E-ISSN: 2595-7414
Revista Brasileira de Direito Social - RBDS, Belo horizonte, v. 9, n. 2, p. 71-81, 2026

[direito previdenciário digital]

PROTEÇÃO E VAZAMENTO DE DADOS NO INSS: UMA ANÁLISE MACRO DA IMPORTÂNCIA DAS INFORMAÇÕES PARA A PREVIDÊNCIA SOCIAL

Mateus Silva[1]
José Ricardo Caetano Costa[2]

Resumo

O presente artigo analisa os desafios relacionados à proteção de dados pessoais no Brasil, com foco nos incidentes de vazamento de informações no âmbito do Instituto Nacional do Seguro Social (INSS). A partir da promulgação da Lei Geral de Proteção de Dados Pessoais (LGPD — Lei nº 13.709/2018), o tema ganhou centralidade no debate jurídico, técnico e social, impondo obrigações de governança, transparência e segurança ao setor público. O estudo revisita o caso do vazamento de dados do INSS em 2022, avalia a atuação da Autoridade Nacional de Proteção de Dados (ANPD) e discute as consequências jurídicas para o instituto e para os segurados. A análise está fundamentada em literatura científica disponível no Portal de Periódicos da CAPES, contribuindo para o entendimento das implicações constitucionais, administrativas e civis da proteção de dados previdenciários.

Palavras-chave: LGPD; INSS; vazamento de dados; proteção de dados pessoais; ANPD; justiça social.

DATA PROTECTION AND BREACHES AT INSS: A MACRO ANALYSIS OF THE IMPORTANCE OF INFORMATION FOR SOCIAL SECURITY

Abstract

This article analyzes the challenges related to the protection of personal data in Brazil, with a focus on data breach incidents within the National Institute of Social Security (INSS). Since the enactment of the General Data Protection Law (LGPD — Law No. 13,709/2018), the topic has gained prominence in legal, technical, and social debates, imposing governance, transparency, and security obligations on the public sector. The study revisits the INSS data breach case of 2022, assesses the role of the National Data Protection Authority (ANPD), and discusses the legal consequences for the institute and its beneficiaries. The analysis is grounded in scientific literature available through the CAPES Journals Portal, contributing to the understanding of the constitutional, administrative, and civil implications of social security data protection.

Keywords: LGPD; INSS; data breach; personal data protection; ANPD; social justice.

[1] Mestrando em Direito e Justiça Social no Programa de Pós-Graduação em Direito e Justiça Social (PPGDJS) da Universidade Federal do Rio Grande (FURG); pós-graduando lato-sensu em Direito Societário na Faculdade Legale. Bacharel em Direito pela Universidade Federal do Rio Grande. E-mail: dasilvamateus@furg.br.

[2] Doutor em Serviço Social pela Pontifícia Universidade Católica do Rio Grande do Sul (PUC/RS), Professor da Faculdade de Direito (FADIR) e do Programa de Pós-Graduação em Direito e Justiça Social (PPGDJS) da Universidade Federal do Rio Grande (FURG). E-mail: jrcc.pel@gmail.com.

1 INTRODUÇÃO

A sociedade contemporânea vive sob o signo da informação. O Estado brasileiro, cada vez mais digitalizado, coleta, armazena e processa dados pessoais dos cidadãos em larga escala. Nesse contexto, a proteção desses dados passa a ser um dos pilares da confiança institucional. O INSS, responsável pela gestão previdenciária, detém bases de dados altamente sensíveis, cujo vazamento pode causar danos sociais e econômicos de grandes proporções.

O episódio de 2022, em que milhões de registros do INSS foram expostos, trouxe à tona a fragilidade dos sistemas públicos de informação e evidenciou a urgência de políticas robustas de governança de dados. Como afirma Oliveira e Silva (2025), "o incidente envolvendo o INSS revelou não apenas a vulnerabilidade dos sistemas, mas também as deficiências nas respostas institucionais, sobretudo no que tange à comunicação com os titulares" (Oliveira; Silva, 2025, p. 7).

Este artigo tem como objetivo examinar os aspectos jurídicos e sociais do vazamento de dados no INSS, à luz da LGPD, destacando a atuação da ANPD e discutindo as responsabilidades decorrentes do caso.

2 MATERIAL E MÉTODOS

Para a execução da pesquisa, foram mobilizados recursos materiais, humanos e financeiros adequados às diferentes etapas do projeto. Foi imprescindível o acesso a bases de dados jurídicas e acadêmicas, como o Portal de Periódicos CAPES, LexisNexis, Web of Science e Scopus, que se mostraram fundamentais para a realização da pesquisa bibliográfica com o rigor científico necessário. O acesso a repositórios institucionais de teses, dissertações e periódicos também se mostrou essencial para a revisão de literaturas.

A pesquisa adotou uma abordagem qualitativa de caráter exploratório e descritivo, voltada à análise dos desafios e perspectivas da implementação da Lei Geral de Proteção de Dados no âmbito do Instituto Nacional do Seguro Social (INSS). O estudo se fundamentou em pesquisa bibliográfica e documental, complementada pela análise de casos concretos de vazamentos de dados ocorridos na autarquia em 2022. A escolha dessa metodologia justificou-se pela necessidade de compreender em profundidade o fenômeno estudado, contemplando tanto seus aspectos normativos quanto suas repercussões práticas para a gestão de dados sensíveis no contexto previdenciário.

Segundo Rodrigues e Grubba (2023), a pesquisa qualitativa busca compreender a complexidade dos fenômenos sociais a partir da profundidade das informações coletadas, priorizando a qualidade das percepções e significados atribuídos pelos participantes. Nesse tipo de abordagem, a amostragem tende a ser reduzida, pois o foco não reside na quantificação, mas na interpretação dos dados a partir de categorias, atributos ou modalidades que não podem ser expressos numericamente. Os autores ainda destacam que o número de participantes não é previamente definido, sendo delimitado em função da saturação das informações ao longo da coleta.

A pesquisa bibliográfica contemplou literatura especializada em proteção de dados pessoais, direito previdenciário e segurança da informação, priorizando publicações

posteriores à promulgação da LGPD, em 2018. Foram privilegiadas obras de referência, artigos científicos publicados em periódicos e revistas, bem como teses e dissertações disponíveis no Banco de Teses e Periódicos da CAPES. Essa etapa possibilitou a construção de um referencial teórico consistente, que fundamentou a análise e evidenciou as principais correntes doutrinárias sobre o tema, estabelecendo bases conceituais sólidas para o desenvolvimento da investigação.

A pesquisa documental concentrou-se na análise de fontes primárias, como a legislação pertinente (Lei nº 13.709/2018, Decreto nº 10.046/2019, além de Portarias e Instruções Normativas do INSS relacionadas à proteção de dados).

Esse percurso metodológico viabilizou uma análise ampla e multidimensional do objeto de estudo, contemplando tanto os aspectos jurídico-normativos quanto os elementos técnicos e organizacionais indispensáveis à compreensão dos desafios da proteção de dados no âmbito previdenciário. Os resultados alcançados ofereceram subsídios relevantes para a formulação de propostas de aprimoramento da governança de dados no INSS, bem como para o desenvolvimento de políticas públicas voltadas à proteção de dados sensíveis no sistema previdenciário brasileiro.

3 A LGPD E A PROTEÇÃO DE DADOS NO SETOR PÚBLICO

A promulgação da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) representou um marco no ordenamento jurídico brasileiro, inserindo o país em um cenário normativo alinhado às exigências globais de tutela da privacidade e da segurança da informação. Inspirada em legislações internacionais, especialmente no Regulamento Geral sobre a Proteção de Dados da União Europeia (GDPR), a LGPD estabeleceu princípios, direitos e obrigações aplicáveis a todos os agentes de tratamento de dados pessoais — sejam eles privados ou públicos.

No âmbito do setor público, a LGPD assumiu papel ainda mais sensível. Isso porque a administração pública, em especial órgãos como o INSS, é depositária de enormes bases de dados que abarcam informações pessoais, muitas delas classificadas como dados sensíveis (informações biométricas, bancárias, de saúde e de vida laboral dos cidadãos). A potencialidade de dano em caso de vazamento é imensa, pois envolve não apenas riscos econômicos imediatos, mas também violações graves de direitos fundamentais.

Conforme Gonçalves, Salvador e Agostinho (2024), “a proteção de dados pessoais, quando analisada na esfera estatal, transcende a esfera da mera relação jurídica entre controlador e titular, convertendo-se em verdadeiro dever constitucional de proteção à dignidade da pessoa humana” (p. 217). Ou seja, o Estado, ao coletar e gerenciar dados, não pode se comportar como mero agente administrativo, mas como guardião de informações cuja preservação está intimamente ligada à garantia da cidadania.

A LGPD introduziu, nesse sentido, princípios norteadores que devem orientar a atuação da administração pública, como a finalidade (os dados só podem ser tratados para propósitos legítimos, específicos e explícitos), a necessidade (limitação do tratamento ao mínimo indispensável), a transparência (dever de comunicação clara e acessível ao titular) e a segurança (adoção de medidas técnicas e administrativas aptas a proteger os dados contra acessos não autorizados ou situações ilícitas).

A especificidade da aplicação da LGPD ao setor público está prevista em seu art. 23, que determina que o tratamento de dados pela administração deve observar sua finalidade pública e respeitar os princípios da lei, sempre visando ao interesse público. Isso inclui órgãos federais como o INSS, que não apenas coletam dados para concessão de benefícios, mas também operam em cooperação com outros entes da federação e instituições bancárias para pagamento de aposentadorias e auxílios, ampliando a complexidade do tratamento.

De acordo com Oliveira e Silva (2025), "a LGPD impôs um novo paradigma de governança de dados no setor público, exigindo que a administração pensasse seus fluxos informacionais e adotasse mecanismos de prevenção e resposta a incidentes" (p. 5). Entretanto, a autora ressalta que a implementação dessa governança ainda é marcada por desafios estruturais, como carência de recursos tecnológicos, ausência de cultura organizacional voltada à segurança da informação e limitações na capacitação de servidores.

Um dos pontos centrais da LGPD é a previsão de que, em caso de incidentes de segurança, deve haver comunicação imediata tanto à ANPD quanto aos titulares dos dados afetados. Essa obrigação assume maior relevância no setor público porque envolve direitos de coletividades inteiras, como segurados e beneficiários previdenciários. O silêncio ou a demora na comunicação pode ser interpretado como violação direta do princípio da transparência e do direito à informação, protegido constitucionalmente.

Outro aspecto fundamental é o regime de responsabilização imposto pela LGPD. Ainda que haja certa dificuldade em aplicar sanções pecuniárias diretas a órgãos da administração pública, a lei prevê a possibilidade de medidas corretivas, como a publicização da infração, recomendações de melhoria e a própria responsabilização civil do Estado. Nas palavras de Gonçalves, Salvador e Agostinho (2024), "a LGPD reforça a noção de que o Estado não está imune às exigências de tutela da privacidade, cabendo-lhe responder pelos danos advindos de sua negligência" (p. 221).

No contexto da temática, Pinheiro (2023) destaca uma preocupação central com a proteção de dados pessoais, especialmente quando o tratamento envolve indivíduos em situações de vulnerabilidade, como crianças, adolescentes e idosos. O reconhecimento dos dados de pessoas vulneráveis como de alto risco reforça a responsabilidade das organizações em implementar medidas de proteção mais rigorosas, com o objetivo de preservar os direitos e a dignidade desses indivíduos, em conformidade com os princípios de segurança e ética estabelecidos pela Lei Geral de Proteção de Dados (LGPD).

A proteção de dados, portanto, não deve ser vista como mera formalidade burocrática, mas como elemento estruturante da confiança social. No caso do INSS, que lida diariamente com informações de milhões de brasileiros, o cumprimento da LGPD significa mais do que resguardar dados: significa proteger trajetórias de vida, garantir segurança a populações vulneráveis e assegurar que a previdência cumpra seu papel de amparo e dignidade.

4 O INCIDENTE DE VAZAMENTO DE DADOS DO INSS EM 2022

O ano de 2022 marcou um dos episódios mais emblemáticos da fragilidade da proteção de dados no setor público brasileiro: o vazamento em larga escala de informações

previdenciárias no âmbito do Instituto Nacional do Seguro Social (INSS). Entre agosto e setembro daquele ano, foram detectados acessos anômalos aos sistemas SISBEN (Sistema Corporativo de Benefícios) e BLH00 (sistema único de benefícios da Dataprev), resultando em um volume de consultas extraordinário: aproximadamente 90 milhões de acessos suspeitos no SISBEN e 9 milhões no BLH00, números muito superiores ao padrão dos meses anteriores (Oliveira; Silva, 2025).

Esses acessos indicavam a possibilidade concreta de extração massiva de dados de segurados, que abrangiam informações como: nome completo, número de CPF, NIT (Número de Identificação do Trabalhador), data de nascimento, filiação, sexo, categoria profissional, dados bancários, número de dependentes e vínculos previdenciários. Trata-se, portanto, de dados de alta sensibilidade, que, se utilizados de forma indevida, podem gerar fraudes financeiras, golpes direcionados a aposentados e pensionistas, além de violações graves à privacidade.

Segundo Oliveira e Silva (2025), "a extensão do incidente revelou não apenas uma vulnerabilidade técnica dos sistemas do INSS, mas uma falha estrutural de governança de dados, já que não havia mecanismos preventivos adequados para conter ou reduzir a gravidade do vazamento" (p. 9). Esse diagnóstico expõe um problema recorrente em órgãos públicos: a ausência de políticas sólidas de segurança da informação, associada à defasagem tecnológica e à falta de investimentos em cibersegurança.

Além dos aspectos técnicos, o episódio trouxe à tona outro ponto crítico: a resposta institucional do INSS. Apesar da magnitude do incidente, a autarquia demorou a notificar a Autoridade Nacional de Proteção de Dados (ANPD) e não conseguiu comunicar de forma clara os titulares de dados possivelmente afetados. O argumento utilizado pelo instituto foi o de "inviabilidade técnica" para identificar e notificar individualmente os milhões de segurados impactados. Contudo, tal justificativa não foi aceita pela ANPD, que entendeu que a omissão configurava descumprimento direto da LGPD, especialmente no que se refere ao princípio da transparência e ao dever de comunicação de incidentes de segurança.

A competência fiscalizadora da ANPD inclui a investigação de incidentes de segurança, como vazamentos de dados, e a imposição de sanções administrativas a empresas e órgãos públicos que não cumpram a legislação vigente. De acordo com a Autoridade Nacional de Proteção de Dados (Brasil, 2024, p. 13-14), um incidente de segurança com dados pessoais é definido como um evento adverso confirmado que comprometa a confidencialidade, a integridade ou a disponibilidade dos dados pessoais. Tais incidentes podem ser resultado de ações voluntárias ou acidentais, ocasionando a divulgação, alteração, perda ou acesso não autorizado a dados pessoais, independentemente do meio em que estes estejam armazenados.

Ainda que as decisões da ANPD sobre casos concretos envolvendo o tratamento de dados no setor previdenciário sejam limitadas, elas desempenham um papel crucial como precedentes fundamentais para a interpretação e aplicação da LGPD nesse contexto específico. Conforme destacado por Bioni et al. (2021), essas decisões são essenciais para estabelecer diretrizes claras sobre como a legislação deve ser aplicada ao tratamento de dados sensíveis no âmbito da previdência social. A partir dessas decisões, a ANPD contribui para a formação de uma jurisprudência adaptada às particularidades do setor, ajudando a equilibrar a proteção de dados pessoais com as necessidades operacionais

das instituições públicas, como o INSS, e garantindo a segurança e a conformidade com as normativas legais.

Essa postura gerou críticas na literatura especializada. Gonçalves, Salvador e Agostinho (2024) destacam que "o silêncio institucional em face de um incidente de tamanha proporção equivale à negação de direitos fundamentais, pois impede que os cidadãos afetados adotem medidas de autoproteção, como bloqueio de contas bancárias ou atualização de credenciais" (p. 221). Em outras palavras, ao não informar os segurados, o INSS não apenas descumpriu a lei, mas também fragilizou a autonomia dos indivíduos diante dos riscos decorrentes do vazamento.

Outro aspecto relevante foi a repercussão social do episódio. Notícias sobre o vazamento circularam amplamente na imprensa e nas redes sociais, gerando insegurança entre aposentados e pensionistas — muitos deles pertencentes a grupos vulneráveis, com baixa escolaridade ou acesso limitado a recursos digitais. Essa população ficou duplamente exposta: por um lado, à ameaça concreta de fraudes; por outro, à falta de informações institucionais que pudessem orientá-los.

De acordo com Oliveira e Silva (2025), "o caso do INSS foi paradigmático porque obrigou a ANPD a afirmar sua autoridade, aplicando sanções e estabelecendo parâmetros de atuação para futuros incidentes no setor público" (p. 12). Assim, o vazamento não pode ser visto apenas como falha, mas também como oportunidade para o amadurecimento do regime de proteção de dados no Brasil.

Em relação ao tema, Gonçalves, Salvador e Agostinho (2024) ressaltam que, ao identificar o vazamento de dados, o INSS deveria ter ativado imediatamente seu plano de resposta a incidentes. Isso inclui a identificação e contenção do vazamento, bem como uma análise detalhada das causas e consequências do ocorrido. Além disso, a LGPD exige que o controlador colabore com a ANPD durante todo o processo, fornecendo relatórios sobre o incidente e permitindo auditorias, quando necessário.

Em síntese, o incidente de 2022 revelou três dimensões críticas: (i) a fragilidade estrutural dos sistemas de informação do INSS; (ii) a insuficiência das respostas institucionais; e (iii) a necessidade de fortalecimento da governança de dados no setor público. Essas dimensões, quando analisadas conjuntamente, evidenciam que o desafio não é apenas técnico, mas também jurídico, político e cultural.

5 VAZAMENTO DE DADOS NO INSS: IMPLICAÇÕES E DESAFIOS

O vazamento de dados no âmbito do Instituto Nacional do Seguro Social (INSS) representa um dos maiores riscos à privacidade dos cidadãos brasileiros, considerando a dimensão e a natureza das informações que a autarquia detém. O órgão é responsável pela gestão de benefícios previdenciários e assistenciais, como aposentadorias, pensões e auxílios diversos, o que implica no tratamento de uma base de dados altamente sensível, composta por dados pessoais, patrimoniais, familiares, laborais e, em alguns casos, médicos. Assim, qualquer falha de segurança nesse contexto não apenas coloca em xeque a proteção da intimidade dos segurados, mas também expõe vulnerabilidades institucionais e jurídicas.

De acordo com Amaral (2021), incidentes de vazamento de dados no setor público têm efeito devastador sobre a confiança do cidadão no Estado, pois transmitem a

percepção de ineficiência e falta de preparo para lidar com os avanços tecnológicos que já estão consolidados em outras esferas sociais. Além disso, a fragilidade da segurança digital abre espaço para práticas criminosas, como fraudes, golpes e comercialização de dados no submundo digital (Amaral, 2021).

No caso do INSS, é possível imaginar que um simples vazamento de informações sobre aposentadorias ou benefícios assistenciais pode gerar consequências dramáticas para a vida de milhões de pessoas. Outro ponto que merece atenção é a responsabilidade jurídica da Administração Pública frente a tais vazamentos. A Lei Geral de Proteção de Dados (Lei nº 13.709/2018) prevê que o controlador — no caso, o INSS — é responsável por adotar medidas de segurança adequadas para proteger os dados pessoais dos cidadãos. Quando tais medidas se mostram insuficientes, surge o dever de responsabilização, que pode implicar não apenas em sanções administrativas pela Autoridade Nacional de Proteção de Dados (ANPD)

Do ponto de vista ético, a situação torna-se ainda mais delicada. O INSS lida predominantemente com dados de pessoas idosas e em situação de vulnerabilidade, grupo que, muitas vezes, possui menor domínio tecnológico e, portanto, menos condições de identificar ou reagir a possíveis golpes. Nesse cenário, o vazamento não se limita a um problema abstrato de segurança da informação, mas se converte em um ataque direto à dignidade da pessoa humana.

Diante desse cenário, os desafios são múltiplos. O INSS precisa modernizar suas estruturas de segurança digital, adotar protocolos de prevenção e resposta rápida a incidentes, capacitar servidores e promover uma cultura de proteção de dados. Paralelamente, é necessário que haja maior articulação entre a ANPD e os órgãos de controle interno e externo da Administração Pública, de modo a garantir transparência, fiscalização e responsabilização em casos de vazamento.

Portanto, os vazamentos de dados no INSS não devem ser compreendidos apenas como falhas técnicas, mas como reflexos de um problema estrutural que envolve gestão pública, responsabilidade legal, ética e proteção da cidadania em sua dimensão mais elementar: a confiança no Estado como guardião de informações sensíveis.

6 A IMPORTÂNCIA DA PROTEÇÃO DE DADOS PARA A CIDADANIA DIGITAL

A proteção de dados pessoais deixou de ser um tema restrito ao campo da tecnologia e passou a ocupar um lugar central no debate democrático, especialmente em sociedades cada vez mais conectadas. No Brasil, o reconhecimento do direito fundamental à proteção de dados, previsto pela Emenda Constitucional nº 115/2022, reforça a relevância do tema como condição necessária para o exercício pleno da cidadania digital. No contexto do INSS, tal proteção adquire contornos ainda mais significativos, já que se trata de um órgão que concentra informações de milhões de brasileiros, em sua maioria idosos e em condição de vulnerabilidade social.

A cidadania digital pressupõe não apenas o acesso às ferramentas tecnológicas, mas também a existência de mecanismos que assegurem confiança na relação entre indivíduo e Estado. Quando um segurado do INSS compartilha seus dados, espera que o governo atue como guardião dessas informações, garantindo que elas não sejam manipuladas de forma abusiva ou expostas indevidamente. Como apontam Gomes e

Vieira (2020), a confiança digital é um dos pilares da governança pública contemporânea, sendo fator determinante para a legitimidade das instituições (Gomes; Vieira, 2020).

Nesse cenário, o papel do INSS transcende a simples administração de benefícios. Sua responsabilidade na proteção dos dados dos segurados é também um compromisso democrático, na medida em que fortalece a relação de confiança entre Estado e cidadão. O vazamento de informações não é apenas uma falha técnica, mas um atentado à própria cidadania, capaz de fragilizar direitos e expor a população a riscos sociais, econômicos e psicológicos.

Portanto, a proteção de dados no âmbito do INSS deve ser vista como um alicerce da cidadania digital, garantindo não apenas segurança, mas também dignidade, confiança e participação efetiva no espaço público digital. A construção de uma sociedade digital justa e democrática passa, inevitavelmente, pela consolidação de políticas sólidas de proteção de dados pessoais.

7 RESULTADOS E DISCUSSÃO

Os resultados da pesquisa evidenciaram três dimensões centrais no caso do vazamento de dados do INSS em 2022: a vulnerabilidade técnica dos sistemas, a insuficiência das respostas institucionais e a necessidade de fortalecimento da governança de dados no setor público. Essas dimensões foram analisadas à luz da LGPD, da literatura científica e da atuação da ANPD, permitindo uma visão abrangente do fenômeno.

Em primeiro lugar, constatou-se que o incidente expôs fragilidades estruturais dos sistemas de informação utilizados pelo INSS. O elevado número de acessos anômalos aos sistemas SISBEN e BLH00, sem detecção e contenção imediata, revelou ausência de mecanismos preventivos adequados. Essa constatação confirma diagnósticos anteriores presentes na literatura (Amaral, 2021; Oliveira; Silva, 2025), que apontam a defasagem tecnológica e a carência de investimentos em segurança da informação no setor público.

Além disso, a análise mostrou que a resposta institucional do INSS não foi proporcional à gravidade do incidente. A demora na comunicação à ANPD e a ausência de notificações claras aos segurados afetados configuraram descumprimento do princípio da transparência previsto na LGPD. Esse aspecto foi especialmente criticado por Gonçalves, Salvador e Agostinho (2024), para quem o silêncio institucional equivale à negação de direitos fundamentais, pois impede que os cidadãos adotem medidas de autoproteção. A postura do INSS, ao alegar “inviabilidade técnica” para comunicar os titulares, fragilizou ainda mais a confiança social no órgão.

A atuação da ANPD mostrou-se decisiva para a consolidação do regime de proteção de dados no Brasil. Embora ainda incipiente em termos de jurisprudência administrativa, a Autoridade estabeleceu parâmetros importantes ao exigir transparência e responsabilização do INSS. Nesse sentido, corroborando Bioni et al. (2021), os precedentes da ANPD tendem a exercer papel normativo relevante, orientando futuras decisões sobre incidentes de dados no setor público.

A discussão também revelou que o vazamento afetou de maneira desproporcional segurados em situação de vulnerabilidade, como idosos e pessoas com baixa escolaridade, ampliando riscos de golpes e fraudes financeiras. Essa constatação dialoga com Pinheiro

(2023), que alerta para a necessidade de medidas reforçadas de proteção quando os dados envolvem grupos vulneráveis. Assim, o episódio não se limitou a um problema técnico de cibersegurança, mas configurou uma ameaça direta à cidadania digital e à dignidade da pessoa humana.

Por fim, a análise evidenciou que a proteção de dados no INSS transcende a dimensão normativa da LGPD e se projeta como condição essencial para a confiança social e a legitimidade institucional. Conforme destacam Gomes e Vieira (2020), a confiança digital é elemento central da governança pública contemporânea. Nesse contexto, o cumprimento efetivo da LGPD pelo INSS não deve ser compreendido apenas como exigência legal, mas como compromisso democrático na preservação da privacidade, da dignidade e da cidadania dos segurados.

8 CONCLUSÃO

O estudo realizado permitiu uma análise aprofundada dos desafios e implicações da proteção e do vazamento de dados no Instituto Nacional do Seguro Social (INSS), à luz da Lei Geral de Proteção de Dados Pessoais (LGPD). A investigação demonstrou que o episódio de 2022 não representou apenas uma falha técnica de segurança da informação, mas um marco que evidenciou fragilidades institucionais, jurídicas e sociais na gestão de dados previdenciários no Brasil.

Os resultados mostraram que a vulnerabilidade dos sistemas de informação do INSS está diretamente relacionada à falta de investimentos consistentes em infraestrutura tecnológica e à ausência de mecanismos preventivos robustos de cibersegurança.

Outro ponto crítico identificado foi a insuficiência da resposta institucional. A demora do INSS em comunicar a Autoridade Nacional de Proteção de Dados (ANPD) e a ausência de notificações transparentes aos titulares afetados configuraram violação direta ao princípio da transparência e ao direito fundamental à informação. Tal postura fragilizou a confiança social no órgão e ampliou a exposição de segurados a riscos concretos, como fraudes financeiras e golpes direcionados, especialmente em grupos vulneráveis, como idosos. A alegação de “inviabilidade técnica” para proceder à comunicação revelou não apenas a falta de preparo organizacional, mas também a carência de protocolos claros de resposta a incidentes de segurança.

Nesse cenário, a atuação da ANPD assumiu relevância central. Embora a autoridade ainda se encontre em processo de consolidação institucional, sua intervenção no caso do INSS reforçou a importância de se estabelecer precedentes administrativos capazes de orientar a aplicação da LGPD no setor público. Ao exigir medidas corretivas e responsabilização, a ANPD contribuiu para fortalecer o regime jurídico da proteção de dados no Brasil, ainda que as limitações estruturais do Estado dificultem a imposição de sanções mais severas.

A pesquisa também demonstrou que a proteção de dados pessoais no âmbito previdenciário transcende a esfera normativa. Trata-se de um elemento estruturante da confiança social e da própria cidadania digital. O INSS, enquanto depositário de informações sensíveis de milhões de brasileiros, não pode ser compreendido apenas como um agente administrativo, mas como guardião de trajetórias de vida, cuja preservação se relaciona diretamente à dignidade da pessoa humana. Nesse sentido,

a efetividade da LGPD não se resume a evitar sanções legais, mas implica garantir a segurança, a confiança e a participação dos cidadãos em um ambiente digital protegido.

Diante desse panorama, três recomendações centrais emergem da análise: (i) a necessidade urgente de investimentos em infraestrutura tecnológica e protocolos de prevenção e resposta a incidentes de segurança; (ii) a criação de uma cultura organizacional no INSS voltada à proteção de dados, com capacitação contínua de servidores e adoção de mecanismos de governança digital; e (iii) o fortalecimento da articulação entre a ANPD, o INSS e os órgãos de controle, de modo a garantir fiscalização efetiva, responsabilização e transparência em casos de vazamento de dados.

Além disso, o caso do INSS trouxe à tona a importância de se reconhecer que a proteção de dados não pode ser vista como mera exigência burocrática, mas como pilar democrático. O vazamento de 2022 demonstrou que falhas na proteção de dados não afetam apenas a esfera individual, mas repercutem coletivamente, comprometendo a confiança no Estado e expondo a população a riscos sociais e econômicos significativos. A construção de uma cidadania digital sólida, amparada pela confiança mútua entre cidadãos e instituições, depende do fortalecimento contínuo das práticas de proteção de dados no setor público.

Em síntese, o caso analisado revelou que os desafios da proteção de dados no Brasil vão além das limitações técnicas e jurídicas, envolvendo também dimensões culturais, políticas e éticas. O episódio de 2022 no INSS, ainda que marcado por falhas, representou um ponto de inflexão importante para o amadurecimento do regime de proteção de dados no país, ao evidenciar a urgência de medidas mais eficazes e a necessidade de consolidação da ANPD como órgão regulador e fiscalizador.

Portanto, a proteção de dados no âmbito previdenciário deve ser compreendida como um compromisso constitucional e democrático, indispensável para a preservação da dignidade da pessoa humana e para a consolidação da cidadania digital no Brasil. O episódio do INSS mostrou que ainda há um longo caminho a percorrer, mas também abriu espaço para avanços significativos na governança pública da informação.

REFERÊNCIAS

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**: seção 1, Brasília, DF, ano 155, n. 157, p. 59, 15 ago. 2018.

BRASIL. Ministério da Justiça e Segurança Pública. Autoridade Nacional de Proteção de Dados. **Guia de Resposta a Incidentes de Segurança. Programa de Privacidade e Segurança da Informação** (PPSI), versão 3.3, Brasília, DF: ANPD, 2024.

BIONI, B. R.; DIAS, Daniel; SCHERTEL MENDES, Laura; RIBEIRO, Márcio Moretto; LUCIANO, Maria; RIELLI, Mariana Marques; KITAYAMA, Marina; MARTINS, Pedro; ZANATTA, Rafael A.; MONTEIRO, Renato Leite. **Proteção de dados**: contexto, narrativas e elementos fundantes. Organização Bruno Ricardo Bioni. São Paulo: B. R. Bioni Sociedade Individual de Advocacia, 2021.

GONÇALVES, Gilmara Valéria; SALVADOR, Sergio Henrique; AGOSTINHO, Theodoro Vicente. INSS e a indenização por vazamento de dados sob a perspectiva da LGPD e os desafios de aprimoramento da proteção constitucional previdenciária. **Revista de Direito do Trabalho e Seguridade Social**, São Paulo, n. 236, jul./ago. 2024, p. 215-227. Disponível em: https://dspace.almg.gov.br/handle/11037/56518. Acesso em: 13 set. 2025.

OLIVEIRA, Gislaine Ferreira; SILVA, Rosane Leal da. A atuação da ANPD no caso do vazamento de dados do INSS em 2022: garantindo a proteção dos direitos fundamentais em tempos de crise. **Revista de Direito, Governança e Novas Tecnologias**, Florianópolis, v. 10, n. 2, 2025. Disponível em: https://www.indexlaw.org/index.php/revistadgnt/article/view/11002. Acesso em: 13 set. 2025.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais**: comentários à Lei nº 13.709/2018 (LGPD). 4. ed. São Paulo: Saraivajur, 2023.

RODRIGUES, Horácio Wanderlei; GRUBBA, Leilane Serratine. **Pesquisa jurídica aplicada**. Florianópolis: Habitus Editora, 2023.

Histórico
Recebido em: 28 set. 2025. **Aprovado em**: 27 abr. 2026. **Publicado em**: 08 jun. 2026.