CENTRO UNIVERSITÁRIO DE LAVRAS

CURSO DE GRADUAÇÃO EM DIREITO

Trabalho de Conclusão de Curso

A LEI GERAL DE PROTEÇÃO DE DADOS NO ÂMBITO DO INSS

LINCOLN BORGES DOS SANTOS

LAVRAS – MG

2024

LINCOLN BORGES DOS SANTOS

A LEI GERAL DE PROTEÇÃO DE DADOS NO ÂMBITO DO INSS

Trabalho de Conclusão de Curso apresentado ao Centro Universitário de Lavras, como parte das exigências da disciplina Trabalho de Conclusão de Curso (TCC), curso de graduação em Direito.

ORIENTADOR

Prof. Dr. Guilherme Scodeler de Souza Barreiro

LAVRAS – MG

2024

Ficha Catalográfica preparada pelo Setor de Processamento
Técnico da Biblioteca Central do UNILAVRAS

Santos, Lincoln Borges.
S237I A lei geral de proteção de dados no âmbito do INSS / Lincoln Borges dos Santos – Lavras: Unilavras, 2024.

42f.

Monografia (Graduação em Direito) – Unilavras, Lavras, 2024.

Orientador: Prof. Guilherme Scodoler de Souza Barreiro.

1. Proteção de dados. 2. Privacidade. 3.Tratamento de dados. 4. INSS. I. Barreiro, Guilherme Scodeler de Souza. (Orient.). II. Título.

LINCOLN BORGES DOS SANTOS

A LEI GERAL DE PROTEÇÃO DE DADOS NO ÂMBITO DO INSS

Trabalho de Conclusão de Curso apresentado ao Centro Universitário de Lavras, como parte das exigências da disciplina Trabalho de Conclusão de Curso (TCC), curso de graduação em Direito.

Aprovado em: 29/11/2024

MEMBROS DA BANCA EXAMINADORA

Presidente - Prof. Pós-Dr. Denilson Victor Machado Teixeira / UNILAVRAS

Orientador - Prof. Dr. Guilherme Scodeler de Souza Barreiro/ UNILAVRAS

LAVRAS – MG

2024

Dedico este trabalho aos meus pais, Hilário Borges dos Santos e Ione Alvarenga Gonçalves Costa dos Santos.

AGRADECIMENTOS

Agradeço primeiramente a Deus por toda a força para chegar até aqui, possibilitando a realização deste momento. Aos meus pais, Hilário Borges dos Santos e Ione Gonçalves Costa dos Santos por todo ensinamento e exemplo de pessoas para minha vida. Aos meus professores que foram fontes de inspiração durante a graduação, sendo eles exemplos de profissionais. Ao meu orientador, Prof. Dr. Guilherme Scodeler de Souza Barreiro, por toda atenção e aconselhamento para a conclusão deste trabalho. E aos meus amigos por todo apoio dado até este momento.

.

“A internet e muito mais que uma tecnologia. É um meio de comunicação, de interação e de organização social”.
Manuel Castells (1942)

RESUMO

Introdução: A Lei Geral de Proteção de Dados (LGPD) (13.709/2018) tem como principal proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da pessoa natural. A LGPD veio para organizar e sistematizar a coleta e armazenamento de dados, de forma a garantir a segurança dos dados sensíveis e pessoais dos titulares destes dados. **Objetivo:** O intuito da presente monografia é estudar a adequação da LGPD ao do Instituto Nacional do Seguro Social (INSS) e conforme o desenvolver do trabalho e os conhecimentos adquiridos utilizá-la como um reforço aos dados coletados e armazenados pelo INSS. **Resultados:** Existe uma relação entre os bancos e o INSS, tendo em vista que a maioria das fraudes ou vazamento de dados acontecem diretamente usando os bancos como intermediários para o fim delituoso, tendo em vista a relação mencionada neste resumo. Para isso é necessário, utilizarmos a Lei como instrumento que se adeque da melhor forma na proteção dos dados, vendo pontos positivos e negativos da Lei, exclusivamente no que cabe ao INSS para que seja feito o levantamento de hipóteses visando o melhoramento do dispositivo ou ampliar a forma com que o ente público garanta a segurança de seus beneficiários. **Metodologia:** A pesquisa foi estruturada na metodologia de revisão bibliográfica, com a exposição de artigos dos principais autores do tema, bem como jurisprudências e doutrinas. **Conclusão:** Conclui-se, portanto, que após a análise das diretrizes, dispositivos legais existentes na LGPD e a relação de com INSS, trarão diversos benefícios à segurança dos dados dos beneficiários, além disso trará maior fiscalização bem como mitigação do assédio causados pelos bancos.

Palavras-chave: LPGD, Privacidade, INSS, Tratamento de Dados, ANPD

.

ABSTRACT

Introduction: The General Data Protection Law (LGPD) (13.709/2018) primarily aims to protect the fundamental rights of freedom and privacy and the free development of the natural person. The LGPD was created to organize and systematize the collection and storage of data, ensuring the security of sensitive and personal data of their holders. **Objective:** The purpose of this monograph is to study the adequacy of the LGPD to the National Institute of Social Security (INSS) and, as the work develops and knowledge is acquired, to use it as reinforcement for the data collected and stored by the INSS. **Results:** There is a relationship between banks and the INSS, considering that most frauds or data leaks occur directly using banks as intermediaries for illicit purposes, given the relationship mentioned in this summary. Therefore, it is necessaryto use the Law as an instrument that best fits data protection, analyzing the positive and negative points of the Law, exclusively concerning the INSS, to hypothesize improvements to the device or expand the way the public entity ensures the security of its beneficiaries. **Methodology:** The research was structured on the methodology of bibliographic review, with the presentation of articles by the main authors on the subject, as well as jurisprudence and doctrines. **Conclusion:** It is concluded, therefore, that after analyzing the guidelines, existing legal provisions in the LGPD, and the relationship with the INSS, various benefits will be brought to the security of the beneficiaries' data. Moreover, it will bring greater oversight as well as mitigate harassment caused by banks.

Keywords: LGPD, Privacy, INSS, Data Processing, ANPD

.

LISTA DE SIGLAS

LGPD	**Lei Geral de Proteção de Dados**
INSS	**Instituto Nacional do Seguro Social**
ANPD	**Agência Nacional de Proteção de Dados**
LAI	**Lei de Acesso à informação**

SUMÁRIO

1 INTRODUÇÃO

A presente pesquisa dispõe sobre a LGPD e suas aplicabilidades na segurança dos dados pessoais dos segurados do INSS. Portanto, para isso será explorado os conceitos de proteção de dados e a partir de uma revisão bibliográfica, será feito uma análise dos desafios enfrentados pela LGPD e os direitos dos titulares envolvidos.

O objetivo principal geral é verificar a aplicação da Lei acima mencionada como um instrumento aprimorador da segurança dos dados, bem como garantir o respeito aos princípios constitucionais, da privacidade, do livre desenvolvimento da personalidade da pessoa natural.

Em relação à metodologia usada, a exposição de conceitos e princípios garantidos tanto pela Lei, quanto Constituição Federal de 1988, serão os norteadores para uma compreensão da importância da segurança de dados dos titulares.

O procedimento adotado coletar esses dados é preponderantemente bibliográfico e meios práticos de realização do tratamento e armazenamentos de dados. Para isso, será usado leituras académicas, a Lei vigente e exemplos práticos para atingir o objetivo esperado.

Para isso, o trabalho será divido em três tópicos. Sendo o primeiro uma exposição da Lei Geral de Proteção de Dados, Lei nº 13.709/18 e seus desafios existentes na implementação nos processos de armazenamentos e coleta de dados sensíveis e pessoais

Já no segundo tópico é trabalho como é a relação do poder público com a LGPD, tendo em vista que a dispositivos específicos na Lei que regulam a forma de tratamento de dados pelas entidades públicas que também serão submetidas as diretrizes da nova Lei, como o INSS

E por fim, no último tópico será abordado a relação dos segurados do INSS em relação aos bancos, tendo o poder público como agente principal na relação entre os dois retromencionados, tendo em vista que as informações pessoais dos segurados são fonte de interesse dos bancos que necessitam de novos clientes e fornecer empréstimos para garantir sua arrecadação com os juros do mercado. Essa relação dos três entes acima mencionados pode gerar diversos prejuízos a sociedade e a

garantias constitucionais. A LGPD veio como um suprimento para aperfeiçoar a relação nos processos de tratamentos de dados e a tecnologia.

2 REVISÃO DE LITERATURA

2.1 DESAFIOS ENFRENTADOS PELA LGPD

No Brasil, já existiam leis abordando a proteção de dados pessoais, como a Lei nº 12.527 de 18 de novembro de 2011, conhecida como Lei de Acesso à Informação (LAI), e a Lei nº 12.965 de 23 de abril de 2014, chamada de Marco Civil da Internet. No entanto, faltava uma legislação específica para proteger as informações pessoais dos cidadãos. Nesse contexto, surgiu a Lei 13.709 de 14 de agosto de 2018, chamada de Lei Geral de Proteção de Dados Pessoais (LGPD). Esta lei regula o tratamento de dados pessoais em meios físicos e digitais, tanto por pessoas naturais quanto jurídicas de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural. As normas gerais da LGPD são de interesse nacional e, por isso, devem ser observadas por União, Estados, Distrito Federal e Municípios.

Os autores Bioni, da Silva e Martins (2022) dizem:

> [...] a relação de complementaridade entre as leis é tamanha que, antes mesmo da LGPD existir, a Lei de Acesso à Informação trouxe um balanceamento e regras de proporcionalidade para o fluxo informacional regulado por ela. Conforme evidenciado pelo art. 31, informações relativas à intimidade, à vida privada e à honra e à imagem podem ter seu acesso restrito ou condicionado ao consentimento do titular. Pode-se traçar um forte paralelo entre os princípios da finalidade, necessidade e adequação, previstos pela LGPD, com essa limitação trazida pela LAI. Uma vez que o objetivo desta última é o acesso a informações de interesse público, não há razão de se divulgar dados relativos à vida privada e que não se apresentam como de interesse público. (2022, p. 12).

Uma grande influência na elaboração da LGPD foi o GDPR (General Data Protection Regulation) europeu, que trata da privacidade e proteção de dados pessoais na União Europeia. A LGPD representa um avanço significativo na proteção de dados no Brasil, empoderando os titulares de dados com uma série de direitos e estabelecendo ferramentas que promovem a transparência nas relações estatais. A LGPD não visa proibir a coleta e compartilhamento de dados pessoais, mas disciplinar o tratamento desses dados.

A LGPD foi aprovada em agosto de 2018 e, conforme a Medida Provisória nº 869 de 27 de dezembro de 2018, posteriormente convertida na Lei nº 13.853 de 8 de julho de 2019, deveria entrar em vigor em agosto de 2020, exceto as sanções administrativas pela Autoridade Nacional de Proteção de Dados (ANPD), que só começaram a ser aplicadas em 1º de agosto de 2021. Contudo, a MP nº 959 de 29 de abril de 2020 previa o adiamento da vigência da LGPD para maio de 2021, alteração que foi rejeitada pelo Congresso Nacional. Com a sanção da Lei nº 14.058 de 17 de setembro de 2020, a LGPD entrou em vigor em 18 de setembro de 2020. Desde então, o INSS tem buscado, discutido e implementado ações para cumprir com as diretrizes da LGPD.

Dessa forma, a implementação da LGPD no Brasil não apenas fortalece a proteção dos dados pessoais dos cidadãos, mas também estabelece um marco regulatório concreto e necessário para acompanhar as exigências de uma sociedade cada vez mais digital. A conformidade com a LGPD promove a confiança dos cidadãos nas instituições públicas e privadas, incentivando um ambiente de transparência e responsabilidade. Além disso, ao alinhar-se com padrões internacionais como o GDPR, o Brasil demonstra seu compromisso com as melhores práticas globais de proteção de dados, favorecendo a cooperação internacional e a competitividade das empresas brasileiras no cenário global. Portanto, a LGPD não apenas protege os direitos individuais, mas também contribui para o desenvolvimento econômico e social do país, criando um ambiente mais seguro e ético para o tratamento de dados pessoais.

Autores como Maria Celina Bodin de Moraes, em apresentação à obra de Stefano Rodotà, compreende que o tratamento de dados e especialmente a sua coleta “não pode ser tomada como uma “rede jogada ao mar para pescar qualquer peixe”. Ao contrário, as razões de coleta, principalmente quando se tratar de “dados sensíveis”, devem ser objetivas e limitadas” (Moraes, 2008, p. 9).

Sendo também entendido que, a medida dessa objetividade e limitação será determinada justamente pela finalidade legítima do tratamento, que fica condicionada “à comunicação preventiva ao interessado sobre como serão usadas as informações coletadas; e para algumas categorias de dados especialmente sensíveis estabelece que a única finalidade admissível é o interesse da pessoa considerada” (Rodotá, 2008, p. 87).

Como descreve Blum (2021, p.14):

> “Na atualidade, informações absolutamente sensíveis, como as de saúde, por exemplo, são coletadas e tratadas sem maiores cautelas por muitas instituições, empresas e, inclusive, pelo Poder Público. Detalhes da vida pessoal registrados em fotos e vídeos nas redes sociais (como orientação religiosa, política ou sexual) podem estar sendo compartilhados entre empresas e tratados sem conhecimento de seus titulares.”

Percebe-se assim que a com a atualidade, convivemos diariamente com uma abundância de dados e informações circulando por aí sem controle e proteção, é necessário um olhar atento a forma de tratamento e armazenamento desses dados de forma segura e discreta.

Através da LGPD, ocorreram diversos avanços, tanto na proteção dos direitos individuais, quando nos meios técnicos para salvaguardar os dados dos titulares, pois a cada dia que passa, as diretrizes impostas pela Lei vem se adaptando nos sistemas das instituições, bem como das empresas privadas. A implementação da Lei veio para revolucionar a forma de coleta e tratamento desses dados, numa era tão importante que é a digital.

É necessário evoluir os sistemas que esses dados circulam, não só a forma de gerenciar, mas também o sistema que irá armazenar esses dados, a era digital tem sido um mar para vários tipos de invasões, gerando vazamento de dados, ferindo direitos constitucionais garantidos.

A proteção de dados atualmente é tão importante que em 10 de fevereiro de 2022, a LGPD foi oficialmente reconhecida como um direito fundamental na nossa Constituição através da Emenda Constitucional n. 115/2022. Antes disso, como mencionado, a legislação já defendia a proteção dos indivíduos cujos dados pessoais eram tratados. Contudo, a principal inovação foi estabelecer uma ampla responsabilização para pessoas físicas e jurídicas que invadissem a privacidade dos titulares dos dados, utilizando essas informações sem cumprir os requisitos autorizadores para seu tratamento.

É entendido que "Proteção de dados pessoais é mais que um direito; é uma garantia fundamental que resguarda a liberdade e a privacidade individual, reconhecendo a importância de salvaguardar a integridade dos dados na era digital." (Silva, J. 2023, p.61). Bem como que "A constitucionalização da proteção de dados pessoais representa um avanço significativo na garantia da privacidade e da liberdade

individual, assegurando que tais dados sejam tratados com o devido respeito e segurança." (Ferreira, M. 2023, p.81).

O reconhecimento da proteção de dados como um dos direitos fundamentais no Brasil, por meio da Emenda Constitucional n. 115/2022, é um avanço significativo na legislação do país. Este reconhecimento reforça a importância de proteger a privacidade e a integridade dos dados pessoais em uma sociedade cada vez mais digitalizada e cibernética.

Ao elevar a proteção de dados à categoria de direito constitucional, o Brasil se alinha com as melhores práticas internacionais, como as estabelecidas pelo GDPR na União Europeia. Este movimento não só promove a transparência no tratamento dos dados, mas também impõe uma maior responsabilidade às entidades públicas e privadas, que agora devem seguir protocolos rigorosos para a coleta, armazenamento e utilização das informações pessoais.

Essa mudança legislativa reflete um compromisso contínuo do Estado brasileiro com a defesa dos direitos dos cidadãos, especialmente no que diz respeito à privacidade. O fortalecimento da segurança jurídica e a responsabilização das empresas e órgãos governamentais pela proteção dos dados pessoais são passos importantes para construir uma cultura de respeito à privacidade no país.

A LGPD, portanto, não apenas estabelece normas claras para o tratamento de dados, mas também confere aos cidadãos/titulares ferramentas para exercerem controle sobre suas informações, bem como mecanismos de responsabilizar em casos de vazamentos. Isso inclui o direito de saber como seus dados são utilizados, solicitar a exclusão de informações desnecessárias e exigir a correção de dados incorretos. Essa legislação coloca o Brasil em um patamar elevado na proteção dos dados pessoais, incentivando um ambiente mais seguro e transparente tanto para consumidores quanto para empresas.

Logo nasce também, a necessidade de se proliferar a cultura de proteção de dados no Brasil, pois, desta forma estaremos nos adaptando aos novos desafios que surgem com o desenvolvimento tecnológico e as nuances que o acompanham.

Nas palavras de Doneda (2011, p. 98):

> “Nestas leis procura-se enfocar o problema integral da informação, pois elas presumem que não se pode basear a tutela dos dados pessoais

> simplesmente na escolha individual – são necessários instrumentos que elevem o padrão coletivo de proteção.”

A implementação da LGPD no Brasil trouxe muitos benefícios, mas também apresenta diversos desafios:

1) Conscientização e Cultura: Adotar uma cultura de proteção de dados é essencial, mas ainda é um desafio em muitas organizações no Brasil. Empresas e órgãos públicos precisam educar seus funcionários sobre a importância da privacidade e garantir que todos os procedimentos de tratamento de dados estejam de acordo com a LGPD. Isso requer tempo e esforço contínuo para mudar mentalidades e hábitos arraigados.

Conforme mencionado por Lugati e Almeida (2022), a Lei Geral de Proteção de Dados (LGPD) tem como objetivo principal fomentar uma cultura de proteção de dados dentro das empresas, promovendo a implementação contínua e sustentável da legislação e dos seus benefícios.

2) Infraestrutura e Recursos: A implementação das exigências da LGPD pode ser custosa, especialmente para pequenas e médias empresas que talvez não disponham de recursos financeiros ou tecnológicos suficientes. Investir em sistemas de segurança da informação, contratar especialistas e realizar treinamentos contínuos são medidas necessárias, mas que exigem investimentos consideráveis. Logo: “Uma infraestrutura de TI bem projetada e mantida permite às organizações mapear e controlar o fluxo de dados, garantindo que as informações pessoais sejam armazenadas, processadas e transmitidas com segurança." (TECNOCOMP, 2023).

3) Consentimento e Direitos dos Titulares: Empresas devem ser transparentes sobre como coletam, utilizam e compartilham dados pessoais, garantindo que os titulares compreendam seus direitos e saibam como exercê-los. Isso inclui informar claramente as finalidades do tratamento de dados e obter consentimento explícito dos indivíduos, o que pode ser um processo complicado e demorado. Para isso, esse tratamento de dados deve ser realizado conforme uma base legal, para que assim ele seja considerado lícito e legítimo. Tais bases legais, são apresentadas na LGPD de forma geral, devendo serem adequadas conforme cada caso pelas autoridades competentes, a Autoridade nacional de proteção de dados (ANPD), o poder Legislativo e o poder Judiciário. (TEFFÉ, VIOLA, 2020, p. 3).

Cada um desses pontos apresenta alguns desafios significativos, passos essenciais para garantir o cumprimento do tratamento de dados em conformidade com a LGPD. Proteger os dados pessoais no Brasil é direto fundamental, que deve ser trabalhado em etapas progressivas, buscando sempre atingir a finalidade de buscar uma sociedade segura e comprometida com seus cidadãos.

Um dos pilares para estabelecer uma cultura de proteção de dados é investir em programas de treinamento contínuos para todos os funcionários. Workshops, seminários e cursos online são ferramentas eficazes para disseminar o conhecimento sobre a importância da proteção de dados e as melhores práticas para garantir a segurança das informações. A educação constante é fundamental para que todos compreendam seus papéis e responsabilidades no tratamento dos dados pessoais.

A busca por desenvolvimento e implementação de políticas de privacidade claras é outro passo crucial. Essas políticas devem estabelecer procedimentos detalhados para o tratamento de dados pessoais e ser facilmente acessíveis a todos os funcionários. Além disso, é essencial que essas políticas sejam revisadas e atualizadas constantemente para refletir as melhores práticas e garantir conformidade com a legislação vigente.

Através de setorização com líderes, deve-se demonstrar um compromisso inabalável com a proteção de dados, servindo de exemplo para todos os funcionários. Quando os líderes priorizam a privacidade, isso se reflete na cultura organizacional e encoraja todos a seguir o mesmo caminho. A liderança proativa e engajada é essencial para fomentar um ambiente de respeito e responsabilidade em relação à proteção de dados.

Com isso, o intuito deve-se manter uma comunicação clara e aberta sobre a importância da proteção de dados, informando os funcionários sobre incidentes de segurança e as medidas tomadas para corrigi-los, promovendo uma cultura de transparência e confiança. A comunicação eficaz garante que todos estejam cientes das práticas e procedimentos de proteção de dados da organização.

Para isso, o investimento em tecnologias de segurança cibernética é fundamental para proteger os dados contra acessos não autorizados e vazamentos. Ferramentas como firewalls, criptografia e sistemas de detecção de intrusões são essenciais para garantir a integridade e a confidencialidade das informações. A

adoção dessas tecnologias deve ser acompanhada de uma política de segurança robusta e eficaz.

Obtendo assim, envolvimento ativo dos funcionários na proteção de dados se torna essencial para atingir a finalidade proposta pela Lei, logo para cominar com isso, a realização de campanhas internas de conscientização e a criação de um ambiente onde todos se sintam responsáveis pela proteção das informações pessoais são estratégias eficazes. O engajamento de todos os níveis da organização é fundamental para construir uma cultura robusta e duradoura de proteção de dados.

2.1.1 O poder público e a LGPD

A aplicação da LGPD no Brasil de um modo geral terá vários desafios a serem enfrentados, tanto tecnológicos quantos cultura. A ótica a ser observado neste momento será no setor público, tendo o Estado como coadjuvante na implementação da LGPD a sua estrutura organizacional.

Há uma previsão exclusiva para o tratamento de dados pelo poder público, na Lei 13.709/18, no capítulo IV, O artigo 23, I da LGPD dispõe:

> Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:
>
> I - Sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos;

O Artigo se destaca como uma das bases legais que autorizam o tratamento de dados pelo Poder Público, complementando os artigos 7º, III, e 11, II, b:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
>
> 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;

> Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
> II - Sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
> b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

Esses dispositivos permitem o tratamento de dados para a execução de políticas públicas, estabelecendo que o tratamento de dados deve atender a uma finalidade pública, sempre em alinhamento com o interesse público para executar suas funções legais ou cumprir as atribuições do serviço público. Ele busca conciliar a LGPD com a Lei de Acesso à Informação (Lei nº 12.527/2011), visto que ambas se aplicam a entidades públicas e privadas que desempenham atividades de interesse público.

Isso reforça que na busca pelo interesse público, os princípios de proteção de dados devem ser respeitados. Como evidenciado pela expressão “desde que” no caput do artigo 23. Ou seja, para cumprir a finalidade pública, é necessário fornecer as informações especificadas no inciso I e designar um responsável pelo tratamento de dados. Tal previsão encontra base legal no princípio da supremacia do interesse público, que é um princípio implícito extraído da Constituição Federal de 1988.

Celso Antônio Bandeira de Mello (2009, p. 69) conceitua o princípio da supremacia do interesse público da seguinte maneira:

> “Trata-se de verdadeiro axioma reconhecível no moderno Direito Público. Proclama a superioridade do interesse da coletividade, firmando a prevalência dele sobre o do particular, como condição, até mesmo, da sobrevivência e asseguramento deste último. É pressuposto de uma ordem social estável, em que todos e cada um possam sentir-se garantidos e resguardados”.

Conforme Pietro (2018, p.132): "Esse princípio está presente tanto no momento da elaboração da lei quanto no momento da sua execução em concreto pela Administração Pública. Ele inspira o legislador e vincula a autoridade administrativa em toda a sua atuação".

A clareza e atualidade das informações exigidas para o tratamento de dados exercido pelo Poder Público refletem o foi disposto no art. 2º, IV, do Marco Civil da Internet, que defende a abertura e a colaboração como um dos fundamentos para o uso da internet no Brasil. Nesse contexto, o governo eletrônico deve se comprometer

com valores democráticos, garantindo assim o aumentando na transparência e o acesso à informação pela sociedade, permitindo que os cidadãos desenvolvam um senso crítico e tomem decisões de forma consciente sobre assuntos de seus interesses, bem como para que o Estado possa ter o controle correto das informações em prol da sociedade.

Valendo-se disso, o Ministro Ruy Rosado de Aguiar (1995) dispôs sobre o assunto neste julgado, nos seguintes termos:

> "A inserção de dados pessoais do cidadão em bancos de informações tem se constituído em uma das preocupações do Estado moderno, onde o uso da informática e a possibilidade de controle unificado das diversas atividades da pessoa, nas múltiplas situações de vida, permitem o conhecimento de sua conduta pública e privada, até nos mínimos detalhes, podendo chegar à devassa de atos pessoais, invadindo área que deveria ficar restrita à sua intimidade; ao mesmo tempo, o cidadão objeto dessa indiscriminada colheita de informações, muitas vezes, sequer sabe da existência de tal atividade, ou não dispõe de eficazes meios para conhecer o seu resultado, retificá-lo ou cancelá-lo. E assim como o conjunto dessas informações pode ser usado para fins lícitos, públicos e privados, na prevenção ou repressão de delitos, ou habilitando o particular a celebrar contratos com pleno conhecimento de causa, também pode servir, ao Estado ou ao particular, para alcançar fins contrários à moral ou ao Direito, como instrumento de perseguição política ou opressão econômica. STJ, Recurso Especial n. 22.337/RS, rel. Ministro Ruy Rosado de Aguiar, DJ 20/03/1995, p. 6119."

O tema proteção de dados pelo poder público e discutido diariamente nos tribunais deste País, conforme os julgados a seguir:

> EMENTA MEDIDA CAUTELAR EM AÇÃO DIRETA DE INCONSTITUCIONALIDADE. REFERENDO. MEDIDA PROVISÓRIA Nº 954/2020. EMERGÊNCIA DE SAÚDE PÚBLICA DE IMPORTÂNCIA INTERNACIONAL PROVOCADA PELO NOVO CORONAVÍRUS (COVID-19). COMPARTILHAMENTO DE DADOS DOS USUÁRIOS DO SERVIÇO TELEFÔNICO FIXO COMUTADO E DO SERVIÇO MÓVEL PESSOAL, PELAS EMPRESAS PRESTADORAS, COM O INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. PRESENÇA DO FUMUS BONI JURIS E DO PERICULUM IN MORA. DEFERIMENTO. 1. Decorrências dos direitos da personalidade, foram positivados, o respeito à privacidade e o respeito à autodeterminação informativa, no art. 2º, I e II, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais) como fundamentos específicos da disciplina da proteção de dados pessoais. 2. Na medida em que relacionados à identificação – efetiva ou potencial – de pessoa natural, o tratamento e a manipulação de dados pessoais hão de observar os limites delineados pelo âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII), sob pena de lesão a esses direitos. O compartilhamento, com ente público, de dados pessoais custodiados por concessionária de serviço público há de assegurar mecanismos de proteção e segurança quanto a esses dados. 3. O Regulamento Sanitário Internacional

> (RSI 2005) adotado no âmbito da Organização Mundial de Saúde exige, quando essencial o tratamento de dados pessoais para a avaliação e o manejo de um risco para a saúde pública, a garantia de que os dados pessoais manipulados sejam "adequados, relevantes e não excessivos em relação a esse propósito" e "conservados apenas pelo tempo necessário." (artigo 45, § 2º, alíneas "b" e "d"). 4. Consideradas a necessidade, a adequação e a proporcionalidade, não emerge da Medida Provisória nº 954/2020, nos moldes em que editada, interesse público legítimo no compartilhamento dos dados pessoais dos usuários dos serviços de telefonia. 5. Ao não definir apropriadamente como e para que serão utilizados os dados coletados, a MP nº 954/2020 desatende a garantia do devido processo legal (art. 5º, LIV, da CF), na dimensão substantiva, por não oferecer condições de avaliação quanto à sua adequação e necessidade, assim entendidas a compatibilidade do tratamento com as finalidades informadas e sua limitação ao mínimo necessário para alcançar suas finalidades. 6. Ao não apresentar mecanismo técnico ou administrativo apto a proteger, de acessos não autorizados, vazamentos acidentais ou utilização indevida, seja na transmissão, seja no tratamento, o sigilo, a higidez e, quando o caso, o anonimato dos dados pessoais compartilhados, a MP nº 954/2020 descumpre as exigências que exsurgem do texto constitucional no tocante à efetiva proteção dos direitos fundamentais dos brasileiros. 7. Mostra-se excessiva a conservação de dados pessoais coletados, pelo ente público, por trinta dias após a decretação do fim da situação de emergência de saúde pública, tempo manifestamente excedente ao estritamente necessário para o atendimento da finalidade declarada. 8. Agrava a ausência de garantias de tratamento adequado e seguro dos dados compartilhados a circunstância de que, embora aprovada, ainda não vigora a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), definidora dos critérios para a responsabilização dos agentes por eventuais danos ocorridos em virtude do tratamento de dados pessoais. O fragilizado ambiente protetivo impõe cuidadoso escrutínio sobre medidas como a implementada na MP nº 954/2020. 9. O cenário de urgência decorrente da crise sanitária deflagrada pela pandemia global da COVID-19 e a necessidade de formulação de políticas públicas que demandam dados específicos para o desenho dos diversos quadros de enfrentamento não pode ser invocado como pretextos para justificar investidas visando ao enfraquecimento de direitos e atropelo de garantias fundamentais consagradas na Constituição. 10. Fumus boni juris e periculum in mora demonstrados. Deferimento da medida cautelar para suspender a eficácia da Medida Provisória nº 954/2020, a fim de prevenir danos irreparáveis à intimidade e ao sigilo da vida privada de mais de uma centena de milhão de usuários dos serviços de telefonia fixa e móvel. 11. Medida cautelar referendada.

E é entendido neste julgado o seguinte:

> Ementa: DIREITO CONSTITUCIONAL. DIREITOS FUNDAMENTAIS À PRIVACIDADE E AO LIVRE DESENVOLVIMENTO DA PERSONALIDADE. TRATAMENTO DE DADOS PESSOAIS PELO ESTADO BRASILEIRO. COMPARTILHAMENTO DE DADOS PESSOAIS ENTRE ÓRGÃOS E ENTIDADES DA ADMINISTRAÇÃO PÚBLICA FEDERAL. ADI E ADPF CONHECIDAS E, NO MÉRITO, JULGADAS PARCIALMENTE PROCEDENTES. INTERPRETAÇÃO CONFORME À CONSTITUIÇÃO. DECLARAÇÃO DE INCONSTITUCIONALIDADE COM EFEITOS FUTUROS. 1. A Ação Direta de Inconstitucionalidade é cabível para impugnação do Decreto 10.046/2019, uma vez que o ato normativo não se esgota na simples regulamentação da Lei de Acesso à Informação e da Lei Geral de Proteção de Dados Pessoais, mas inova na ordem jurídica com a criação do Cadastro Base do Cidadão e do Comitê Central de Governança de Dados. A Arguição

de Descumprimento de Preceito Fundamental é cabível para impugnar o ato do poder público tendente à lesão de preceitos fundamentais, qual seja, o compartilhamento de dados da Carteira Nacional de Habilitação entre o SERPRO e a ABIN, ante a inexistência de outras ações aptas a resolver a controvérsia constitucional de forma geral, definitiva e imediata. 2. No julgamento da Ação Direta de Inconstitucionalidade 6.387, Rel. Min. Rosa Weber, o Supremo Tribunal Federal reconheceu a existência de um direito fundamental autônomo à proteção de dados pessoais e à autodeterminação informacional. A Emenda Constitucional 115, de 10 de fevereiro de 2022, positivou esse direito fundamental no art. 5º, inciso LXXIX, da Constituição Federal. 3. O tratamento de dados pessoais pelo Estado é essencial para a prestação de serviços públicos. Todavia, diferentemente do que assevera o ente público, a discussão sobre a privacidade nas relações com a Administração Estatal não deve partir de uma visão dicotômica que coloque o interesse público como bem jurídico a ser tutelado de forma totalmente distinta e em confronto com o valor constitucional da privacidade e proteção de dados pessoais. 4. Interpretação conforme à Constituição para subtrair do campo semântico da norma eventuais aplicações ou interpretações que conflitem com o direito fundamental à proteção de dados pessoais. O compartilhamento de dados pessoais entre órgãos e entidades da Administração Pública, pressupõe: a) eleição de propósitos legítimos, específicos e explícitos para o tratamento de dados (art. 6º, inciso I, da Lei 13.709/2018); b) compatibilidade do tratamento com as finalidades informadas (art. 6º, inciso II); c) limitação do compartilhamento ao mínimo necessário para o atendimento da finalidade informada (art. 6º, inciso III); bem como o cumprimento integral dos requisitos, garantias e procedimentos estabelecidos na Lei Geral de Proteção de Dados, no que for compatível com o setor público. 5. O compartilhamento de dados pessoais entre órgãos públicos pressupõe rigorosa observância do art. 23, inciso I, da Lei 13.709/2018, que determina seja dada a devida publicidade às hipóteses em que cada entidade governamental compartilha ou tem acesso a banco de dados pessoais, “fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos”. 6. O compartilhamento de informações pessoais em atividades de inteligência deve observar a adoção de medidas proporcionais e estritamente necessárias ao atendimento do interesse público; a instauração de procedimento administrativo formal, acompanhado de prévia e exaustiva motivação, para permitir o controle de legalidade pelo Poder Judiciário; a utilização de sistemas eletrônicos de segurança e de registro de acesso, inclusive para efeito de responsabilização em caso de abuso; e a observância dos princípios gerais de proteção e dos direitos do titular previstos na LGPD, no que for compatível com o exercício dessa função estatal. 7. O acesso ao Cadastro Base do Cidadão deve observar mecanismos rigorosos de controle, condicionando o compartilhamento e tratamento dos dados pessoais à comprovação de propósitos legítimos, específicos e explícitos por parte dos órgãos e entidades do Poder Público. A inclusão de novos dados na base integradora e a escolha de bases temáticas que comporão o Cadastro Base do Cidadão devem ser precedidas de justificativas formais, prévias e minudentes, cabendo ainda a observância de medidas de segurança compatíveis com os princípios de proteção da Lei Geral de Proteção de Dados Pessoais, inclusive a criação de sistema eletrônico de registro de acesso, para fins de responsabilização em caso de abuso. 8. O tratamento de dados pessoais promovido por órgãos públicos que viole parâmetros legais e constitucionais, inclusive o dever de publicidade fora das hipóteses constitucionais de sigilo, importará a responsabilidade civil do Estado pelos danos suportados pelos particulares, associada ao exercício do direito de regresso contra os servidores e agentes políticos responsáveis pelo ato ilícito, em caso de dolo ou culpa. 9. Declaração de inconstitucionalidade, com efeitos pro futuro, do art. 22 do Decreto

> 10.046/2019. O Comitê Central de Governança de Dados deve ter composição independente, plural e aberta à participação efetiva de representantes de outras instituições democráticas, não apenas dos representantes da Administração Pública federal. Ademais, seus integrantes devem gozar de garantias mínimas contra influências indevidas.

O setor público enfrenta desafios significativos na implementação da LGPD, incluindo a necessidade de adaptar processos e sistemas existentes, capacitar servidores e alinhar políticas internas às exigências da lei. A vasta diversidade e a complexidade das estruturas governamentais tornam essa tarefa ainda mais desafiadora, pelo fato de gerir milhões de dados de pessoas com informações extremamente delicadas.

O entendimento acerca do tratamento de dados realizado pelo poder público foi tratado da seguinte forma:

> Ementa: DIREITO CONSTITUCIONAL. DIREITOS FUNDAMENTAIS À PRIVACIDADE E AO LIVRE DESENVOLVIMENTO DA PERSONALIDADE. TRATAMENTO DE DADOS PESSOAIS PELO ESTADO BRASILEIRO. COMPARTILHAMENTO DE DADOS PESSOAIS ENTRE ÓRGÃOS E ENTIDADES DA ADMINISTRAÇÃO PÚBLICA FEDERAL. ADI E ADPF CONHECIDAS E, NO MÉRITO, JULGADAS PARCIALMENTE PROCEDENTES. INTERPRETAÇÃO CONFORME À CONSTITUIÇÃO. DECLARAÇÃO DE INCONSTITUCIONALIDADE COM EFEITOS FUTUROS. 1. A Ação Direta de Inconstitucionalidade é cabível para impugnação do Decreto 10.046/2019, uma vez que o ato normativo não se esgota na simples regulamentação da Lei de Acesso à Informação e da Lei Geral de Proteção de Dados Pessoais, mas inova na ordem jurídica com a criação do Cadastro Base do Cidadão e do Comitê Central de Governança de Dados. A Arguição de Descumprimento de Preceito Fundamental é cabível para impugnar o ato do poder público tendente à lesão de preceitos fundamentais, qual seja, o compartilhamento de dados da Carteira Nacional de Habilitação entre o SERPRO e a ABIN, ante a inexistência de outras ações aptas a resolver a controvérsia constitucional de forma geral, definitiva e imediata. 2. No julgamento da Ação Direta de Inconstitucionalidade 6.387, Rel. Min. Rosa Weber, o Supremo Tribunal Federal reconheceu a existência de um direito fundamental autônomo à proteção de dados pessoais e à autodeterminação informacional. A Emenda Constitucional 115, de 10 de fevereiro de 2022, positivou esse direito fundamental no art. 5º, inciso LXXIX, da Constituição Federal. 3. O tratamento de dados pessoais pelo Estado é essencial para a prestação de serviços públicos. Todavia, diferentemente do que assevera o ente público, a discussão sobre a privacidade nas relações com a Administração Estatal não deve partir de uma visão dicotômica que coloque o interesse público como bem jurídico a ser tutelado de forma totalmente distinta e em confronto com o valor constitucional da privacidade e proteção de dados pessoais. 4. Interpretação conforme à Constituição para subtrair do campo semântico da norma eventuais aplicações ou interpretações que conflitem com o direito fundamental à proteção de dados pessoais. O compartilhamento de dados pessoais entre órgãos e entidades da Administração Pública, pressupõe: a) eleição de propósitos legítimos, específicos e explícitos para o tratamento de dados (art. 6º, inciso I, da Lei 13.709/2018); b) compatibilidade do tratamento com as finalidades informadas (art. 6º, inciso II); c) limitação do compartilhamento ao mínimo

> necessário para o atendimento da finalidade informada (art. 6º, inciso III); bem como o cumprimento integral dos requisitos, garantias e procedimentos estabelecidos na Lei Geral de Proteção de Dados, no que for compatível com o setor público. 5. O compartilhamento de dados pessoais entre órgãos públicos pressupõe rigorosa observância do art. 23, inciso I, da Lei 13.709/2018, que determina seja dada a devida publicidade às hipóteses em que cada entidade governamental compartilha ou tem acesso a banco de dados pessoais, "fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos". 6. O compartilhamento de informações pessoais em atividades de inteligência deve observar a adoção de medidas proporcionais e estritamente necessárias ao atendimento do interesse público; a instauração de procedimento administrativo formal, acompanhado de prévia e exaustiva motivação, para permitir o controle de legalidade pelo Poder Judiciário; a utilização de sistemas eletrônicos de segurança e de registro de acesso, inclusive para efeito de responsabilização em caso de abuso; e a observância dos princípios gerais de proteção e dos direitos do titular previstos na LGPD, no que for compatível com o exercício dessa função estatal. 7. O acesso ao Cadastro Base do Cidadão deve observar mecanismos rigorosos de controle, condicionando o compartilhamento e tratamento dos dados pessoais à comprovação de propósitos legítimos, específicos e explícitos por parte dos órgãos e entidades do Poder Público. A inclusão de novos dados na base integradora e a escolha de bases temáticas que comporão o Cadastro Base do Cidadão devem ser precedidas de justificativas formais, prévias e minudentes, cabendo ainda a observância de medidas de segurança compatíveis com os princípios de proteção da Lei Geral de Proteção de Dados Pessoais, inclusive a criação de sistema eletrônico de registro de acesso, para fins de responsabilização em caso de abuso. 8. O tratamento de dados pessoais promovido por órgãos públicos que viole parâmetros legais e constitucionais, inclusive o dever de publicidade fora das hipóteses constitucionais de sigilo, importará a responsabilidade civil do Estado pelos danos suportados pelos particulares, associada ao exercício do direito de regresso contra os servidores e agentes políticos responsáveis pelo ato ilícito, em caso de dolo ou culpa. 9. Declaração de inconstitucionalidade, com efeitos pro futuro, do art. 22 do Decreto 10.046/2019. O Comitê Central de Governança de Dados deve ter composição independente, plural e aberta à participação efetiva de representantes de outras instituições democráticas, não apenas dos representantes da Administração Pública federal. Ademais, seus integrantes devem gozar de garantias mínimas contra influências indevidas.

Percebe-se que no Brasil, a proteção de dados já vinha se desenvolvendo a um certo tempo, se conectando com vários institutos legais e encontrando respaldos principiológicos na Constituição Federal. Logo, a LGPD surge num momento crucial para a era digital que estamos vivendo e para isso teve que, através de seus artigos, sistematizar e organizar a forma de operar, tratar e cuidar desses dados. Com isso, no âmbito do Poder Público a Lei disciplina e determinar em seu artigo 39 a obrigatoriedade de nomear um encarregado pelo tratamento de dados pessoais. Esse profissional ficará responsável por garantir a consonância e zelo com a legislação, se atentar às demandas dos titulares dos dados e informar com a Autoridade Nacional

de Proteção de Dados (ANPD) algum possível vazamento ou situação de risco para os titulares.

As entidades públicas, assim como as privadas, estão sujeitas a sanções em caso de descumprimento da LGPD. Isso inclui multas e outras penalidades aplicadas pela ANPD. A responsabilização visa garantir que o tratamento de dados pessoais pelo setor público ocorra de forma ética, segura e transparente.

As sanções administrativas aplicáveis aos entes públicos são relativamente mais brandas em comparação às destinadas aos entes privados e estão detalhadas no §3º do artigo 52 da LGPD. As sanções incluem:

> I - Advertência, com prazo estipulado para a adoção de medidas corretivas;
> IV - Divulgação da infração após sua apuração e confirmação;
> V - Bloqueio dos dados pessoais relacionados à infração até que sejam regularizados;
> VI - Eliminação dos dados pessoais relacionados à infração.

Embora os entes públicos não estejam sujeitos à punição de multa, sanções como o bloqueio dos dados pessoais podem impactar significativamente suas atividades. É importante destacar que empresas públicas e sociedades de economia mista que operam em regime de concorrência, conforme a Constituição, também estão sujeitas a sanções pecuniárias. Além da LGPD, o setor público deve cumprir outras legislações, como a Lei de Improbidade Administrativa, o Estatuto do Servidor Público Federal e a Lei de Acesso à Informação.

O Poder Público deve ter rigor na proteção de dados de seus cidadãos, buscar ser um exemplo na proteção de dados. Proliferar essa cultura em sua estrutura, gera não só benefícios aos tutelados, mas também uma política comprometida com seu País, tendo em vista que as práticas de segurança de dados já algo real e está sendo executada por todos os países. O próximo tópico abordaremos a LGPD em umas de suas autarquias e os desafios a serem enfrentados para garantir a segurança dos beneficiados pelo INSS.

2.2 ADEQUAÇÃO DO INSS À LGPD

O Instituto Nacional do Seguro Social (INSS) é uma autarquia federal brasileira, vinculada ao Ministério da Previdência Social, responsável pela administração das

contribuições e benefícios previdenciários dos trabalhadores brasileiros. O INSS desempenha um papel crucial na estrutura de proteção social do país, garantindo a seguridade social e o bem-estar de milhões de cidadãos.

Criado em 27 de junho de 1990 pela Lei nº 8.029, o INSS surgiu da fusão do Instituto Nacional de Previdência Social (INPS) com o Instituto de Administração Financeira da Previdência e Assistência Social (IAPAS). Seu principal objetivo é assegurar a proteção previdenciária dos trabalhadores e suas famílias, fornecendo benefícios em casos de doença, invalidez, idade avançada, morte e outros riscos sociais.

A Constituição Federal de 1988 definiu a Seguridade Social como: "um conjunto integrado de ações de iniciativas dos Poderes Públicos e da sociedade destinada a assegurar os direitos relativos à saúde, à previdência e à assistência social" (BRASIL, 1988).

O tema encontra suporte nas lições de Canotilho (1993, p. 61), para quem:

> “os direitos sociais apresentam uma dimensão subjetiva, como anteriormente apontado, decorrente da sua consagração como verdadeiros direitos fundamentais e da radicação subjetiva das prestações, instituições e garantias necessárias à concretização dos direitos reconhecidos na Constituição.”

O Instituto Nacional do Seguro Social (INSS), como órgão responsável pela gestão de dados de milhões de cidadãos, deve se adequar a essas normas para garantir a proteção das informações sensíveis dos beneficiários, bem como garantir que terceiro não tentem se apoderar de suas bases de dados visando proveito pessoal ou para fins ilícitos.

Desde a data de abril de 2015, em conformidade com a Lei nº 13.134, de 16 de junho de 2015, o INSS também ficou responsável por receber e processar os requerimentos, habilitar os beneficiários e decidir sobre a concessão do Seguro-Desemprego do Pescador Artesanal (SDPA), popularmente conhecido como Seguro Defeso. Além das competências estabelecidas na legislação pertinente, cabe ao INSS, conforme disposto no art. 5º da Lei nº 11.457/2007:

a) Emitir certidões relativas ao tempo de contribuição;

b) Gerir o Fundo do Regime Geral de Previdência Social;

c) Calcular o montante das contribuições mencionadas no art. 2º da referida lei e emitir o correspondente documento de arrecadação, visando a concessão ou revisão dos benefícios requeridos.

A implementação da LGPD pelo INSS envolve diversas etapas essenciais para assegurar a conformidade com as normas e garantir a proteção adequada dos dados pessoais dos beneficiários. A adequação é fundamental para melhorar a eficiência na gestão dessas informações, bem como evitar vazamento de dados que gerem prejuízos a sociedade.

De acordo com o Art. 2º da LGPD, a proteção dos direitos de privacidade e liberdade dos cidadãos é um princípio fundamental da lei. Ao se adequar à LGPD, o INSS garante que os dados pessoais dos beneficiários sejam tratados de forma segura e responsável, conforme os princípios da finalidade, adequação e necessidade descritos nos Art. 6º e 7º. Isso fortalece a confiança dos cidadãos na instituição e faz surtir efeito os dispositivos legais existentes, atingindo assim a finalidade de proteger os dados,

A conformidade com a LGPD minimiza os riscos de sanções administrativas e jurídicas decorrentes de possíveis violações de dados. Conforme o Art. 52 da LGPD, as penalidades por não conformidade podem incluir multas de formas significativas e outras sanções impostas pela Lei. Ao aderir às diretrizes da LGPD, o INSS reduz a possibilidade de sofrer essas sanções, protegendo sua imagem e evitando perdas financeiras à instituição. A conformidade, portanto, não é apenas uma medida de segurança, mas também uma estratégia de gestão visando assim a mitigação de riscos possíveis.

A LGPD, em seu Art. 37, incentiva a implementação de práticas de gestão de dados mais eficientes e transparentes. Com a adequação à LGPD, o INSS pode melhorar significativamente a maneira como coleta, armazena e utiliza os dados dos beneficiários. Processos bem definidos e políticas claras de tratamento de dados facilitam o acesso e a utilização correta das informações, tanto pelos beneficiários quanto pela administração pública, resultando em um serviço mais ágil e transparente.

O INSS, através do sistema DATAPREV, mantém um acervo consideras um dos maiores bancos de dados do mundo na atualidade do mundo, armazenando informações de vários trabalhadores brasileiros desde os anos 1970. Este banco de dados inclui também registros e cadastros de salários recebidos de inúmeros

trabalhadores em empregos formais que contribuem desde os anos de 1975, com uma certeza dessas informações a partir dos anos de 1994. É estimado que o Cadastro Nacional de Informações Sociais (CNIS) registre entre 2 e 3 milhões de acessos todos os dias, atendendo a uma demanda imensa de informações. Conforme o Decreto nº 10.047/2019, o INSS é agora oficialmente responsável pela gestão e administração do tratamento de dados do CNIS, bem como pela proteção de dados na previdência, além de promover pesquisas acerca dos seus tutelados nesta base de dados.

A LGPD ainda determina as limitações do poder público no compartilhamento de dados dos cidadãos, reforçando a proteção de dados na previdência da seguinte forma:

> 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);
> 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.

Inicialmente, a LGPD proibia o compartilhamento de dados entre órgãos do Poder Público e empresas privadas, exceto em casos específicos previstos na Lei. Contudo, a Medida Provisória n°869/2018 flexibilizou essa regra para as autarquias.

A responsabilização prevista na LGPD será definida pela jurisprudência atuis dos tribunais, mas algumas considerações sobre a aplicação das normas de proteção de dados na previdência já podem ser feitas, com base nos entendimentos existentes. A figura do controlador é a organização que detém e trata os dados, e o operador é definido como a pessoa que movimenta os dados.

No contexto previdenciário, o controlador será INSS ou o regime próprio de previdência, e o operador será servidor público responsável pela gestão dos dados sob sua custódia. Se houver vazamento de dados por um servidor da área de TI sem

o conhecimento do controlador, o poderá INSS ser responsabilizado pelos danos sofridos pelos titulares dos direitos.

Entretanto, se o INSS puder provar e mostrar quem foi o responsável pelo compartilhamento ou vazamento, a pena para a autarquia deve ser mitigada, e o servidor responsável deve ser responsabilizado e punido, vejamos o que prevê a Lei:

> Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.
>
> § 1º A fim de assegurar a efetiva indenização ao titular dos dados:
>
> I – o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;
>
> II – os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.
>
> § 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.
>
> § 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente.
>
> § 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.
>
> Mas ainda é preciso avaliar se o INSS ou RPPS respeitou as regras e a legislação para atribuir a autorização aos servidores, bem como realizou treinamento e preparação deste servidor acerca da proteção de dados:
>
> Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:
>
> I – que não realizaram o tratamento de dados pessoais que lhes é atribuído;
>
> II – que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou
>
> III – que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.
>
> Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:
>
> I – o modo pelo qual é realizado;
>
> II – o resultado e os riscos que razoavelmente dele se esperam;
>
> III – as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.
>
> Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano.

Nota-se que com o desenvolver do trabalho é possível verificar que a proteção de dados é algo fundamental, que lida com uma mudança cultural e organizacional de toda uma estrutura, seja pública ou privada, mas que também a Lei dispõe de mecanismos para individualizar e responsabilizar quem realmente causou o prejuízo no tratamento de dados.

A mudança trazida pela Lei, transforma não só a sociedade, mas um desafio para harmonizar a Lei ao cotidiano das pessoas e dos mecanismos para sua execução, nas palavras de Tepedino (2023, p. 54):

> "Como se observa, enorme é a repercussão da LGPD no dia a dia das relações sociais, consagrando direitos aos titulares e deveres e responsabilidades aos agentes de tratamento. Afinal, o desenvolvimento seguro da sociedade tecnológica, cujas fronteiras se mostram ainda desconhecidas, depende visceralmente do assenhoreamento da autodeterminação informativa e da consolidação de mecanismos de controle dos dados pessoais. A sociedade como um todo deve se adaptar a essa verdadeira mudança cultural, cabendo à doutrina, ao Judiciário e à Autoridade Nacional de Proteção de Dados harmonizarem a interpretação e aplicação da lei."

2.3 COMPARTILHAMENTO DE DADOS COM OS BANCOS

Conforme demonstrado no tópico acima, a adequação da LGPD ao INSS terá vários percalços a serem observados, como a vasta base de dados que o instituto terá que gerenciar, os desafios de garantir a segurança dos dados de seus titulares e as diretrizes estabelecidas pela LGPD.

O compartilhamento de dados do INSS com os bancos pode ocorrer em algumas situações específicas, como por meio do sistema de Open Banking. Esse sistema permite que os clientes compartilhem seus dados financeiros com outros bancos para receber ofertas de produtos e serviços personalizados1. No entanto, é importante destacar que qualquer compartilhamento de dados deve ser feito com o consentimento informado do cliente e seguir as regras estabelecidas pela Lei Geral de Proteção de Dados (LGPD).

É crucial que a Autoridade Nacional de Proteção de Dados (ANPD) atue de forma rigorosa para fiscalizar o cumprimento da Lei Geral de Proteção de Dados (LGPD), especialmente quanto à aplicação das penalidades previstas, que se tornaram efetivas em agosto deste ano. Importante destacar que o INSS tem sido

omisso em relação aos empréstimos não solicitados e ao constante assédio aos beneficiários, apesar da Instrução Normativa nº 28/2008 proibir contatos das instituições financeiras antes de 180 dias após a concessão do benefício, vejamos:

> "§3º. Fica expressamente vedado às instituições financeiras e sociedades de arrendamento mercantil que mantenham Convênios e/ou Acordos de Cooperação Técnica com o INSS, diretamente ou por meio de interposta pessoa, física ou jurídica, qualquer atividade de marketing ativo, oferta comercial, proposta, publicidade direcionada a beneficiário específico ou qualquer tipo de atividade tendente a convencer o beneficiário do INSS a celebrar contratos de empréstimo pessoal e cartão de crédito, com pagamento mediante consignação em benefício, antes do decurso de 180 (cento e oitenta) dias contatos a partir da respectiva DDB.
> §4º. As atividades referidas no § 3º deste artigo, se realizadas no prazo de vedação, serão consideradas assédio comercial, e serão punidas nos termos do Capítulo XII, sem prejuízo de assim também serem consideradas outras práticas qualificadas como abusivas pelos órgãos de defesa do consumidor.
> Artigo 52 — Constatadas irregularidades nas operações de consignação/retenção/RMC realizadas pelas instituições financeiras ou por correspondentes bancários a seu serviço, na veiculação, na ausência de respostas ou na prestação de informações falsas ou incorretas aos beneficiários, sem prejuízo das operações regulares, o INSS aplicará as seguintes penalidades: (…)
> III — Suspensão do recebimento de novas consignações/retenções/RMC por 45 (quarenta e cinco) dias corridos, a contar da comunicação, quando for confirmada a existência de ocorrência que contrarie o disposto no § 4º do artigo 1º, inciso II do artigo 3º e inciso I do artigo 15, independentemente dos procedimentos estabelecidos no artigo 46".

Uma situação bastante comum é o aposentado ou pensionista ser alvo de múltiplos contatos de diversas instituições bancárias, que buscam oferecer empréstimos consignados. Esse assédio atinge níveis extremos, especialmente quando o beneficiário acaba de se aposentar, muitas vezes sabendo da concessão do benefício antes mesmo de ser informado oficialmente pelo INSS. Na maioria dos casos, as instituições financeiras já têm acesso ao valor do benefício, à previsão de pagamento e a outros dados relevantes. A modalidade de empréstimo consignado,

instituída pela Lei n° 10.820/2003, vem crescendo exponencialmente desde a sua criação.

Percebe-se que esse assédio é algo negativo que interfere no livre desenvolvimento da pessoa natural. "O direito ao livre desenvolvimento da personalidade é um direito subjetivo, na medida em que o indivíduo tem a faculdade de impor seus interesses ao Estado, exigindo-lhe uma conduta omissiva" (MIRANDA, 2023, p. 5).

Assim, a proteção deste direito é essencial para a construção de uma sociedade que valorize a liberdade, a diversidade, a dignidade humana e as individualidades de cada pessoa.

Outra situação que ocorre de forma frequente são os golpes contra os aposentados/clientes, tendo em vista que os bancos por terem acesso aos dados dos titulares, em certos momentos podem ser entendidas por facilitadoras ou por falta de observância na realização de proteção destes dados, causam vazamentos. Vejamos casos concretos:

> CONSUMIDOR. RECURSO ESPECIAL. AÇÃO DECLARATÓRIA DE INEXIGIBILIDADE
> DE DÉBITO POR VAZAMENTO DE DADOS BANCÁRIOS CUMULADA COM INDENIZAÇÃO POR DANOS MORAIS E REPETIÇÃO DE INDÉBITO. GOLPE DO BOLETO.
> TRATAMENTO DE DADOS PESSOAIS SIGILOSOS DE MANEIRA INADEQUADA. FACILITAÇÃO DA ATIVIDADE CRIMINOSA. FATO DO SERVIÇO. DEVER DE INDENIZAR PELOS PREJUÍZOS. SÚMULA 479/STJ. RECURSO ESPECIAL PROVIDO.
> 1. Ação declaratória de inexigibilidade de débito por vazamento de dados bancários cumulada com indenização por danos morais e repetição de indébito, ajuizada em 13/2/2020, da qual foi extraído o presente recurso especial, interposto em 15/2/2022 e concluso ao gabinete em 19/6/2023.
> 2. O propósito recursal consiste em decidir se a instituição financeira responde por falha na prestação de serviços bancários, consistente no vazamento de dados que facilitou a aplicação de golpe em desfavor do consumidor.
> 3. Se comprovada a hipótese de vazamento de dados da instituição financeira, será dela, em regra, a responsabilidade pela reparação integral de eventuais danos. Do contrário, inexistindo elementos objetivos que comprovem esse nexo causal, não há que se falar em responsabilidade das instituições financeiras pelo vazamento de dados utilizados por estelionatários para a aplicação de golpes de engenharia social (REsp 2.015.732/SP, julgado em 20/6/2023, DJe de 26/6/2023).
> 4. Para sustentar o nexo causal entre a atuação dos estelionatários e o vazamento de dados pessoais pelo responsável por seu tratamento, é imprescindível perquirir, com exatidão, quais dados estavam em poder dos criminosos, a fim de examinar a origem de eventual vazamento e, consequentemente, a responsabilidade dos agentes respectivos. Os nexos de causalidade e imputação, portanto, dependem da hipótese concretamente analisada.

> 5. Os dados sobre operações bancárias são, em regra, de tratamento exclusivo pelas instituições financeiras. No ponto, a Lei Complementar 105/2001 estabelece que as instituições financeiras conservarão sigilo em suas operações ativas e passivas e serviços prestados (art. 1º), constituindo dever jurídico dessas entidades não revelar informações que venham a obter em razão de sua atividade profissional, salvo em situações excepcionais. Desse modo, seu armazenamento de maneira inadequada, a possibilitar que terceiros tenham conhecimento de informações sigilosas e causem prejuízos ao consumidor, configura defeito na prestação do serviço (art. 14 do CDC e art. 44 da LGPD).
> 6. No particular, não há como se afastar a responsabilidade da instituição financeira pela reparação dos danos decorrentes do famigerado "golpe do boleto", uma vez que os criminosos têm conhecimento de informações e dados sigilosos a respeito das atividades bancárias do consumidor. Isto é, os estelionatários sabem que o consumidor é cliente da instituição e que encaminhou e-mail à entidade com a finalidade de quitar sua dívida, bem como possuem dados relativos ao próprio financiamento obtido (quantidade de parcelas em aberto e saldo devedor do financiamento).
> 7. O tratamento indevido de dados pessoais bancários configura defeito na prestação de serviço, notadamente quando tais informações são utilizadas por estelionatário para facilitar a aplicação de golpe em desfavor do consumidor.
> 8. Entendimento em conformidade com Tema Repetitivo 466/STJ e Súmula 479/STJ: "As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias".
> 9. Recurso especial conhecido e provido para reformar o acórdão recorrido e reestabelecer a sentença proferida pelo Juízo de primeiro grau.

A LGPD visa principalmente aumentar a transparência e a segurança no uso de dados pessoais. As instituições bancárias têm a responsabilidade de assegurar que todas as informações coletadas sejam protegidas contra acessos não autorizados e utilizadas somente para os fins específicos previamente consentidos pelos clientes.

2.3.1 Do direito à privacidade

O direito à privacidade é um pilar fundamental dos direitos humanos, reconhecido internacionalmente por diversas convenções e legislado em muitos países. Este direito protege a autonomia individual, a dignidade e a liberdade, assegurando que os indivíduos possam controlar informações sobre si mesmos e se proteger contra intromissões indevidas em suas vidas pessoais.

À privacidade envolve o direito de uma pessoa de manter em segredo seus pensamentos, sentimentos, comunicações e informações pessoais. Ele está intrinsecamente ligado ao respeito pela dignidade humana e à proteção contra a vigilância excessiva e a coleta indevida de dados. É reconhecido em várias

convenções internacionais, como a Declaração Universal dos Direitos Humanos (Artigo 12) e o Pacto Internacional sobre Direitos Civis e Políticos (Artigo 17).

A privacidade da informação refere-se à proteção de dados pessoais contra coleta, armazenamento e compartilhamento não autorizados. Inclui a segurança de dados pessoais online e offline. A CF prevê o seguinte:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
>
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;(BRASIL, 1988)

Percebe-se, portanto, que os direitos demonstrados neste trabalho, são garantias constitucionais, ou seja, de suma importância, logo o respeito e a manutenção desses é responsabilidade máxima de todos os envolvidos, neste caso, dos entes responsáveis pela proteção dos dados, que envolvem o poder público, a autarquia INSS e no fim da cadeia as instituições financeiras.

A privacidade pessoal é essencial não apenas para a proteção dos dados pessoais, mas também para o exercício da liberdade de expressão e da liberdade de associação das pessoas. Sem privacidade, indivíduos podem ser expostos de forma negativa e dependendo do que foi infligido por essa exposição gerar facilidade a terceiros de má-fé, que utilizam das informações para proveitos criminosos.

O direito à privacidade é crucial para a proteção da liberdade e da dignidade humana. Em um mundo cada vez mais interconectado, é essencial que as leis continuem a evoluir para proteger os indivíduos contra novas formas de intrusão. A sociedade como um todo deve valorizar e defender esse direito para garantir que a privacidade continue sendo uma parte fundamental da vida humana.

Nesta visão, pontuam Maria Eugenia Finkelstein e Claudio Finkelstein (2019, p. 288):

> [...] a questão da privacidade na Internet vem cada vez mais recebendo atenção das cortes internacionais, uma vez que o seu tênue limite é cada vez mais invadido pela tecnologia. Ademais, sempre que um usuário adentra um site, preenche formulários virtuais. E o que é pior, não se sabe se os dados fornecidos são verdadeiros nem se pode ter certeza acerca da forma de utilização desta informação. Sabe-se que na atual fase tecnológica em que a sociedade se encontra,10 a informação é um dos bens de maior valor. Por esta razão, a sua proteção deve ser questão de importância

> máxima, merecendo a atenção do legislador. Claro está que o desenvolvimento tecnológico não apresenta somente aspectos negativos. A evolução da tecnologia dos mecanismos de monitoramento proporciona uma queda no tempo e nas despesas envolvidas em buscas.

A necessidade de proteção está no seu momento de maior urgência, tendo em vista que a era digital está criando um acervo pessoal de todos que se torna um produto comerciável, que parte das instituições financeiras podem se valer disso para sobrecarregar as pessoas com ofertas e produtos, que na maioria vezes não são desejadas e ofendem princípios fundamentas.

Nas palavras de Maria Eugenia Finkelstein e Claudio Finkelstein (2019, p. 290):

> [...] a comercialização dos dados coletados pelos sites para outros fins, para empresas comerciais ou de prestação de serviços não coligadas à empresa que os coletou, merece maior atuação do Direito em defesa dos usuários e de sua privacidade. Este tipo de comércio é um claro caso de violação de privacidade, que caracteriza uma não observância aos direitos e garantias fundamentais da pessoa. Neste sentido e em resposta a esta necessidade, veio a Lei Geral de Proteção de Dados (LGPD).

E em complementação:

> Para entender a necessidade de uma legislação protetiva de dados pessoais, faz-se necessário entender o ingresso da sociedade em um novo patamar de produção de bens e serviços. Nesta sociedade da informação, a geração, o armazenamento e a transferência das informações são realizados instantaneamente, sendo que as novas tecnologias agregam valor à informação. Vale dizer: a informação passou a ser considerada um produto, podendo, inclusive, vir a ser objeto de transações comerciais. Na sociedade da informação há, assim, excesso de informações e riscos relacionados ao uso indevido dos instrumentos computadorizados para desvios ou abusos relacionados aos dados coletados ou armazenados. Nesta realidade, os empresários podem obter informações fundamentais para suas operações cotidianas através da inteligência e do armazenamento de dados (FINKELSTEIN; FINKELSTEIN, 2019, p. 291).

Sendo desta forma, o sistema de informação tecnológica sempre passa por uma evolução exponencial, que gera à necessidade de proteção, especialmente em relação à privacidade das pessoas, fato este que fez surgir a Lei Geral de Proteção de Dados no Brasil.

3 CONCLUSÃO

O presente artigo buscou observar a Lei Geral de Proteção de Dados no Âmbito do Instituto Nacional do Seguro Social, de forma a análise os desafios e benefícios da aplicabilidade da Lei no instituto.

Para isso, buscou-se explicar todo o caminho que a lei percorre, seus dispositivos legais e os agentes que fazem o tratamento dessas informações para demonstrar as dificuldades e soluções cabíveis em cada situação. A LGPD e os agentes vinculados nesse âmbito do INSS que foram citados no texto, formam uma grande cadeia de possibilidades para tratamento de dados, sendo o dispositivo legal um marco para a sociedade brasileira, tendo em vista que os temas discutidos no texto são de suma importância para o dia a dia dos aposentados, beneficiados e a sociedade. O assunto revelou como os direitos abordados no trabalho são fundamentais e necessitam a cada dia aperfeiçoamento.

Foi identificado que, a Lei Geral de Proteção de Dados no âmbito do INSS, lida diariamente com vários dados sensíveis e pessoais de cidadãos e que tem o objetivo de garantir e proteger direitos fundamentais assegurados na Constituição Federal de 1988. Sendo assim, será necessário não só adaptar os sistemas que operam esses dados, mas fazer a gestão das pessoas responsáveis pelo tratamento, valendo-se assim da Lei para garantir a aplicação de sanções caso sejam necessárias.

Também foi trabalhado a relação do INSS com os bancos, tendo em vista que os dados são compartilhados com as instituições financeiras e que algumas situações podem gerar assédio aos aposentados. Os desafios abordados neste trabalho, buscavam trazer à tona como seria a aplicação da Lei no INSS e de as complicações de cada operação e agentes vinculados.

Diante do desafio da pesquisa, foi apresentado as diretrizes da Lei Geral de Proteção de Dados, onde foi possível verificar que os procedimentos previstos na Lei são robustos e norteiam os encarregados em proteger os dados para uma gestão com segurança.

Além disso, a busca acerca da proteção de dados foi além da relação INSS e pessoa beneficiada, abordou-se também a relação com os bancos e todo o assédio sofrido pelas pessoas. Essa análise proporcionou a importância da fiscalização bem como da aplicação correta dos dispositivos legais para uma melhor a implementação

da Lei Geral de Proteção de Dados no INSS. As diretrizes constantes na Lei visam direcionar a forma como deve ser fornecido as informações, bem como quem serão os responsáveis e possivelmente direcionar quem sofrerá as sanções por prejuízos sofrido pelos titulares das informações.

Contudo, verificou-se que a Lei Geral de Proteção de Dados, bem como os direitos envolvidos no trabalho são considerados fundamentais e foi demonstrado através de doutrinas, bem como jurisprudências tal afirmação. O fato do assédio sofrido pelos titulares em relação aos bancos, evidenciam que a LGPD não só traz organicidade ao sistema de tratamento de dados, mas também meios para as pessoas lesadas buscarem a indenização cabível, pois foi mostrado que a maioria das situações acontecem antes mesmo do recebimento do benefício pela pessoa, fato este que gera um tremendo desconforto, pois grande parte dos casos se tratam de pessoas com pouca instrução que acabam sendo levadas a consórcios e empréstimos forçados.

É entendido que a LGPD é uma Lei nova e ainda muitas empresas e entidades públicas ainda estão se adequando e investindo em suas estruturas para chegar no que é o essencial para uma proteção de dados eficaz. Através da LGPD, será transformado todo um sistema existente, que é o do INSS, ficando assim mais organizado e efetivo. Para isso, o primeiro passo é começa de cima, adequando a estrutura de dados e a relação com os beneficiados e com isso atingindo o fim da cadeia que seria a relação com os bancos, tornando o serviço prestado, que é fundamental numa sociedade que respeita os direitos individuais, assegurando uma sociedade democrática e transparente.

REFERÊNCIAS

ANPD. Guia do poder público ANPD. Versão final. Brasília: **Autoridade Nacional de Proteção de Dados, 2024**. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em: 15 nov. 2024.

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

BLUM, Renato M. S. Opice. **GDPR – General Data Protection Regulation: destaques da regra europeia e seus reflexos no Brasil**. Revista dos Tribunais, São Paulo, v. 107, n. 994, p. 205-221, ago. 2018.

BLUM, Renato Opice; ZAMPERLIN, Emelyn. **Compliance, responsabilidade empresarial e segurança da informação**. Lex Magister. Disponível em: file:///D:/LGPD/(BLUM,%20Renato%20Opice;%20ZAMPERLIN,%20Emelyn)%20Compliance,%20responsabilidade%20empresarial%20e%20seguran%C3%A7a%20da%20informa%C3%A7%C3%A3o.%20-%20Lex%20Doutrina%20(1).pdf. Acesso em: 09 set. 2024.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa doBrasil de 1988**. Promulgada em 5 de outubro de 1988. Diário Oficial da União, Brasília, DF, 5 out. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 05 out. 2024. Acesso em: 04 out. 2024.

_____. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais. Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 20 out. 2024.

CUEVA, Ricardo Villas Bôas. A insuficiente proteção de dados pessoais no Brasil. **Revista de Direito Civil Contemporâneo**, São Paulo, v. 13, p. 59-67, out.-dez.2017.

CANOTILHO, J. J. Gomes. Direito Constitucional. Coimbra: **Almedina**, 1993.

DONEDA, Danilo; MENDES, Laura Schertel. Reflexões Iniciais sobre a Nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor**, São Paulo, v. 120, p. 469-483, nov.-dez. 2018.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: elementos da formação da Lei geral de proteção de dados.** São Paulo: Thomson Reuters Brasil, 2019.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law** [EJJL], [S. l.], v. 12, n. 2, p. 91–108, 2011. Disponível em: https://periodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em: 16 nov. 2024.

DONEDA, Danilo. **A proteção de dados pessoais nas relações de consumo: para além da informação creditícia**. Escola Nacional de Defesa do Consumidor. Brasília: SDE/DPDC, 2010. p. 22.

FINKELSTEIN, Maria Eugenia; FINKELSTEIN, Claudio. Privacidade e Lei Geral de Proteção de Dados Pessoais. **Revista de Direito Brasileira**. Florianópolis, v. 23, nº. 9, p. 284-301, maio/ago. 2019.

LIMA, Cíntia Rosa Pereira de. **ANPD e LGPD: Desafios e perspectivas**. São Paulo: Almedina Brasil, 2021. E-book. p. 48. ISBN 9786556272764. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786556272764/>. Acesso em: 19 out. 2024.

LUGATI, L. N.; ALMEIDA, J. E. de. A LGPD e a construção de uma cultura de proteção de dados. **Revista de Direito,** [S. l.], v. 14, n. 01, p. 01–20, 2022. DOI: 10.32361/2022140113764. Disponível em: https://periodicos.ufv.br/revistadir/article/view/13764. Acesso em: 17 nov. 2024.

MIGALHAS. **LGPD e setor público: aspectos gerais e desafios**. Disponível em: <https://www.migalhas.com.br/depeso/300585/lgpd-e-setor-publico--aspectos-gerais-e-desafios>. Acesso em: 06 nov. 2024.

MARTINS, Gustavo Afonso. **A relação entre a pessoa jurídica e a LGPD**. Consultor Jurídico, 2020. Disponível em: <https://www.conjur.com.br/2020-gustavo-martins-relacao-pessoa-juridica-lgpd>. Acesso em: 09 out. 2024.

ROSSO, Ângela Maria. **LGPD e setor público: aspectos gerais e desafios**. Disponível em: https://www.migalhas.com.br/depeso/300585/lgpd-e-setor-publico--aspectos-gerais-e-desafios. Acesso em: 07 nov. 2024.

SILVA, J. Os Dados Pessoais como o Novo Petróleo da Era Digital. **Revista Brasileira de Proteção de Dados**, v. 5, n. 3, p. 120-135, 2023.

TEPEDINO, G. Desafios da Lei Geral de Proteção de Dados (LGPD). **Revista Brasileira de Direito Civil**, [S. l.], v. 26, n. 04, p. 11, 2021. Disponível em: https://rbdcivil.ibdcivil.org.br/rbdc/article/view/689. Acesso em: 13 nov. 2024.

TEFFÉ, C. S. DE; VIOLA, M. **Tratamento de dados pessoais na LGPD: estudo sobre as bases legais**. civilistica.com, v. 9, n. 1, p. 1-38, 9 maio 2020. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/510. Acesso em: 13 nov. 2024.

TEIXEIRA, Tarcísio; GUERREIRO, Ruth M. **Lei Geral de Proteção de Dados Pessoais (LGPD): Comentada Artigo por Artigo**. 4. ed. Rio de Janeiro: Saraiva Jur, 2022. E-book. p. 12. ISBN 9786555599015. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786555599015/>.Acesso em: 19 out. 2024.

TECNOCOMP. **LGPD: sua infraestrutura pode atrapalhar?** TECNOCOMP, 2023. Disponível em: https://tecnocomp.com.br/lgpd-sua-infraestrutura-pode-interferir/. Acesso em: 06 nov. 2024.