DERECHO Y CAMBIO SOCIAL
FUNDADA EL AÑO 2000

COMPARTILHAMENTO DE DADOS PELO PODER PÚBLICO: UM CAMINHO PARA A TRANSPARÊNCIA E MELHORIA DOS SERVIÇOS

DATA SHARING BY GOVERNMENT: A PATH TO TRANSPARENCY AND IMPROVED SERVICES

EL INTERCAMBIO DE DATOS POR PARTE DE LOS GOBIERNOS: UN CAMINO HACIA LA TRANSPARENCIA Y LA MEJORA DE LOS SERVICIOS

Maycon Neves da Silva[1], Mauro Monteiro Ferreira[2]

DOI: 10.54899/dcs.v22i79.105
Recibido: 27/12/2024 | Aceptado: 17/01/2025 | Publicación en línea: 11/02/2025.

RESUMO

Este estudo analisa o impacto do compartilhamento de dados pelo poder público na transparência administrativa e na eficiência dos serviços públicos, com base na Lei Geral de Proteção de Dados (LGPD) e no Regulamento Geral de Proteção de Dados (GDPR). A pesquisa adota uma abordagem qualitativa, fundamentada em análise documental e estudo de casos relevantes, explorando legislações nacionais e internacionais e práticas adotadas por diferentes países. Os resultados evidenciam que a implementação de políticas consistentes de compartilhamento de dados pode promover a confiança pública, estimular a inovação e melhorar a prestação de serviços, desde que respeitados os princípios éticos e a segurança das informações pessoais. Apesar disso, desafios como a falta de capacitação técnica, interoperabilidade de sistemas e alinhamento entre normas internacionais e tratadas internacionalmente ainda limitam sua efetividade. O estudo destaca a necessidade de investimentos em tecnologias e governança sólida, garantindo um equilíbrio entre a proteção de dados e a eficiência governamental.

Palavras-chave: Compartilhamento de Dados. Poder Público. Transparências. Direito Digital. Tecnologia.

ABSTRACT

This study analyzes the impact of data sharing by public authorities on administrative transparency and the efficiency of public services, based on the General Data Protection Law (LGPD) and the General Data Protection Regulation (GDPR). The research adopts a qualitative approach, based on documentary analysis and relevant case studies, exploring national and international legislation and practices adopted by different countries. The results show that the implementation of consistent data sharing policies can promote public trust, stimulate innovation and improve the provision of services, as long as ethical principles and the security of personal

[1] Graduando em Direito, Universidade Estadual do Tocantins (UNITINS), Augustinópolis, Tocantins, Brasil.
E-mail: umtaldemaycola@gmail.com Orcid: https://orcid.org/0009-0001-2025-6922
[2] Graduando em Direito, Faculdade Católica Dom Orione, Araguaína, Tocantins, Brasil.
E-mail: Monteiiro.mauro@gmail.com Orcid: https://orcid.org/0009-0002-6106-7797

information are respected. Despite this, challenges such as the lack of technical capacity, system interoperability and alignment between international standards and international treaties still limit its effectiveness. The study highlights the need for investments in technologies and solid governance, ensuring a balance between data protection and government efficiency.

Keywords: Data Sharing. Public Authorities. Transparency. Digital Law. Technology.

RESUMEN

Este estudio analiza el impacto de la cesión de datos por parte de las administraciones públicas en la transparencia administrativa y la eficiencia de los servicios públicos, con base en la Ley General de Protección de Datos (LGPD) y el Reglamento General de Protección de Datos (RGPD). La investigación adopta un enfoque cualitativo, basado en el análisis documental y estudios de casos relevantes, explorando la legislación y las prácticas nacionales e internacionales adoptadas por diferentes países. Los resultados muestran que la implementación de políticas consistentes de intercambio de datos puede promover la confianza pública, estimular la innovación y mejorar la prestación de servicios, siempre que se respeten los principios éticos y la seguridad de la información personal. A pesar de ello, desafíos como la falta de capacidad técnica, interoperabilidad de sistemas y alineación entre estándares internacionales y tratados internacionales aún limitan su efectividad. El estudio destaca la necesidad de invertir en tecnologías y en una gobernanza sólida, garantizando un equilibrio entre la protección de datos y la eficiencia gubernamental.

Palabras clave: Intercambio de Datos. Poder Público. Transparencias. Derecho Digital. Tecnología.

INTRODUÇÃO

Durante os séculos, o Brasil experimentou diversas estruturas de poder, desde o domínio colonial até a proclamação da República em 1889, se ajustando de acordo com a época. A Constituição Federal de 1988 estabeleceu princípios e normas fundamentais que regem a organização do Estado, promovendo a participação nos assuntos da sociedade e o bem-estar social por meio de ações públicas nas áreas de saúde, educação, segurança e entre outras. Assim, uma nova adaptação foi exigida do país. Com o progresso da tecnologia, o planeta está se tornando cada vez mais digital, com uma conexão global em expansão as pessoas recebem continuamente uma vasta quantidade de informações, que são transmitidas de forma muito rápida.

Nesse contexto, para garantir a boa-fé e bem-estar social, o governo deve cooperar com tecnologia para proporcionar a proteção dos direitos dos cidadãos, facilitando o acesso aos serviços públicos e promovendo a transparência com o uso de dados, a fim de promover uma gestão mais eficiente e eficaz. Ressalta-se, também, que é importante garantir a segurança cibernética e a proteção das informações dos cidadãos, a fim de gerar vantagens e enfrentar possíveis problemas e perigos.

Nesse sentido, ao dispor sobre dados pessoais, o legislador promoveu importante alterações na constituição de 1988, com a emenda constitucional n°115 de 2022, para acrescentar que é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais, ainda dispondo que compete privativamente à União legislar sobre proteção e tratamento de dados pessoais. De tal importância é o assunto que preteritamente à emenda n°115 de 2022, o legislador em 14 de agosto de 2018 editou a denominada Lei Geral de Proteção de Dados (LGPD), lei infraconstitucional para normatizar a questão da proteção dos dados pessoais. Falar sobre proteção de dados implica necessariamente saber o seu significado bem como saber o porquê da proteção é indispensável.

A LGPD em seu artigo 5° traz diversos conceitos relacionados à tal normatividade, dentre eles, destacam-se o conceito de dados pessoais, dados pessoais sensíveis e uso compartilhado de dados, assim sendo, para fins de entendimento, considera-se dado pessoal a informação relacionada a pessoa natural identificada ou identificável, por sua vez, dado pessoal sensível é o 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, e por fim, uso compartilhado de dados, que é a comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

A CONSTITUCIONALIDADE DA PROTEÇÃO DE DADOS

A segurança dos dados é um direito essencial garantido pela Constituição Federal, que protege a privacidade e a intimidação dos indivíduos, garantindo o uso seguro e responsável de

suas informações pessoais. Segundo Barreto (2013), a proteção de dados é um direito fundamental garantido por lei, que protege a privacidade, a vida privada, a honra e a imagem das pessoas. O autor também pontua que a proteção de dados tem como objetivo preservar a autonomia e a liberdade individual dos cidadãos, garantindo o correto e seguro manejo das informações pessoais.

Por esse aspecto, a importância da legalidade da proteção de dados é fundamental para garantir a privacidade e a segurança das informações dos indivíduos, levantando-se uma discussão sobre a legitimidade do controle do Estado sobre tais informações. Dessa forma, é responsabilidade do Estado garantir a proteção dos dados dos cidadãos, garantindo a segurança e a privacidade das informações recolhidas e armazenadas pelas entidades governamentais. Entretanto, é essencial ressaltar que as autoridades devem atuar de maneira transparente e seguir os princípios da legalidade, proporcionalidade e especificamente ao utilizar essas informações. Diante disso, a Lei Geral de Proteção de Dados (LGPD), inspirada no Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, estabelece normas e diretrizes para o tratamento de dados pessoais no Brasil, visando garantir a privacidade e a segurança das informações dos usuários.

Portanto, o poder público tem legitimidade e controle das informações dos cidadãos, respeitando os direitos fundamentais e as leis constitucionais. Ademais, é essencial a existência de métodos de monitoramento e supervisão para garantir que as informações sejam usadas de modo ético e em conformidade com a lei em vigor.

PRINCÍPIOS ÉTICOS E DE PRIVACIDADE NO COMPARTILHAMENTO DE DADOS PÚBLICOS

O compartilhamento de dados pelo Poder Público deve seguir princípios éticos e de privacidade para garantir a proteção das informações dos cidadãos. Isso inclui a necessidade de anonimização e pseudonimização dos dados, respeitando a identidade e a intimidade das pessoas. Assim, é fundamental estabelecer regras claras para o uso e acesso aos dados, considerando a finalidade específica para a qual foram coletados.

A transparência sobre as práticas de compartilhamento, bem como a prestação de contas (accountability), são elementos essenciais para assegurar a confiança da sociedade no uso dessas informações pelo poder público. Por isso, é fundamental para mensurar os efeitos das estratégias

implementadas, bem como identificar pontos de melhoria. Por meio de análises rigorosas, é possível verificar se os objetivos almejados foram alcançados, além de avaliar os impactos positivos e negativos gerados.

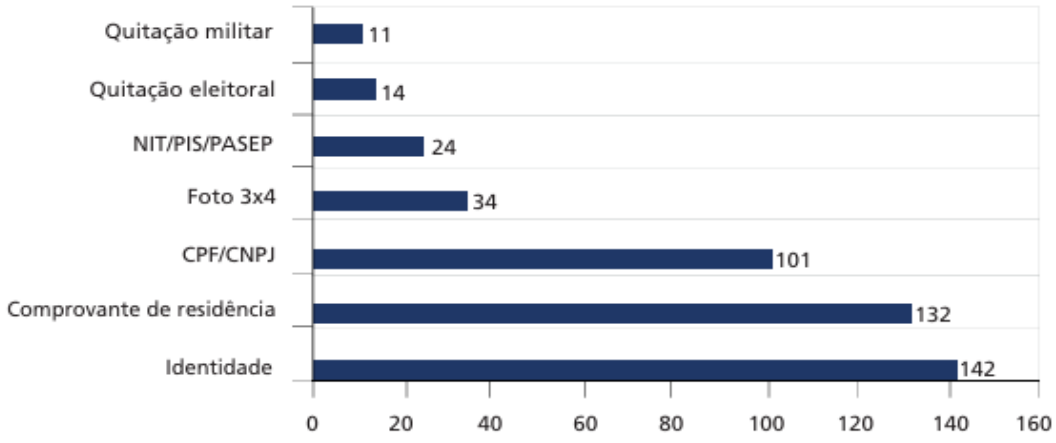
Dessa forma, é possível embasar decisões futuras e aprimorar as políticas de compartilhamento de dados, garantindo sua efetividade e contribuindo para a transparência e aperfeiçoamento do uso de informações governamentais.

ARTIGO 26 E 27 DA LGPD – LEI GERAL DE PROTEÇÃO DE DADOS

A Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, foi criada para normatizar o controle de informações pessoais no Brasil, determinando obrigações e responsabilidades para as empresas que obtêm e manuseiam dados de pessoas. Os artigos 26 e 27 da LGPD estabelecem condições essenciais para o compartilhamento de dados pessoais pelo poder público, priorizando a proteção da privacidade e a segurança das informações dos cidadãos. Assim, é indispensável que os órgãos públicos e entidades sigam essas normas e adotem procedimentos responsáveis no manejo de informações pessoais. O gráfico abaixa demonstra os documentos mais exigidos pelo poder público:

Figura 1

Documentos mais exigidos para acesso aos 208 serviços públicos da amostra.



Fonte: IPEA – Instituto de Pesquisa Econômico Aplicada.

Diante dessa informação, os dados pessoais que estão em conhecimento do governo, devem ser usados de maneira racional e justificada, ou seja, somente pode ser feita quando

importante para suas funções legais. Ressaltando, o propósito do compartilhamento é especificamente definido e comunicado ao titular dos dados.

ARTIGO 26: CONDIÇÕES PARA O COMPARTILHAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO

"Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei.

§ 1º É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto:

> I - em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) ;
> III - nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei.
> IV - quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres; ou (Incluído pela Lei nº 13.853, de 2019)
> V - na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades. (Incluído pela Lei nº 13.853, de 2019)"
> § 2º Os contratos e convênios de que trata o § 1º deste artigo deverão ser comunicados à autoridade nacional.

O Artigo 26 da LGPD determina as regras e restrições para a troca de informações pessoais entre os órgãos e entidades governamentais. Com o objetivo de proteger a privacidade e segurança dos dados dos cidadãos, essa norma se esforça para garantir que o processamento das informações pessoais seja feito de maneira clara e responsável.

Nesse sentido, é essencial que as autoridades sigam as diretrizes da LGPD e implementem medidas de segurança e transparência ao compartilhar informações pessoais. É fundamental que os usuários tenham conhecimento de seus direitos e possam controlar suas informações pessoais para garantir sua privacidade e segurança, garantindo transparência e prestação de contas no tratamento desses dados.

ARTIGO 27: COMPARTILHAMENTO COM ENTIDADES PÚBLICAS E PRIVADAS

Art. 27. A comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado será informada à autoridade nacional e dependerá de consentimento do titular, exceto:

> I - nas hipóteses de dispensa de consentimento previstas nesta Lei;
> II - nos casos de uso compartilhado de dados, em que será dada publicidade nos termos do inciso I do caput do art. 23 desta Lei; ou
> III - nas exceções constantes do § 1º do art. 26 desta Lei.
> Parágrafo único. A informação à autoridade nacional de que trata o caput deste artigo será objeto de regulamentação. (Incluído pela Lei nº 13.853, de 2019)

De acordo com o artigo 27 da LGPD, é necessário que o poder público tenha permissão ou autorização do titular dos dados para compartilhar informações pessoais com outras entidades públicas ou privadas de maneira legal e legítima. Além disso, a transferência de informações pessoais pelo governo deve ser feita em conformidade com as regras da LGPD e outras leis relevantes.

Para os órgãos públicos, a partilha de dados pode ser essencial para o correto desempenho dos serviços públicos, tais como saúde, educação, segurança, entre outros. Por exemplo, as informações de saúde de um paciente podem ser trocadas entre hospitais e postos de saúde para garantir um atendimento eficaz e unificado.

Dentro das organizações privadas, a troca de informações pode contribuir para aprimorar os produtos e serviços disponibilizados, personalizar campanhas de marketing, detectar fraudes, entre outras utilidades. Entretanto, as empresas devem seguir as leis e obter permissão dos usuários para compartilhar suas informações.

Dessa maneira, é fundamental que os órgãos e entidades do poder público implementem ações de monitoramento e supervisão para garantir a conformidade com as normas da LGPD.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD)

A Autoridade Nacional de Proteção de Dados (ANPD) é um órgão criado pela Lei Geral de Proteção de Dados (LGPD), de 2018, que visa regular e fiscalizar o tratamento de dados pessoais no Brasil. A ANPD tem como objetivo garantir a privacidade e a segurança das informações dos cidadãos, além de promover a transparência e a responsabilidade no manuseio desses dados pelas organizações.

A autoridade está relacionada ao fato de que, com o avanço da tecnologia e a crescente quantidade de informações digitais, a proteção dos dados pessoais se tornou fundamental para prevenir abusos e garantir a privacidade dos indivíduos. Com isso, existiu a necessidade da criação da ANPD, que representa um avanço significativo na legislação brasileira, contando com uma autoridade independente e especializada para fiscalizar o cumprimento das normas de proteção de dados. Sua atuação abrange diversos aspectos, como a elaboração de normas e diretrizes para o tratamento de dados pessoais, a fiscalização das organizações quanto ao cumprimento da LGPD e a aplicação de sanções em caso de infrações. Ademais, a autoridade também é responsável por receber denúncias e reclamações dos cidadãos em relação ao uso inadequado de seus dados pessoais, desempenhando um papel fundamental na proteção da privacidade e segurança dos dados pessoais dos cidadãos brasileiros, garantindo o cumprimento da legislação de proteção de dados e promovendo a transparência e responsabilidade no tratamento das informações digitais.

Então, é um grande passo na proteção dos direitos individuais e na promoção da segurança digital no Brasil, esse avanço coloca o país em conformidade com as principais leis internacionais, como o GDPR da União Europeia, sendo um marco na proteção de dados no território nacional. Devendo-se ao fato de que é responsabilidade do Estado garantir a segurança e o bem-estar da sociedade, utilizando informações para prevenir atividades ilegais e manter a ordem pública.

No Brasil, a Lei Geral de Proteção de Dados (LGPD) define como diretrizes para a coleta, guarda, processamento e compartilhamento de dados pessoais, fundamentais para garantir a integridade, confidencialidade e disponibilidade das informações. Dessa forma, é essencial implementar medidas de proteção de dados que englobem a categorização das informações, restrição de acesso, supervisão, supervisão de sistemas e antecipação de ocorrências. Além disso, é preciso implementar medidas de segurança de informações pessoais de acordo com a lei em

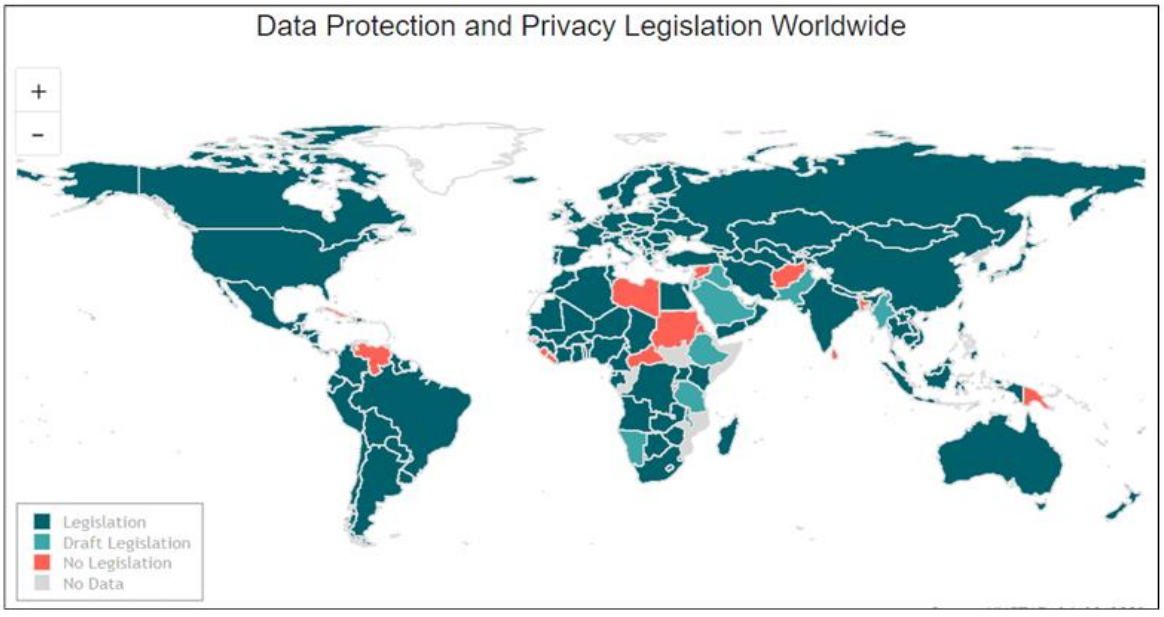
vigor, como a LGPD, para garantir a privacidade e os direitos dos indivíduos. Colocar na prática medidas de segurança cibernética, avaliar riscos e treinar funcionários públicos são importantes para reduzir ameaças e manter a confiança da sociedade no compartilhamento de dados pelo governo.

ANÁLISE DAS POLÍTICAS DE COMPARTILHAMENTO DE DADOS ADOTADAS PELO PODER PÚBLICO EM DIFERENTES PAÍSES

As políticas de disponibilização de informações adotadas pelo poder público variam de nação para nação, com diferentes abordagens para garantir a salvaguarda dos dados dos cidadãos e facilitar o aproveitamento eficaz dessas informações para aprimorar os serviços públicos. Nos Estados Unidos, por exemplo, o governo tem impulsionado a iniciativa de Dados Abertos, que busca disponibilizar informações governamentais de maneira acessível e transparente para o público em geral. Isso inclui a criação de portais de informações públicas, onde os cidadãos podem acessar e utilizar uma ampla gama de dados governamentais. Mostra-se a figura 2, que apresenta o cenário mundial em relação a proteção de dados:

Figura 2

Legislação sobre proteção de dados pessoais e privacidade ao redor do mundo



Fonte: United Nations Conference on Trade and Development (2021).

Como demonstrado na figura, a maioria dos países se adaptaram com a rápida evolução da tecnologia, porém território é responsável por sua própria legislação. Por exemplo, o Reino

Unido, o governo adotou uma abordagem mais focada na salvaguarda da privacidade dos cidadãos, implementando regulamentos rigorosos para garantir o uso responsável e seguro dos dados. Isso envolve a Lei de Proteção de Dados e o Regulamento Geral de Proteção de Dados (GDPR), que estabelecem normas claras sobre como os dados pessoais devem ser coletados, armazenados e compartilhados. Em nações como a China, se tem aderido políticas de compartilhamento de informações mais centralizadas, com ênfase na coleta em larga escala de informações dos cidadãos para fins de monitoramento e controle. Isso levanta preocupações sobre a privacidade e a segurança dos dados dos cidadãos, principalmente em um contexto de vigilância governamental cada vez mais intensa.

Contudo, muitos países têm implementado regulações específicas para garantir que a partilha de dados seja feita de forma legal e segura. Um exemplo disso é o Regulamento Geral de Proteção de Dados (GDPR), uma legislação da União Europeia que estabelece normas claras sobre como as empresas e organizações devem lidar com os dados pessoais dos cidadãos europeus. O GDPR impõe restrições ao uso e partilha de dados pessoais, exige o consentimento prévio dos indivíduos para a recolha e processamento dos seus dados, e estabelece sanções para o não cumprimento das regras. Alguns países, como os Estados Unidos, também têm regulações específicas para a partilha de dados pelo governo.

Também, a Lei de Proteção à Privacidade Online (COPPA), como, estabelece regras para a recolha e partilha de dados de crianças menores de 13 anos. Na China, o governo implementou o Cybersecurity Law, uma legislação que impõe restrições à partilha de dados pessoais e exige que as empresas de tecnologia armazenem os dados dos cidadãos chineses dentro do país.

Dessa maneira, as táticas de compartilhamento de dados utilizadas pelo governo em diferentes países refletem uma crescente atenção à proteção da privacidade e segurança das informações dos habitantes. O GDPR e outras leis semelhantes são eficazes para proteger esses direitos, ao mesmo tempo que promovem a inovação e o avanço ético da tecnologia. Dessa forma, é fundamental que o setor público melhore constantemente suas estratégias de compartilhamento de dados, garantindo que estejam em conformidade com as melhores práticas de segurança da informação.

A legislação GDPR da União Europeia, em vigor desde 25 de maio de 2018, tem como objetivo garantir a segurança e a confidencialidade das informações pessoais dos cidadãos europeus. O Regulamento Geral de Proteção de Dados define diretrizes precisas sobre a forma como as organizações devem coletar, armazenar e manipular dados pessoais, bem como os

direitos dos indivíduos em relação aos seus dados. Mas o GDPR requer consentimento explícito para coleta e processamento de dados pessoais, permite que os cidadãos acessem, corrijam e eliminem informações, exige que as empresas notifiquem autoridades e cidadãos sobre publicações de dados e sanções severas para não cumprir suas regras.

Todas as empresas e organizações que lidam com dados pessoais de indivíduos da União Europeia, mesmo que não estejam sedadas na UE, devem cumprir o Regulamento Geral de Proteção de Dados (RGPD). As empresas que não cumpram as normas do RGPD podem enfrentar multas de até 20 milhões de euros ou 4% da receita anual global, o que é maior.

DESAFIOS PARA EFETIVAÇÃO DO PODER PÚBLICO NO USO E PROTEÇÃO DE DADOS PESSOAIS

A falta de investimento em segurança cibernética por parte do poder público pode resultar em vazamentos de dados pessoais, o que viola a privacidade e a intimidade dos indivíduos. Segundo a Constituição Federal, em seu artigo 5º, inciso X, "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito à indenização pelo dano material ou moral decorrente de sua violação". Segundo o doutrinador Carlos Ari Sundfeld, "o poder público muitas vezes enfrenta dificuldades na implementação de políticas de proteção de dados, seja por falta de estrutura adequada, seja pela resistência de servidores públicos em aderir às novas práticas". Isso pode dificultar a efetiva proteção dos dados pessoais dos cidadãos. Também, enfrenta desafios no controle do uso adequado dos dados pessoais coletados, evitando que sejam utilizados para finalidades não consentidas pelos titulares. A LGPD (Lei Geral de Proteção de Dados), em seu artigo 7º, estabelece princípios como a finalidade, adequação e necessidade no tratamento de dados pessoais, visando garantir a proteção dos direitos dos cidadãos.

E como a falta de padronização e interoperabilidade entre os sistemas de diferentes órgãos, dificultando a integração e a análise conjunta das informações. Além disso, as questões relacionadas à segurança cibernética e privacidade dos dados são pontos sensíveis, exigindo investimentos em tecnologias e processos de proteção, e a capacitação de servidores públicos com a gestão e compartilhamento de dados também é um desafio, assim como a conscientização da sociedade sobre a importância e os benefícios desse processo para a transparência e eficiência do governo. Por fim, a burocracia e a resistência à mudança em estruturas consolidadas podem representar limitações para a implementação efetiva do compartilhamento de dados pelo Poder

Público.

Diante disto, compreende que o governo precisa adaptar seus processos internos para garantir a proteção adequada dos dados pessoais. Isso envolve revisar procedimentos, treinar servidores e adotar medidas técnicas e administrativas. Com intuito de uma construção da cultura organizacional voltada à proteção de dados é essencial e diretrizes de boas práticas e governança devem nortear as ações relacionadas ao tratamento de dados dentro da organização. Se exigindo da utilização de medidas técnicas e administrativas para proteger os dados pessoais contra acessos não autorizados, destruição, perda, alteração, comunicação ou difusão, devendo estar ciente das sanções administrativas previstas na LGPD, que podem ser aplicadas em caso de descumprimento das normas. Tendo como finalidade o uso compartilhado de dados pessoais entre órgãos públicos requer atenção especial, sendo importante considerar a relação entre as normas de proteção de dados e o acesso à informação pública.

A legislação existente muitas vezes não é clara o suficiente para lidar com as especificidades do compartilhamento de dados pelo Poder Público, o que acarreta em interpretações divergentes e precedentes jurisprudenciais ainda em evolução. Além disso, a conformidade com leis internacionais e acordos de compartilhamento de dados entre países também representam dificuldades adicionais, exigindo uma análise detalhada de cada caso e um acompanhamento constante das mudanças legais e jurisprudenciais

A LEGALIDADE DOS ÓRGÃOS JUDICIÁRIOS ACESSAREM E COMPARTILHAREM DADOS PESSOAIS DOS CIDADÃOS

Conforme o artigo 7º da LGPD, o tratamento de dados pessoais por órgãos públicos deve obedecer aos princípios da finalidade, adequação, necessidade, livre acesso, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas. Desse modo, possibilita o melhoramento da qualidade dos serviços prestados à população, através da customização e personalização dos atendimentos, de acordo com as necessidades e características individuais de cada cidadão. Como destaca o artigo "Benefícios do uso de dados em serviços públicos", do Instituto Brasileiro de Governança Pública (IBGP), "o acesso a dados pessoais dos cidadãos permite que os órgãos públicos identifiquem demandas específicas e desenvolvam soluções mais eficazes e eficientes para atender às necessidades dos cidadãos".

Destaca-se que a relevância do judiciário ter acesso e compartilhar dados pessoais é

garantir uma justiça mais eficaz e transparente para a sociedade. Ao ter acesso a essas informações, o sistema judiciário poderá examinar com maior precisão e imparcialidade os casos legais que são submetidos, garantindo a proteção dos direitos dos indivíduos e a observância da legislação. Exemplo disso é o Infojud, que é o Sistema de Informações ao Judiciário, foi desenvolvido a partir de uma parceria entre o CNJ e a Receita Federal do Brasil, utilizando outros sistemas como referência. É um serviço exclusivo para membros do poder judiciário (e servidores autorizados), que visa atender às solicitações dos magistrados. O Bacenjud, por sua vez, conecta dados da Justiça e do Banco Central do Brasil, agilizando informações e ordens judiciais ao Sistema Financeiro Nacional. O Sisbajud permite que magistrados solicitem informações ao Banco Central. Já o Renajud é um sistema de restrição judicial de veículos interligando o Judiciário ao Denatran.

Com base no que foi dito, os órgãos públicos têm o direito de utilizar e compartilhar dados pessoais, mesmo que isso signifique ignorar a privacidade, pois é fundamental garantir a qualidade, segurança e eficiência na gestão das informações, priorizando o interesse coletivo em detrimento do individual. Isso inclui estabelecer políticas, regulamentos e orientações para o uso, compartilhamento e proteção de dados públicos, e também desenvolve estruturas de governança que determinam responsabilidades específicas e mecanismos de supervisão. A governança de dados também busca garantir a transparência e a responsabilidade, de modo a garantir que o uso dos dados respeite os interesses públicos e esteja em conformidade com a legislação em vigor.

BENEFÍCIOS, OPORTUNIDADES E DESENVOLVIMENTO DO COMPARTILHAMENTO DE DADOS PÚBLICOS

O compartilhamento de dados públicos traz inúmeros benefícios e oportunidades para a sociedade, governos e setor privado. Ao disponibilizar informações abertas, há potencial para impulsionar a inovação, promover a transparência e aumentar a eficiência dos serviços públicos, o acesso a dados pode facilitar a criação de soluções para desafios sociais, como saúde, educação e mobilidade urbana. Também pode estimular a economia, com a geração de empregos e o desenvolvimento de novos mercados. Diante desse cenário, o compartilhamento de dados públicos se configura como uma ferramenta fundamental para promover o desenvolvimento sustentável e a melhoria da qualidade de vida da população.

A oportunidade da colaboração entre o setor público e privado no compartilhamento de

dados públicos é essencial para garantir a eficiência e a segurança da troca de informações. Através de parcerias estratégicas, ambos os setores podem contribuir com suas respectivas expertises, conhecimentos e recursos para viabilizar o compartilhamento de dados de forma responsável e benéfica para a sociedade. É importante estabelecer diretrizes claras e mecanismos de governança que promovam a transparência, a proteção de dados e a adesão aos princípios éticos, garantindo que a colaboração seja pautada pelo interesse público e pelo respeito aos direitos individuais dos cidadãos. Desse modo, a cooperação entre setor público e privado pode impulsionar a inovação e o desenvolvimento de soluções tecnológicas avançadas que potencializem o aproveitamento dos dados compartilhados, com desenvolvimento de políticas e estratégias para o compartilhamento de dados públicos requer um profundo conhecimento das necessidades e demandas da sociedade, bem como a criação de mecanismos de governança eficazes.

É essencial a realização de consultas públicas e envolvimento dos diversos atores interessados, além de contar com especialistas em tecnologia da informação, proteção de dados e direito para a elaboração de normativas robustas. A transparência e prestação de contas devem ser pilares dessas políticas, proporcionando segurança e confiança à população, que devem proporcionar o estabelecimento de parcerias estratégicas com o setor privado, academia e organizações da sociedade civil também é crucial para o sucesso das políticas de compartilhamento de dados públicos e a maximização dos benefícios para a sociedade.

TECNOLOGIAS, FERRAMENTAS E ESTUDO PARA O COMPARTILHAMENTO DE DADOS PÚBLICOS

Diferentes tecnologias e ferramentas podem simplificar a partilha de dados públicos, como plataformas de nuvem para armazenamento seguro, ferramentas de análise de dados para identificar padrões e tendências, e APIs que facilitam a integração de sistemas e a troca de informações de maneira eficaz. Além disso, a utilização de blockchain pode garantir a proteção e a permanência dos dados partilhados, ao passo que a adoção de normas abertas e interoperáveis simplifica a interligação entre diversos sistemas e entidades governamentais. Finalmente, o uso de ferramentas de visualização de dados ajuda a tornar as informações mais acessíveis e compreensíveis para os cidadãos e demais partes interessadas.

A implementação de um portal de transparência em um município é um exemplo de

compartilhamento de dados públicos, onde a população pode acessar e baixar informações sobre gastos, licitações e contratos. Em outra situação seria a colaboração entre o governo e as instituições de ensino superior para trocar informações de pesquisas que possam auxiliar no avanço de políticas públicas e na tomada de decisões embasadas. Ademais, estabelecer um banco de dados nacional de saúde contendo dados anônimos de pacientes pode ser visto como uma forma de compartilhamento de informações para ampliar estudos e controle de doenças. Estes exemplos mostram diversas formas e vantagens de compartilhamento de informações pelo governo.

Nesse sentido, deve garantir a eficiência e segurança na disponibilização de informações é crucial, sendo fundamental o desenvolvimento da infraestrutura de dados para o compartilhamento público. Isso inclui o desenvolvimento de plataformas fortes e compatíveis, juntamente com o estabelecimento de normas e diretrizes para a comunicação de informações entre órgãos governamentais. Outrossim, é essencial alocar recursos em tecnologias que garantam a segurança e o correto dos dados, respeitando as normas de privacidade e segurança da informação. Uma execução a proteção e o tratamento adequado das informações, levando em consideração as diretrizes de privacidade e segurança da informação. Também, a implementação de uma infraestrutura sólida contribui para a transparência e acessibilidade das informações, promovendo a confiança da sociedade no compartilhamento de dados pelo poder público.

CASOS E PRECEDENTES

Casos de sucesso no compartilhamento de dados incluem a utilização de informações de várias fontes para aprimorar os serviços públicos, como a união de dados de diferentes entidades para facilitar o acesso do público a vantagens sociais, a utilização de dados de saúde para vigiar e evitar epidemias, e o intercâmbio de informações entre organizações de segurança para combater delitos. Além do mais, em decisões judiciais importantes, o STF já opinou sobre a legalidade do compartilhamento de informações pelo Governo. Estas decisões foram abordadas sobre a segurança das informações pessoais, a importância da transparência e da responsabilidade do governo, e os limites de acesso do Estado a dados privados dos indivíduos.

Implementação de Políticas Públicas: A utilização de dados é fundamental para executar políticas públicas, como aquelas externas para a saúde e a educação. Durante a pandemia de COVID-19, por exemplo, o compartilhamento de dados foi essencial para rastrear a propagação

do vírus e coordenar as campanhas de vacinação.

Além disso, o compartilhamento de informações entre órgãos públicos visa aprimorar a eficácia e a excelência dos serviços prestados à comunidade. Uma ilustração disso é a união de sistemas de segurança pública que combate à criminalidade de maneira mais eficiente.

Também, O STF determinou que, mesmo em situações de emergência, a troca de informações pelo governo deve seguir os direitos fundamentais dos cidadãos. Essas escolhas enfatizam a importância de uma legislação sólida e a segurança das informações individuais.

Num processo conjunto, o Supremo Tribunal Federal ressaltou os riscos de imprecisão da definição de interesse público e da importância de diretrizes claras para a troca de informações. A decisão destacou a relevância de uma boa governança e o respeito aos direitos dos donos dos dados.

JUSTIFICATIVA

O compartilhamento de dados pelo poder público é um tema de crescente importância em virtude da digitalização dos processos administrativos e do volume de dados sensíveis tratados pelo governo. Além de estar alinhado às demandas da sociedade por transparência e eficiência, o estudo se justifica pelo impacto direto que políticas bem inovadoras podem ter no fortalecimento da governança e na proteção de direitos fundamentais, como a privacidade. Considerando o contexto brasileiro, onde a implementação da LGPD ainda enfrenta desafios, esta pesquisa fornece uma análise aprofundada que ajuda como subsídio para aprimorar as práticas de gestão de dados.

METODOLOGIA

A pesquisa utiliza abordagem qualitativa e descritiva, com foco em análise documental e estudo de casos. Inicialmente, foram identificadas e provas as legislações relacionadas ao compartilhamento de dados, como a LGPD e o GDPR, a partir de uma revisão bibliográfica estruturada. Paralelamente, foram selecionados casos emblemáticos de políticas de dados inovadoras no Brasil e em outros países, a fim de identificar boas práticas e limitações. As informações foram organizadas em categorias temáticas para análise comparativa. Além disso,

considerações éticas foram observadas, especialmente no que diz respeito ao uso de dados e à proteção dos envolvidos.

RESULTADOS E DISCUSSÕES

Os resultados da pesquisa destacam que o compartilhamento de dados pelo poder público, quando implementado de forma ética e segura, pode gerar benefícios significativos, como maior transparência administrativa, eficiência na prestação de serviços e estímulo à inovação tecnológica. Países que adotam regulamentações robustas, como o GDPR na União Europeia, apresentam avanços importantes na proteção de dados e no equilíbrio entre privacidade e acesso à informação, opcionalmente de referência para o contexto brasileiro.

No entanto, uma análise revelou desafios persistentes no Brasil, como a falta de interoperabilidade entre sistemas públicos, a capacitação insuficiente de servidores públicos e a resistência organizacional às mudanças. Esses fatores comprometem a eficácia do compartilhamento de dados, gerando insegurança jurídica e redução de confiança pública.

Além disso, estudos de caso mostram que a implementação de portais de transparência e o uso de tecnologias como blockchain podem minimizar riscos de vazamento de informações e melhorar a rastreabilidade. Assim, reforçar-se-á a importância de investimentos contínuos em governança, inovação e adaptação das normas locais às demandas globais.

CONCLUSÃO

Ao finalizar esta análise detalhada sobre o compartilhamento de dados pelo Poder Público, destaca-se a fundamental importância da transparência e segurança no manuseio de informações tão críticas para a sociedade. Foi destacado a necessidade imediata de implementar políticas consistentes que garantam a segurança dos dados confidenciais dos cidadãos, sem impedir o acesso a informações confidenciais e confidenciais

A utilização de tecnologias avançadas e inovadoras, juntamente com a formação constante de profissionais inovadores e atualizados, é crucial para lidar com os desafios complexos do compartilhamento de dados pelo Governo. Evidencia-se a relevância fundamental de manter um comprometimento constante e forte com a ética e a responsabilidade no uso dessas

informações importantes, já que essa dedicação é essencial para garantir um benefício concreto para toda a sociedade.

Olhando para o futuro, é crucial compreender a importância da era digital e como ela afeta a maneira como os dados são compartilhados. À medida que avançamos para uma sociedade cada vez mais conectada, é essencial adotar abordagens proativas para lidar com os desafios emergentes e fortalecer a segurança. A cooperação entre diversos setores e esferas governamentais eficiente, bem como a sociedade civil, é fundamental para estabelecer uma cultura de compartilhamento responsável e coletivo, com foco na segurança dos direitos individuais e coletivos.

Além disso, é ressaltado o imperativo de investir constantemente em pesquisa e desenvolvimento de soluções inovadoras para garantir a integridade e acessibilidade dos dados. A utilização de métodos fundamentados em evidências para a tomada de decisões é crucial, incluindo a realização de análises de dados sólidos e a utilização de ferramentas analíticas avançadas para avaliar o impacto das políticas aplicadas. Essa metodologia garante que os dados sejam utilizados de forma eficiente, justa e equitativa, evitando qualquer tipo de prejuízo para as partes envolvidas.

Concluindo, que em suma, o compartilhamento de dados pelo Poder Público é crucial para reforçar a governança, melhorar serviços e fomentar a participação cidadã. Mas, para que seja efetuado de forma equitativa, são necessárias garantias robustas de direitos individuais, aprimoramento da cibersegurança e total transparência. Uma abordagem abrangente, ética e inovadora é fundamental para edificar uma sociedade digital inclusiva, onde o compartilhamento de dados propicie desenvolvimento sustentável e bem-estar para \todos.

REFERÊNCIAS

ANPD. *"Guia Orientativo para a Aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD)".* Disponível em: https://www.gov.br/anpd/pt-br. Acesso em: 10 jan. 2025.

Barreto, Bernardo Pereira de Lucena**.** *O direito fundamental à proteção de dados pessoais no Brasil.* Revista de direito do consumidor, v. 85, p. 95-115, 2013.

Brasil. *Constituição da República Federativa do Brasil.* Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 10 jan. 2025.

Carvalho, Sérgio Tadeu Neiva. *COMPARTILHAMENTO DE DADOS ENTRE ÓRGÃOS E ENTIDADES DA ADMINISTRAÇÃO PÚBLICA.* 2018. IPEA – Instituto de Pesquisa

Econômico Aplicada. Disponível em: https://portalantigo.ipea.gov.br/. Acesso em: 10 jan. 2025.

Lei Geral de Proteção de Dados (LGPD). Lei nº 13.709, de 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 07 jan. 2025.

Decisões do Supremo Tribunal Federal (STF): *Ação Direta de Inconstitucionalidade (ADI) 6.387, 6.388, 6.389, 6.390 e 6.393*. Disponível em: https://portal.stf.jus.br/. Acesso em: 04 jan. 2025.

Ação Direta de Inconstitucionalidade (ADI) 6.649 e Arguição de Descumprimento de Preceito Fundamental (ADPF) 695. Disponível em: https://portal.stf.jus.br/. Acesso em: 13 jan. 2025.

Doneda, Danilo. *"Da Privacidade à Proteção de Dados Pessoais."* Revista de Direito do Consumidor, vol. 100, 2016.

FB de Menezes, BMR Pilon - Revista da ESDM, 2022 - revista.esdm.com.br. *A LEI GERAL DE PROTEÇÃO DE DADOS EA ADMINISTRAÇÃO PÚBLICA.* Disponível em: esdm.com.br. Acesso em: 02 jan. 2025.

H Osswald - Revista Eletrônica Ciência & Tecnologia …, 2024 - revista.grupofaveni.com.br. **A** *LEI GERAL DE PROTEÇÃO DE DADOS APLICADA AO DIREITO ADMINISTRATIVO.* Disponível em: grupofaveni.com.br. Acesso em: 10 jan. 2025.

JL de Sousa Chaves - Caderno Virtual, 2021 - portaldeperiodicos.idp.edu.br**.** *O IMPACTO DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) NAS INVESTIGAÇÕES ADMINISTRATIVAS.*Disponível em: idp.edu.br. Acesso em: 20 dez. 2024.

L de Jesus Oliveira, TG Novais - Revista Ibero-Americana de …, 2024 - periodicorease.pro.br. *LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS: RESPONSABILIDADE CIVIL NO VAZAMENTO DE INFORMAÇÕES.* Disponível em: periodicorease.pro.br. Acesso em: 10 jan. 2025.

LMR Gonçalves - Ratio Juris. Revista Eletrônica da Graduação da …, 2023 - fdsm.edu.br. *Lei geral de proteção de dados e privacidade.* Disponível em: fdsm.edu.br. Acesso em: 10 jan. 2025.

MGC Cavenaghi, LRP Paris… - … ISSN: 2674-8576 …, 2024 - prospectus.fatecitapira.edu.br. *Lei Geral de Proteção de Dados e a Segurança da Informação: Atuação do Gestor de Tecnologia da Informação.* Disponível em: fatecitapira.edu.br. Acesso em: 06 dez. 2025.

TCE-RO.*Tratamento de Dados Pelo Poder Público – LGPD***.** Disponível em: (tcero.tc.br). Acesso em: 07 jan. 2025.

UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT. Trade and Development Report 2018. New York e Genebra: United Nations, 2018.

Viola, Eduardo Magrani. *"Internet das Coisas: A Internet das Coisas e o Direito."* Revista de Direito, vol. 2, 2018.