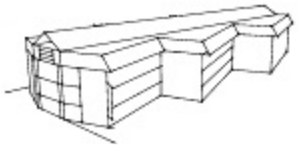

UNIVERSIDADE FEDERAL DE UBERLÂNDIA

FACULDADE DE DIREITO

GRADUAÇÃO EM DIREITO

ALFEU DE OLIVEIRA JÁCOME

APLICAÇÃO DA LGPD, NO COMPARTILHAMENTO DE DADOS DO PORTAL GOV.BR

APLICAÇÃO DA LGPD, NO COMPARTILHAMENTO DE DADOS DO PORTAL GOV.BR

Trabalho de conclusão de curso apresentado ao curso de apresentado à Faculdade de Direito da Universidade Federal de Uberlândia

Orientador: Prof. Dr. Ricardo Padovini Pleti Ferreira

Uberlândia - MG

2026

APLICAÇÃO DA LGPD, NO COMPARTILHAMENTO DE DADOS DO PORTAL GOV.BR

Trabalho aprovado para a obtenção do título de Bacharel em Direito pelo Curso de Graduação em Direito da Universidade Federal de Uberlândia (MG), após avaliação da banca examinadora composta por:

_____

Prof. Dr. Ricardo Padovini Pleti Ferreira, UFU/MG

_____

Prof. Dr. [nome do professor]

_____

Prof. Dr. [nome do professor]

Uberlândia, [dia] de [mês] de [ano].

DEDICATÓRIA

À minha querida mãe, que enquanto estava presente entre nós, foi fonte de apoio irrestrito.

AGRADECIMENTOS

Aos colegas de jornada, pelo auxílio e compreensão nesta jornada comum, de formação acadêmica;

Aos professores, por compartilharem o seu tempo e conhecimento no esforço para contribuir com a minha formação profissional, durante a graduação;

Ao meu orientador por trazer direcionamento e incentivo, para que este trabalho pudesse ser concluído.

À minha família por entender as ausências necessárias na busca da minha formação acadêmica

Meus mais sinceros agradecimentos!

JÁCOME, Alfeu de Oliveira Jácome. **Aplicação da LGPD, no compartilhamento de dados do portal gov.br**. Trabalho de Conclusão de Curso. Bacharelado em Direito. Faculdade de Direito de Uberlândia-MG. 2026.

RESUMO

A aplicação da Lei Geral de Proteção de Dados (LGPD) no contexto estratégico do governo digital e a centralização das informações pelo portal Gov.br é um problema a ser investigado, com o objetivo de se verificar os riscos a privacidade e a autodeterminação informativa que são decorrentes, do compartilhamento entre os vários órgãos estatais, que poderia em tese, favorecer a vigilância de uma forma massiva, o perfilamento discriminatório dos cidadãos e a violação da integridade contextual, problema intensificado, quando se leva em consideração que as técnicas de anonimização na era do *Big Data*, se tornam bastante fragilizadas. O objetivo foi de se avaliar a eficácia da legislação trazida pela LGPD, como um mecanismo de enfrentamento e controle do poder estatal em relação a estas ameaças. A metodologia utilizada foi análise empírica através de estatísticas oficiais, indicadores de desempenho e estudos de caso. A conclusão de que a Lei Geral de Proteção de Dados (LGPD), proporciona ampla proteção aos dados sob controle estatal, foi confirmada ao se detalhar os dispositivos trazidos na lei e na constituição federal, somado as técnicas computacionais para seguranças dos dados, a elaboração obrigatória de Relatórios de Impacto à Proteção de Dados (RIPD) e a governança realizada por meio da Autoridade Nacional de proteção de Dados (ANDP), mitiga os riscos advindos da centralização de dados no portal Gov.br, capturados nos diversos órgãos governamentais para finalidades específicas de cada órgão da Administração Pública, garantindo que o cidadão não seja tratado como mero “objeto de informação”.

Palavras-chave: Lei Geral de Proteção de Dados. Relatório de Impacto à Proteção de Dados Pessoais. Lei de Acesso à Informação. Autodeterminação informativa. Privacidade contextual. Vigilância estatal.

JÁCOME, Alfeu de Oliveira. **Application of the LGPD in data sharing on the gov.br portal**. Undergrad Thesis (Bachelor of Laws). Faculty of Law, Uberlândia-MG, Brazil. 2026**.**

ABSTRACT

The application of the General Data Protection Law (LGPD) within the strategic context of digital government and the centralization of information through the Gov.br portal constitutes a problem to be investigated. This study aims to verify the resulting risks to privacy and informative self-determination arising from data sharing among various state agencies, which could, in theory, foster mass surveillance, discriminatory profiling of citizens, and the violation of contextual integrity. This issue is intensified considering that anonymization techniques in the Big Data era have become increasingly fragile. The objective was to evaluate the effectiveness of the LGPD as a mechanism for confronting and controlling state power regarding these threats. The methodology employed was empirical analysis through official statistics, performance indicators, and case studies. The conclusion that the LGPD provides comprehensive protection for data under state control was confirmed by detailing the provisions established in the law and the Federal Constitution. Furthermore, computational data security techniques, the mandatory preparation of Data Protection Impact Reports (DPRR/RIPD), and governance carried out by the National Data Protection Authority (ANPD) mitigate the risks stemming from data centralization on the Gov.br portal—data captured across various government agencies for their specific purposes—ensuring that the citizen is not treated as a mere 'object of information'

Keywords: General Data Protection Law. Data Protection Impact Assessment, Access to Information Act, Informational Self-determination. Contextual Privacy. State Surveillance.

Sumário

1. Introdução

O crescente volume de dados de natureza pessoal, que passou a ser compartilhado no ambiente digital, colocou a proteção de dados como um ponto central nos debates atuais. No caso brasileiro, para atender a esta necessidade, o legislador elaborou, em 14 de agosto de 2018, a Lei nº 13.709, conhecida como Lei Geral de Proteção de Dados (LGPD), um conjunto de normas que traz princípios e garantias que promovem a proteção de dados, podendo ser aplicada tanto no setor privado, quanto no setor público.

Como forma de atender aos cidadãos com maior eficiência, o Estado lançou, em 1º de agosto de 2019, por meio do Decreto nº 9.756/2019, o portal Gov.br, que buscou centralizar, em uma única plataforma, os serviços governamentais que antes se encontravam dispersos em diversos sites estatais. Assim, os dados dos cidadãos que buscam os serviços governamentais passaram a ser centralizados sob a gestão de um único portal.

Essa centralização levanta um importante questionamento quanto a uma possível vulnerabilidade, em razão da presença de dados cadastrais e biométricos entre os registros mantidos pelo portal Gov.br. Levando em consideração que de forma isolada as técnicas computacionais para garantir a proteção dos dados, como anonimização, se tornaram frágeis, em razão do avanço tecnológico das técnicas de reidentificação, principalmente pelo uso da chamado *Big Data*, faz-se necessária uma avaliação de como a Lei Geral de Proteção de Dados pode ser utilizada como instrumento garantidor da proteção dos dados sob a guarda do Estado, sobretudo quando o compartilhamento dessas informações pode ser realizado entre os diversos órgãos governamentais.

Nesse contexto, faz-se necessária uma avaliação criteriosa sobre como o compartilhamento de dados, desprovido de um regramento estrito, pode desvirtuar a finalidade pública da coleta e violar o direito fundamental à autodeterminação informativa.

O objetivo do presente artigo é analisar a eficácia da proteção conferida pela Lei Geral de Proteção de Dados (Lei nº 13.709/2018) no âmbito da Administração Pública, como mecanismo de controle para tais riscos. Para tanto, adotar-se-á análise empírica através de estatísticas oficiais, indicadores de desempenho e estudos de caso, para a condução do processo investigativo.

2. Da privacidade à proteção de dados: como controlar o poder estatal

A avaliação jurídica do conceito de privacidade sofreu transformações significativas ao longo dos anos, especialmente em razão dos avanços tecnológicos que alteraram, de forma profunda, a relação entre o cidadão e o Estado. A concepção clássica de privacidade, entendida como o "direito de ser deixado só" (*the right to be let alone*), formulada por Warren e Brandeis em 1890, na obra *The Right to Privacy,* tinha como foco principal a proteção contra a exposição indevida nas mídias. Contudo, esse entendimento mostrou-se insuficiente diante do cenário contemporâneo, marcado pela coleta massiva de dados nas diversas interações dos indivíduos com sistemas computacionais — desde simples cadastros para acesso a serviços até informações provenientes de interações em redes sociais, amplamente difundidas na atualidade.

Na sociedade da conectividade, a proteção da pessoa não pode mais se restringir ao isolamento ou à preservação do segredo. Torna-se necessário atuar como regulador do fluxo informacional, garantindo mecanismos de controle, limitação e transparência sobre o tratamento de dados pessoais. A transição do eixo composto por pessoa, informação e segredo para o modelo pessoa, informação, circulação e controle constitui elemento central para a consolidação de um novo patamar de tutela dos dados pessoais, superando a noção tradicional de privacidade e incorporando a lógica da autodeterminação informativa. Segundo Doneda (2020), a busca pela garantia de privacidade na atualidade está diretamente ligada a direitos fundamentais, como liberdade e igualdade. Assim nos apresenta Doneda, em sua obra *Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados:*

> É própria do nosso tempo a preocupação com a privacidade e como garanti-la. E a forma pela qual o direito a abordou durante muito tempo foi pela sua associação à busca de alguma forma de isolamento, refúgio ou segredo. A formação do conceito de privacidade, no entanto, aponta para elementos referentes a necessidades diversas, como a busca da igualdade, da liberdade de escolha, do anseio em não ser discriminado, entre outros. E, ainda, a privacidade está fortemente ligada à personalidade e ao seu desenvolvimento, para o qual é elemento essencial, em uma complexa teia de relações ainda a ser completamente vislumbrada pelo direito. (DONEDA, 2020, p. 31)

A proteção de dados, enquanto disciplina, surge como reação aos mecanismos de vigilância, sejam eles estatais ou privados, afastando-se do conceito inicial de preservação da intimidade restrita aos indivíduos mais abastados ou politicamente relevantes na sociedade.

De acordo com Doneda, em sua obra *Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados*, uma mudança significativa ocorreu na década de 1960, com a proposta de criação do *National Data Center*, nos Estados Unidos. O objetivo inicialmente apresentado era gerar economia de escala por meio da centralização, em âmbito federal, de dados censitários, fiscais e trabalhistas. Essa proposta levou o Congresso norte-americano a promover um amplo debate, que culminou na conclusão de que o ganho de escala não justificaria o risco às liberdades civis, risco esse inexistente quando os dados permaneciam distribuídos entre diversos órgãos independentes. A justificativa para tal entendimento foi a de que, uma vez na posse de um banco de dados centralizado, o Estado poderia mapear o perfil dos cidadãos, eliminando o sigilo necessário à manutenção da liberdade individual, que ficaria exposta às punições decorrentes da fiscalização estatal.

Esse episódio histórico permite concluir que sistemas centralizados tendem a facilitar práticas autoritárias relacionadas ao uso da informação armazenada, ampliando o potencial de vigilância e controle sobre os indivíduos. Como contraponto a esse risco, as legislações evoluíram para estabelecer formas efetivas de controle do fluxo informacional, com o objetivo de garantir que a finalidade estabelecida no momento da coleta seja fielmente aplicada nos momentos de tratamento e compartilhamento, de modo que, apesar de centralizados, os dados não sejam cruzados de maneira irrestrita, permitindo violações de direitos e discriminação dos titulares.

Segundo Bruno Bioni, em sua obra *Proteção de dados pessoais: a função e os limites do consentimento*, a decisão jurídica que iluminou esse cenário foi o importante julgado proferido pelo Tribunal Constitucional da Alemanha, em 1983, no caso relativo à Lei do Censo (*Volkszählungsurteil*) (ALEMANHA, 1983), acórdão de 15 de dezembro de 1983, BVerfGE 65, 1. Nessa decisão, reconheceu-se a faculdade do indivíduo de decidir sobre o uso e a divulgação de seus dados pessoais, estabelecendo as bases do que posteriormente seria denominado autodeterminação informativa. A proteção de dados pessoais foi alçada à condição de direito autônomo da personalidade. Assim, enquanto a privacidade resguarda o íntimo do indivíduo contra exposições indevidas, a proteção de dados atua como salvaguarda contra a transformação da pessoa em mero "objeto de informação", prevenindo ações discriminatórias decorrentes do uso de algoritmos que se valem desses dados.

Com o avanço das tecnologias de processamento, não é mais possível considerar determinados dados como insignificantes. O cruzamento de informações e sua correta

contextualização permitem, de forma relativamente simples, a identificação de perfis que podem ser utilizados para abordagens invasivas aos indivíduos assim segmentados. Dessa forma, a proteção deve deslocar seu foco do dado em si para as possíveis classificações e segregações que podem ser produzidas a partir do refinamento de dados brutos e desconexos. O indivíduo pode sofrer consequências nefastas do mau uso dessas informações, como segregações e discriminações, apenas por estar enquadrado em determinado perfil. Assim nos apresenta Bioni a importância da correção dos dados, para garantir o perfeito gozo do seu direito de personalidade, indo de encontro ao apresentado no julgado. Conforme afirmado no livro *Proteção de dados pessoais: a função e os limites do consentimento*, de Bioni:

> Ao lado do princípio da qualidade dos dados, o direito de correção é uma construção que deriva da perspectiva da identidade do sujeito e não do direito à privacidade. É o primeiro direito de personalidade que determina a necessidade de haver uma correspondência fidedigna entre a pessoa e seus dados pessoais. A esfera do que é público ou privado revela-se incompleta para dar vazão a esse tipo de dinâmica normativa. Por isso, os dados que influem na projeção de uma pessoa e na sua esfera relacional adéquam-se conceitualmente como um novo direito da personalidade. Alocar a proteção dos dados pessoais nessa categoria jurídica é uma construção dogmática necessária. Além de dar coerência normativa a uma série de faculdades jurídicas próprias desse direito (e.g automatizadas etc.), trata-se de um norte que facilita a sua interpretação e aplicação para não empolar a compreensão de seus conceitos basilares. (BIONI, 2019, p. 100)

A chamada anonimização de dados, frequentemente apresentada pelo governo como solução para evitar a identificação dos cidadãos a partir de bases centralizadas em ambientes governamentais, revela-se extremamente frágil diante da capacidade de processamento típica da era do Big Data. Essa capacidade permite, por meio de inferências e cruzamentos entre os diversos dados coletados nas interações dos cidadãos com as plataformas oficiais do país, a reidentificação de indivíduos — conforme alertam Carlos Barbieri, em *Governança de dados e LGPD: práticas, conceitos e novos caminhos*, e Bruno Bioni, em *Proteção de dados pessoais: a função e os limites do consentimento*. Do ponto de vista tecnológico, o Big Data é descrito como um modelo composto por cinco elementos: volume, velocidade, variedade, veracidade e valor. Seu fluxo operacional envolve etapas de coleta e ingestão, armazenamento em *data lakes*, processamento distribuído e, por fim, análise e visualização. Todo esse processo robusto, sustentado por elevado poder computacional, possibilita, com relativa facilidade, a reidentificação dos titulares das informações.

Pesquisas realizadas em diferentes países demonstram, de forma convincente, a fragilidade da técnica de anonimização. Um exemplo emblemático é o estudo conduzido pela

cientista da computação norte-americana Latanya Sweeney, publicado no artigo *Simple Demographics Often Identify People Uniquely* (*Carnegie Mellon University*), que evidenciou que o simples cruzamento de dados demográficos como CEP, gênero e data de nascimento permite identificar, de maneira individualizada, uma parcela significativa da população. A separação entre dados pessoais e dados anonimizados, portanto, depende diretamente da técnica empregada, tanto na fase de armazenamento quanto, sobretudo, na de manipulação.

Considerando que a anonimização apresenta fragilidades capazes de expor dados sensíveis e potencialmente segregar cidadãos, plataformas como o Gov.br não podem se apoiar exclusivamente em barreiras tecnológicas. É indispensável que o arcabouço jurídico assegure uma governança robusta, capaz de evitar desvios em relação às finalidades originalmente estabelecidas. Essa governança deve estar alinhada às melhores práticas, contemplando a avaliação da qualidade dos dados, garantindo sua correção, sua disponibilidade apenas a quem de fato se destina, conforme previsto na Lei de Acesso à Informação (LAI), bem como segurança e privacidade, nos termos da Lei Geral de Proteção de Dados (LGPD), além da conformidade com os normativos internos de cada órgão estatal.

O risco não se limita à possibilidade de vazamentos, mas se manifesta, sobretudo, no potencial de perfilamento estatal, mediante o uso de dados sensíveis, como informações de saúde, movimentações financeiras e dados biométricos centralizados em uma única plataforma digital. Caso não sejam rigorosamente controlados pelo titular e adequadamente regulados, esses dados podem ser utilizados para fins de vigilância digital ou até mesmo resultar em discriminação algorítmica.

3. Os limites irredutíveis ao uso de dados pelo governo (Gov.br)

A interoperabilidade trazida pela plataforma Gov.br, das mais diversas bases de dados da administração pública, necessita que os princípios de finalidade e adequação defendidos pela Lei Geral de Proteção de Dados (LGPD) sejam respeitados. A mera defesa de eficiência administrativa, que com certeza se mostra muito relevante, não pode sobrepor o princípio da finalidade e nem tão pouco da integridade contextual do correto fluxo das informações.

A autorização para o tratamento de dados que atendam ao interesse público deve estar condicionada ao estabelecido no art. 23, caput, da LGPD, que exige "finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais", e ao art. 6º, I, da LGPD: princípio da finalidade como princípio autônomo, e atenda ao princípio da legalidade estrita na Administração Pública, estabelecida no art. 37 da CF/88.

Assim, as informações de saúde obtidas durante um atendimento realizado no Sistema Único de Saúde (SUS) podem ser compartilhadas com outros órgãos da Administração Pública, como a Receita Federal, desde que sejam atendidos os preceitos no art. 23 da LGPD, a finalidade seja compatível com a saúde pública e estejam presentes as garantias do art. 6º, §4º. Caso contrário, teríamos uma violação da integridade de contexto e estaria comprometida a relação de confiança estabelecida no momento da coleta.

Não se pode permitir que haja o estabelecimento de uma finalidade genérica, fundamentada apenas no interesse público, pois, como estabelece o art. 23 da LGPD, o tratamento das informações tem que obrigatoriamente ter uma finalidade pública e específica para execução de competências legais.

A proteção dos dados pessoais não pode acontecer de forma independente do contexto em que a informação foi coletada. De Acordo com o autor Bruno Bioni, em seu livro *Proteção de dados pessoais: a função e os limites do consentimento*, que utilizada como base teórica a "privacidade contextual" de Helen Nissenbaum, do livro *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, nos apresenta que as violações à privacidade ocorrem quando o fluxo de dados não está de acordo com normas informacionais, que controlam um determinado contexto.

Para o caso aqui examinado do portal Gov.br, o fornecimento de dados pelos cidadãos, ocorrem de forma apartada, assim dados de saúde são fornecidos ao SUS, dados fiscais à

Receita Federal e dados biométricos à justiça eleitoral. O controle estatal destes dados, tem que necessariamente estar estabelecida em bases legais, como a Lei Geral de proteção de dados (LGPD), o Decreto nº 7.724/2012 (Infraestrutura Nacional de Dados), o Decreto nº 10.046/2019 (Gov.br) e outras inúmeras normas setoriais, evitando assim a utilização por órgãos distintos da administração pública em desacordo com a legislação. A título de exemplo, a transferência de dados relativos à saúde, mesmo para outro órgão da área saúde como a agência Nacional de Vigilância Sanitária (ANVISA), deve estar em acordo com os arts. 6º, §4º, e 23 da LGPD, além da Lei nº 13.709/2018 e do Código de Ética Médica.

O artigo 23 da LGPD, impõe um regime severo de tratamento de dados a ser feito pelo Estado, dispondo que este tratamento tenho um fim específico, para atingimento do interessa público, com a finalidade de execução de competências atribuídas por lei ou no cumprimento de suas atribuições legais, pertinentes ao serviço público.

Dados coletados para concessão de benefício social, como os do Bolsa Família, não podem ser utilizados em investigações de ordem financeira ou criminal, salvo mediante requisição judicial fundamentada em lei específica que autorize tal acesso, hipótese em que a LGPD exige garantias adicionais de proporcionalidade e necessidade (art. 7º, §3º).

O poder público está submetido ao que está imposto pela legislação brasileira, no que diz respeito ao tratamento a ser aplicado em relação ao dado coletado, com informações claras e atualizadas sobre a finalidade e a previsão legal, para sua utilização. O compartilhamento de dados na esfera do portal Gov.br, está de acordo com o fluxo de dados, estabelecido por política pública na forma de lei ou em convênios que respeitem os princípios da proteção de dados.

Outra abordagem extremamente importante diz respeito a utilização dos dados, estatais que são divulgados publicamente. O autor Bruno Bioni, em sua obra *Proteção de dados pessoais: a função e os limites do consentimento*, nos chama a atenção para o fato da LGPD, ter rompido com a separação clássica entre o que é público e o que é privado. Isto significa que dados públicos como a remuneração dos servidores públicos ou as informações de processos judiciais, não podem ser utilizados de maneira indiscriminada, sem nenhum controle de finalidade, permitindo o seu uso por exemplo na montagem de perfis de comportamento ou sua venda para terceiros.

A disponibilização de acesso público, a determinados dados, estabelecido na Lei de acesso à Informação (LAI), segue os princípios da finalidade e boa-fé e envolve o interesse

público, que justifique a sua divulgação. Desta forma estes dados que estão sob controle governamental, estão submetidos às obrigações que limitam o seu uso, garantindo que a transparência governamental, não se desvie do seu objetivo.

O objetivo de melhorar a transparência, dos gastos e alocações do de recursos do Estado, que é um dos objetivos da Lei de acesso à informação (LAI), que tem como princípios, a publicidade como regra e sigilo como exceção, estabelecendo que inicialmente todos os dados produzidos pelo Estado devem estar à disposição do cidadão e o sigilo só poderá ser aplicado para os casos de segurança da sociedade ou do Estado.

O Estado tem o dever de promover a divulgação das informações de interesse geral, sem que haja a provocação por parte do cidadão, como acontece com os portais da transparência, que trazem os gastos, licitações e as remunerações dos servidores. Para tanto é recomendado a utilização de meio de comunicação viabilizados por tecnologia, usando a internet e formatos abertos para os arquivos, facilitam a leitura automatizada.

A divulgação destes dados por publicidade oficial contribui para o fomento à cultura de transparência, nos servidores públicos e promovem o desenvolvimento de um controle social da administração pública, permitindo que o cidadão fiscalize o Estado. Tudo isso sob a proteção dos dados trazida pela Lei Geral de Proteção de Dados (LGPD).

Os limites aqui estabelecidos, para que sejam postos em prática, precisam de uma governança robusta baseada no uso em conjunto de técnicas computacionais, processos gerencias, e normas legais, que promovam o enfrentamento de riscos apresentados.

4. Como fazer a governança e a mitigação de riscos

Os riscos trazidos pela centralização dos dados efetuados pelo Gov.br e a sua adequação a legislação da LGPD, não podem ser atacados apenas através de princípios abstratos. A necessária adoção de uma governança de dados, que materializem as normas jurídicas estabelecidas, em técnicas e procedimentos com devida eficiência, é o ponto central para a mitigação dos riscos trazidos pela centralização dos dados. Caso não se proceda assim no cuidado com a privacidade, teremos um campo aberto para a vigilância desmedida.

Para concretização deste objetivo é necessário sair um pouco do contexto meramente jurídico, que estabelece as limitações e se buscar a implementação efetiva, através da utilização técnicas computacionais e de gestão, que permitam um controle adequado e eficaz dos dados sob controle estatal, de forma a garantir e efetividade das normas legais construídas para garantir a captura e armazenamento seguros e um tratamento adequado dos dados dos cidadãos.

Um importante pilar técnico computacional, que permite o compartilhamento dos dados, com um certo grau de segurança é a garantia da anonimização. Mas Carlos Barbieri, no seu e-book **Governança de dados e LGPD**: práticas, conceitos e novos caminhos, nos faz um importante alerta para o dito “mito da anonimização”, na era do Big Data. Com a robustez tecnológica alcançada atualmente a reidentificação, pela combinação de dados que antes estavam registrados em base de dados apartadas e anonimizados, se torna possível como já demostrado em alguns estudos científicos.

A técnica de anonimização que consiste em se usar meios técnicos para que dados percam a associação direta ou indireta com o titular da informação, é feita por uma combinação de técnicas, como a generalização, que substitui por exemplo a informação completa do endereço, por apenas o bairro , ou cidade; a supressão na qual um identificador direto do titular como um CPF é removido, a pseudonimização, na qual os identificadores, são substituídos por chaves; a adição de ruído, na qual são adicionadas informações falsas de maneira aleatória e o chamado “K-Anonimato”, no qual cada registro no banco de dados seja indistinguível de outros k registros. Mesmo a aplicações de todas estas técnicas em conjunto não sobrevive as possibilidades de cruzamentos que o Big Data nos proporciona, tornando falsa a expectativa de segurança focada meramente em tecnologia.

No caso brasileiro no qual Gov.br, agrega bases massivas pertencentes a Receita Federal, SUS e justiça eleitoral, a separação de identificadores diretos, se mostra insuficiente, quando as chaves necessárias para sua reversão estão em posse estatal, ou para um possível caso de vazamento dos metadados. Barbieri, reforça a necessidade da proteção jurídica, considerar que os avanços da tecnologia de identificação, superam a velocidade de desenvolvimento de técnicas de mascaramento, trazendo um peso ainda maior para a necessidade de uma governança rígida sobre os dados em domínio do Estado, para que eles não sejam tratados como mero ativo de tecnologia da informação.

A LGPD impõe a elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD), com o objetivo de buscar a mitigação do perfilamento de dados de forma abusiva, especialmente quando o tratamento trouxer como fundamento o interesse legítimo ou estiverem envolvidos dados sensíveis, que sempre ocorre nos casos de políticas públicas, nas áreas de saúde e assistência social, integradas ao portal do Gov.br. Na definição de Sérgio Pohlmann, na obra *LGPD Ninja: entendendo e implementando a Lei Geral de Proteção de Dados nas empresas*, temos que o RIPD, não é um mero relatório estático, fruto de burocracia, mas dinâmico, que se torna uma ferramenta vital para gerir os riscos envolvidos, trazendo a descrição da natureza dos dados, metodologia utilizada e sua coleta e de forma relevante as medidas adotadas para se mitigar eventuais danos.

No caso específico do governo digital, são pré-requisitos para qualquer compartilhamento entre os órgãos estatais, a elaboração e ampla divulgação do RIPD. Além disso, Pohlmann, no seu livro *LGPD Ninja: entendendo e implementando a Lei Geral de Proteção de Dados nas empresas*, destaca a relevância de se ter um mapeamento de dados rigoroso. De acordo com a metodologia proposta por ele, o Estado deve mapear não apenas o dado em si, como por exemplo CPF, dados de saúde, mas o seu "ciclo de vida", trazendo a base legal que justifica o tratamento, como exemplo, o objetivo de execução de políticas públicas, por quanto tempo o dado será retido e, fundamentalmente, quem são os operadores que terão acesso a essas bases.

Com o objetivo de mitigar o perfilamento abusivo dos dados, em posse do governo, deverá constar do RIPD, a descrição técnica das salvaguardas de segurança, incluindo o detalhamento dos processos de anonimização ou pseudonimização robustos, dos dados armazenados em grandes bancos de dados, seja em banco de dados internos ou em nuvens governamentais, antes de seu compartilhamento entre os órgãos governamentais e garantir que

os backups estejam devidamente criptografados, para que seja evitado o vazamento massivo de destes dados.

É obrigação do Estado, para trazer transparência à sociedade, conhecer a localização de exata do dado, onde se dá o seu tráfego e quem possui acesso a ele. Sem todo este registro, se torna impossível estabelecer a garantia de integridade, ou dar respostas aos incidentes que possam ocorrer, tornando sem efeito o princípio da responsabilidade. Portanto um RIPD, bem elaborado pode funcionar como uma "vacina", jurídica ao demonstrar a proatividade e boa-fé estatal, na gestão dos riscos associada aos dados dos cidadãos, sob seu domínio. Nas palavras de Sérgio Antônio Pohlmann, no livro *LGPD Ninja: entendendo e implementando a Lei Geral de Proteção de Dados nas empresas:*

> O Relatório de impacto deve conter, pelo menos, as seguintes informações: a descrição dos dados coletados ou tratados, com seus respectivos tipos; a metodologia utilizada para a coleta; a metodologia utilizada para garantia da segurança do dado, análise do controlador, em relação às medidas adotadas, e as técnicas utilizadas para controle e mitigação de riscos. (POHLMANN, 2019, p. 208)

A centralização dos dados cria o chamado "ponto único de falha", pois se torna atrativo para atuação de atacantes cibernéticos. A adoção de *frameworks* de segurança robustos, como as normas ISO 27000, que é um conjunto de normas para gestão da informação, que tem por objetivo proteger a confidencialidade, integridade e disponibilidade de dados ou NIST que é um padrão de referência para frameworks de cibersegurança, se tornam fundamentais para que se contemplem criptografia, gestão de identidades e planos de resposta a incidentes, se faz necessário para garantir a conformidade.

Assim aqui não cabe a fiscalização através da autorregulação. A competência legal atribuída a autoridade nacional de proteção de dados (ANPD), permite a solicitação de relatório de impacto ao poder público e auditar a execução do tratamento dos dados estatais. A garantia da atuação legitima do Gov.br, está intrinsicamente ligado a atuação forte e independente da ANPD, que seja capaz de impor sanções ou medidas corretivas para os momentos em que a necessidade de eficiência administrativa, viole os direitos fundamentais dos cidadãos. Nas palavras de Danilo, Doneda, em sua obra *Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados:*

> O recurso a uma autoridade administrativa para a proteção dos dados pessoais, no modelo de uma autoridade independente, é uma tendência fortemente enraizada em vários ordenamentos. Alguns dos aspectos mais relevantes da proteção de dados pessoais, como o fato de que os tratamentos de dados e os seus efeitos são dificilmente passíveis de serem acompanhados de forma eficaz pelo cidadão ou a necessidade de uma constante atualização em função do desenvolvimento tecnológico, entre vários outros, justificaram o recurso a esses órgãos que, hoje, estão presentes na grande maioria dos marcos regulatórios nessa matéria, quase sempre como um de seus sustentáculos. (DONEDA, 2020, p. 301)

5. Considerações finais

A estratégia de governo digital implementada através da plataforma Gov.br, nos traz um avanço considerável no que diz respeito a modernização da administração pública brasileira, buscando alcançar o princípio da eficiência administrativa, presente na constituição federal de 1988 no seu art. 37, como um "Dever de Modernização", que impõe à Administração Pública a entrega máxima de resultados com o mínimo de recursos. No mundo digital, isso pode significar a desburocratização, que permite ao cidadão a dispensa de entrega de documentos físicos a diferentes órgãos se o Estado já possui esses dados digitalizados, a interoperabilidade, representada pela capacidade de diferentes sistemas (Receita Federal, INSS, Bancos) "conversarem" entre si através do Gov.br e a economicidade através da Redução de custos com papel, arquivos físicos e atendimento presencial.

A análise feita durante a construção deste artigo trouxe luz sobre as indagações quanto aos riscos de violação de privacidade, trazido pela centralização de dados dos cidadãos pelo Estado, no portal Gov.br, demonstrando de forma clara, que a legislação integrante de Lei Geral de Proteção de dados, é um arcabouço jurídico robusto que mitiga fortemente qualquer possibilidade de compartilhamento ou tratamento indevido por parte de qualquer órgão público.

Desta forma através dos princípios presentes no art. 6º da LGPD, como: o princípio da Finalidade, que é realização de tratamento para propósitos legítimos, específicos e informados ao titular, evitando usos ocultos ou genéricos dos dados, proibindo mudar a finalidade depois sem nova base legal, exigindo uma comunicação clara ao titular; o princípio da Adequação, ou seja um tratamento deve ser compatível com a finalidade informada, garantindo a coerência entre o que foi prometido e o que é feito, evita interpretações amplas ou distorcidas da finalidade; o princípio da Necessidade, que limita o tratamento ao mínimo necessário, evitando a coleta excessiva, exigindo a justificativa para cada dado solicitado e reduzindo riscos e responsabilidades; o princípio da Segurança, com a adoção de medidas técnicas e

administrativas para proteger os dados contra: acessos não autorizados, destruição, perda, alteração, comunicação indevida.

Já o Art. 18 da LGPD estabelece os direitos que todo titular de dados pode exercer perante o controlador, como: a confirmação da existência de tratamento, permitindo ao titular questionar ao controlador se seus dados estão sendo tratados mesmo antes de pedir acesso; acesso aos dados que permite que o titular veja quais dados o controlador possui e como eles são tratados; correção de dados incompletos, inexatos ou desatualizados; anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade, informação sobre compartilhamento de dados, o controlador deve informar com quem compartilhou dados empresas, órgãos públicos, parceiros etc.

Mesmo considerando as possíveis fragilidades técnicas relacionadas à segurança dos dados especialmente diante da limitação dos processos de anonimização frente ao poder de reidentificação proporcionado pelas tecnologias de Big Data esse risco é mitigado pelo conjunto de controles previstos na Lei Geral de Proteção de Dados (LGPD). Além disso, a governança exercida pela Autoridade Nacional de Proteção de Dados (ANPD) reforça essa proteção ao realizar auditorias e fiscalizações necessárias para assegurar o cumprimento integral das normas de segurança aplicáveis.

A governança estabelecida através do relatório de impacto de Proteção de dados (RIPD), se demonstra com um forte ferramenta, que abriga todos os itens necessários para que a gestão adequada dos dados controlados pelo Estado, esteja com todo o seu fluxo bem documentado, sendo um insumo extremante útil, para auxiliar a Autoridade Nacional de Proteção de Dados (ANPD), no seu papel fiscalizador, que no presente artigo esta focado na avaliação da dos dados sob controle da Administração Pública, tornando ainda mais relevante a autonomia deste órgão.

A resposta à questão central deste trabalho, é que o compartilhamento de dados no portal Gov.br, encontra os limites bem estabelecidos na autodeterminação informativa e na privacidade contextual. Assim a LGPD, traz a obrigação para Estado de não tratar o cidadão como simples “objeto de informação”, o que permite o compartilhamento de dados sob o controle estatal, entre os diversos órgãos governamentais, com total transparência, controle e segurança, através da aplicação da Lei Geral de Proteção de Dados (LGPD), aliada a técnicas computacionais adequadas, que mesmo ameaçadas por processos de reidentificação facilitado pelo uso de *Big Data,* se mostra fundamental e um boa governança por parte da Autoridade Nacional de Proteção de Dados, partindo da analise do Relatório de Impacto de Proteção de

Dados (RIPD), para verificar se estão presentes todos os itens que garantem uma boa proteção aos dados e realizando a auditoria nos ambientes de captura, armazenamento e ciclo de compartilhamento de dados, para atestar se estão conforme apresentados no referido relatório.

6. Referências bibliográficas

BARBIERI, Carlos. **Governança de dados e LGPD**: práticas, conceitos e novos caminhos. [S.l.]: CBCA, 2020. E-book (PDF).

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: fundamentos da Lei Geral de Proteção de Dados. 2. ed. rev. e atual. São Paulo: Revista dos Tribunais, 2020.

LGPD: riscos no atendimento operacional. [S.l.: s.n.], [20--?]. 1 e-book.

O IMPACTO da Lei Geral de Proteção de Dados (LGPD) nas empresas brasileiras: adequação e desafios para o e-commerce. **Jusbrasil**, [S.l.], 16 nov. 2025. Disponível em: https://www.jusbrasil.com.br/artigos/o-impacto-da-lei-geral-de-protecao-de-dados-lgpd-nas-empresas-brasileiras-adequacao-e-desafios-para-o-e-commerce/2858685887. Acesso em: 07 fev. 2026.

PEREIRA, Caroline de Vargas; GONÇALVES, Luis Eduardo Diehl. **Caderno de mapas mentais**: conhecimentos bancários: Lei Geral de Proteção de Dados; Lei Complementar nº 105/2001; Resolução CMN nº 4.658/2018. [S.l.]: Mapas da Loli, 2021. E-book.

POHLMANN, Sérgio Antônio. **LGPD Ninja**: entendendo e implementando a Lei Geral de Proteção de Dados nas empresas. [S.l.]: Editora Fross, 2019.

L. Sweeney, Simple Demographics Often Identify People Uniquely. Carnegie Mellon University, Data Privacy Working Paper 3. Pittsburgh 2000.

WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. ***Harvard Law Review****, Cambridge, v. 4, n. 5, p. 193-220, dec. 15, 1890*

Privacy in Context: Technology, Policy, and the Integrity of Social Life"*, publicado em 2010 pela Stanford Law Books*