, científica e cultural, destacando-se em diversas áreas do conhecimento e sendo responsável por grande parte da produção científica nacional. Seu impacto vai muito além do ensino e pesquisa: a universidade desempenha um papel crucial na formação de cidadãos críticos, na promoção do desenvolvimento social e na implementação de políticas públicas voltadas para o bem-estar da população. Sua estrutura abrange múltiplos campi, com destaque para a Cidade Universitária, localizada na Ilha do Fundão, que concentra grande parte das suas atividades. A universidade oferece cursos de graduação e pós-graduação em praticamente todas as áreas do conhecimento, além de ser um centro de referência em pesquisas avançadas.

A contribuição científica da UFRJ é reconhecida internacionalmente. Diversos grupos de pesquisa atuam em áreas de ponta, como biotecnologia, engenharia, saúde, ciências sociais e humanas, entre outras. A produção científica da UFRJ é responsável por uma parcela significativa das publicações acadêmicas brasileiras em revistas internacionais de alto impacto. Além disso, a universidade possui programas de cooperação internacional com instituições renomadas, promovendo intercâmbios de conhecimento e ampliando a inserção do Brasil no cenário científico global.

No campo social, a UFRJ tem um papel fundamental na formação de profissionais altamente qualificados que atuam em setores estratégicos para o desenvolvimento do país. Os egressos da universidade ocupam posições de destaque em instituições públicas e privadas, contribuindo para o avanço tecnológico, a formulação de políticas públicas e o desenvolvimento econômico e social. A instituição, portanto, não apenas forma profissionais, mas também cidadãos comprometidos com a justiça social e o desenvolvimento sustentável.

Além de sua atuação no ensino e na pesquisa, a UFRJ é protagonista em diversas políticas públicas voltadas para o bem-estar social, a inovação tecnológica e a preservação cultural.

A universidade tem uma forte tradição na área da saúde, especialmente por meio de seus hospitais universitários, como o Hospital Universitário Clementino Fraga Filho (HUCFF), e unidades de saúde que atendem as comunidades do Rio de Janeiro e arredores. O hospital oferece assistência médica gratuita, funcionando como um importante pilar do Sistema Único de Saúde (SUS) e um campo de formação prática para estudantes das áreas de saúde, incluindo medicina, enfermagem, odontologia e psicologia.

Durante a pandemia de COVID-19, a UFRJ desempenhou um papel crucial no combate ao vírus, seja na linha de frente com profissionais de saúde, seja na pesquisa de tratamentos e vacinas. Laboratórios da universidade participaram de estudos sobre o comportamento do vírus, além de desenvolverem soluções tecnológicas e biológicas para mitigar os impactos da crise sanitária.

A UFRJ também se destaca em políticas de incentivo à pesquisa e inovação, desenvolvendo projetos que visam resolver problemas complexos da sociedade, especialmente nas áreas de energia, meio ambiente e tecnologia da informação. O Parque Tecnológico da universidade, localizado no campus da Ilha do Fundão, é um exemplo disso, reunindo startups, empresas multinacionais e grupos de pesquisa para promover a inovação e o desenvolvimento de soluções tecnológicas. Além disso, a universidade participa de iniciativas públicas e privadas voltadas para a pesquisa de energias renováveis, mudanças climáticas e sustentabilidade, promovendo o avanço de tecnologias verdes que buscam enfrentar os desafios ambientais contemporâneos. As pesquisas em biocombustíveis, por exemplo, são um dos grandes destaques da universidade, alinhando-se às políticas nacionais e internacionais de redução de emissões de carbono.

Outro aspecto relevante da atuação da UFRJ está nas suas políticas de extensão universitária, que têm como objetivo a interação direta com a sociedade. Projetos de extensão aproximam a universidade da população, promovendo ações que vão desde a educação popular até a inclusão social de grupos marginalizados. A UFRJ promove iniciativas em áreas como direitos humanos, cultura, educação básica e formação de professores, atendendo diretamente a comunidades em situação de vulnerabilidade social.

Uma das vertentes mais importantes dessas políticas é o compromisso da UFRJ com a educação pública. Programas voltados para o fortalecimento da educação básica, como o Instituto de Aplicação Fernando Rodrigues da Silveira (Cap-UFRJ), e projetos de formação continuada para professores da rede pública são exemplos do esforço da universidade para melhorar a qualidade da educação no país.

A UFRJ também desempenha um papel vital na preservação e difusão da cultura e do patrimônio histórico. A universidade abriga o Fórum de Ciência e Cultura, uma das mais antigas e respeitadas instituições culturais do Rio de Janeiro, que promove eventos, exposições e debates sobre temas culturais, científicos e sociais. O Fórum de Ciência e Cultura é um espaço de diálogo entre a universidade e a sociedade, contribuindo para a democratização do conhecimento. Além disso, a UFRJ é responsável pela preservação de importantes acervos históricos, como o Museu Nacional, devastado por um incêndio em 2018. Após a tragédia, a universidade liderou um esforço global para a reconstrução e restauração do museu, com o objetivo de preservar um dos mais importantes patrimônios científicos e culturais do Brasil. Esse esforço de reconstrução reafirma o compromisso da UFRJ com a memória e a cultura do país.

Como uma instituição pública de grande porte, a universidade lida diariamente com uma imensa quantidade de informações, que vão desde dados acadêmicos até registros administrativos. Gerir esse volume de informações com eficiência e segurança é um desafio significativo, especialmente em um cenário de crescente preocupação com a privacidade e proteção de dados, regulamentado pela Lei Geral de Proteção de Dados Pessoais (LGPD).

As informações acadêmicas envolvem dados pessoais e educacionais dos estudantes, como históricos escolares, matrículas, notas, frequência, pesquisas desenvolvidas, estágios e atividades extracurriculares. Além disso, incluem-se dados dos docentes e pesquisadores, como produção científica, projetos de pesquisa e relatórios de atividades acadêmicas. A universidade, sendo uma das principais produtoras de conhecimento no país, também gera e gerencia uma quantidade significativa de informações relativas a publicações científicas, patentes e inovações tecnológicas.

Outro aspecto relevante são os dados relativos aos programas de pós-graduação e aos centros de pesquisa, que englobam desde os projetos de pesquisa realizados até as parcerias com outras instituições e financiadores, além dos resultados de investigações científicas que, muitas vezes, envolvem dados sensíveis ou estratégicos.

Na esfera administrativa, a UFRJ lida com informações que incluem contratos, convênios, licitações, dados financeiros, recursos humanos e informações logísticas. Os dados administrativos não apenas asseguram o funcionamento da instituição, mas também devem ser divulgados de forma transparente ao público, conforme previsto pela Lei de Acesso à Informação (LAI). A universidade também é responsável pela gestão de documentos que envolvem a contratação de funcionários, controle de folha de pagamento, planos de carreira,

licitações e contratos com fornecedores, além de registros sobre o uso de instalações e serviços. Portanto, gerencia uma infraestrutura complexa e diversificada que inclui dados de natureza distinta e, em muitos casos, sensíveis. Além disso, o volume de dados cresce continuamente à medida que novos estudantes ingressam, pesquisas são conduzidas, e processos administrativos se acumulam.

Com um volume tão grande e variado de informações, a UFRJ enfrenta desafios significativos na gestão e proteção desses dados. Um deles está relacionado à integração de sistemas e infraestrutura de Tecnologia da Informação. Atualmente, a UFRJ opera com diversos sistemas de informação para gerenciar dados acadêmicos, administrativos e financeiros. Com a entrada em vigor da LGPD, a UFRJ se depara com o desafio de proteger os dados pessoais de seus estudantes, docentes e servidores, além de garantir que os dados sensíveis sejam tratados de acordo com os princípios da legislação. Outro desafio está na conscientização e capacitação dos funcionários sobre as boas práticas de segurança da informação. A UFRJ precisa garantir que todos os servidores compreendam a importância de proteger os dados e sigam protocolos rigorosos para o tratamento seguro de informações, além de evitar negligências ou falhas humanas que possam comprometer a segurança.

Submetida a diversas regulamentações, como a LGPD e a LAI, que exigem que a instituição adote uma postura proativa tanto em termos de proteção de dados pessoais quanto de transparência pública, a universidade precisa assegurar que o acesso às informações públicas ocorra de forma transparente, sem comprometer a privacidade dos cidadãos. Essa conformidade exigiu da Instituição a implementação de políticas internas claras sobre o tratamento e o compartilhamento de dados, a designação de um encarregado de proteção de dados (DPO) e a criação de mecanismos para responder adequadamente a solicitações de acesso à informação, sempre em conformidade com as normativas legais.

Outro desafio encontrado pela universidade foi o de criar uma cultura de proteção de dados. A capacitação contínua dos servidores e a conscientização dos estudantes e pesquisadores sobre a importância da privacidade e da segurança da informação foram cruciais. Isso incluiu promover treinamentos, elaborar manuais de boas práticas e estabelecer canais de comunicação que esclareçam as responsabilidades de cada cidadão no manejo seguro de informações.

A gestão de informações na UFRJ, portanto, é um processo complexo que envolve desafios técnicos, legais e culturais. A instituição lida com um volume crescente de dados acadêmicos e administrativos, e a implementação de sistemas eficazes de gestão e proteção de

informações é fundamental para garantir tanto a segurança dos dados quanto a transparência exigida pela sociedade e pela legislação. À medida que a UFRJ avança na implementação de boas práticas de segurança e conformidade com a LGPD, ela se posiciona como uma universidade que não apenas forma profissionais e gera conhecimento, mas também zela pela proteção e integridade das informações que lhe são confiadas.

3.1. Política Pública de Tratamento de Dados Pessoais na UFRJ

A entrada em vigor da Lei Geral de Proteção de Dados Pessoais (LGPD) em 2020 trouxe mudanças significativas para todas as instituições que processam e gerenciam dados pessoais no Brasil, incluindo as universidades públicas. A Universidade Federal do Rio de Janeiro (UFRJ), como uma das maiores e mais importantes instituições de ensino superior do país, teve que se adaptar a essa nova realidade. A implementação da LGPD na UFRJ exigiu não apenas mudanças administrativas, mas também a criação de uma política pública para garantir o tratamento seguro e adequado de dados pessoais, equilibrando as necessidades de transparência e acesso à informação com a proteção à privacidade.

Importante destacar que, antes mesmo do advento da LGPD, a UFRJ já se preocupava com a segurança da informação. Em 15 de junho de 2012, o Reitor da universidade, por meio da Portaria nº 4579/2012, publicou a política de segurança da informação da UFRJ, de acordo com a aprovação do Conselho Gestor de Tecnologia da Informação e Comunicação, em sessão de 14 de dezembro de 2011. O objetivo da Política de Segurança da Informação era adotar o compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda, devendo ser cumprida por toda sua comunidade. Seu propósito era estabelecer as diretrizes a serem seguidas pela UFRJ no que diz respeito à adoção de procedimentos e mecanismos relacionados à segurança da informação.[45]

Outra questão definida na Portaria foi a comunicação de ocorrência de incidente de segurança, que contempla o registro formal dos incidentes, uma equipe focada em atendê-los e a resolução com avaliação de medidas para evitar novas ocorrências. E, nos casos de violação da Política ou Normas de Segurança da Informação, sanções administrativas e legais poderão ser adotadas. Essa política de segurança ainda está em vigor na universidade e é interessante

[45] A Portaria 4579/2012 está disponível no link https://www.security.ufrj.br/wp-content/uploads/2013/09/Portaria_4579_Pol%C3%ADtica_de_Segurança_da_Informação_da_UFRJ.pdf

notar que, apesar de ter sido criada em 2011, a essência da norma está relacionada à LGPD, apesar de não tratar especificamente de tratamento de dados pessoais.

A implementação da LGPD demandou uma transformação na forma como a universidade coleta, armazena, processa e compartilha informações, além de obrigar a instituição a criar políticas e mecanismos específicos para garantir a conformidade com a legislação.

Um dos principais impactos da LGPD na UFRJ foi a necessidade de readequar as práticas de coleta e tratamento de dados pessoais. Por exemplo, desde o momento da matrícula dos estudantes até a gestão de dados acadêmicos e administrativos, a universidade passou a justificar a coleta de cada dado, assegurando que ele seja realmente necessário para a finalidade pretendida. Isso inclui informações como nome, CPF, histórico escolar, dados de saúde (especialmente em cursos de áreas médicas), contatos de emergência, entre outros. Essas mudanças exigiram uma revisão dos formulários e sistemas utilizados pela UFRJ, garantindo que todos os dados pessoais coletados estejam de acordo com os princípios da LGPD. Além disso, a universidade teve que implementar mecanismos claros de consentimento, informando aos titulares de dados sobre o uso, a finalidade e o prazo de retenção de suas informações, além de garantir que esses dados sejam mantidos seguros e só sejam compartilhados mediante bases legais apropriadas.

Na Pró-Reitoria de gestão e Governança da universidade foi criado um guia prático acerca do tratamento de dados conforme a LGPD. Neste guia, a administração contextualizou a necessidade de adequação dos atos administrativos à LGPD, ressaltando que para o tratamento dos dados pessoais, a fim de exercer suas competências legais e execução de políticas públicas, não é necessário o consentimento do titular. Contudo, ainda assim deve-se atuar no sentido de proteger dados como nome, RG, CPF, estado civil, Siape, dentre outros que permitam identificar ou tornar possível a identificação de uma pessoa natural.

Outra orientação foi para se evitar a divulgação irregular de dados pessoais. Para isso, cada seção/divisão da Pró-Reitoria de Gestão e Governança deveria iniciar medidas garantidoras da segurança e sigilo dos dados o mais breve possível, visando à adequação aos termos da LGPD. Desta forma, editais de licitação, minutas de contratos, aditivos dentre outros documentos deverão ser enviados à Divisão de Governança já com as tarjas nos locais adequados. Os documentos constantes no processo eletrônico no SEI que contenham dados pessoais relativos à intimidade, vida privada, honra e imagem devem ter seu acesso restrito com base nos princípios expostos no Art. 6º, no Art. 18, IV, Art. 46 e 47 da referida lei, assim como

os documentos que sejam divulgados em portais de transparência, tenham os dados pessoais tarjados com a ferramenta PDF24. O julgamento quanto à necessidade de restringir deverá ser realizado com base no contexto e por meio do julgamento do próprio servidor, com base nas orientações detalhadas no manual de utilização do SEI.[46]

Outro grande impacto da LGPD na UFRJ foi a necessidade de reestruturar seus sistemas de informação para garantir que os dados pessoais estejam protegidos contra acessos não autorizados, vazamentos e outras vulnerabilidades. Com o volume de dados acadêmicos e administrativos geridos pela universidade, foi preciso investir em melhorias na infraestrutura tecnológica. Além disso, a UFRJ teve que garantir que os diferentes departamentos e setores da universidade atuem de forma integrada, aplicando as mesmas regras de proteção de dados em todas as suas unidades. Isso é bastante desafiador em uma instituição tão diversificada quanto a UFRJ, onde cada faculdade, instituto ou unidade de pesquisa pode ter necessidades e práticas específicas para o tratamento de dados pessoais.

A adequação à LGPD também exigiu da universidade um esforço significativo de treinamento e capacitação dos servidores. Garantir a conformidade com a legislação não depende apenas de mudanças tecnológicas e procedimentais, mas também da conscientização de toda a comunidade acadêmica e administrativa sobre a importância da proteção de dados pessoais. Para isso, a UFRJ tem promovido ações de sensibilização e capacitação sobre a LGPD. Esse processo inclui a elaboração de manuais de boas práticas e a criação de canais de comunicação para tirar dúvidas e resolver questões relacionadas à proteção de dados. [47]Com essas ações, a universidade busca criar uma cultura de proteção de dados, em que cada pessoa compreenda o papel que desempenha na garantia da privacidade e segurança das informações pessoais.[48]

Importante destacar que, para atender às exigências da LGPD, a universidade desenvolveu uma política pública de dados pessoais voltada para garantir a conformidade com a legislação e proteger os direitos dos titulares de dados. Essa política envolve a criação de estruturas de governança interna, como a designação de um encarregado de proteção de dados

[46] Para mais detalhes, acesse o link https://portal.sei.ufrj.br/2022/09/publicidade-como-regra-restricao-como-excecao/

[47] Foi criada uma cartilha da Lei Geral de Proteção de Dados, constante no link https://ufrj.br/wp-content/uploads/2022/06/lgpd-cartilha-ufrj-21-06-22.pdf

[48] Veja o Guia Prático para tratamento de dados pessoais no link https://gestão.ufrj.br/images/Governanca/Restricao_de_acesso_SEI_e_Censura_de_DPs_com_PDF24_Rev3.pdf

(*Data Protection Officer – DPO*) e a implementação de procedimentos formais para lidar com solicitações e incidentes relacionados à privacidade.[49]

Uma das principais exigências da LGPD é a nomeação de um encarregado de proteção de dados, responsável por garantir que a universidade esteja em conformidade com a lei. O DPO na UFRJ, nomeado pela Portaria nº 232, de 8 de janeiro de 2021, tem a função de supervisionar as práticas de proteção de dados, atuar como ponto de contato com a Autoridade Nacional de Proteção de Dados (ANPD) e atender às demandas dos titulares de dados que queiram exercer seus direitos, como o direito de acesso, correção ou exclusão de informações. A presença de um DPO garante que a UFRJ tenha uma estrutura dedicada à proteção de dados, capaz de monitorar continuamente as práticas internas, implementar melhorias e resolver questões de privacidade de forma ágil e eficaz.

Outra parte essencial da política pública de dados pessoais na UFRJ foi a manutenção de procedimentos para lidar com incidentes de segurança, agora adequado à LGPD. Isso incluiu a adoção de planos de resposta a incidentes, com protocolos claros sobre como agir em caso de vazamento de dados ou acessos não autorizados, além da obrigação de comunicar rapidamente os titulares de dados e a ANPD sobre qualquer incidente que possa comprometer a privacidade das informações.[50]

Esses procedimentos foram fundamentais para mitigar os danos em caso de incidentes e demonstram o compromisso da UFRJ com a segurança da informação, reforçando a confiança dos estudantes, servidores e parceiros na instituição.

Contudo, apesar do foco na proteção de dados pessoais, a universidade também precisou equilibrar essa proteção com o compromisso de transparência e acesso à informação pública, conforme previsto na Lei de Acesso à Informação (LAI).

[49] Na UFRJ, as ações envolvendo a LGPD se encontram sob a égide do Comitê de Governança Digital, instituído pela reitora por meio da Portaria nº 5.199, de 27 de julho de 2020. Trata-se de órgão colegiado estratégico, permanente e de natureza deliberativa, de competências normativas, consultivas e deliberativas sobre as políticas gerais que envolvem governança digital, tecnologias da informação e comunicação e áreas correlatas, visando à eficiência, à estruturação da governança de tecnologias da informação e ao alinhamento das ações da área com os objetivos da instituição. Para ais detalhes, acesse o link https://ufrj.br/acesso-a-informacao/lgpd/.

[50] Um incidente de segurança pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de informação levando a perda de um ou mais princípios básicos de Segurança da Informação: confidencialidade, integridade e disponibilidade. A denúncia de um incidente pode ser realizada por qualquer cidadão, seja da comunidade acadêmica da UFRJ ou não. E, através da página eletrônica da SegTIC, poderá ser feita de forma anônima. Para mais detalhes, acesse o link https://cartaservicos.hom.tic.ufrj.br/servico/56.

Uma das principais ferramentas utilizadas pela UFRJ para cumprir a LAI é o Portal da Transparência, onde são disponibilizados dados sobre contratos, licitações, despesas e relatórios de gestão etc. Esse portal permite que qualquer cidadão tenha acesso a informações sobre como os recursos públicos estão sendo utilizados, fortalecendo o compromisso da UFRJ com a prestação de contas.[51]

Além disso, a universidade conta com o serviço de informação ao cidadão. O Serviço de Informação ao Cidadão (SIC) da UFRJ é uma unidade destinada a atender as demandas de acesso à informação dos cidadãos, em conformidade com a Lei de Acesso à Informação (Lei n.º 12.527/2011). O objetivo principal do SIC é assegurar que qualquer pessoa, física ou jurídica, possa solicitar e obter informações públicas produzidas ou custodiadas pela universidade, promovendo a transparência na gestão pública.

Integrado ao sistema de transparência ativa da universidade, o SIC é acessível tanto de forma presencial quanto por meio eletrônico. Ele faz parte da estrutura administrativa responsável por receber, processar e responder aos pedidos de informação feitos por cidadãos. A UFRJ disponibiliza o SIC por meio de uma plataforma online (Fala.BR/CGU), onde os pedidos podem ser registrados de maneira fácil e direta, permitindo ao solicitante acompanhar o andamento do seu pedido.

Quando um pedido de informação é registrado no SIC, ele é direcionado ao setor competente da universidade, no caso, a Ouvidoria-Geral da UFRJ, que analisa a solicitação e prepara a resposta de acordo com as normativas da Lei de Acesso à Informação. O processo é conduzido com base nos princípios da transparência e publicidade, mas também deve considerar os limites impostos pela Lei Geral de Proteção de Dados (LGPD), garantindo que dados pessoais sensíveis sejam protegidos ou anonimizados, conforme necessário.

O SIC da UFRJ é um mecanismo essencial para garantir o direito de acesso à informação e promover uma gestão pública mais transparente e participativa, sempre em consonância com as exigências legais relativas à privacidade e proteção de dados. Porém, o desafio que surge é justamente o equilíbrio entre essa transparência e a proteção de dados pessoais. A UFRJ precisa, ao disponibilizar informações públicas, garantir que nenhum dado pessoal sensível seja exposto de maneira inadequada. Para lidar com essa questão, a universidade implementou

[51] No link https://ufrj.br/acesso-a-informacao/ é possível acessar as principais informações da UFRJ. Se o conteúdo desejado não estiver disponível, o cidadão pode solicitá-lo por meio do Serviço de Informação ao Cidadão (SIC). Basta apenas que se identifique e especifique o seu pedido de informação; não é preciso justificar o pedido.

procedimentos de anonimização e pseudonimização de dados, técnicas recomendadas pela LGPD para proteger a privacidade dos cidadãos enquanto atende às demandas de transparência.

Portanto, atualmente o principal desafio para a UFRJ tem sido encontrar o ponto de equilíbrio entre a necessidade de garantir a privacidade dos dados pessoais e o dever de transparência, especialmente em um contexto de crescente cobrança por *accountability* por parte da sociedade. Para enfrentar essa situação, a universidade tem investido em uma governança de dados que inclui a revisão constante de suas políticas de proteção de dados e transparência, assegurando que ambas as legislações sejam observadas de maneira integrada.

Um exemplo prático desse equilíbrio pode ser observado nos pedidos de acesso à informação feitos por cidadãos à UFRJ por meio do Serviço de Informações ao Cidadão (SIC). Em muitos casos, esses pedidos envolvem o acesso a informações que podem conter dados pessoais, como lista de aprovados em concursos públicos ou informações sobre processos administrativos. A universidade adota um procedimento no qual esses pedidos são cuidadosamente analisados, considerando os princípios da LGPD e da LAI. Quando necessário, os dados pessoais são anonimizados antes da divulgação, garantindo que a privacidade dos envolvidos seja protegida, sem comprometer o direito de acesso à informação.

Responsável pelo atendimento das demandas do SIC, a Ouvidoria-Geral da UFRJ da UFRJ desempenha um papel fundamental no gerenciamento dessa tensão. Ela atua como um canal de comunicação entre a universidade e a sociedade, recebendo sugestões, reclamações e pedidos de informação. Nesse processo, a ouvidoria também deve seguir os protocolos da LGPD, assegurando que dados pessoais não sejam indevidamente divulgados. Entre suas atribuições estão receber e gerenciar manifestações; analisar e encaminhar denúncias; fiscalizar o cumprimento da LAI; proteger dados pessoais e atuar como mediadora.

Contudo, a atuação da Ouvidoria da UFRJ foi ampliada após a promulgação da LGPD, que trouxe a necessidade de proteger e gerenciar adequadamente os dados pessoais no contexto do acesso à informação. Nesse sentido, a Ouvidoria exerce um papel de equilíbrio entre o direito à transparência pública e o direito à privacidade. Ao receber reclamações, denúncias ou pedidos de informação que contenham dados pessoais, a Ouvidoria deve garantir que tais dados sejam tratados de forma segura e que apenas as informações estritamente necessárias sejam divulgadas. Isso envolve a adoção de medidas de anonimização ou pseudonimização de dados quando necessário, especialmente em casos que envolvem informações sensíveis de cidadãos, como processos administrativos, históricos acadêmicos ou documentos de saúde.

A Ouvidoria também tem o papel de promover a conscientização da comunidade acadêmica sobre a importância da proteção de dados pessoais. Ela atua como um canal de orientação tanto para os servidores quanto para os cidadãos sobre como as informações pessoais devem ser tratadas dentro dos limites da LGPD e da LAI. Ainda, trabalha em conjunto com o Encarregado de Proteção de Dados (DPO) da UFRJ, figura exigida pela LGPD para supervisionar o cumprimento das normas de proteção de dados. Essa cooperação é essencial para garantir que as demandas relacionadas a dados pessoais sejam gerenciadas de forma adequada, minimizando riscos de vazamentos ou violações de privacidade.

Caso haja denúncias ou reclamações de violação de privacidade, a Ouvidoria é responsável por encaminhar essas demandas para o setor de Proteção de Dados ou para as instâncias superiores da UFRJ, assegurando que os processos sejam devidamente investigados e que medidas corretivas sejam adotadas. A Ouvidoria também tem um papel pedagógico dentro da universidade, promovendo a disseminação de boas práticas de governança, orientando sobre a aplicação da LAI e da LGPD e garantindo que a comunidade acadêmica esteja ciente das suas responsabilidades legais em relação ao tratamento de dados pessoais.

Em um cenário onde o acesso à informação é regra e o sigilo é exceção, o grande desafio da Ouvidoria, dentro desse novo contexto normativo, é conciliar a exigência de transparência trazida pela LAI com a necessidade de proteger os dados pessoais, conforme a LGPD. Nesse cenário, a Ouvidoria atua como um órgão facilitador, garantindo que a UFRJ continue sendo transparente e responsável perante a sociedade, ao mesmo tempo que protege os direitos à privacidade e à segurança de informações pessoais.

3.2. Análise das Demandas do SIC-UFRJ

O Serviço de Informação ao Cidadão (SIC) da Universidade Federal do Rio de Janeiro (UFRJ) foi criado em 2012, em cumprimento à Lei de Acesso à Informação (LAI), que entrou em vigor no Brasil em 16 de maio de 2012. A Ouvidoria-Geral da UFRJ ficou responsável pela implementação da LAI e pelo SIC na instituição, passos importantes na efetivação de uma política pública de transparência na universidade.[52]

[52] Para mais detalhes sobre a implantação do SIC na UFRJ, veja Memórias da Ouvidoria: Aprendizados de 2009 a 2021, elaborado pela então Ouvidora-Geral da UFRJ, Cristina Ayoub Riche. Veja informações no Link: http://www.ouvidoria.ufrj.br/images/_ouvidoria/documentos/Memorias_da_Ouvidoria_UFRJ.pdf

A implementação do SIC visou facilitar a solicitação de informações e atender aos princípios da LAI, assegurando que qualquer pessoa pudesse acessar dados públicos relacionados à gestão da universidade, como contratos, convênios, despesas e outras informações relevantes. O SIC funciona como um canal estruturado para atender às demandas de acesso à informação e promover a transparência na gestão pública universitária.

A Coordenação do Serviço de Informação ao Cidadão da UFRJ atende a pedidos de informação pública, requeridos com base na Lei n. 12.527/2011, regulamentada pelo Decreto nº. 7.724/2012, e desenvolve atividades diretamente ligadas à transparência institucional, por meio da transparência ativa e passiva. De acordo com o art. 40 da LAI, cada órgão designa uma autoridade para assegurar o cumprimento das normas relativas ao acesso à informação. Na UFRJ, a autoridade de monitoramento é também a Ouvidora-Geral da Universidade, conforme a Portaria nº 4, de 7 de janeiro de 2022.[53]

Importante destacar o importante trabalho do SIC durante esses anos no que tange à transparência e acesso à informação. De 15/05/2012 a 29 de setembro de 2024, o Serviço de Informação ao Cidadão recebeu 4.614 pedidos de informação; desses, 99,567 foram respondidos, 0,433% em tramitação.

Gráfico a seguir mostra a evolução dos pedidos no período mencionado.

Fonte: https://centralpaineis.cgu.gov.br/visualizar/lai

53 Designa Autoridade de Monitoramento da LAI na UFRJ, nos termos da Lei de Acesso à Informação. A Publicação da Portaria está no link https://ufrj.br/wp-content/uploads/2022/07/Portaria-UFRJ-no-5-de-7-de-janeiro-de-2022.pdf.

Do total de pedidos, 71.09% deles teve o acesso concedido. Os demais tiveram o acesso negado ou parcialmente concedidos. Houve também situações diversas que impediram o demandante a ter acesso ao dado solicitado, tais como: informação inexistente; não se tratava de solicitação de informação nos termos da LAI; pergunta duplicada ou o órgão não tinha competência para responder sobre o assunto, conforme mostrado no gráfico a seguir.

Decisão da Manifestação	%Pedidos Respondidos (decisão)
Acesso Concedido	71,09%
Acesso Negado	7,90%
Acesso Parcialmente Concedido	3,53%
Informação Inexistente	3,96%
Não se trata de solicitação de informação	5,72%
Órgão não tem competência para responder sobre o assunto	6,01%
Pergunta Duplicada/Repetida	1,78%

Fonte: https://centralpaineis.cgu.gov.br/visualizar/lai

A classificação da decisão, em tese, sem analisar o teor das demandas, está fundamentada na LAI, conforme dados do gráfico a seguir.

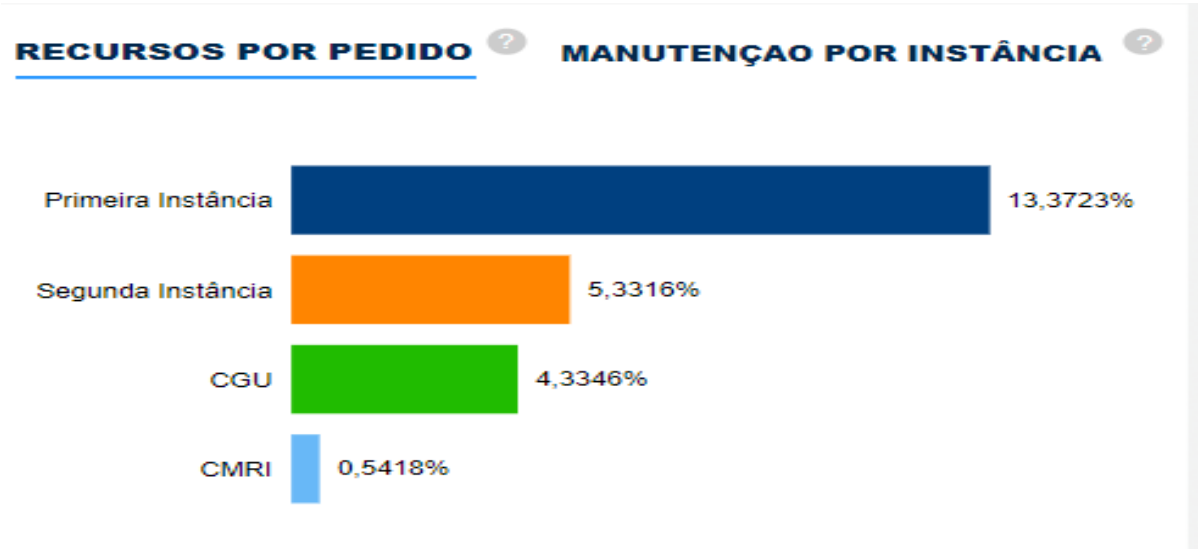
Classificação da decisão	Percentual	Quantidade Total
Pedido genérico	2,46%	113
Parte da informação demandará mais tempo para produção	1,68%	77
Dados pessoais	1,41%	65
Pedido incompreensível	1,39%	64
Parte da informação inexistente	0,85%	39
Informação sigilosa de acordo com legislação específica	0,83%	38
Pedido desproporcional ou desarrazoado	0,78%	36
Pedido exige tratamento adicional de dados	0,54%	25
Processo decisório em curso	0,41%	19
Parte do pedido é genérico	0,26%	12
Informação sigilosa classificada conforme a Lei 12.527/2011	0,17%	8
Parte da informação é de competência de outro órgão/entidade	0,17%	8
Parte da informação contém dados pessoais	0,15%	7
Parte da informação é sigilosa de acordo com legislação específica	0,13%	6
Parte do pedido é incompreensível	0,11%	5
Parte da informação é sigilosa e classificada conforme a Lei 12.527/2011	0,04%	2
Parte do pedido é desproporcional ou desarrazoado	0,02%	1

Fonte: https://centralpaineis.cgu.gov.br/visualizar/lai

Importante ressaltar que, no período de 2012 a 2024, 1,41% dos pedidos teve seu acesso indeferido por motivo de dados pessoais; 0,83% indeferido por motivo de informação sigilosa de acordo com legislação específica e 0,17% por constar informação sigilosa nos termos da lei 12.527/2011 (LAI).

Do total dos pedidos, deferidos e indeferidos, foram impetrados, no período de 2012 a 2024, 1088 recursos: 13,37% à UFRJ, em 1ª instância; 5,33% à UFRJ, em 2ª instância (ao chefe máximo da Instituição); 4,33% à CGU, em 3ª instância e 0,5418 à Comissão Mista de Reavaliação de Informações (CRMI).

Fonte: https://centralpaineis.cgu.gov.br/visualizar/lai



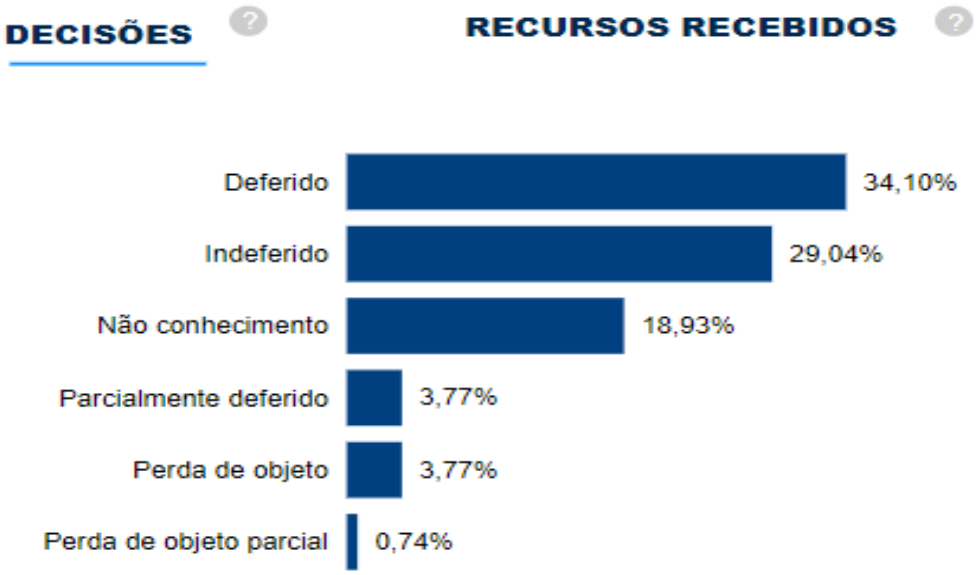
Fonte: https://centralpaineis.cgu.gov.br/visualizar/

Os motivos para a impetração de recursos foram vários, conforme dados da tabela a seguir.

Tipo do Recurso	%GT QtdRecursos
Informação incompleta	49,82%
Informação recebida não corresponde à solicitada	22,24%
Outros	15,53%
Resposta não foi dada no prazo	4,32%
Justificativa para o sigilo insatisfatória/não informada	4,14%
Ausência de justificativa legal para classificação	1,47%
Informação recebida por meio diferente do solicitado	1,10%
Informação classificada por autoridade sem competência	1,01%
Grau de sigilo não informado	0,28%
Grau de classificação inexistente	0,09%

Fonte: https://centralpaineis.cgu.gov.br/visualizar/lai

Dos recursos apresentados, nem todos foram deferidos, ou pela UFRJ ou pela CGU ou pela CMRI. Eis os dados da tabela:



Fonte: https://centralpaineis.cgu.gov.br/visualizar/lai

Ao se fazer um recorte e uma análise paralela de dois períodos, ou seja, de antes e depois do advento da LGPD, o cenário que se apresenta é este:

Período: maio de 2012 a agosto de 2020

Decisão da Manifestação	%Pedidos Respondidos (decisão)
Acesso Concedido	71,36%
Acesso Negado	7,12%
Acesso Parcialmente Concedido	3,75%
Informação Inexistente	1,86%
Não se trata de solicitação de informação	6,38%
Órgão não tem competência para responder sobre o assunto	7,22%
Pergunta Duplicada/Repetida	2,31%

Classificação da decisão	Percentual	Quantidade Total
Pedido genérico	2,60%	81
Parte da informação demandará mais tempo para produção	2,12%	66
Dados pessoais	1,44%	45
Pedido incompreensível	1,28%	40
Parte da informação inexistente	0,64%	20
Pedido exige tratamento adicional de dados	0,61%	19
Pedido desproporcional ou desarrazoado	0,45%	14
Parte do pedido é genérico	0,38%	12
Informação sigilosa de acordo com legislação específica	0,32%	10
Informação sigilosa classificada conforme a Lei 12.527/2011	0,26%	8
Parte da informação é de competência de outro órgão/entidade	0,22%	7
Processo decisório em curso	0,19%	6
Parte da informação contém dados pessoais	0,13%	4
Parte da informação é sigilosa de acordo com legislação específica	0,10%	3
Parte do pedido é incompreensível	0,10%	3
Parte da informação é sigilosa e classificada conforme a Lei 12.527/2011	0,03%	1

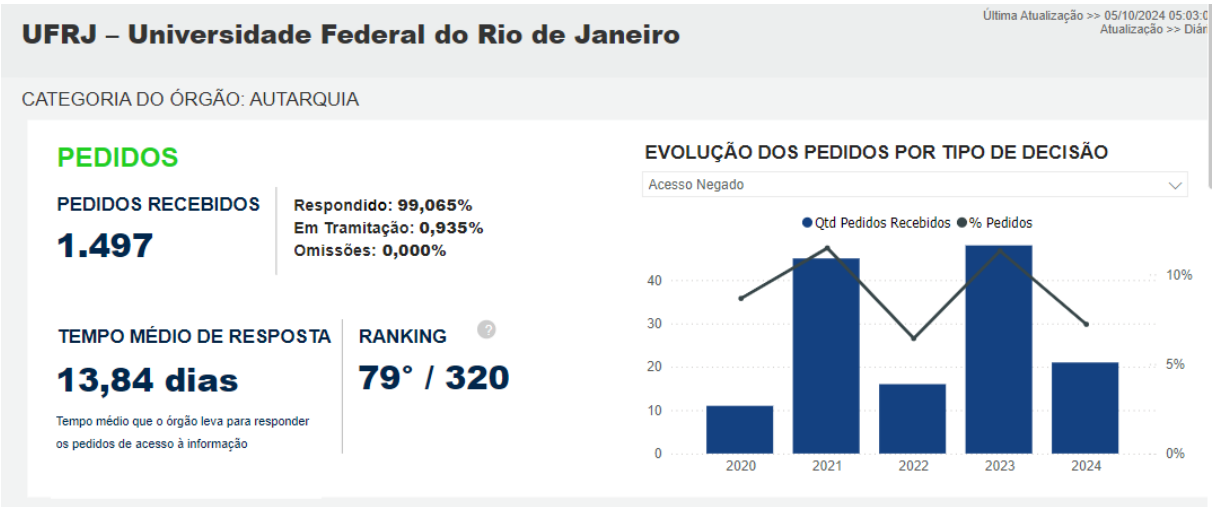
Fonte: https://centralpaineis.cgu.gov.br/visualizar/lai

Analisando o período de maio de 2012, quando o serviço de informação ao cidadão foi implantado na UFRJ, até agosto de 2020, antes de a LGPD entrar em vigor, a universidade

recebeu 3.118 pedidos de informação. Desse total, 71,36% dos pedidos foram deferidos; o restante, indeferido ou parcialmente deferido por vários motivos; dentre eles, 1,44% por conter dados pessoais e 0,13% por parte da informação conter dados pessoais. Importante destacar que apesar de parte da informação conter dados pessoais, o acesso à informação foi negado, ou seja, não houve, por parte do SIC, a providência de tarjar as informações pessoais e disponibilizar as demais informações na demanda específica.

Em um outro cenário, com a LGPD em vigor, analisando os pedidos de informação, no período de agosto de 2020 a setembro de 2024, a UFRJ recebeu 1.497 pedidos. Desse total, 70,60% dos pedidos foram deferidos; o restante, indeferido ou parcialmente deferidos por vários motivos; dentre eles, 1,35% por conter dados pessoais e 0,20% por parte da informação conter dados pessoais. Também importante destacar que apesar de parte da informação conter dados pessoais, o acesso à informação foi negado. Da mesma forma, não foi disponibilizada a informação pública com o tarjamento dos dados pessoais. Outra observação é que não houve alteração significativa no percentual de demandas indeferidas por conter dados pessoais, no período anterior e posterior ao advento da LGPD, levantando-se a hipótese de que a Lei Geral de Proteção de Dados não aumentou o número de negativas de acesso à informação no SIC-UFRJ.

Período: setembro de 2020 a setembro de 2024



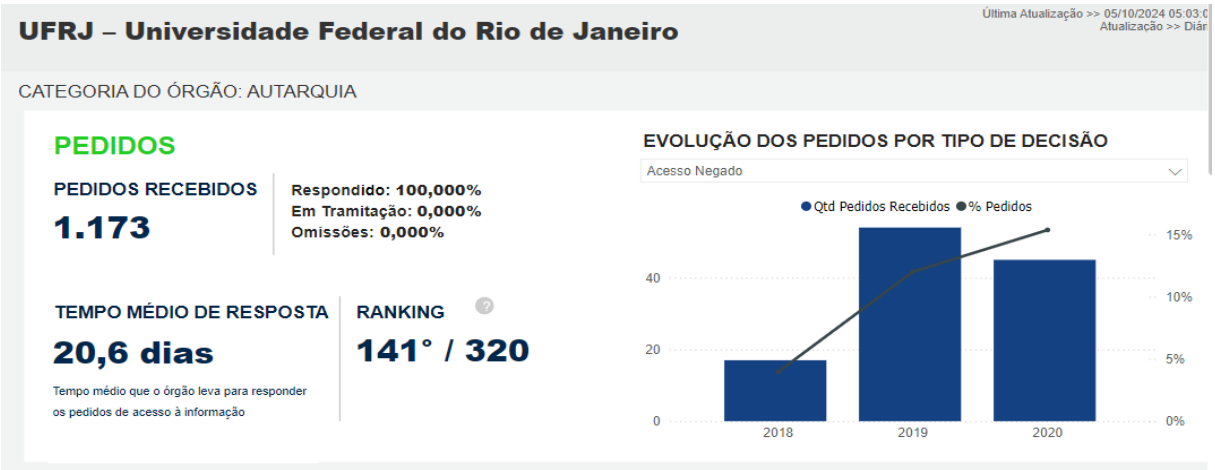
Decisão da Manifestação	%Pedidos Respondidos (decisão)
Acesso Concedido	70,60%
Acesso Negado	9,51%
Acesso Parcialmente Concedido	3,03%
Informação Inexistente	8,43%
Não se trata de solicitação de informação	4,32%
Órgão não tem competência para responder sobre o assunto	3,44%
Pergunta Duplicada/Repetida	0,67%

Classificação da decisão	Percentual	Quantidade Total
Pedido genérico	2,16%	32
Informação sigilosa de acordo com legislação específica	1,89%	28
Pedido incompreensível	1,62%	24
Pedido desproporcional ou desarrazoado	1,48%	22
Dados pessoais	1,35%	20
Parte da informação inexistente	1,28%	19
Processo decisório em curso	0,88%	13
Parte da informação demandará mais tempo para produção	0,74%	11
Pedido exige tratamento adicional de dados	0,40%	6
Parte da informação contém dados pessoais	0,20%	3
Parte da informação é sigilosa de acordo com legislação específica	0,20%	3
Parte do pedido é incompreensível	0,13%	2
Parte da informação é de competência de outro órgão/entidade	0,07%	1
Parte da informação é sigilosa e classificada conforme a Lei 12.527/2011	0,07%	1

Fonte: https://centralpaineis.cgu.gov.br/visualizar/lai

Analisando, mais especificamente, os pedidos de informação do SIC-UFRJ, incluindo os números de demandas e a análise do teor dos pedidos no período de janeiro de 2018 a dezembro de 2023, temos o seguinte cenário, antes e depois da LGPD.

Período: janeiro de 2018 a agosto de 2020 (antes da LGPD)



Decisão da Manifestação	%Pedidos Respondidos (decisão)
Acesso Concedido	78,09%
Acesso Negado	9,89%
Acesso Parcialmente Concedido	3,41%
Informação Inexistente	2,90%
Não se trata de solicitação de informação	3,24%
Órgão não tem competência para responder sobre o assunto	1,45%
Pergunta Duplicada/Repetida	1,02%

Classificação da decisão	Percentual	Quantidade Total
Pedido genérico	3,58%	42
Dados pessoais	2,81%	33
Parte da informação inexistente	1,45%	17
Parte da informação demandará mais tempo para produção	1,02%	12
Pedido incompreensível	0,94%	11
Pedido desproporcional ou desarrazoado	0,85%	10
Informação sigilosa classificada conforme a Lei 12.527/2011	0,60%	7
Informação sigilosa de acordo com legislação específica	0,60%	7
Parte do pedido é genérico	0,43%	5
Processo decisório em curso	0,34%	4
Parte da informação contém dados pessoais	0,17%	2
Parte da informação é sigilosa de acordo com legislação específica	0,17%	2
Pedido exige tratamento adicional de dados	0,17%	2
Parte da informação é de competência de outro órgão/entidade	0,09%	1

Fonte: https://centralpaineis.cgu.gov.br/visualizar/lai

De janeiro de 2018 a agosto de 2020, antes de a LGPD entrar em vigor, do total de 1.173 pedidos de informação recebidos pela UFRJ, 78,09% foram concedidos. Do total de pedidos negados ou parcialmente concedidos, 2,81% continham dados pessoais e 0,17 continham parte das informações com dado pessoal. De setembro de 2020 a dezembro de 2023, já com a LGPD em vigor, do total de 1.192 pedidos de acesso à informação, 1,59% foram negados por conter dados pessoais e 0,25% por parte da informação conter tais dados.

Período: setembro de 2020 a dezembro de 2023.

Decisão da Manifestação	%Pedidos Respondidos (decisão)
Acesso Concedido	69,30%
Acesso Negado	10,07%
Acesso Parcialmente Concedido	2,85%
Informação Inexistente	7,97%
Não se trata de solicitação de informação	5,03%
Órgão não tem competência para responder sobre o assunto	3,94%
Pergunta Duplicada/Repetida	0,84%

Classificação da decisão	Percentual	Quantidade Total
Pedido genérico	2,60%	31
Informação sigilosa de acordo com legislação específica	1,93%	23
Pedido incompreensível	1,68%	20
Dados pessoais	1,59%	19
Pedido desproporcional ou desarrazoado	1,43%	17
Parte da informação inexistente	1,34%	16
Parte da informação demandará mais tempo para produção	0,67%	8
Processo decisório em curso	0,50%	6
Pedido exige tratamento adicional de dados	0,42%	5
Parte da informação contém dados pessoais	0,25%	3
Parte da informação é sigilosa de acordo com legislação específica	0,25%	3
Parte da informação é de competência de outro órgão/entidade	0,08%	1
Parte da informação é sigilosa e classificada conforme a Lei 12.527/2011	0,08%	1
Parte do pedido é incompreensível	0,08%	1

Fonte: https://centralpaineis.cgu.gov.br/visualizar/lai

Da análise desses números, verifica-se que não houve alteração significativa quanto ao número de indeferimentos de pedido de acesso à informação por conter dados pessoais, vislumbrando-se, desta forma, a hipótese de que a LGPD não alterou o cenário de acesso à informação no âmbito da UFRJ, no que tange aos motivos de negativa de acesso aos dados.

Quanto ao teor das demandas analisadas, no período de 2018 a 2023, destacam-se algumas que exemplificam negativas de acesso à informação por conter dados pessoais. Sobre tais demandas, foram impetrados recursos à CGU, que acabou por deferir totalmente alguns desses recursos; outros, parcialmente, como veremos a seguir.

O Recurso nº 23480.011558/2018-06[54] trata de pedido de acesso à informação em que o requerente solicita os nomes e as informações referentes aos sujeitos pesquisados no âmbito

[54] Mais detalhes no link https://buscaprecedentes.cgu.gov.br/

da pesquisa acadêmica “Lesbocídio: as histórias que ninguém conta”, realizada no âmbito da Universidade Federal do Rio de Janeiro (UFRJ). [55]

O requerente solicitou os nomes e as informações das pessoas envolvidas nos 126 crimes de ódio contra mulheres homossexuais entre 2014 e 2017, no âmbito da pesquisa acadêmica, coordenada pela Dra. Maria Clara Marques Dias do Instituto de Filosofia e Ciências Sociais.

O SIC da UFRJ negou o acesso às informações solicitadas, pois entendeu que a referida pesquisa não se encontrava submetida ao escopo de aplicação da Lei nº 12.527/11, por não receber qualquer subsídio governamental, e que a demanda objetivava o acesso a informações pessoais sensíveis de terceiras pessoas, o que iria de encontro ao disposto no artigo 31 da Lei de Acesso à Informação. Nesse sentido, esclareceu-se que a divulgação dos dados solicitados poderia implicar risco ao exercício e gozo dos direitos de personalidade inscritos no art. 5º, X da Constituição Federal, especialmente porque tratam de informações que estão diretamente relacionadas à imagem das vítimas e que tiveram impacto negativo diante de seus familiares.

Por sua vez, ao analisar o recurso impetrado pelo requerente, a CGU opinou, inicialmente, no Parecer n. 2333 de 19/11/2028, pelo provimento parcial, de modo que fossem disponibilizados ao requerente os dados coletados no âmbito da pesquisa “Lesbocídio: as histórias que ninguém conta” em relação à idade da vítima, cidade/estado/região onde o caso ocorreu, a profissão da vítima, o método do assassinato, o vínculo com o assassino, o sexo do assassino, o tipo de lésbica e a raça/etnia da lésbica assassinada, bem como o número do processo judicial ao qual o crime se refere, proibindo-se a identificação da vítima ou do assassino, de modo que estas informações sejam tarjadas ou desidentificadas, nos termos do artigo 31, § 3º, III da Lei nº 12.527/2011 c/c o artigo 2º, VI, da Resolução nº 510, de 07 de abril de 2016, do Conselho Nacional de Saúde.

Posteriormente, a CGU emitiu o Parecer de Revisão (N. 38/2019) que decidiu pela revisão de ofício da decisão exarada no Parecer n. 2333 de 19/11/2018, mantendo- se o provimento parcial do recurso, alterando-se apenas o escopo dos dados a serem disponibilizados

[55] O projeto de pesquisa “Lesbocídio: As Histórias que Ninguém Conta” é uma iniciativa acadêmica da Universidade Federal do Rio de Janeiro (UFRJ), que visa resgatar informações e registrar casos de lesbocídios no Brasil, com ênfase nos assassinatos de lésbicas. O projeto resultou na elaboração de um dossiê que foi apresentado durante uma reunião do Conselho Nacional de Combate à Discriminação e Promoção dos Direitos de LGBT, órgão vinculado ao Ministério dos Direitos Humanos e da Cidadania. Para mais detalhes, acesse o link https://www.gov.br/mdh/pt-br/assuntos/noticias/2018/agosto/dossie-sobre-lesbocidios-no-brasil-e-apresentado-durante-reuniao-do-cndc-lgbt-orgao-que-compoe-a-estrutura-do-mdh?utm_source=chatgpt.com.

ao requerente. A revisão do Parecer ocorreu por conta da existência de contenda judicial entre as autoras da pesquisa e o requerente (processo 0027541- 28.2018.8.19.0210), e foi relativa aos dados sobre região ou cidade onde ocorreu o crime e os números dos processos judiciais aos quais os crimes se referem. No primeiro caso, a especificação do espaço geográfico poderia vulnerabilizar a identidade das vítimas, o que estaria em desacordo com o disposto no artigo 31 da Lei no 12.527/2011. No segundo caso, o número dos processos poderia levar o requerente a conhecer a orientação sexual dos indivíduos citados nos documentos. Segundo a CGU, a possibilidade de aferimento da relação entre pessoas e sua orientação sexual é, por si só, razão suficiente para que se verifique a potencialidade de dano ao direito à intimidade de terceiras pessoas.

Por fim, a CGU decidiu que deveriam ser disponibilizados ao solicitante o nome descaracterizado dos sujeitos das pesquisas, identificando-os apenas pelas letras iniciais de seus nomes, o estado onde o caso ocorreu, a profissão da vítima, o vínculo com o assassino, o sexo do assassino, o tipo de lésbica e a raça/etnia da lésbica assassinada.[56]

A decisão da Controladoria-Geral da União (CGU) mostra-se acertada ao permitir a divulgação de parte das informações da pesquisa, mas ao mesmo tempo restringir a divulgação de vários dados dos envolvidos. A Constituição Federal, em seu artigo 5º, inciso X, assegura que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas". A divulgação dos nomes dos envolvidos em uma pesquisa pode constituir uma violação desse direito fundamental, uma vez que expõe dados pessoais e sensíveis, o que pode prejudicar a integridade e a segurança das pessoas envolvidas. A LGPD também estabelece o princípio da necessidade, que determina que o tratamento de dados deve se limitar ao mínimo necessário para atingir os objetivos específicos da pesquisa ou da atividade. No caso da pesquisa, a divulgação de informações relacionadas à temática ou ao conteúdo da pesquisa, sem identificar os envolvidos, já é suficiente para garantir a transparência e o direito à informação pública, sem que se viole a privacidade dos cidadãos.

Por sua vez, há também o risco de identificação indireta. Mesmo que os nomes dos envolvidos não sejam divulgados, a combinação de outros dados de uma pesquisa pode, em algumas circunstâncias, possibilitar a identificação indireta dos participantes. A divulgação de informações que permitam essa identificação pode ser vista como um risco à privacidade das

[56] Para analisar mais detalhes da decisão, acesse o link https://buscaprecedentes.cgu.gov.br/?idAnexo=51174&fileName=Decisão%20nº%2048-2019-NUP%2023480.011558-2018-06.pdf&handler=DownloadFile.

pessoas envolvidas, o que justificaria a restrição da divulgação de tais dados, conforme prevê a LGPD.

Outro caso analisado foi o do recurso nº 23480.020672/2020-33[57], em que o requerente solicita informações acerca de pagamentos pendentes de exercícios anteriores cadastrados no SIAPE, não tendo sido disponibilizada a lista contendo os nomes dos servidores e os respectivos valores que cada um tem direito.

Em resposta ao pedido inicial e aos recursos interpostos, o SIC da UFRJ negou acesso a essa parte do pedido por entender envolver informação pessoal de servidores, cujo acesso é restrito, com base no art. 55 do Decreto nº 7724/2012. Em virtude da negativa de acesso, o requerente apresentou recurso à Controladoria-Geral da União – CGU, reiterando sua solicitação. Por sua vez, após análise do recurso, a CGU opinou pelo conhecimento e, no mérito, pelo seu provimento quanto à disponibilização de lista contendo os nomes dos servidores e dos respectivos valores a receber em cada um dos processos referentes a pagamentos pendentes de exercícios anteriores de servidores lotados na UFRJ, com fundamento no art. 7º, inciso II e VII da Lei nº 12.527/2011.[58]

Importante destacar que neste caso, antes mesmo da decisão do Órgão de Controle**,** a Reitoria da Universidade solicitou Parecer Jurídico à sua Procuradoria, que foi favorável à divulgação das informações solicitadas pelo requerente. Com isso, a Universidade reavaliou o seu posicionamento inicial e decidiu pela disponibilização dos dados pendentes. [59]

A possibilidade de divulgação de pagamentos pendentes de exercícios anteriores na administração pública, especificamente na UFRJ, deve ser analisada à luz dos princípios da transparência e da publicidade previstos na Constituição Federal, na Lei de Acesso à Informação e nas diretrizes da Lei de Responsabilidade Fiscal (Lei Complementar nº 101/2000).

A Constituição Federal de 1988, em seu artigo 37, impõe que a administração pública deve seguir os princípios da legalidade, impessoalidade, moralidade, publicidade e eficiência.

---

[57] Mais detalhes no link https://buscaprecedentes.cgu.gov.br/.

[58] Art. 7º O acesso à informação de que trata esta Lei compreende, entre outros, os direitos de obter: II - informação contida em registros ou documentos, produzidos ou acumulados por seus órgãos ou entidades, recolhidos ou não a arquivos públicos; VII - informação relativa: a) à implementação, acompanhamento e resultados dos programas, projetos e ações dos órgãos e entidades públicas, bem como metas e indicadores propostos;
b) ao resultado de inspeções, auditorias, prestações e tomadas de contas realizadas pelos órgãos de controle interno e externo, incluindo prestações de contas relativas a exercícios anteriores.

[59] Mais detalhes sobre a decisão da UFRJ e da CGU, veja link https://buscaprecedentes.cgu.gov.br/?idAnexo=67845&fileName=SEI_23480.020672_2020_33.pdf&handler=DownloadFile.

A publicidade dos atos administrativos, especialmente no que diz respeito a despesas e pagamentos, é fundamental para garantir a transparência na gestão pública e a fiscalização por parte da sociedade. A divulgação de pagamentos pendentes de exercícios anteriores na UFRJ, portanto, estaria em consonância com esse princípio, uma vez que a sociedade tem o direito de saber como os recursos públicos estão sendo administrados, incluindo as dívidas e pendências financeiras da instituição.

Por sua vez, a Lei nº 12.527/2011 assegura a todos os cidadãos o direito de obter informações dos órgãos públicos, com exceções específicas para proteger informações pessoais, sigilosas ou que possam prejudicar a segurança da sociedade e do Estado. A LAI, ao estabelecer um regime de acesso amplo e irrestrito à informação, fortalece a transparência e possibilita que cidadãos, jornalistas, pesquisadores e outras partes interessadas possam acessar informações detalhadas sobre as finanças públicas, incluindo os pagamentos pendentes de exercícios anteriores. O artigo 8º da LAI determina que as informações sobre a execução orçamentária e financeira dos órgãos públicos sejam divulgadas de forma proativa. Isso inclui dados sobre as obrigações pendentes, o que é uma prática que contribui para a prestação de contas de uma administração pública eficiente e ética.

A Lei Complementar nº 101/2000, conhecida como Lei de Responsabilidade Fiscal (LRF), estabelece que o planejamento, a execução e o controle das finanças públicas devem ser feitos de forma responsável. A LRF também exige a publicação de relatórios fiscais periódicos que detalham a execução orçamentária e financeira dos órgãos públicos. A divulgação de pagamentos pendentes de exercícios anteriores contribui para o cumprimento das metas fiscais e facilita o acompanhamento da regularização dessas pendências no planejamento orçamentário das administrações públicas.

Portanto, a divulgação de pagamentos pendentes de exercícios anteriores na UFRJ não só é compatível com os princípios da transparência e publicidade previstos na Constituição Federal, mas também está em conformidade com a Lei de Acesso à Informação e a Lei de Responsabilidade Fiscal. A divulgação dessas informações é plenamente legal, vantajosa e deve ser incentivada como parte do compromisso com a boa gestão e com a transparência pública.

Mais uma demanda analisada se refere ao recurso nº 23480.005044/2020-28[60], que trata de pedido dirigido à Universidade Federal do Rio de Janeiro UFRJ, no qual o cidadão requer acesso a um processo administrativo, que autoriza o afastamento do país de servidora para participar de congresso internacional, em Vancouver/Canadá - com ônus para a FAPERJ.

[60] Mais detalhes sobre o assunto podem ser obtidos por meio do link https://buscaprecedentes.cgu.gov.br/

Inicialmente, o SIC da universidade negou o acesso à informação sob os seguintes fundamentos: não havia amparo legal para fornecer a cópia do processo a terceiro, que não é parte interessada nos autos e que, no processo requerido, constam dados pessoais que devem ser protegidos nos termos do art. 31. § 1º, incisos I e II. Da Lei nº 12.527/2011. Por sua vez, ao analisar o recurso do demandante, a CGU opinou pelo conhecimento e, no mérito, pelo provimento parcial, para que fosse franqueado o acesso ao processo de número 23079.202791/2020-54, por se tratar de informação pública, na forma do art. 7º, inciso II, § 2º da Lei nº 12.527/2011, mantendo-se a restrição de acesso em relação às informações pessoais constantes dos autos que devem ser tarjadas, com fundamento no art. 31, § 1º, inciso I da mesma lei.[61]

Importante mencionar que, após analisar o recurso impetrado pelo requerente à CGU, em 3ª instância, o SIC da UFRJ, de forma proativa, enviou mensagem à CGU e encaminhou o processo solicitado, para que fosse disponibilizado ao requerente. Essa conduta, segundo a Controladoria-Geral da União, demonstrou o interesse do órgão em cumprir o disposto na Lei no 12.527/2011 e em franquear o acesso à informação que avalia que tem natureza pública.

Ainda, fora analisado o recurso nº 23546.078808/2023-35[62], que trata de pedido de informação dirigido à Universidade Federal do Rio de Janeiro - UFRJ, por meio do qual a cidadã requer acesso à ata da aplicação de prova do concurso público edital 491/2023, cargo técnico de laboratório - biomedicina, realizada no dia 03/09/2023, na faculdade de Letras, bloco H, sala 222. O Serviço de Informação ao Cidadão da UFRJ negou o acesso à informação pois entendeu que o documento requerido é de uso exclusivo da Comissão do Concurso em pauta. Explicou que compõem o documento diversas informações, das quais destacou: os horários praticados; o controle de candidatos presentes e ausentes; os registros de ocorrências na aplicação da prova e até mesmo dados sobre os candidatos presentes na aplicação da prova. Arguiu que a justificativa para negar o acesso à ata requerida foi pautada no fato de que o documento, assim como outros relacionados a concursos públicos podem conter dados pessoais sensíveis, o que inviabiliza a sua divulgação.

A CGU, no entanto, Opinou pelo conhecimento do recurso e, no mérito, pelo provimento parcial, com fundamento no art. 7º, inciso II e §2º da Lei nº 12.527/2011, para que fosse franqueado o acesso à ata da aplicação de prova do concurso público - edital 491/2023, cargo técnico de laboratório - biomedicina, realizada no dia 03/09/2023, na faculdade de Letras,

[61] Para verificar mais detalhes sobre a decisão da CGU, veja o link https://buscaprecedentes.cgu.gov.br/?idAnexo=61476&fileName=CGU_23480005044202028_UFRJ..pdf&handler=DownloadFile.

[62] Veja mais detalhes no link https://buscaprecedentes.cgu.gov.br/

bloco H, sala 222, com o tarjamento, estritamente, de informações pessoais sensíveis e de dados biográficos inerentes a aspectos da vida privada do titular que, eventualmente, sejam constantes do documento, tais como: CPF, número de identidade, endereço físicos e de correios eletrônicos, assinaturas, etc, em atendimento ao disposto no art. 31, § 1º, inciso I da mesma lei.

O Órgão de Controle argumentou que que este pedido de informação perpassa pelas disposições do Enunciado CGU nº 08/2023, cujo teor define que os documentos e informações relacionados a candidatos aprovados em seleções para o provimento de cargos públicos, inclusive provas orais, são passíveis de acesso público, visto que a transparência dos processos seletivos está diretamente relacionada à promoção dos controles administrativo e social da Administração Pública, ressalvadas as informações pessoais sensíveis.

O entendimento é que deve ser garantida a publicidade dos documentos diretamente relacionados a concursos públicos, para que seja possível exercer o controle administrativo e social do processo. Neste caso, o interesse público, quando se refere a concursos, prevalece sobre a proteção da intimidade e da privacidade dos candidatos, uma vez que é necessário fornecer os meios que viabilizem o controle e a fiscalização dos procedimentos de ocupação de cargos públicos.

Além disso, é importante destacar que a UFRJ alegou a presença de dados pessoais no conteúdo da ata e que o documento precisava ser tratado para que esses dados fossem removidos. Contudo, a CGU destacou que os nomes dos candidatos e dos servidores responsáveis pela aplicação da prova, isoladamente, não configuram uma informação pessoal. Portanto, só seria necessário o ocultamento caso o nome de uma pessoa estivesse vinculado a uma informação sensível, conforme previsto no artigo 5º, inciso II, da Lei nº 13.709/2018.

No Parecer, a CGU destacou que a LAI e a LGPD são normas que se complementam de maneira harmoniosa. O Enunciado nº 04/2022 da Controladoria-Geral da União reforça essa compatibilidade ao afirmar que "a LAI, a Lei nº 14.129/2021 (Lei de Governo Digital) e a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) são sistematicamente compatíveis entre si e harmonizam os direitos fundamentais do acesso à informação, da intimidade e da proteção aos dados pessoais, não existindo antinomia entre seus dispositivos."

Assim, quando o documento contiver dados pessoais, deve-se garantir o acesso à parte não sigilosa, ocultando-se apenas o conteúdo protegido por sigilo, conforme orienta o art. 7º, §2º da Lei nº 12.527/2011. No caso específico, os dados pessoais sensíveis e biográficos precisam ser ocultados, a fim de resguardar a privacidade e a intimidade da pessoa natural,

conforme estipulado no art. 31, §1º, inciso I da mesma lei e alinhado com as diretrizes do Enunciado CGU nº 12/2023. [63]

> O fundamento "informações pessoais" não pode ser utilizado de forma geral e abstrata para se negar pedidos de acesso a documentos ou processos que contenham dados pessoais, uma vez que esses podem ser tratados (tarjados, excluídos, omitidos, descaracterizados, etc) para que, devidamente protegidos, o restante dos documentos ou processos solicitados sejam fornecidos. Além disso, a proteção de dados pessoais deve ser compatibilizada com a garantia do direito de acesso à informação, podendo aquela ser flexibilizada quando, no caso concreto, a proteção do interesse público geral e preponderante se impuser, nos termos do art. 31, § 3o, inciso V da Lei no 12.527/2011. (Enunciado CGU n. 12/2023 – Informação pessoal)

Importante observar que as demandas inicialmente indeferidas pelo SIC, após deliberação do gestor, por interpretar que as informações solicitadas continham dados pessoais ou sensíveis, tiveram seu recurso apreciado pela CGU e, no mérito, totalmente ou parcialmente deferidos. Quando parcialmente deferidos, sugeriu a CGU o tarjamento dos dados pessoais e sensíveis, com fundamento na Lei Federal nº 12.527/2011.

Inicialmente, alguns gestores entendem que a demanda deve ser indeferida por conter dados pessoais ou sensíveis. Entretanto, quando a CGU analisa o mérito do recurso impetrado pelo demandante, além de deferir o acesso à informação, ela orienta o gestor a tarjar as informações pessoais ou sensíveis. Dessa forma, o acesso à informação é efetivado com a devida proteção dos dados pessoais.

Isso demonstra a tese de que é possível conceder o acesso aos dados desde que eles sejam devidamente tratados e, quando forem pessoais ou sensíveis, devem ser tarjados para que a privacidade do cidadão seja respeitada. Por isso, é importante destacar que a LGPD não é uma barreira ao cumprimento da LAI, pelo contrário, é uma aliada à transparência e legitimidade no tratamento de dados pessoais.

Dos casos analisados, o que deve ser destacado é que, na análise do gestor que delibera o acesso à informação, quando um determinado documento contém alguns dados pessoais não pode ser divulgado. Essa análise inicial contribui para uma avaliação equivocada de que a LGPD pode ser um impasse à política de acesso à informação, o que tem gerado o problema da suposta oposição entre a LAI e a LGPD.

---

[63] Para ver mais detalhes do referido Parecer da CGU, veja o link https://buscaprecedentes.cgu.gov.br/?idAnexo=112465&idAws=AnexosRecurso%2F189050%2F61b095a1-27e4-48a9-b050-e0bf0a8367e3&fileName=SEI_23546078808202335_Parecer_Recurso_de_3ª_Instancia_1638.pdf&handler=DownloadFile.

Contudo, considerando os números do Painel de Acesso à Informação, verifica-se que não houve alteração significativa nos casos de indeferimento do pedido por conter dados pessoais, ou seja, a LGPD não mudou o cenário numérico de pedidos indeferidos por esse motivo, o que se vislumbrava que poderia acontecer. Ainda, os recursos analisados demonstram que a negativa de acesso está mais relacionada à hermenêutica das normas do que a oposição entre elas. O que se busca, portanto, com esta análise é descontruir o discurso de que a LGPD é um impedimento à política pública de acesso à informação. O que se tem, na análise dos dados apresentados é justamente o inverso, a LGPD como aliada à transparência e segurança dos dados tratados pela universidade. Na verdade, a própria LAI já previa a proteção de dados pessoais e a LGPD só veio corroborar com esta diretriz fundamental para o direito à privacidade.

3.3. SIC-UFRJ: Transparência e Legitimidade no Tratamento de Dados Pessoais

Para analisar os dados disponíveis no Painel da Lei de Acesso à Informação (LAI) no portal gov.br, referentes ao órgão Universidade Federal do Rio de Janeiro (UFRJ), no que diz respeito aos pedidos de informação negados antes e depois da entrada em vigor da Lei Geral de Proteção de Dados (LGPD), foi essencial observar os aspectos legais e operacionais que regeram a relação entre transparência e privacidade de dados.

A LAI, em vigor desde 2011, foi um marco para a promoção da transparência pública no Brasil, ao permitir que qualquer cidadão solicitasse informações de órgãos públicos, sem necessidade de justificar o motivo do pedido. Em 2020, a LGPD trouxe novas exigências relacionadas ao tratamento de dados pessoais, impondo limites e cuidados adicionais para a coleta, armazenamento, compartilhamento e uso dessas informações. Embora a LGPD tenha como foco principal a proteção de dados pessoais, ela se integra ao arcabouço legal existente, especialmente à LAI, ao tratar da necessidade de resguardar a privacidade e os dados sensíveis, sem prejudicar o direito de acesso à informação pública.

Diante disso, a análise dos pedidos de informação negados pela UFRJ antes e depois da LGPD permitiu avaliar se houve mudanças no comportamento da instituição em relação à transparência e ao cumprimento das solicitações, bem como o impacto das exigências de proteção de dados. Para realizar essa análise, foi fundamental acessar os dados disponíveis no Painel da LAI do portal gov.br, referentes à UFRJ. Esse painel oferece uma visão detalhada

sobre a quantidade de pedidos de informação recebidos, respondidos e negados, além de especificar os motivos para eventuais negativas.

Outro ponto crucial foi a divisão entre o período antes e depois da LGPD, que entrou em vigor em setembro de 2020, que permitiu identificar eventuais mudanças nos padrões de atendimento aos pedidos de acesso à informação. A seguir, analisamos os dados de forma comparativa entre esses dois períodos.

A análise do painel do SIC revela que a UFRJ tem sido eficiente em responder às demandas de informação. A maioria das solicitações é atendida dentro dos prazos estipulados pela LAI, demonstrando o compromisso da instituição com a transparência. De maio de 2012 a setembro de 2024, a universidade recebeu 4.614 pedidos de informação, ficando em 56º lugar no ranking das autarquias federais. As solicitações abrangem uma variedade de temas, como contratos, despesas, informações acadêmicas e dados administrativos.

Com a entrada em vigor da LGPD, muitas instituições públicas enfrentaram o desafio de ajustar seus processos de tratamento de dados para garantir conformidade com a nova legislação. No entanto, os dados disponíveis no Painel do SIC da UFRJ mostram que a implementação da LGPD não comprometeu a política de transparência da universidade.

Conforme dados do Painel da LAI, de janeiro de 2018 a agosto de 2020, a instituição recebeu 1.173 pedidos de informação e 100% foram respondidos. Desses pedidos, 78.09% tiveram acesso concedido, 9,89%, o acesso negado; 3,41%, o acesso parcialmente concedido; 2,90%, informação inexistente; 3,24%, não se tratava de solicitação de informação; 1,45%, o órgão não tinha competência para responder sobre o assunto e 1,02% era de pergunta duplicada ou repetida. Dos pedidos indeferidos nesse período, apenas 2,81% por motivo de dados pessoais e 0,17% por parte da informação conter dados pessoais.

Após o advento da LGPD, especificamente no período de setembro de 2020 a dezembro de 2024, o SIC-UFRJ recebeu 1.192 pedidos de informação, com 100% deles respondidos. Desses pedidos, 68,30% tiveram acesso concedido, 10,07%, o acesso negado; 2,85%, o acesso parcialmente concedido; 7,97%, informação inexistente; 5,03%, não se tratava de solicitação de informação; 3,94%, o órgão não tinha competência para responder sobre o assunto e 0,84% era de pergunta duplicada ou repetida. Dos pedidos indeferidos nesse período, apenas 1,59% por motivo de dados pessoais e 0,25% por parte da informação conter dados pessoais.

De acordo com as estatísticas do SIC, a quantidade de solicitações atendidas pela UFRJ manteve-se estável mesmo após a implementação da LGPD, o que indica que a proteção de dados pessoais não interferiu no atendimento às demandas por informação pública. Na verdade,

o Painel SIC apresenta uma diversidade de informações solicitadas, como dados sobre orçamentos, contratos e serviços prestados pela UFRJ, demonstrando que a universidade continua a garantir o acesso a informações relevantes e de interesse público.

Antes da vigência da LGPD, o Painel da LAI revela que a UFRJ recebia um número consistente de pedidos de acesso à informação. Os dados indicam que a maioria dos pedidos era atendida dentro do prazo e que as negativas eram, em sua maior parte, fundamentadas em critérios estabelecidos pela LAI. Entre os pedidos negados, um pequeno percentual foi relativo a dados pessoais e dados parcialmente pessoais. Mesmo antes da LGPD, já existiam proteções legais na lei 12.527/2011que impediam a divulgação de dados pessoais, como informações de servidores e estudantes que não fossem de caráter público. Contudo, durante esse período, observa-se uma política de transparência consolidada, em que a UFRJ mantinha um índice elevado de respostas positivas aos pedidos de informação.

Com a LGPD em vigor, o cenário de tratamento de dados pessoais trouxe exigências mais rigorosas em relação à proteção de dados, especialmente no que se refere à coleta e divulgação de informações sensíveis.

Analisando os dados do Painel da LAI da UFRJ pós-LGPD, é possível identificar uma leve alteração no número de pedidos de informação negados, o que pode estar relacionado à maior precaução por parte da universidade ao lidar com informações que envolvem dados pessoais. No entanto, o impacto da LGPD nas negativas de pedidos não foi substancial a ponto de comprometer a política de transparência da instituição. Inclusive, de setembro de 2020 a dezembro de 2024, o SIC-UFRJ recebeu 1.192 pedidos de informação, e, dos 10,07%, dos pedidos de acesso negado e 2,85%, do acesso parcialmente concedido, apenas 1,59% por motivo de dados pessoais e 0,25% por parte da informação conter dados pessoais.

Com base nos dados analisados, é possível afirmar que a implementação da LGPD não causou um aumento expressivo nas negativas de pedidos de informação na UFRJ, mas sim uma adequação necessária às novas exigências legais. As negativas que ocorreram após a LGPD refletem a cautela da instituição em relação ao tratamento de dados pessoais bem como um problema relacionado à hermenêutica jurídica, sem, no entanto, comprometer o princípio da transparência.

Observa-se, portanto, que a UFRJ tem conseguido equilibrar a transparência e a proteção de dados pessoais, respondendo à grande maioria dos pedidos. Esse equilíbrio entre transparência e privacidade é essencial para o fortalecimento da confiança pública nas

instituições, garantindo que tanto o direito à informação quanto a proteção de dados pessoais sejam respeitados.

Importante ressaltar, também, o papel da Controladoria-Geral da União (CGU) no monitoramento e avaliação do cumprimento da Lei de Acesso à Informação (LAI) pelas UFRJ. No contexto das demandas que envolvem dados pessoais, a CGU atua como instância recursal e orientadora, especialmente em casos de negativa de acesso à informação.

Quando o SIC da UFRJ, por exemplo, nega o acesso a certas informações com base em justificativas como a proteção de dados pessoais, ou com base em quaisquer outros motivos, caso o cidadão não concorde com esta negativa, pode recorrer à CGU. Essa análise recursal é importante porque a CGU revisa as decisões da universidade sob a ótica da hermenêutica jurídica que envolve tanto a LAI quanto à LGPD, além de ponderar princípios, julgados, enunciados e a própria Constituição Federal.

Nos casos em que a CGU defere recursos contra a negativa do SIC da UFRJ, ela geralmente orienta a instituição sobre como interpretar corretamente os limites do acesso à informação, sem comprometer a proteção de dados sensíveis. Assim, a Controladoria estabelece diretrizes claras sobre o que constitui dado pessoal e como as informações podem ser tratadas de forma anonimizada ou parcial, preservando tanto o direito à informação quanto a privacidade.

Esses precedentes ajudam a universidade a desenvolver melhores práticas no tratamento das demandas, principalmente no que se refere à aplicação dos princípios de necessidade, adequação e minimização de dados previstos na LGPD. Dessa forma, a CGU contribui não só para a correção de procedimentos específicos, mas também para a construção de uma cultura institucional mais alinhada com as exigências de proteção de dados pessoais e transparência.

Convém destacara, em nossa análise, que as intervenções da Controladoria-Geral da União, sempre que motivadas, também têm sido uma oportunidade para a UFRJ ajustar suas políticas internas, especialmente no que tange à delimitação de dados acessíveis versus dados pessoais protegidos, com base em casos concretos analisados pela CGU. Além das intervenções nos casos concretos, a CGU publica enunciados relativos à LAI[64], que auxiliam o responsável do SIC e os gestores a tratarem as demandas, garantindo a transparência e legitimidade no tratamento dos dados pessoais.

64 https://www.gov.br/acessoainformacao/pt-br/entendimentos-e-estudos-sobre-a-lai/enunciados-da-lai.

Os enunciados elaborados e publicados pelo órgão de controle desempenham um papel crucial no processo de decisão dos gestores públicos no que se refere ao acesso à informação. Esses enunciados, que são interpretações normativas de caráter orientativo, visam uniformizar o entendimento e a aplicação da Lei de Acesso à Informação (Lei nº 12.527/2011) pelos diversos órgãos e entidades da administração pública.

Um dos principais desafios enfrentados pelos gestores públicos é a interpretação adequada das normas relacionadas ao acesso à informação, especialmente em casos complexos que envolvem sigilo, proteção de dados pessoais e transparência. Nesse contexto, os enunciados da CGU oferecem diretrizes claras e fundamentadas, auxiliando na harmonização entre a necessidade de acesso à informação pela sociedade e a proteção de direitos fundamentais, como a privacidade e a segurança.

O Enunciado CGU nº 4, de 10 de março de 2002, por exemplo, que trata de procedimento acerca de pedidos de acesso à informação e recursos, orienta o gestor quanto às decisões que tratam da publicidade de dados de pessoas naturais. Tais decisões, afirma o enunciado, devem ser fundamentadas nos artigos 3º e 31, da lei nº 12.527/2011, pois, por ser mais específica, á a norma de regência processual e material a ser aplicada no processamento desses dados. O texto final do enunciado afirma que a LAI e a LGPD são sistematicamente compatíveis entre si e harmonizam os direitos fundamentais do acesso à informação, da intimidade e da proteção aos dados pessoais, não havendo, portanto, antinomia entre seus dispositivos

Outro tema importante, no âmbito da UFRJ, é o pedido de informação aos processos de licitações, contratos e gastos da universidade. Surge, para os gestores, dúvida quanto a publicação desses processos, tendo em vista que alguns contêm dados pessoais, como CPF, endereço e e-mail das partes envolvidas ou dados que podem ser sigilosos. Para decidir sobre esse caso, o gestor pode conjugar o entendimento dos Enunciados CGU nº 5/2023 e nº 12/2023, que trata do sigilo de licitações, contratos e gastos governamentais, e da informação pessoal, respectivamente.

O Enunciado CGU nº 5/2023 afirma que informações sobre licitações, contratos e gastos governamentais, inclusive as que dizem respeito a processos conduzidos pelas Forças Armadas e pelos órgãos de polícia e de inteligência, são em regra públicas (art. 7º, VI) e eventual restrição de acesso somente pode ser imposta quando o objeto a que se referem estritamente se enquadrar em uma das hipóteses legais de sigilo (art. 22) ou forem classificadas, nos termos do art. 23 da Lei nº 12.527, de 18 de novembro de 2011. E o Enunciado CGU nº 12/2023 afirma que o

fundamento informações pessoais não pode ser utilizado de forma geral e abstrata para se negar pedidos de acesso a documentos ou processos que contenham dados pessoais, uma vez que esses podem ser tratados (tarjados, excluídos, omitidos, descaracterizados etc.) para que, devidamente protegidos, o restante dos documentos ou processos solicitados sejam fornecidos, conforme preceitua o § 2º do art. 7º da Lei nº 12.527, de 18 de novembro de 2011, assegurando-se o acesso à parte não sigilosa por meio de certidão, extrato ou cópia com ocultação da parte sob sigilo. Além disso, a proteção de dados pessoais deve ser compatibilizada com a garantia do direito de acesso à informação, podendo aquela ser flexibilizada quando, no caso concreto, a proteção do interesse público geral e preponderante se impuser, nos termos do art. 31, § 3º, inciso V da Lei n. 12.527, de 2011, e dos arts. 7º, § 3º, e 23, caput, da Lei nº 13.709, de 14 de agosto de 2018.[65]

Outra informação solicitada ao SIC é relativa a títulos acadêmicos e currículos de servidores. Considerando que tais documentos contêm dados pessoais, surge a dúvida quanto à divulgação. Contudo, o Enunciado CGU nº 7/2023 esclarece que informações sobre currículos de agentes públicos, como títulos, experiência acadêmica e experiência profissional, são passíveis de acesso público, uma vez que são utilizadas para a avaliação da capacidade, aptidão e conhecimento técnico para o exercício de cargos e funções públicas.

Outro enunciado importante para subsidiar decisão dos gestores é o de nº 8/2023, que trata de provas e concursos públicos. Este enunciado afirma que a divulgação de documentos e informações relacionados a candidatos aprovados em seleções para o provimento de cargos públicos, inclusive provas orais, são passíveis de acesso público, visto que a transparência dos processos seletivos está diretamente relacionada à promoção dos controles administrativo e social da Administração Pública, ressalvadas as informações pessoais sensíveis.

---

[65] Lei nº 12.527/2011. Art. 31. 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. (...) § 3º O consentimento referido no inciso II do § 1º não será exigido quando as informações forem necessárias: (...) V - à proteção do interesse público e geral preponderante.
Art. 7º (...) § 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.
Lei nº 13.709/2018. 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, (...).

Por fim, uma questão que também ocasiona dúvidas aos gestores é quanto à divulgação de procedimentos disciplinares. Para dirimir dúvidas, a CGU publicou o Enunciado nº 14, de 31 de maio de 2016, que trata da restrição de acesso dos procedimentos disciplinares. Afirma o respectivo enunciado que os procedimentos disciplinares têm acesso restrito para terceiros até o julgamento, nos termos do art. 7º, parágrafo 3º, da Lei nº12.527/2011, regulamentado pelo art. 20, caput, do Decreto nº7.724/2012, sem prejuízo das demais hipóteses legais sobre informações sigilosas.

Importante destacar que esses enunciados harmonizam a implementação da LAI e da LGPD no caso concreto. Essa harmonização depende de uma análise criteriosa de cada caso, de forma a balancear os direitos supostamente em conflito. Um dos princípios previstos é o da proporcionalidade, que exige que a restrição a um direito, em prol da privacidade, no caso da LGPD, seja justificada e limitada ao estritamente necessário para garantir outro direito, transparência, no caso da LAI. Assim, ao avaliar um pedido de informação, é preciso considerar se a divulgação de dados pessoais é realmente necessária e se não há outra forma de fornecer a informação sem violar a privacidade do titular.

Além de analisar os casos pelo princípio da proporcionalidade, os enunciados tratam de procedimentos de anonimização, pseudonimização e tarjamento de dados pessoais. Visando sempre à regra constitucional, que é o acesso à informação, esses procedimentos auxiliam o gestor na condução do tratamento dos dados pessoais ao se divulgar uma informação por meio do SIC.

A anonimização remove elementos identificáveis dos dados, permitindo que a informação seja divulgada sem expor os dados pessoais do titular. A pseudonimização, embora não elimine completamente a possibilidade de identificação, também pode ser aplicada como uma técnica intermediária para aumentar a segurança dos dados. Essas técnicas garantem que as informações públicas possam ser acessadas sem que a privacidade seja comprometida, promovendo um equilíbrio entre os dois regimes legais.

Outro aspecto crucial na harmonização é a definição clara do que constitui “interesse público” para fins de divulgação de informações. A jurisprudência e os órgãos responsáveis pela aplicação da LAI, como a Controladoria-Geral da União (CGU), têm ajudado a estabelecer parâmetros para a aplicação desse critério. Em casos envolvendo dados pessoais, a divulgação só pode ocorrer se o interesse público prevalecer sobre a privacidade. Um exemplo seria a divulgação de salários de servidores públicos, que, embora sejam dados pessoais, são considerados de interesse público em virtude da transparência da administração pública.

A importância desses enunciados reside, portanto, na sua função de subsidiar a tomada de decisões informadas e embasadas juridicamente, garantindo que os gestores públicos atuem de maneira consistente com os princípios da administração pública, como a legalidade, eficiência e transparência. Ao seguir as orientações da CGU, os gestores podem mitigar riscos de interpretações equivocadas que poderiam resultar em sanções administrativas ou na negação indevida de informações de interesse público.

Além disso, os enunciados contribuem para a criação de uma cultura de transparência e responsabilidade, ao incentivar uma gestão pública mais proativa e alinhada com as demandas sociais por acesso à informação. Eles também fortalecem a *accountability*, na medida em que garantem que as decisões sobre o acesso à informação sejam pautadas por critérios técnicos, transparentes e consistentes, evitando arbitrariedades ou subjetividades na aplicação da lei.

3.4 A Complementariedade entre a LAI e a LGPD

A complementariedade de leis no âmbito jurídico refere-se à relação de harmonização e coexistência entre diferentes normas legais que tratam de aspectos conexos ou sobrepostos de um determinado tema. O seu conceito implica que uma lei não anula ou substitui a outra, mas ambas atuam de forma conjunta para garantir a proteção dos direitos e a regulação adequada de determinadas condutas ou áreas de atuação. Em muitos casos, as leis são criadas com finalidades específicas e distintas, mas podem incidir sobre um mesmo campo de atuação. Nesse contexto, o papel dos intérpretes do direito, como magistrados e operadores jurídicos, é fundamental para garantir que essas leis atuem em harmonia, respeitando suas esferas de regulação.

Outro aspecto relevante da complementariedade diz respeito à relação entre normas gerais e normas especiais. O princípio de que a "lei especial prevalece sobre a lei geral" (*lex specialis derogat legi generali)* é uma expressão típica da complementariedade, uma vez que uma lei específica sobre determinado assunto atua em conjunto com a lei geral, sem que esta última seja revogada ou esvaziada. Assim, a norma geral permanece aplicável em situações em que a lei especial não trata de determinados aspectos. Um exemplo clássico é a relação entre o Código Civil brasileiro (norma geral) e legislações específicas, como o Código de Defesa do Consumidor (Lei nº 8.078/1990). O Código Civil regula de maneira abrangente as relações jurídicas privadas, enquanto o Código de Defesa do Consumidor traz regras específicas sobre as relações de consumo. Ambos coexistem, sendo o Código de Defesa do Consumidor aplicado

de maneira preferencial quando se trata de relações entre fornecedores e consumidores, sem que isso anule a vigência ou aplicabilidade do Código Civil em outros contextos.

No campo dos direitos fundamentais, a complementariedade de leis é essencial para a ampliação e a garantia desses direitos. Leis que tratam de diferentes facetas de um mesmo direito ou de direitos conexos muitas vezes necessitam ser interpretadas e aplicadas de forma conjunta. Isso ocorre, por exemplo, nas legislações que versam sobre o direito à privacidade e o direito à liberdade de expressão. Enquanto uma lei pode proteger a privacidade, outra pode assegurar a liberdade de manifestação e opinião. A complementariedade jurídica garante que ambas sejam respeitadas de forma equilibrada, sem que uma norma anule ou restrinja indevidamente a outra.

A interpretação e aplicação da complementariedade de leis cabe, em grande parte, ao Poder Judiciário, que, diante de um caso concreto, deve conciliar normas aparentemente contraditórias ou sobrepostas. Para isso, o juiz ou tribunal pode recorrer a métodos hermenêuticos, como a interpretação sistemática, que analisa o ordenamento jurídico como um todo coerente, buscando garantir a máxima eficácia das normas envolvidas.

Por meio da interpretação sistemática, é possível garantir que leis complementares atuem em conjunto, contribuindo para a realização dos objetivos de justiça e equidade pretendidos pelo ordenamento jurídico. Esse processo de harmonização evita conflitos normativos e assegura que os diversos ramos do direito se integrem de maneira eficiente, promovendo a segurança jurídica e a estabilidade nas relações sociais e econômicas.

No cenário jurídico brasileiro, a Lei de Acesso à Informação (LAI) e a Lei Geral de Proteção de Dados (LGPD) são legislações fundamentais para o exercício da transparência e da proteção de dados pessoais. Embora possa parecer que essas leis estejam em conflito — uma promovendo a abertura de informações públicas e outra impondo restrições ao tratamento de dados pessoais —, uma análise mais aprofundada revela que elas são, na verdade, complementares.

A LAI (Lei 12.527/2011) foi criada com o propósito de garantir o direito à informação e promover a transparência nas atividades públicas, possibilitando um maior controle social sobre o Estado. Seu foco é assegurar o acesso à informação pública, com exceções restritas a informações cujo sigilo seja necessário para garantir a segurança do Estado, a defesa nacional ou o sigilo pessoal justificado. Por outro lado, a LGPD (Lei 13.709/2018), inspirada em normas internacionais como o Regulamento Geral sobre a Proteção de Dados (GDPR), tem como

objetivo regular o tratamento de dados pessoais, garantindo a privacidade dos titulares desses dados e impondo limites claros para sua coleta, uso, armazenamento e compartilhamento.

A discussão sobre a complementariedade entre a LAI e a LGPD passa, em grande parte, pela interdependência entre os conceitos de transparência e privacidade. Solove (2006) propõe que o direito à privacidade não deve ser visto de maneira absoluta, mas como parte de um sistema mais amplo de direitos que interagem entre si. Ele argumenta que a privacidade está intimamente conectada à proteção contra a vigilância abusiva e ao controle do uso de informações pessoais, enquanto o acesso à informação pública é um pilar fundamental de governos democráticos. Para Solove (2006), a privacidade e a transparência precisam ser equilibradas. O direito à informação é vital para a *accountability* e o controle social, mas isso não deve ocorrer à custa da violação da privacidade dos cidadãos. Esse raciocínio é aplicado no contexto brasileiro quando consideramos a interação entre a LAI e a LGPD: enquanto a LAI garante a abertura de dados públicos, a LGPD assegura que essa abertura seja feita com cuidado, preservando os direitos dos titulares de dados pessoais.

A ideia de complementariedade entre as duas legislações é concretizada na prática ao observar como a LGPD regula o tratamento de dados pessoais no âmbito de solicitações de informação pública feitas por meio da LAI.

A Lei de Acesso à Informação tem por base o princípio da transparência pública, de modo a assegurar que as informações públicas sejam amplamente acessíveis. Contudo, o artigo 6º da LAI define a obrigatoriedade de as autoridades públicas garantirem a proteção de informações sigilosas e pessoais, evidenciando que já previa salvaguardas à privacidade. O inciso III deste mesmo artigo trata da proteção de "informações sigilosas e pessoais", indicando que, ao mesmo tempo em que busca promover a transparência, a LAI reconhece a importância de proteger dados que possam comprometer a privacidade dos cidadãos.

> Art. 6º Cabe aos órgãos e entidades do poder público, observadas as normas e procedimentos específicos aplicáveis, assegurar a:
>
> I - gestão transparente da informação, propiciando amplo acesso a ela e sua divulgação;
>
> II - proteção da informação, garantindo-se sua disponibilidade, autenticidade e integridade; e
>
> III - proteção da informação sigilosa e da informação pessoal, observada a sua disponibilidade, autenticidade, integridade e eventual restrição de acesso.

O artigo 31 detalha as condições de acesso às informações pessoais, estabelecendo um regime de restrição e excepcionando o acesso a essas informações sem o consentimento do

titular. Esse dispositivo deixa evidente que a LAI reconhece os limites do direito ao acesso à informação, priorizando a proteção da privacidade em certas situações.

> Art. 31. 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.
>
> § 1º As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem:
>
> I - terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem; e
>
> II - poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem.
>
> (...)
>
> § 3º O consentimento referido no inciso II do § 1º não será exigido quando as informações forem necessárias:
>
> I - à prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusivamente para o tratamento médico;
>
> II - à realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, sendo vedada a identificação da pessoa a que as informações se referirem;
>
> III - ao cumprimento de ordem judicial;
>
> IV - à defesa de direitos humanos; ou
>
> V - à proteção do interesse público e geral preponderante.

A LGPD, embora tenha como foco principal a proteção de dados pessoais, contém disposições que permitem a conciliação entre o direito à privacidade e o interesse público na transparência. Ela regula o tratamento de dados pessoais, buscando garantir que esse tratamento ocorra de maneira transparente, segura e legítima. Vários dispositivos da LGPD reforçam essa complementariedade com a LAI.

O artigo 6º da LGPD elenca os princípios que norteiam o tratamento de dados pessoais. Entre eles, destacam-se:

a) Inciso I – Finalidade: Prevê que o tratamento de dados pessoais deve ter uma finalidade específica, legítima e explícita, o que permite que a administração pública utilize dados pessoais desde que o tratamento atenda a um objetivo claramente definido.
b) Inciso VI – Transparência: Este princípio reforça que os titulares de dados têm o direito de saber como suas informações estão sendo tratadas, e a transparência sobre o

tratamento de dados pessoais está na base da interação entre as duas leis. A divulgação de informações deve respeitar os limites impostos pela privacidade e pela necessidade do tratamento.

O Artigo 7º da LGPD estabelece as bases legais que permitem o tratamento de dados pessoais no Brasil. Entre essas bases, encontram-se o consentimento do titular (inciso I), o cumprimento de obrigações legais (inciso II), a execução de políticas públicas (inciso III), e o cumprimento de contratos (inciso V), entre outras. Essas bases são fundamentais para assegurar que o tratamento de dados pessoais ocorra de maneira legítima e segura, protegendo a privacidade.

Especificamente, para o contexto do acesso à informação pública, as bases mais relevantes são aquelas relacionadas ao cumprimento de obrigação legal e à execução de políticas públicas. A coleta e tratamento de dados pessoais por entes públicos ou por entidades privadas que prestam serviços de interesse público podem, em diversas ocasiões, ser justificadas pela necessidade de execução de funções públicas, de modo a garantir a transparência administrativa sem violar direitos fundamentais.

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
>
> I - mediante o fornecimento de consentimento pelo titular;
>
> II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
>
> III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
>
> IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
>
> V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; (...)

Outra questão importante a ser analisada é a possibilidade de anonimização e pseudonimização dos dados pessoais, que permitem atender a solicitações de informação sem violar a privacidade dos titulares de dados. Essas técnicas, quando aplicadas corretamente, garantem que informações pessoais sejam acessadas de forma segura, sem que haja risco de reidentificação.

A anonimização de dados é uma ferramenta crucial para conciliar a transparência e a privacidade. Ao tornar os dados irreversíveis e não identificáveis, a anonimização permite que informações sejam divulgadas para fins de controle social e transparência, sem comprometer a privacidade. Já a pseudonimização, técnica que substitui identificadores pessoais por

pseudônimos, oferece uma camada de proteção adicional, mas que pode ser revertida em casos específicos, permitindo o tratamento seguro de dados sensíveis.

Outro ponto que reforça a complementariedade entre as legislações é a interpretação jurídica e a jurisprudência que vem sendo formada no Brasil. Decisões judiciais e orientações da Controladoria-Geral da União (CGU) têm afirmado que a LAI e a LGPD devem ser aplicadas de forma conjunta e harmônica. A proteção de dados pessoais não pode ser utilizada como pretexto para negar acesso à informação pública, mas deve ser aplicada como uma salvaguarda para proteger os direitos fundamentais. Ou seja, o interesse público na transparência deve ser ponderado com o respeito à privacidade.

A análise teórica e prática demonstrada neste trabalho confirma que a LAI e a LGPD não são leis em conflito, mas sim complementares. A LGPD, ao introduzir parâmetros claros para o tratamento de dados pessoais, oferece uma estrutura que assegura tanto a proteção da privacidade quanto o acesso responsável à informação pública.

No contexto da UFRJ, observou-se que a LGPD não é um obstáculo à transparência na universidade, mas sim uma aliada para uma política de acesso à informação mais responsável e ética. A LGPD introduziu um nível de cuidado adicional no tratamento de informações sensíveis, garantindo que os direitos fundamentais sejam respeitados ao mesmo tempo em que se mantém o compromisso com a transparência pública. Na prática, isso significa que a UFRJ continua a oferecer informações detalhadas sobre suas atividades, mas adota medidas adicionais para assegurar que dados pessoais, como CPF, endereços e outros identificadores, não sejam divulgados de forma indevida.

Antes da LGPD, o número de acessos negados por envolver dados pessoais já era regulado pela própria LAI, especialmente em seu artigo 31, que trata da restrição de acesso a informações relacionadas à intimidade, vida privada, honra e imagem de pessoas. Após a entrada em vigor da LGPD, a expectativa poderia ser de um aumento expressivo nas negativas de acesso a informações públicas devido à ampliação do escopo de proteção de dados pessoais. Contudo, os números do SIC da UFRJ mostram um cenário diferente, que confirma a complementaridade entre as duas legislações. Esses números indicam que, após a implementação da LGPD, o número de acessos negados com base em dados pessoais não aumentou de maneira significativa. Isso demonstra que a LGPD não foi aplicada de forma automática e indiscriminada para negar pedidos de acesso à informação. Pelo contrário, as solicitações de acesso a informações públicas continuam sendo analisadas caso a caso, com

base na ponderação entre o interesse público e a proteção da privacidade, seguindo os mesmos critérios estabelecidos pela LAI.

Essa constatação reflete o fato de que a LGPD não estabelece uma proibição absoluta à divulgação de dados pessoais, mas, em vez disso, introduz critérios claros para seu tratamento, como a necessidade de bases legais adequadas e o princípio da minimização de dados. Quando um pedido de acesso a informações públicas envolve dados pessoais, a análise segue sendo feita com base no interesse público, conforme previsto na LAI, mas agora com a adição de uma avaliação mais detalhada sobre os riscos à privacidade e a necessidade de proteção dos dados pessoais envolvidos.

Uma análise comparativa entre os números de pedidos negados antes e depois da LGPD no painel do SIC da UFRJ revela que, embora a justificativa de proteção de dados pessoais continue sendo utilizada, não houve um aumento desproporcional nas negativas. Isso comprova que a LGPD não está sendo usada como um "escudo" para impedir o acesso à informação. Pelo contrário, ela complementa a LAI ao estabelecer critérios mais rigorosos para a proteção de dados, sem comprometer o princípio da transparência.

Antes da LGPD, muitos pedidos de acesso a informações que envolviam dados pessoais já eram analisados à luz do artigo 31 da LAI. Após a implementação da LGPD, essa análise se tornou mais robusta, com o apoio de bases legais mais detalhadas, como o cumprimento de obrigações legais, execução de políticas públicas e o legítimo interesse, conforme previsto nos artigos 7º e 23 da LGPD. Esses critérios ampliam a segurança jurídica para a divulgação de dados pessoais quando há justificativa legítima, garantindo que a transparência não seja prejudicada.

Outro aspecto relevante para a demonstração de que não existe divergência entre a LAI e a LGPD no contexto dos dados do SIC da UFRJ é o uso crescente de técnicas de anonimização e minimização de dados. A LGPD introduz essas práticas como mecanismos que permitem a divulgação de informações sem comprometer a privacidade dos titulares dos dados. Portanto, nos casos em que o pedido envolve dados sensíveis, a UFRJ passou a aplicar técnicas de anonimização, permitindo que a informação fosse divulgada de forma a não identificar diretamente os envolvidos. A anonimização e a pseudonimização são ferramentas fundamentais na integração entre a LAI e a LGPD. A anonimização, por ser irreversível, garante que dados pessoais não possam ser reidentificados, o que possibilita a divulgação segura de informações. Já a pseudonimização, embora seja reversível sob certas condições, permite que dados sejam parcialmente protegidos, ainda que acessíveis sob certas condições.

No entanto, o grande desafio das instituições reside em reconhecer essa complementariedade e implementá-la no caso concreto. Apesar de serem leis complementares, as instituições muitas vezes enfrentam barreiras práticas e interpretativas para alinhar esses dois regimes jurídicos, o que gera conflitos no momento de sua aplicação. Contudo, o reconhecimento dessa complementariedade é essencial para a efetivação dos direitos fundamentais à informação e à privacidade. A falta desse entendimento adequado prejudica tanto a confiança pública quanto a capacidade de controle social sobre os atos do Estado e das organizações.

Em alguns casos, a aplicação excessiva de medidas de proteção de dados acaba por impedir a transparência, criando uma espécie de "blindagem institucional" que vai contra o espírito da LAI. Por outro lado, a desconsideração da LGPD em processos de acesso à informação pode resultar na violação de direitos fundamentais dos titulares de dados, expondo as instituições a riscos jurídicos e perda de confiança pública.

Apesar dessas dificuldades, o reconhecimento da complementariedade entre a LAI e a LGPD é inevitável e necessário. Ambas as leis compartilham uma finalidade comum: promover um ambiente de governança responsável, onde a informação flui de forma transparente, mas com o devido respeito aos direitos de privacidade. A transparência sem proteção de dados pode levar à violação de direitos individuais, enquanto a proteção de dados sem transparência pode comprometer a *accountability* e o controle social.

O reconhecimento dessa complementariedade implica, primeiramente, em entender que a proteção de dados pessoais, prevista na LGPD, não é um obstáculo absoluto ao acesso à informação. A LGPD prevê, em seu artigo 7º, que o tratamento de dados por órgãos públicos pode ocorrer para o cumprimento de uma obrigação legal, como a própria LAI. Da mesma forma, a LAI, ao garantir o acesso à informação pública, impõe o respeito à privacidade e à proteção de dados pessoais, conforme previsto em seu artigo 31. Essas disposições indicam que as leis foram elaboradas para coexistirem, e não para se excluírem mutuamente.

Para que as instituições consigam implementar a complementariedade entre a LAI e a LGPD de forma efetiva, é necessário adotar uma abordagem proativa e estratégica. A implementação de políticas de governança de dados bem estruturadas, que contemplem o uso responsável de informações e a proteção de dados pessoais, é fundamental. Isso inclui o desenvolvimento de protocolos claros para o tratamento de dados em pedidos de acesso à informação, incluindo a adoção de práticas como a anonimização e a minimização de dados, garantindo que apenas as informações necessárias sejam divulgadas.

Além disso, é crucial investir na capacitação contínua dos servidores públicos e gestores para que entendam as nuances de ambas as legislações. Uma abordagem integrada de treinamento, que aborde as interseções entre a LAI e a LGPD, permitirá que os tomadores de decisão estejam mais bem equipados para lidar com situações complexas de acesso à informação que envolvam dados pessoais.

Outro aspecto importante é o fortalecimento do diálogo interinstitucional, especialmente entre as Ouvidorias, Controladorias e a Autoridade Nacional de Proteção de Dados (ANPD). Essas instituições precisam atuar de forma colaborativa, desenvolvendo diretrizes conjuntas para a aplicação harmoniosa da LAI e da LGPD. A criação de jurisprudência administrativa sobre como conciliar pedidos de informação e proteção de dados pessoais também é essencial para consolidar boas práticas e fornecer segurança jurídica aos gestores.

CONCLUSÃO

A relação entre a Lei de Acesso à Informação (LAI) e a Lei Geral de Proteção de Dados (LGPD) frequentemente suscita debates sobre sua aplicação conjunta. No entanto, compreendê-las como legislações em conflito, em que uma seria revogada pela prevalência da outra, é um equívoco. Essas normativas não se colocam em cotejo como lei geral e lei especial; ao contrário, são intrinsecamente complementares, formando um sistema jurídico harmônico que concilia o direito de acesso à informação com a proteção da privacidade e dos dados pessoais.

Se a relação entre a LAI e a LGPD fosse tratada como um embate jurídico, em que uma das legislações precisasse sobrepor-se à outra, estaríamos diante de um cenário de retrocesso institucional e democrático. A revogação ou anulação de uma das normas representaria o enfraquecimento de direitos fundamentais: de um lado, o direito à transparência e à informação, essencial para o controle social; de outro, o direito à privacidade, um valor constitucional que protege o cidadão contra abusos no tratamento de seus dados. Em vez disso, essas legislações operam em sinergia, reconhecendo que a proteção de dados pessoais é condição necessária para a efetividade do acesso à informação.

É crucial afastar a interpretação de que a LGPD se impõe como uma exigência externa ou um "escudo" destinado a restringir o acesso à informação pública. Essa percepção ignora a essência da LGPD, que emerge não como uma barreira, mas como uma salvaguarda de direitos fundamentais, assegurando que o tratamento de dados pessoais ocorra de maneira ética, responsável e em conformidade com os princípios do Estado democrático de direito. Não se trata de limitar o acesso, mas de qualificar esse acesso, garantindo que os dados sensíveis ou pessoais de cidadãos não sejam expostos de forma inadequada, prejudicial ou desnecessária.

Nesse contexto, é inerente ao próprio direito de acesso à informação a responsabilidade pelo tratamento e proteção dos dados pessoais e sensíveis. O Estado, ao disponibilizar informações públicas, tem a obrigação de resguardar a privacidade do cidadão, assegurando que a transparência administrativa não se dê às custas da exposição de dados pessoais. Assim, o equilíbrio entre transparência e proteção é alcançado por meio da aplicação coordenada da LAI e da LGPD, que juntas estruturam um modelo de governança pública ético e responsável.

A LAI e a LGPD, portanto, não são antagonistas, mas aliadas no fortalecimento de um Estado que reconhece tanto a importância do acesso à informação para a cidadania ativa quanto a necessidade de proteger a privacidade como valor essencial para a dignidade humana. Essa complementariedade evidencia que a transparência e a proteção de dados não são direitos opostos, mas interdependentes, unidos pelo compromisso de construir uma relação de confiança entre o Estado e a sociedade.

A Lei Geral de Proteção de Dados Pessoais (LGPD) e a Lei de Acesso à Informação (LAI), longe de se apresentarem como normativas em conflito, devem ser compreendidas sob uma perspectiva de complementariedade. Ambas refletem valores fundamentais da sociedade democrática brasileira: a proteção à privacidade e a promoção da transparência pública. Ao garantir o acesso à informação, a LAI fortalece a *accountability* e o controle social, elementos essenciais para a consolidação de uma governança transparente e participativa. Por outro lado, a LGPD protege a privacidade e os dados pessoais e estabelece critérios claros para o tratamento de informações sensíveis.

O desafio que se coloca, à luz da hermenêutica jurídica, não é escolher entre transparência ou privacidade, mas encontrar o ponto de equilíbrio que permita a coexistência harmoniosa desses direitos. A partir dos princípios constitucionais da proporcionalidade e da razoabilidade, é possível harmonizar a aplicação de ambas as legislações, resguardando tanto o direito de acesso à informação quanto a proteção de dados pessoais.

A compatibilidade entre a Lei Geral de Proteção de Dados Pessoais (LGPD) e a Lei de Acesso à Informação (LAI) não apenas é possível, mas necessária, uma vez que ambas as legislações compartilham objetivos essenciais para o fortalecimento da democracia e para a construção de uma administração pública responsável e transparente. Em uma leitura hermenêutica que privilegia a coexistência de direitos fundamentais, é possível argumentar que a LGPD e a LAI, em vez de se anularem, atuam em campos complementares e podem se reforçar mutuamente.

A LGPD foi concebida com o propósito de proteger a privacidade no contexto do tratamento de seus dados pessoais, garantindo que o uso dessas informações seja realizado de maneira responsável, segura e transparente. No entanto, a própria lei prevê exceções para garantir que o tratamento de dados não comprometa a transparência necessária à administração pública, ao permitir o compartilhamento de informações de interesse coletivo ou geral, desde que observados os limites relativos à privacidade e à proteção de dados sensíveis. Assim, a

proteção de dados pessoais, embora essencial, não pode servir de escudo para práticas que ocultem informações relevantes para o controle social e a prestação de contas por parte do Estado.

Por sua vez, a LAI promove o direito de acesso às informações públicas, um elemento central para a transparência e para o exercício da cidadania. Entretanto, a própria LAI reconhece que esse direito não é absoluto, especialmente quando envolve informações de caráter pessoal. A necessidade de proteger a privacidade, conforme estabelecido na Constituição Federal, é incorporada pela LAI, que estabelece salvaguardas para evitar o uso indevido de dados pessoais. Dessa forma, a LAI também reforça os princípios da LGPD ao respeitar a confidencialidade de informações pessoais, garantindo, ao mesmo tempo, a transparência das ações governamentais.

A complementariedade entre essas legislações pode ser vista na forma como elas estabelecem um equilíbrio entre o interesse público e a proteção de direitos fundamentais. A LGPD, ao regulamentar o tratamento de dados pessoais, fornece critérios claros para que a administração pública possa garantir a privacidade dos cidadãos sem comprometer a transparência de suas atividades. A LAI, por sua vez, define as bases para que o acesso à informação pública seja exercido de maneira responsável, respeitando os direitos previstos na LGPD. O resultado é uma convergência entre ambas as leis: a privacidade é preservada, ao mesmo tempo que a transparência e o acesso à informação são garantidos.

Sob esta óptica, o desafio hermenêutico consiste em aplicar esses marcos regulatórios de maneira harmônica, utilizando os princípios jurídicos da proporcionalidade e da razoabilidade para resolver eventuais tensões entre eles. Não se trata de um conflito de direitos, mas de uma coordenação entre normas que protegem, em última instância, os mesmos valores constitucionais. Os operadores do direito, ao lidarem com questões que envolvem o acesso a informações e a proteção de dados, devem buscar soluções que respeitem os limites e as finalidades de ambas as legislações, considerando o interesse público e o direito à privacidade em cada caso concreto.

A própria experiência prática da administração pública brasileira, especialmente do SIC da UFRJ, conforme demonstrado nesta pesquisa, mostra que essa harmonização é possível. Ao analisar o tratamento de demandas da LAI no contexto da LGPD, é possível observar que a maioria dos pedidos de acesso à informação pode ser atendida sem violar as disposições da LGPD, desde que seja aplicado um critério de anonimização ou proteção de dados pessoais. A integração entre essas duas normativas pode ser aprimorada com o desenvolvimento de políticas

públicas que promovam tanto a transparência quanto a proteção de dados, utilizando tecnologias adequadas e processos administrativos que assegurem a conformidade legal.

Portanto, a LGPD não é um obstáculo à efetivação da LAI. Pelo contrário, sua implementação fortalece a transparência ao estabelecer parâmetros claros para o tratamento de dados pessoais, criando um ambiente jurídico mais seguro e previsível tanto para a administração pública quanto para os cidadãos. O caminho para a aplicação conjunta dessas legislações reside na interpretação jurídica que respeite os direitos fundamentais envolvidos, em um esforço de harmonização que reconheça a importância da privacidade e da transparência como pilares de uma democracia madura e eficiente.

REFERÊNCIAS

ALVES, E.B**. Accountability e Transparência Pública: Uma Proposta para a Gestão Pública de Excelência**. Curitiba: 2021.

ANGÉLICO, Fabiano. **Lei de Acesso à Informação Pública e seus possíveis desdobramentos para a accountability democrática no Brasil**. FGV, São Paulo, 2012.

ANS. **Guia Orientativo: Tratamento de Dados Pessoais pelo Poder Público**. Versão 1.0. 2022.

ARCOVERDE, L; RAMOS, M. V; ZANATTA, R. **Transparência sob ataque.** Folha de São Paulo, publicado em 15/10/2021. Disponível em: https://www1.folha.uol.com.br/opiniao/2021/11/transparencia- sob-ataque.shtml.

BARCELLOS, A. P. **A Eficácia Jurídica dos Princípios Constitucionais: o princípio da dignidade da pessoa humana.** 2. Ed. Rio de Janeiro: Renovar, 2008.

BARRETTO, V. P. **O fetiche dos direitos humanos e outros temas.** Rio de janeiro: Lúmen Juris, 2010.

BAUMAN, Zygmunt. **Modernidade líquida**. São Paulo: Editora Schwarcz, 2021.

BENIGER, J. R. **The Control Revolution: Technological and Economic Origins of the Information Society**. Harvard University Press, 1989.

BENTHAM, Jeremy. **Panoptique. Mémoire sur un nouveau principe pour construire des maisons d'inspection, et nommément des maison de force**. Impresso por ordem da Assembléia Nacional. Paris: Imprimerie Nationale: 1791.

BINENBOJM, Gustavo. **Uma Teoria do Direito Administrativo: Direitos Fundamentais, Democracia e Constitucionalização.** 3ª ed. Rio de Janeiro: Renovar, 2014.

BIONI, B. R. **Proteção de Dados Pessoais - A Função e os Limites do Consentimento.** São Paulo: Forense, 2021.

_____. **Regulação e Proteção de Dados Pessoais - O Princípio da Accountability**. São Paulo: Forense, 2022.

BIONI, B.; DONEDA, D.; MENDES, L. S.; RODRIGUES, O.L.; SARLET, I. W. **Tratado de Proteção de Dados Pessoais.** São Paulo: Forense, 2023.

_____; SILVA, P. G. F.; MARTINS, P. B. L. **Intersecções e relações entre a Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação (LAI): análise contextual pela lente do direito de acesso.** Coletânea de artigos da Pós-Graduação em Ouvidoria Pública, 2022. Disponível em https://revista.cgu.gov.br/Cadernos_CGU/article/view/504.

BOBBIO, Norberto. **O Futuro da Democracia: Uma Defesa das Regras do Jogo**. São Paulo: Paz e Terra, 2009.

_____. **Teoria do Ordenamento Jurídico**. Brasília: Unb. 2003.

BOVENS, Mark. **Two Concepts of Accountability: Accountability as a Virtue and as a Mechanism. West European Politics**, 33(5), 946–967. Disponível em\; https://doi.org/10.1080/01402382.2010.486119. Acesso em: 10 jan. 2023

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Senado Federal, 1988.

BRASIL. **Lei Complementar n. 101, de 4 de maio de 2000 (Lei de Responsabilidade Fiscal)**. Diário Oficial da União, 5 maio 2000.

Brasil. **Lei n. 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação - LAI).** Diário Oficial da União, 18 nov. 2011.

BUCCI, M. P. D. **Fundamentos para uma teoria jurídica das políticas públicas.** São Paulo: Saraiva, 2013.

_____. **Regulação e políticas públicas: o papel das agências reguladoras.** In: João Paulo B. Assis (Org.), Políticas Públicas e Governança no Brasil. Belo Horizonte: Fórum, 2017.

CALDERON, M. P. **A Evolução do Direito de Acesso à Informação até a Culminância na Lei nº.12.527/2011.** Revista Brasileira de Ciências Policiais. Brasília, v. 4, n. 2, 2013.

CARVALHO FILHO, J. S. **Manual de Direito Administrativo**. 33 ed. – São Paulo: Atlas, 2019.

CASTELLS, Manuel. **A Sociedade em Rede: A Era da Informação: Economia, Sociedade e Cultura.** Vol. 1. São Paulo: Paz e Terra, 2013.

COUTINHO, D. R. **Direito e economia política na regulação de serviços públicos**. São Paulo: Saraiva, 2014.

CRESWELL, J.W. **Projeto de Pesquisa: Métodos Qualitativo, Quantitativo e Misto**. São Paulo: Artmed, 2010.

DAHL, Robert. **Poliarchy**. New Haven, Yale University Press, 1971.

DILTHEY, Wilhelm. **La esencia da la filosofia**. Buenos Aires: Editorial Losada,1944.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 3. ed. (2. ed. do e- book) São Paulo: Revista dos Tribunais, Thomson Reuters Brasil, 2021. 368 p.

DWORKIN, Ronald. **Levando os Direitos a Sério**. 3ª edição – São Paulo: Editora WMF Martins Fontes, 2010.

DYE, Thomas. **Mapeamento dos Modelos de Análise de Políticas Públicas**. In: HEIDEMANN, Francisco G.; SALM, José Francisco. Políticas Públicas e Desenvolvimento. Brasília: UNB, 2014.

_____. **Understanding Public Policy**. 15th ed. Boston: Pearson, 2016.

FLORIDI, Luciano. **The Philosophy of Information**. Oxford University Press, 2013.

FONTE, F. M. **Políticas Públicas e Direitos Fundamentais**. 2.ed. São Paulo: Saraiva, 2015.

FOUCAULT, Michel. **Vigiar e punir: nascimento da prisão**; tradução de Raquel Ramalhete. Petrópolis, Vozes, 1987.

GIL, A.C. **Métodos e Técnicas de Pesquisa Social**. 4 ed. São Paulo: Atlas, 1994.

HOWLETT, M.; RAMESH, M.; PERL, A. **Política pública: seus ciclos e subsistemas: uma abordagem integral.** Rio de Janeiro: Elsevier, 2013.

KEYNES, John Maynard. **The General Theory of Employment, Interest and Money**. London: Macmillan, 1936.

LANDERDAHL, C.; MAIOLINO, I.; BARBOSA, D.; CARVALHO, L. **Guia Orientativo: Tratamento de Dados Pessoais pelo Poder Público.** Versão 1.0. 2020. Disponível em https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em: 5 jan. 2024.

LEMOS, R.; FELICE, M. **A Vida em Rede**. São Paulo: Papirus 7 Mares, 2014.

LESSIG, Lawrence. **Code and Other Laws of Cyberspace**. New York: Basic Books, 1999.

MATTOS, P.T.L. **O Novo Estado Regulador no Brasil: entre eficiência e legitimidade**. Rio de Janeiro: Revista dos Tribunais, 2017.

MATTIETTO, Leonardo. **Dos Direitos da Personalidade à Cláusula Geral de Proteção da Pessoa.** Revista de Direito da Procuradoria Geral. P. 218 a 232. Edição Especial, 2017.

_____. **Estado de Direito, Jurisdição e Dignidade Humana**. Lex Humana, Petrópolis, v. 11, n. 1, p. 97-109, 2019, ISSN 2175-0947. Universidade Católica de Petrópolis, Petrópolis, Rio de Janeiro, Brasil.

MILL, J. S. **Sobre a Liberdade**. São Paulo: L&PM, 2016. (Obra original publicada em 1859).

MOROZOV, Evgeny. **Big Tech: A ascensão dos dados e a morte da política**. São Paulo: Ubu Editora, 2018.

NISSENBAUM, Helen. **Privacy in Context: technology, policy, and the integrity of social life.** Stanford: Stanford University Press, 2010.

SALM, J. F. **Políticas Públicas e Desenvolvimento**. Brasília: UNB, 2014. p. 109-142.

SARLET, I. W.; MOLINARO, C. A. **Direito à informação e direito de acesso à informação como direitos fundamentais na Constituição brasileira**. Revista da AGU, Brasília-DF, ano XIII, n. 42, p. 09-38, out./dez. 2014.

SARLET, I. W. **A eficácia dos direitos fundamentais.** 13. ed. Porto Alegre: Livraria do Advogado, 2019.

SCHLEIERMACHER, Friedrich. In: Frank, M. (Hg.). **Hermeneutik und Kritik**. Frankfurt, Suhrkamp, 1977.

SCHREIBER, Anderson. **Direitos da personalidade**. São Paulo, Atlas, 2013.

SCOTT, Colin. **Regulation in the Age of Governance: The Rise of the Post- Regulatory State**. IN: Jacint Jordana & David Levi-Faur (ed.). The Politics of Regulation. Capítulo 7, Edward Elgar Publishing, 2004.

SECCHI, Leonardo. **Análise de Políticas Públicas: Diagnóstico de Problemas, Recomendações de Soluções.** São Paulo: Cengage, 2017

_____. **Políticas Públicas: Conceitos, Casos Práticos**. 3ª Edição. São Paulo: Cengage, 2020.

SOLOVE, Daniel J. **I've Got Nothing to Hide' and Other Misunderstandings of Privacy**. San Diego Law Review, Vol. 44, p. 745, 2007.

SOUZA, C. A.; LEMOS, R; BOTTINO, C. **Marco Civil da Internet.** Rio de Janeiro: Revista dos Tribunais, 2018.

SUNDFELD, C. A.; ROSILHO, A. (Org.) **Direito da regulação e políticas públicas**. São Paulo: Malheiros, 2014.

SUNSTEIN. C. R. **Republic.com 2.0**. Princeton: Princeton University Press, 2009.

TEIXEIRA, T.; ARMELIN, R. M. **Lei Geral de Proteção de Dados Pessoais: comentado artigo por artigo.** Salvador: Editora JusPodivm, 2019.

VOGEL, J. S. **Principais Desafios para a Proteção e Tratamento de Dados Pessoais no Brasil, a Partir da Experiência Europeia**. Belo Horizonte: Dialética, 2023.

WARREN, S. D.; BRANDEIS, L. D. **The right to privacy**. Harvard Law Review, p. 123-220, 1890.

GLOSSÁRIO

Acesso à Informação - Direito fundamental que garante aos cidadãos o acesso a informações públicas, permitindo a transparência e o controle social sobre as ações da Administração Pública.

Accountability – É o princípio de responsabilização, onde cidadãos, organizações ou instituições são obrigados a prestar contas por suas ações, decisões e políticas, garantindo transparência e integridade.

Agentes de Tratamento - São o Controlador e o Operador, responsáveis pelo tratamento de dados pessoais. O Controlador toma as decisões sobre o tratamento dos dados, enquanto o Operador realiza o tratamento em nome do Controlador.

Agentes Públicos - Todos aqueles que, por vínculo, ocupação ou função, exercem atividades públicas, incluindo servidores, empregados e prestadores de serviços em órgãos da Administração Pública.

Anonimização de dados - Processo irreversível que elimina ou modifica dados pessoais, de forma que a pessoa não possa mais ser identificada.

Autoridade Nacional de Proteção de Dados (ANPD) - Órgão federal responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território brasileiro, bem como regulamentar questões específicas relativas à proteção de dados pessoais.

Bases Legais - Fundamentos jurídicos que autorizam o tratamento de dados pessoais. A LGPD estabelece bases legais, incluindo o consentimento, cumprimento de obrigação legal, proteção da vida, execução de contrato, entre outros.

Classificação da Informação - Procedimento pelo qual informações públicas podem ser classificadas, temporariamente, como sigilosas, com base em critérios de segurança e interesse público, nos níveis de ultrassecreto, secreto ou reservado.

Consentimento - Manifestação livre, informada e inequívoca pela qual o titular dos dados concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

Controlador - Pessoa física ou jurídica, de direito público ou privado, que toma decisões sobre o tratamento de dados pessoais. O Controlador determina as finalidades e os meios do tratamento.

Dados pessoais identificados - Informações que permitem identificar diretamente uma pessoa, como nome, CPF ou RG.

Dados pessoais identificáveis - Informações que, isoladas ou combinadas, podem levar à identificação de uma pessoa, como endereço ou IP.

Dados Pessoais Sensíveis - Subconjunto de dados pessoais que inclui informações sobre origem racial ou étnica, convicção religiosa, opinião política, saúde, vida sexual, genética ou biometria, dados que exigem maior proteção por implicarem maior risco aos direitos e liberdades do titular.

Desclassificação - Ato administrativo que retira o sigilo de uma informação anteriormente classificada, tornando-a acessível ao público.

Encarregado (Data Protection Officer - DPO) - Pessoa indicada pelo Controlador e Operador para atuar como canal de comunicação entre o Controlador, os titulares dos dados e a ANPD, responsável por garantir a conformidade com a LGPD.

Finalidade - Propósito específico, legítimo, explícito e informado que justifica o tratamento de dados pessoais. A LGPD exige que os dados sejam tratados de acordo com finalidades pré-estabelecidas e transparentes para o titular.

Informação Pessoal - Dados relacionados a uma pessoa identificada ou identificável, cuja divulgação possa violar a privacidade, intimidade, honra e imagem, sendo protegida pela legislação.

Informações Públicas - Dados e registros produzidos ou geridos pelo setor público, independentemente de sua forma, suporte ou natureza, que não estejam classificados como sigilosos.

Interesse Público - Interesse da coletividade que justifica a divulgação de informações de relevância social, política ou econômica, relacionadas à gestão pública e à garantia dos direitos fundamentais.

Operador - Pessoa física ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do Controlador, conforme as instruções recebidas.

Órgãos e Entidades Públicas - Conjunto de instituições que compõem os Poderes Executivo, Legislativo e Judiciário, além de autarquias, fundações públicas, empresas estatais e outros organismos da Administração Pública direta e indireta.

Ouvidoria - Unidade responsável por receber e tratar solicitações, sugestões, reclamações e denúncias dos cidadãos, assegurando o exercício dos direitos de acesso à informação e participação social.

Pedido de Informação - Solicitação formal realizada por um cidadão ou pessoa jurídica para acessar dados ou informações em poder dos órgãos e entidades públicas.

Portabilidade de Dados - Direito do titular de solicitar a transferência de seus dados pessoais a outro fornecedor de serviço ou produto, conforme regulamentação da ANPD.

Proteção da Informação - Medidas adotadas para garantir a integridade, confidencialidade e disponibilidade de informações, especialmente as classificadas como sigilosas ou de caráter pessoal.

Pseudonimização de dados - Técnica que substitui dados pessoais por identificadores artificiais, reduzindo a chance de identificação, mas permitindo a reversão sob condições específicas.

Recurso Administrativo - Instrumento que permite ao cidadão contestar, no âmbito da administração pública, a negativa de acesso à informação solicitada, de acordo com os prazos e procedimentos previstos na lei.

Relatório de Impacto à Proteção de Dados Pessoais - Documento que o Controlador deve elaborar para descrever os processos de tratamento de dados pessoais, avaliar riscos e implementar medidas de mitigação, principalmente quando o tratamento envolve dados sensíveis.

Responsabilidade do Agente Público - Dever do agente público de zelar pela correta gestão e divulgação das informações públicas, sob pena de responsabilização em caso de omissão ou violação da lei.

Segurança da Informação - Conjunto de medidas técnicas e administrativas implementadas para proteger os dados pessoais contra acessos não autorizados, vazamentos, e outros incidentes que comprometam a integridade e confidencialidade dos dados.

Sigilo - Restrições temporárias ao acesso a determinadas informações, impostas por razões de segurança nacional, defesa do Estado, ou para garantir a privacidade das pessoas.

Titular de Dados - Pessoa natural a quem se referem os dados pessoais que estão sendo objeto de tratamento, detendo direitos sobre a utilização de suas informações.

Transparência - Princípio que exige que as atividades de tratamento de dados sejam conduzidas de maneira clara, acessível e compreensível ao titular, de modo a garantir seu direito de estar plenamente informado sobre como seus dados são tratados.

Transparência Ativa - Obrigação dos órgãos e entidades públicas de disponibilizar, de forma proativa e contínua, informações de interesse coletivo, independentemente de solicitação.

Transparência Passiva - Acesso a informações públicas mediante solicitação formal feita por qualquer cidadão, sendo um direito garantido pela Lei de Acesso à Informação.

Tratamento de Dados Pessoais - Qualquer operação realizada com dados pessoais, como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, entre outros.

Ultrassecreto, Secreto e Reservado - Níveis de classificação de informações sigilosas. "Ultrassecreto" tem prazo de sigilo de até 25 anos; "Secreto", até 15 anos; e "Reservado", até 5 anos.

Usuário da Informação - Qualquer pessoa física ou jurídica que solicita ou utiliza dados públicos em suas atividades, seja para controle social, pesquisa, ou outros fins legítimos.

Violação de Dados Pessoais: Qualquer incidente de segurança que resulte em destruição acidental ou ilegal, perda, alteração, acesso não autorizado ou vazamento de dados pessoais. O Controlador deve comunicar à ANPD e ao titular caso haja risco à integridade dos dados.