Revista de Direito, Governança e Novas Tecnologias

Organização Comitê Científico
Double Blind Review pelo SEER/OJS
Recebido em: 15.02.2025
Aprovado em: 16.02.2025

A ATUAÇÃO DA ANPD NO CASO DO VAZAMENTO DE DADOS DO INSS EM 2022: garantindo a proteção dos direitos fundamentais em tempos de crise

Gislaine Ferreira Oliveira*

Rosane Leal da Silva**

RESUMO

A proteção de dados pessoais é um direito fundamental essencial para garantir a privacidade e segurança dos indivíduos, e o vazamento de dados sensíveis pode causar prejuízos significativos. Nesse contexto, a Autoridade Nacional de Proteção de Dados (ANPD) desempenha um papel crucial ao regulamentar, fiscalizar e sancionar práticas relacionadas ao tratamento de dados. O presente trabalho tem como objetivo analisar a legalidade da atuação da ANPD e a garantia de transparência e proteção dos direitos dos titulares no incidente de segurança do INSS, em 2022, à luz da LGPD. Além de verificar a conformidade das medidas adotadas pela ANPD, como auditorias, recomendações e sanções, com as atribuições legais. Para a execução da pesquisa utiliza-se o método de abordagem indutivo, que examina o caso de vazamento de dados do INSS em 2022 para avaliar a conformidade das medidas adotadas pela ANPD, como auditorias, recomendações e sanções, com suas atribuições legais, aliado ao método de procedimento monográfico e técnicas de pesquisa bibliográfica, documental e estudo de caso. A conclusão mostra que, apesar de sua estrutura ainda em desenvolvimento, nessa quinta decisão da ANPD em incidente de segurança de dados agiu, de forma geral, efetivamente para fiscalizar e sancionar o INSS, demonstrando a importância de sua função na aplicação da LGPD e na proteção dos direitos dos titulares em situações de crise.

Palavras-chaves: Autoridade Nacional de Proteção de Dados; Dados pessoais; Incidente de Segurança; Instituto Nacional de Seguro Social; Vazamento de dados.

THE ANPD's RESPONSE TO THE INSS DATA BREACH IN 2022: ensuring the protection of fundamental rights in times of crisis

ABSTRACT

The protection of personal data is a fundamental right essential for ensuring the privacy and security of individuals, and the leakage of sensitive data can cause significant harm. In this context, the National Data Protection Authority (ANPD) plays a crucial role in regulating, supervising, and sanctioning practices related to data processing. This work aims to analyze the legality of the ANPD's actions and the guarantee of transparency and protection of data subjects'

* Doutoranda em Ciências Sociais pela Universidade Federal de Santa Maria (UFSM), mestre e graduada em Direito pela UFSM. Professora da Universidade Franciscana e da UFSM. Pesquisadora no Núcleo de Direito Informacional (NUDI). E-mail: gislainefoliveira7@gmail.com.

** Doutora em Direito. Professora na Graduação e Mestrado em Direito da Universidade Federal de Santa Maria. Professora da Universidade Franciscana. Coordenadora do Núcleo de Direito Informacional (NUDI). E-mail: rolealdasilva@gmail.com.

rights in the INSS security incident in 2022, in light of the LGPD. It also seeks to assess the compliance of the measures adopted by the ANPD, such as audits, recommendations, and sanctions, with its legal duties. The research employs an inductive approach, examining the INSS data breach case in 2022 to evaluate the compliance of the measures adopted by the ANPD, such as audits, recommendations, and sanctions, with its legal attributions, combined with the monographic method and techniques of bibliographic and documentary research, as well as case study. The conclusion shows that, despite its still-developing structure, in this fifth decision on a data security incident, the ANPD generally acted effectively to supervise and sanction the INSS, demonstrating the importance of its role in enforcing the LGPD and protecting data subjects' rights in crisis situations.

Keyword: National Data Protection Authority; Personal data; Security incident; National Institute of Social Security; Data breach.

1 INTRODUÇÃO

No Brasil, o Instituto Nacional de Seguro Social (INSS) atua como controlador de dados pessoais, uma vez que decide sobre a coleta, armazenamento, processamento e compartilhamento de dados pessoais dos segurados e beneficiários. Por isso, a referida autarquia federal é responsável por adotar medidas técnicas e administrativas pertinentes para proteger os dados pessoais contra acessos não autorizados, vazamentos ou outras maneiras de tratamento indevido ou ilegal.

No período de agosto e setembro de 2022, houve um incidente de segurança em que expôs dados pessoais sensíveis. Tais informações podem ser utilizadas, de forma indevida, para fraudes e roubo de identidade.

Apesar de o INSS ter comunicado a Autoridade Nacional de Proteção de Dados (ANPD) sobre o incidente, posteriormente verificou-se uma resistência por parte do órgão federal em informar os titulares dos dados afetados pela falha na segurança, violando o art. 48 da Lei Geral de Proteção de Dados Pessoais (LGPD). Assim, em 2024, é proferida a quinta decisão em processos sancionadores da ANPD, em que condena o INSS à sanção de publicização da infração ao INSS, seja a partir de publicação de comunicado na página do *site* oficial e pelo envio de mensagem a todos os usuários do aplicativo Meu INSS, além de multa e obrigações de proteção da base de dados.

Nesse contexto, o presente trabalho questiona: a atuação da ANPD no incidente de segurança envolvendo o INSS, em 2022, foi realizada em conformidade com as disposições legais estabelecidas pela LGPD? Ainda, quais são as competências da ANPD em relação à

investigação e fiscalização de incidentes de segurança de acordo com a LGPD, e como essas competências foram executadas no caso em exame?

A pesquisa tem como objetivo analisar a legalidade da atuação da ANPD e a garantia de transparência e proteção dos direitos dos titulares no incidente de segurança do INSS, em 2022, à luz da LGPD. Além de verificar a conformidade das medidas adotadas pela ANPD, como auditorias, recomendações e sanções, com as atribuições legais.

Para a execução da presente pesquisa utilizou-se o método de abordagem indutivo, em que a partir do caso particular do incidente de segurança do INSS, em 2022, e o processo sancionador de competência da ANPD foi possível avaliar como a atuação da ANPD cumpre a função de fiscalização, regulamentação e implementação da LGPD. Como método de procedimento elegeu-se o monográfico, aliado às técnicas de pesquisa bibliográfica, análise documental das publicações da ANPD e o estudo de caso do referido incidente.

Portanto, sem o intuito de esgotar o tema, dividiu-se o presente trabalho em duas partes. No primeiro capítulo apresentar-se-á o incidente de segurança que ocorreu no INSS em 2022, com o processo de incidente de segurança. Enquanto que no segundo capítulo expor-se-á os principais aspectos doutrinários e legais da LGPD sobre o processo sancionador e a atuação da ANPD.

2 O INCIDENTE DE SEGURANÇA DE DADOS PESSOAIS E A AUTUAÇÃO DO INSS

O Sistema Corporativo de Benefícios do INSS (SISBEN) sofreu um incidente de segurança, conforme comunicado à ANPD. O fato teria acontecido em razão de acessos não autorizados, realizados no sistema, pois segundo informado na Comunicação Preliminar, em agosto e setembro de 2022, registraram-se mais de 90 milhões de consultas ao sistema corporativo de benefícios do INSS (SISBEN) e 9 milhões de consultas ao sistema único de benefícios DATAPREV (BLH00), o triplo de acessos, se comparado os meses anteriores.

Esses ingressos indevidos no sistema teriam afetado a base de beneficiários e segurados do INSS, permitindo que pessoas não autorizadas tivessem contato com dados pessoais tais quais nome, CPF, NIT identidade, data de nascimento, sexo, área da atividade profissional, dados bancários e dados sobre a quantidade de dependentes. Conforme informado na comunicação preliminar realizada à ANPD, “o incidente de segurança pode acarretar risco ou

dano relevante aos titulares" (Brasil, 2023, p. 9), incluindo informações sobre pessoas vulneráveis, dentre elas crianças, idosos e pessoas com deficiência.

Ademais, os dados objeto do incidente de segurança também são considerados sensíveis, de acordo com o art. 5º, inciso II, da LGPD, posto que informações referentes à saúde, à vida sexual, dados genético ou biometria associados a uma pessoa identificada ou identificável, os quais podem gerar danos mais graves ao seu titular, que pode se tornar alvo de discriminação (Brasil, 2018).

Cabe ressaltar que o INSS atua como controlador, ou seja, detém o controle do tratamento de dados pessoais, também os repassando ao DATAPREV, operadora do Sistema Corporativo de Benefícios do INSS (SISBEN). Este último agente de tratamento configura-se como pessoa jurídica de direito privado, vinculado ao Ministério da Gestão e Inovação em Serviços Públicos, que realiza o tratamento de dados pessoais em nome do controlador, que é o INSS. Foi na condição de controlador que o INSS fez a comunicação preliminar do incidente, realizada em 19 de outubro de 2022, atendendo ao disposto no Art. 48[1] da Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais - (LGPD) (Brasil, 2024a, p. 3).

O INSS fez a comunicação preliminar e, no dia 3 de novembro de 2022, a Coordenação Geral de Fiscalização, da Autoridade Nacional de Proteção de Dados, notificou eletronicamente o órgão, por meio de e-mail, para que complementasse a comunicação, num prazo de até 30 dias corridos da comunicação preliminar. Conforme o Processo Administrativo Sancionador nº 00261.001888/2023-21, o órgão informou à ANPD que iria complementar a Comunicação Preliminar, enviando os documentos indicativos das providências adotadas desde que constatou o incidente de segurança.

Todavia, ainda que notificado e tendo oferecido esta resposta, o prazo decorreu sem que o agente de tratamento complementasse a documentação. Em 22 de novembro, diante da reiteração feita pelo órgão fiscalizador, foram concedidos cinco dias úteis para resposta do controlador (Brasil, 2024a, p. 3-4).

O descumprimento reiterado, por parte do INSS, das determinações da Coordenação Geral de Fiscalização conduziu à expedição do Aviso nº 33/2022/CGF/ANPD, o que foi feito em 29 de dezembro de 2022, com a autuação daquele agente de tratamento. Nesta ocasião, foi instado, formalmente, a prestar esclarecimentos, na condição de controlador dos dados pessoais,

[1] O art. 48 da LGPD (Brasil, 2018) dispõe: "O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares".

preenchendo o formulário de incidente com informações complementares, o que deveria ser acompanhado do relatório técnico de tratamento do incidente e da comunicação, aos titulares dos dados, da ocorrência do incidente e da consequente violação dos dados pessoais (Brasil, 2024a, p.4).

Nessa ocasião houve atendimento parcial, por parte do agente autuado, que em 30 de dezembro de 2022 apresentou o formulário de comunicação de incidente de segurança complementar. No entanto, não realizou a comunicação do incidente aos titulares de dados pessoais, sob alegação de "estar analisando a legitimidade dos acessos suspeitos" (2023, p. 3). Informou a realização de medidas de contenção e reiterou não saber, especificamente, quem eram os atingidos e quais dados tinham sido violados. Ocorre que, conforme o disposto no art. 48 da Lei Geral de Proteção de Dados, os incidentes de segurança devem ser comunicados aos titulares de dados pessoais, o que o agente controlador se recusava a fazer.

Considerando a resistência do órgão, em 9 de abril de 2023, foi fixado ao controlador o prazo de 10 dias úteis, para que informasse os titulares de dados envolvidos no incidente de segurança, juntando estas comprovações ao processo de apuração. Esta comunicação de incidente não foi feita pelo INSS, que alegou impossibilidade técnica para levantar os nomes dos segurados, arguindo que era uma medida desproporcional fazer a comunicação universal além de postular a prorrogação do prazo para cumprimento das demais medidas. (Brasil, 2024a, p. 4)

Em 23 de junho de 2023, a ANPD expediu o Aviso nº 33, no qual comunicou o agente controlador sobre a instauração do Processo Administrativo Sancionador, com Auto de Infração datado de 3 de agosto de 2023. O agente controlador foi autuado em razão de ausência de comunicação de incidente de segurança aos titulares, conforme determina o Art. 48 da LGPD e falta de atendimento de medida preventiva, conforme Art. 32, § 2º, do Regulamento de Fiscalização. (Brasil, 2024a, p. 5). Com esta autuação o agente controlador teve o prazo de 10 dias úteis, para apresentar sua defesa à Coordenação Geral de Fiscalização da ANPD, o que deveria ser feito via sistema SEI.

Segundo consta no Relatório de Instrução 1/2024/ANPD, o INSS argumentou, em sua defesa, que a comunicação do incidente de segurança aos titulares dos dados deve ficar a critério e ao juízo de pertinência da autoridade pública, que deve realizar a análise do interesse do Estado, critério a ser sopesado em caso de comunicações. Nessa linha argumentativa, o agente controlador sustentou que o interesse público deveria prevalecer sobre os interesses individuais

e que, neste juízo de análise, o INSS entendeu que não era pertinente a comunicação. Ademais, sustentou que a comunicação individual aos titulares, além de ser impossível, geraria uma espécie de "pânico social", pois milhões de pessoas passariam a fazer contato com o INSS para saber se seus dados foram violados e passariam a desconfiar do sistema. Segundo o órgão, a comunicação não protegeria os segurados e beneficiários e levaria o sistema de atendimento a um caos. Logo, além de não ser eficiente e gerar tumulto injustificado ao sistema de atendimento, tal medida não atenderia a supremacia do interesse público, resultando em uma medida irrazoável (Brasil, 2024a, p.10-11).

Em acréscimo, o INSS sustentou que, segundo o disposto no Decreto nº 10.748/2021, as informações sobre incidentes cibernéticos são imprescindíveis à segurança da sociedade e do Estado e estariam protegidas como informações sigilosas, o que impediria a sua notificação ao público, normativa que estava em clara antinomia ao disposto no Art. 48 da LGPD.

A ANPD, por seu órgão fiscalizadores sancionador, não acolheu os argumentos do Instituto Nacional de Seguro Social por entender que houve infração ao Art. 48, da LGPD, segundo qual deve haver a comunicação aos destinatários de direitos quando houver um incidente de segurança que seja qualificado, ou seja, com gravidade em razão do número de pessoas envolvidas e da qualidade dos dados acessados indevidamente. Portanto, a comunicação se faz necessária quando o incidente tiver potencial de produzir danos aos direitos dos indivíduos afetados (Brasil, 2024a, p. 13).

Segundo justificado pela ANPD, a comunicação do incidente aos seus titulares permite que eles adotem medidas mitigadoras dos danos, o que exige rapidez, pois os danos se ampliam e aprofundam à medida que o tempo passa, motivo pelo qual os controladores não devem procrastinar na realização dos procedimentos que são determinados na LGPD. Ademais, ainda que o Art. 48, §1º não imponha um prazo específico para atendimento e comunicação aos titulares, menciona que os procedimentos devem ocorrer em "prazo razoável" (Brasil, 2024a, p. 14).

A decisão da ANPD também contrastou os interesses sociais e públicos com os interesses e direitos individuais dos titulares de dados pessoais e a conclusão apontou pelo dever de cientificar os envolvidos, cujos dados pessoais integravam o banco de dados indevidamente acessado. Para tanto, foi levado em conta o interesse público primário, ou seja, que é a razão de ser e de atuar do próprio Estado, cuja atuação deve visar o atendimento e o bem-estar da

sociedade. Assim, a administração pública não estava, por um anterior deslize na segurança do banco de dados, autorizada a cometer novos equívocos (Brasil, 2024a, p. 20)

Uma vez determinada a responsabilidade do INSS pelo incidente, sobretudo, pela recusa reiterada em cumprir as determinações da RIPD, comunicando os titulares envolvidos, a decisão foi no sentido de aplicar as penalidades, de acordo com o seu nível e os direitos das pessoas afetadas. Entendeu-se que a infração no caso do INSS era de médio porte, em razão do amplo alcance, atingindo titulares de dados pessoais, seus dependentes, abarcando dados sensíveis e de pessoas em condição de vulnerabilidade, tais como idosos, crianças, adolescentes, pessoas com deficiência e segurados em geral (Brasil, 2024a, p. 28).

A aplicação dos critérios de dosimetria conduziu a uma penalidade mais grave do que a mera advertência em razão da natureza grave das infrações, da larga escala e da natureza dos dados, incluindo dados pessoais sensíveis, envolvidos no incidente. Diante da impossibilidade de aplicação das outras sanções previstas no Art. 52 da LGPD, o órgão encarregado pela fiscalização e aplicação dos procedimentos sancionadores entendeu que a medida adequada seria a publicização da infração, após devidamente apurada e confirmada sua ocorrência, sanção descrita no inciso IV, Art. 52 da LGPD. Para tanto, a ANPD sugeriu inclusive o texto a ser publicado nos meios de comunicação, para dar ciência do incidente de segurança aos titulares de dados pessoais (Brasil, 2024a, p. 31-32).

Insta mencionar que os problemas derivados da segurança do banco de dados do INSS e com os acessos desautorizados não se constituem em fatos isolados, pois são frequentes a veiculação de notícias de segurados que reclamam do assédio por parte de fornecedores, dentre eles agentes financeiros e seus representantes. Em alguns casos, os segurados são contactados pelos representantes dos bancos, antes mesmo de receber a comunicação oficial da concessão do benefício.

Tal situação foi objeto de análise na Nota Técnica no 2/2024/FIS/CGF/ANPD (Brasil, 2024b). Publicada a partir de uma fiscalização instaurada para investigar o tratamento de dados pessoais de beneficiários do INSS por instituições financeiras e correspondentes bancários para a oferta de serviços de crédito, como por exemplo de empréstimos consignados.

A referida fiscalização foi motivada por reclamações recebidas pela ANPD, no período de janeiro de 2021 a outubro de 2023, que abordaram casos de “contrato não solicitado”, “dificuldade em exercer o direito de eliminação de dados, “compartilhamento indevido de dados pessoais, inclusive dados sensíveis” e “acesso indevido de dados pessoais” (Brasil,

2024b, p. 2). Sendo o Banco Itaú e o Banco Pan os que receberam mais reclamações, nas posições subsequentes ocupadas pelos Banco Santander e Banco Bradesco.

Muitos beneficiários relataram ter recebido contatos não solicitados para oferta de crédito, antes mesmo de serem notificados acerca da concessão do benefício pelo INSS. Os contatos eram realizados via ligação telefônica, SMS ou mensagens pelo aplicativo WhatsApp, já contendo dados pessoais como nome, CPF, número e valor do benefício. Para fundamentar, os beneficiários apresentaram capturas de tela de conversas, histórico de ligações e mensagens SMS (Brasil, 2024b, p. 2).

Em 19/08/2022, a ANPD expediu o Ofício 1 (3568002) ao INSS requerendo informações sobre o fluxo de dados pessoais para solicitação e pagamento de benefício ao INSS e para aquisição de empréstimo consignado, além de Relatórios de Impacto à Proteção de Dados Pessoais (RIPD) eventualmente realizados. Na data de 11/10/2022, o INSS informou que os dados dos beneficiários são compartilhados com as Instituições Financeiras, apenas após a concessão do benefício e com autorização explícita do titular, através de um termo de autorização. Ainda, alegou que não compartilha dados pessoais que possam ser utilizados para assédio ou contato direto (Brasil, 2024b, p. 3).

Algumas instituições financeiras asseguraram que seguem as normas do INSS para acesso aos dados e realizam o tratamento de dados com base no consentimento dos titulares ou no interesse legítimo. Algumas também utilizaram correspondentes bancários para a oferta dos serviços.

No RIPD, o INSS identificou riscos de compartilhamento indevido de dados e propôs medidas de mitigação, incluindo a definição de políticas de gestão de compartilhamento, monitoramento do compartilhamento de dados pessoais, conscientização dos agentes públicos e implementação de medidas de contingência (Brasil, 2024b, p. 3). Por fim, a ANPD concluiu que o INSS, em tese, não compartilhava dados pessoais para oferta ativa de crédito. No entanto, as medidas adotadas pelo INSS mostraram-se insuficientes, pois os beneficiários continuavam a receber ofertas de crédito mesmo antes de receberem a Carta de Concessão.

Dessa forma, o tratamento de dados pessoais realizado para viabilizar a oferta ativa de crédito foi considerado inadequado. Além disso, há indícios de falhas no cumprimento das

determinações de proteção de dados pessoais, tanto por parte do INSS quanto das instituições financeiras e seus correspondentes bancários.

3 ATUAÇÃO DA ANPD: AS MEDIDAS ADOTADAS NO INCIDENTE DE SEGURANÇA DO INSS EM (DES)CONFORMIDADE COM A LEGISLAÇÃO VIGENTE

Diante dos fatos apresentados no capítulo anterior, destaca-se que a Autoridade Nacional de Proteção de Dados (ANPD) é o órgão responsável pela fiscalização, regulamentação e implementação da Lei Geral de Proteção de Dados Pessoais (LGPD). Assim, a atuação da ANPD é essencial para garantir que as determinações da LGPD sejam respeitadas por todas as instituições, públicas e privadas, que processam e armazenam dados pessoais no país.

A ANPD foi instituída pela Lei nº 13.853 de 2019, que alterou a LGPD e foi regulamentada pelo Decreto nº 10.474 de 2020. Todavia, inicialmente, o Projeto de Lei nº 5.276 de 2016 (Brasil, 2016) não apresentava a criação de uma entidade responsável pela fiscalização e implementação, sendo sua previsão como autoridade federal em regime especial vinculada à Administração indireta decisão posterior em relatório técnico da Comissão da Câmara dos Deputados (Rodriguez, 2021).

Assim, após algumas mudanças legislativas, a partir do Decreto nº 11.348 de 2023 (Brasil, 2023b), a ANPD está vinculada à estrutura organizacional do Ministério da Justiça e Segurança Pública, porém com autonomia administrativa e financeira, conforme previsto no art. 55-A, da LGPD (Brasil, 2018). Conforme destacam Sarlet e Rodriguez (2022, p. 230), "[...] a independência necessária às autoridades reguladoras de proteção de dados não deriva exclusivamente de sua formal separação da administração direta, senão de uma complexa estruturação que permita o seu livre proceder, infenso às influências políticas".

A criação da ANPD foi inspirada em regulamentos internacionais, em especial o GDPR (General Data Protection Regulation) da União Europeia implementado em 2018, que é amplamente reconhecido como um novo padrão global para proteção de dados. Ressalta-se que a União Europeia é precursora na proteção de dados pessoais, sendo que desde 1995 adotou a Diretiva de Proteção de Dados (Diretiva 95/46/CE), que estabeleceu princípios fundamentais

para a proteção de dados pessoais e a livre circulação desses dados entre os Estados-membros, sendo uma das primeiras tentativas globais de proteção de dados pessoais.

Na União Europeia, não existe um único órgão equivalente à ANPD do Brasil[2]. Em vez disso, cada país membro da União Europeia tem sua própria autoridade de proteção de dados, que é responsável pela supervisão da aplicação do Regulamento Geral de Proteção de Dados em seu território, sendo conhecidas como Autoridades de Proteção de Dados (Data Protection Authorities - DPAs) (Lorenzon, 2021, p. 45).

O Decreto regulamentador da ANPD estabeleceu a sua estrutura regimental e as suas atribuições, para concretizar o objetivo de zelar pela proteção dos dados pessoais e pela privacidade dos indivíduos. A estrutura da ANPD é composta por órgãos que incluem o Conselho Diretor, o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, órgãos de assistência direta ao Conselho Diretor e órgãos seccionais como a Corregedoria, a Ouvidoria, entre outros e órgãos específicos singulares (Brasil, 2020).

O Conselho Diretor é o órgão máximo da ANPD, composto por um diretor-presidente e quatro diretores, todos nomeados pelo Presidente da República, após aprovação pelo Senado Federal. Os mandatos são não coincidentes e têm duração de quatro anos, conforme estabelece a LGPD em seu art. 55-D (Brasil, 2018). O presidente da autoridade, atualmente, é o coronel Waldemar Ortunho, nomeado pelo presidente Bolsonaro, e tem mandato até novembro de 2026.

Quanto à competência da ANPD, estão elencadas no art. 55-J da LGPD[3] (Brasil, 2018). Em que se subdivide em competências normativa e deliberativa, fiscalizatória e sancionatória.

[2] De acordo com o art. 51 da GDPR (União Europeia, 2016), as autoridades de controle são independentes, sendo assegurado no item 1 "Os Estados-Membros estabelecem que cabe a uma ou mais autoridades públicas independentes a responsabilidade pela fiscalização da aplicação do presente regulamento, a fim de defender os direitos e liberdades fundamentais das pessoas singulares relativamente ao tratamento e facilitar a livre circulação desses dados na União («autoridade de controlo»)".

[3] Dispõe o art. 55-J da LGPD (Brasil, 2018): "Compete à ANPD: I - zelar pela proteção dos dados pessoais, nos termos da legislação; II - zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º desta Lei; III - elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade; IV - fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso; V - apreciar petições de titular contra controlador após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação; VI - promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança; VII - promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade; VIII - estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis; IX - promover ações de cooperação com autoridades de proteção de dados pessoais de

O poder regulamentar se concretiza a partir da elaboração de guias e recomendações, orientações e procedimentos e até proposições normativas, nos termos da LGPD.

Nessa seara, por exemplo, a ANPD publicou um fascículo de forma didática e ilustrativa, direcionada à população em geral, em parceria com o Cert.Br, Nic.br e CGI.br, sobre vazamento de dados (Brasil, 2024c). No documento, há orientações práticas de como reduzir impactos causados pelo vazamento de dados, a partir de uma atuação rápida e certeira.

O Instituto Nacional do Seguro Social (INSS) alegou que a não divulgação de informações sobre o vazamento de dados pessoais de seus beneficiários teve como objetivo evitar o pânico social. No entanto, uma estratégia mais eficaz para lidar com essa questão seria promover a literacia digital, educando a população sobre os riscos associados ao vazamento de dados e instruindo-a sobre como proceder em tais situações, conforme conteúdo da cartilha em comento.

Ensinar as pessoas a reconhecerem sinais de possíveis fraudes e a adotarem medidas preventivas, como a verificação regular de suas contas e a alteração de senhas, pode minimizar os danos causados por vazamentos de dados. Além disso, uma população bem-informada e

outros países, de natureza internacional ou transnacional; X - dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, respeitados os segredos comercial e industrial; XI - solicitar, a qualquer momento, às entidades do poder público que realizem operações de tratamento de dados pessoais informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento desta Lei; XII - elaborar relatórios de gestão anuais acerca de suas atividades; XIII - editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei; XIV - ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento; XV - arrecadar e aplicar suas receitas e publicar, no relatório de gestão a que se refere o inciso XII do caput deste artigo, o detalhamento de suas receitas e despesas; XVI - realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público; XVII - celebrar, a qualquer momento, compromisso com agentes de tratamento para eliminar irregularidade, incerteza jurídica ou situação contenciosa no âmbito de processos administrativos, de acordo com o previsto no Decreto-Lei nº 4.657, de 4 de setembro de 1942; XVIII - editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se a esta Lei; XIX - garantir que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento, nos termos desta Lei e da Lei nº 10.741, de 1º de outubro de 2003 (Estatuto do Idoso); XX - deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação desta Lei, as suas competências e os casos omissos; XXI - comunicar às autoridades competentes as infrações penais das quais tiver conhecimento;XXII - comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei por órgãos e entidades da administração pública federal; XXIII - articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação; e XXIV - implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta Lei".

preparada é menos suscetível ao pânico, pois tem o conhecimento necessário para agir de maneira segura e responsável, uma vez que "a literacia mediática e digital poderá desempenhar um importante papel, na medida em que permite escolhas mais informadas, seja no plano do relacionamento dos cidadãos com os *media* digitais, seja no do exercício da cidadania" (Barriga, 2023, p. 1).

Ainda, a ANPD tem como função supervisionar e fiscalizar o tratamento dos dados pessoais, incluindo os dados pessoais sensíveis, os quais são informações que requerem um nível mais elevado de proteção devido ao potencial de causar discriminação ou prejuízos aos titulares. Conforme aponta Teffé (2022, p. 36), "a seleção sobre quais dados são sensíveis demonstra que a circulação de determinadas informações pessoais pode acarretar maior potencial lesivo aos seus titulares em uma determinada configuração social e política".

No caso do INSS, que coleta e armazena uma vasta quantidade de dados sensíveis, como informações financeiras e de saúde, a segurança desses dados é ainda mais crítica. Esses dados, muitas vezes pertencentes a pessoas idosas, requerem proteção e tratamento adicional, conforme estipulado pela Lei nº 13.709 de 2018. Conforme assegura o art. 55-j, inciso XIX, da LGPD, é reconhecida a vulnerabilidade de grupos específicos, incluindo idosos, e estabelece que o tratamento de dados pessoais dessas pessoas deve ocorrer de forma que lhes assegure uma proteção adequada e específica, ainda a Resolução CD/ANPD n. 2/2022 ressalta que "[...] quando do tratamento de dados pessoais de vulneráveis (crianças, adolescentes e idosos) em larga escala ou que possa afetar significativamente interesses e direitos fundamentais dos titulares, esse tratamento será considerado de alto risco" (Pinheiro, 2023, p. 103).

A competência fiscalizadora da ANPD abrange a investigação de incidentes de segurança, como vazamentos de dados, e a aplicação de sanções administrativas a empresas e órgãos públicos que não estejam em conformidade com a legislação. Sendo incidente de segurança com dados pessoais conceituado, de acordo com a autoridade nacional (Brasil, 2024d, p. 13-4), como:

> [...] incidente de segurança com dados pessoais é um evento adverso confirmado que comprometa a confidencialidade, integridade ou disponibilidade de dados pessoais. Pode decorrer de ações voluntárias ou acidentais que resultem em divulgação, alteração, perda ou acesso não autorizado a dados pessoais, independentemente do meio em que estão armazenados.

Quando ocorre um incidente de vazamento de dados, como o caso do INSS em que foi acessado dados de beneficiários e segurados sem autorização, a ANPD é responsável por

analisar o impacto do vazamento, determinar se houve falhas nos processos de proteção de dados e, se necessário, aplicar medidas corretivas e sanções para prevenir futuros incidentes. Ressalva-se, bem destacado por Divino (2023, p. 151) que o conceito de vazamento de dados apresentado é um rol exemplificativo, visto que podem surgir novas formas que se concretizam como exposição de dados sem consentimento e "[...] ser caracterizados como incidentes de segurança, tais como a própria discriminação algorítmica e a venda de produtos com preços diferenciados mediante geolocalização".

O procedimento de tratamento de incidentes de segurança envolvendo dados pessoais é uma competência crucial da ANPD, conforme estabelecido pela Lei nº 13.709/2018. Em tais situações, a ANPD é responsável por orientar e fiscalizar as medidas adotadas pelas organizações para responder a esses incidentes, garantindo que sejam realizadas conforme as exigências legais e que os direitos dos titulares dos dados sejam protegidos.

Quando ocorre um incidente de segurança, a LGPD determina que o controlador de dados, ou seja, a entidade responsável pelo tratamento dos dados, deve comunicar o ocorrido à ANPD e aos titulares dos dados, em prazo razoável, segundo o art. 48 da LGPD. Essa comunicação deve incluir informações detalhadas sobre a natureza dos dados afetados, os riscos relacionados ao incidente, as medidas adotadas para mitigar os danos, e os procedimentos que estão sendo implementados para garantir a segurança dos dados (Brasil, 2018).

No caso específico do INSS, ao tomar conhecimento do incidente de segurança, o órgão deveria ter ativado seu plano de resposta a incidentes, o que inclui a identificação e contenção do vazamento, bem como uma análise detalhada das causas e consequências do ocorrido. A LGPD também exige que o controlador colabore com a ANPD durante todo o processo, fornecendo relatórios sobre o incidente e permitindo auditorias, se necessário.

Conforme apontado, o INSS demorou muito para agir, já que os vazamentos aconteceram em agosto e setembro de 2022 e a comunicação preliminar só ocorreu em 19 de outubro do mesmo ano. A LGPD, em seu artigo 48, estipula que os controladores de dados devem notificar a ANPD sobre a ocorrência de incidentes de segurança que possam acarretar risco ou dano relevante aos titulares dos dados. Anteriormente, essa notificação deveria ocorrer

em um "prazo razoável". Todavia, com a regulamentação recente, o prazo foi especificado para três dias[4] (Brasil, 2024e), tornando o processo mais ágil e eficiente.

Ainda, o INSS não cumpriu o prazo para fazer a complementação da comunicação, em que a ANPD teve que reiterar o pedido para ter resposta do controlador de dados. No caso em análise, observa-se no processo um descumprimento reiterado das determinações da Coordenação Geral de Fiscalização pelo INSS, durante as ações de investigação e auditoria para entender a extensão e a causa do incidente, além de não colaborar durante as avaliações das medidas adotadas pela organização envolvida para mitigar os danos.

Quanto à atuação da ANPD no caso do vazamento de dados do INSS, verifica-se que críticas quanto à velocidade da resposta da ANPD ao incidente. A população em geral, incluído os segurados e beneficiários do INSS interessados sentiram que houve demora para iniciar investigações aprofundadas e para fornecer orientações claras sobre as medidas corretivas que o INSS deveria tomar. Nesses casos, a rapidez na resposta é crucial em casos de vazamentos de dados para minimizar o impacto sobre os titulares dos dados e prevenir usos indevidos.

Assim, observa-se que um dos maiores desafios enfrentados pela ANPD é garantir que os titulares dos dados sejam devidamente informados sobre os incidentes de segurança que afetam seus dados pessoais. A transparência nesse processo é fundamental para manter a confiança dos cidadãos e garantir que eles possam tomar medidas para proteger suas informações pessoais.

Também a ANPD foi criticada pela comunicação insuficiente e tardia com os titulares dos dados sobre o vazamento. A ANPD e o INSS enfrentaram críticas por falhas percebidas na comunicação eficaz e oportuna aos cidadãos afetados pelo vazamento. A partir da análise do incidente, é visível que a ANPD e o INSS não cumpriram essa exigência de maneira eficaz,

[4] Art. 9º, da Resolução CD/ANPD nº 15 de 2024 (Brasil, 2024e): "Art. 9º A comunicação de incidente de segurança ao titular deverá ser realizada pelo controlador no prazo de três dias úteis contados do conhecimento pelo controlador de que o incidente afetou dados pessoais, e deverá conter as seguintes informações: I - a descrição da natureza e da categoria de dados pessoais afetados; II - as medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; III - os riscos relacionados ao incidente com identificação dos possíveis impactos aos titulares; IV - os motivos da demora, no caso de a comunicação não ter sido feita no prazo do caput deste artigo; V - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente, quando cabíveis; VI - a data do conhecimento do incidente de segurança; e VII - o contato para obtenção de informações e, quando aplicável, os dados de contato do encarregado".

deixando muitos indivíduos sem informações claras sobre o impacto do vazamento sobre seus dados pessoais.

A competência sancionatória se concretiza quando a ANPD avalia a gravidade do incidente e pode solicitar que o controlador adote ações adicionais, como a comunicação pública do incidente, para prevenir ou mitigar maiores prejuízos aos titulares dos dados. Além de poder aplicar sanções administrativas, como advertências, multas, bloqueios de dados e até a suspensão do funcionamento de bases de dados.

Destaca-se que a LGPD prevê um leque de sanções administrativas no art. 52[5] (Brasil, 2018), porém a decisão de quais sanções aplicar está sujeita a uma série de fatores, como a gravidade do incidente, a extensão do dano, e as medidas tomadas pela organização para mitigar os riscos. A ausência de sanções mais severas foi vista por alguns como uma falha, mas não constitui uma ação contra a LGPD.

No caso em comento, devido a possibilidade de discricionariedade, criticou-se a ANPD sobre a sua decisão de sanção ou falta de sanção adequada. Parte da população esperava a aplicação de sanções mais severas ao INSS para estabelecer um precedente mais forte sobre a responsabilidade de órgãos públicos no tratamento de dados pessoais. A percepção de impunidade ou de uma resposta branda pode enfraquecer a confiança pública na eficácia da ANPD e na proteção dos dados pessoais.

A multa aplicada foi de R$10 milhões, uma das maiores já impostas pela ANPD até aquele momento. Esse valor reflete a seriedade da infração e o tamanho do vazamento de dados. Além da multa, a ANPD exigiu que o INSS implementasse medidas corretivas para melhorar a segurança dos dados e prevenir futuros incidentes. Essas medidas incluíram a revisão e o fortalecimento das práticas de segurança e proteção de dados dentro da organização, ainda foi

[5] O art. 52 da LGPD dispõe que: "Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: I - advertência, com indicação de prazo para adoção de medidas corretivas; II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração; III - multa diária, observado o limite total a que se refere o inciso II; IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência; V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização; VI - eliminação dos dados pessoais a que se refere a infração; X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados".

condenado a publicar um comunicado sobre o vazamento de informação ocorrido, na primeira página de seu site, com permanência de 60 dias (Brasil, 2024a).

Um caso emblemático na União Europeia, que serve de observação da prática internacional de como dar uma resposta às infrações de forma efetiva, está em um caso do Reino Unido, antes de deixar de fazer parte do bloco. Figueiredo (2023, p. 42-3) expõe o evento da seguinte forma:

> Antes de deixar a EU, o Reino Unido possuía uma das APDs mais ativas na punição desse tipo de infração dentro da União. Dois exemplos emblemáticos foram as multas contra a British Airways e o Marriott – de £183 milhões e £99 milhões respectivamente – por falha na notificação de incidentes de vazamento de dados. A justificativa para a determinação de valores tão expressivos, além do número de vítimas afetadas, foi que as organizações devem responder pelos dados pessoais que armazenam, e isso inclui realizar a devida diligência

A atuação da ANPD no caso do INSS mostra que, mesmo em fase de consolidação, o órgão é capaz de aplicar sanções e orientar medidas corretivas para assegurar o cumprimento da LGPD. No entanto, é um órgão que ainda apresenta falhas, visto que no dia 17 de julho de 2024, a Idec e o MPF de São Paulo ajuizaram ação contra o WhatsApp e a ANPD, no que, até o momento, é reconhecida como a maior ação judicial da história do país em proteção de dados pessoais. O motivo para a ANPD ser incluída como ré nesta ação está relacionado à alegação de que o órgão não exerceu adequadamente sua função de fiscalização e proteção de dados pessoais dos usuários brasileiros.

O papel da ANPD vai além da mera fiscalização, ela tem a responsabilidade de proteger o direito fundamental de proteção de dados pessoais, reconhecido a partir da promulgação da Emenda Constitucional nº 115 de 2022, em que inseriu o inciso LXXIX no artigo 5º da Constituição Federal (Brasil, 1988). Principalmente em uma sociedade em rede, onde a datificação dos indivíduos é uma realidade, ou seja, onde informações pessoais são constantemente coletadas, processadas e utilizadas para diversas finalidades, muitas vezes comerciais, a proteção de dados se torna essencial para garantir a privacidade e a segurança dos

cidadãos. A finalidade da ANPD é, portanto, proteger os dados pessoais dos brasileiros e garantir que o tratamento dessas informações ocorra de maneira lícita, justa e transparente.

O desenvolvimento tecnológico facilitou e intensificou a coleta e análise de dados, já que vive-se em uma sociedade conectada. A circulação de dados, sem precedentes, ocorre pelo movimento de datificação da sociedade, onde quase todas as atividades humanas são convertidas em dados digitais que podem ser coletados, armazenados e analisados.

No capitalismo de plataforma, se capitaliza a coleta e o processamento dos dados. Segundo Srnicek (2018, p. 45, tradução nossa), a principal matéria-prima, atualmente, são os dados, ou seja, "[...] as plataformas se tornaram uma forma eficiente de monopolizar, extrair, analisar e usar as quantidades crescentes de dados que eram gravados. Agora esse modelo se expande por toda a economia e muitas empresas incorporam as plataformas [...][6].

As informações são utilizadas de forma ampla e ilimitada, uma vez que os indivíduos perdem o direito da autodeterminação dos dados pessoais. Shoshana Zuboff (2019, p. 21) sustenta que:

> O capitalismo de vigilância reivindica de maneira unilateral a experiência humana como matéria-prima gratuita para a tradução em dados comportamentais. Embora alguns desses dados sejam aplicados para o aprimoramento de produtos e serviços, o restante é declarado como superávit comportamental do proprietário, alimentando avançados processos de fabricação conhecidos como "inteligência de máquina" e manufaturado em produtos de predição que antecipam o que um determinado indivíduo faria agora, daqui a pouco e mais tarde.

Nesse contexto, é imprescindível a discussão sobre a proteção de dados pessoais para garantir a autodeterminação dos dados, isto é, permitir que os indivíduos possam controlar as informações que são coletadas, utilizadas e compartilhadas. É importante destacar que o Brasil demorou a estabelecer uma legislação específica de proteção de dados pessoais, a ausência de um marco regulatório robusto permitiu que práticas invasivas se tornassem comuns, sem que houvesse uma autoridade reguladora para impedir abusos ou proteger os direitos dos titulares de dados. A criação da LGPD foi, portanto, um passo essencial para alinhar o Brasil aos padrões internacionais de proteção de dados e para assegurar que os direitos de privacidade dos cidadãos sejam devidamente respeitados.

[6] No original: las plataformas se volvieron una manera eficiente de monopolizar, extraer, analizar y usar las cantidades cada vez mayores de datos que estabam registrando. Ahora este modelo se ha expandido por toda economía, y muchas empresas incorporam plataformas [...].

4 CONCLUSÃO

A atuação da ANPD é fundamental para a efetivação da LGPD no Brasil, especialmente no que diz respeito à proteção dos direitos fundamentais de privacidade e segurança dos dados dos cidadãos. O caso do vazamento de dados do INSS evidencia a importância da ANPD em garantir o cumprimento das normas estabelecidas pela LGPD. Durante o processo, ficou claro que o INSS não cumpriu os prazos legais para comunicar o incidente de segurança e não colaborou de forma adequada com as investigações conduzidas pela ANPD. Diante disso, a ANPD aplicou uma sanção rigorosa, mas coerente com a gravidade do vazamento de dados sensíveis, demonstrando seu compromisso com a proteção dos dados pessoais dos brasileiros.

A imposição de uma sanção dura ao INSS por parte da ANPD reflete não apenas a seriedade com que a autoridade trata os incidentes de segurança, mas também a sua função pedagógica de promover uma cultura de proteção de dados no país. A LGPD foi criada para assegurar que o tratamento de dados pessoais ocorra de maneira responsável, transparente e segura, respeitando os direitos dos titulares. A atuação da ANPD no caso do INSS reforça a mensagem de que o descumprimento dessas normas terá consequências significativas, incentivando tanto o setor público quanto o privado a adotar medidas adequadas de proteção de dados.

Apesar de ainda estar em fase de estruturação e consolidação, a ANPD tem se mostrado uma peça essencial no novo cenário regulatório brasileiro. O Brasil demorou para adotar uma lei de proteção de dados pessoais, o que permitiu, por muitos anos, que práticas invasivas e o tratamento inadequado de dados se proliferassem sem um controle adequado. Agora, com a LGPD em vigor e a ANPD atuando de forma ativa, o país começa a alinhar-se aos padrões internacionais de proteção de dados, promovendo um ambiente mais seguro e confiável para o tratamento de informações pessoais.

Em conclusão, a importância da ANPD vai além da aplicação de sanções; ela representa a defesa dos direitos fundamentais dos cidadãos em uma sociedade cada vez mais digital e interconectada. A atuação no caso do INSS é um exemplo claro de sua função regulatória e fiscalizatória, assegurando que o tratamento de dados pessoais seja feito em conformidade com a LGPD e protegendo a privacidade dos indivíduos. Com o tempo e a consolidação de suas

práticas, espera-se que a ANPD continue a desempenhar um papel crucial na promoção de uma cultura de respeito à privacidade e na proteção dos dados pessoais no Brasil.

REFERÊNCIAS

BARRIGA, Antónia do Carmo. Lugares (ausentes) de literacia mediática e digital. **Configurações:** Revista Ciências Sociais, 31, 2023. Disponível em: <https://journals.openedition.org/configuracoes/17005>. Acesso em: 30 jul. 2024.

BRASIL.Câmara dos Deputados. **Projeto de Lei nº 5.275, de 2016.** Dispõe sobre a proteção de dados pessoais. Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1457370&filename=Tramitacao-PL%205275/2016>. Acesso em: 1 set. 2024.

BRASIL. **Constituição (1988)**. Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal, 1988. Disponível em: <https://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm >. Acesso em: 1 set. 2024.

BRASIL. **Decreto nº 10.474, de 26 de agosto de 2020.** Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança da Autoridade Nacional de Proteção de Dados e remaneja e transforma cargos em comissão e funções de confiança. 2020. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10474.htm>. Acesso em: 30 jul. 2024.

BRASIL. **Decreto nº 11.348, de 1º de janeiro de 2023.** Estabelece medidas para a modernização da administração pública federal. 2023b. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11348.htm#:~:text=DECRETO%20N%C2%BA%2011.348%2C%20DE%201%C2%BA%20DE%20JANEIRO%20DE%202023&text=Aprova%20a%20Estrutura%20Regimental%20e,comiss%C3%A3o%20e%20fun%C3%A7%C3%B5es%20de%20confian%C3%A7a.>. Acesso em: 30 jul. 2024.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Dispõe sobre a Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 30 jul. 2024.

BRASIL. Ministério da Justiça e Segurança Pública. Autoridade Nacional de Proteção de Dados. **Auto de Infração: 03/08/2023 – Auto de Infração nº 1/2023/CGF/ANPD (SEI nº 0048146)**. 2023a. Brasília, DF: Autoridade Nacional de Proteção de Dados, 2023. Disponível em: <https://www.gov.br/anpd/pt-br/composicao-1/coordenacao-geral-de-fiscalizacao/PAS_INSS_principal_publica.pdf>. Acesso em: 30 maio 2024.

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, 2024d. Disponível em:

<https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_resposta_incidentes.pdf>. Acesso em: 1 set. 2024.

BRASIL. Ministério da Justiça e Segurança Pública. Autoridade Nacional de Proteção de Dados. **Nota Técnica no 2/2024/FIS/CGF/ANPD, 2024b.** Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/sei_0049668_nota_tecnica_2_versao_publica__1_.pdf. Acesso em: 30 maio 2024.

BRASIL. Ministério da Justiça e Segurança Pública. Autoridade Nacional de Proteção de Dados. **Relatório de Instrução no 01/2024/CGF/ANPD, 2024a.** Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/relatorio-de-instrucao-1_2024.pdf. Acesso em: 30 maio 2024.

BRASIL. Ministério da Justiça e Segurança Pública. Autoridade Nacional de Proteção de Dados. **Resolução CD/ANPD nº 15, de 24 de abril de 2024.** Estabelece normas complementares à Lei Geral de Proteção de Dados Pessoais. 2024e. Disponível em: <https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024>. Acesso em: 1 set. 2024.

BRASIL. Ministério da Justiça e Segurança Pública. Autoridade Nacional de Proteção de Dados. **Vazamento de dados.** Brasília, DF: ANPD, 2024c. Disponível em: <https://cartilha.cert.br/fasciculos/vazamento-de-dados/fasciculo-vazamento-de-dados.pdf>. Acesso em: 1 set. 2024.

DIVINO, Sthéfano Bruno Santos. Comunicação de incidentes de segurança: prazo, regulatory enforcement e a competência da Autoridade Nacional de Proteção de Dados. **Revista de Direito Administrativo,** *282*(3), 143–175, 2023. Disponível em: <https://doi.org/10.12660/rda.v282.2023.90158>. Acesso em: 30 jul. 2024.

Figueiredo, Nanny Santana Leal de. ENFORCEMENT DA LEI GERAL DE PROTEÇÃO DE DADOS: como a atuação efetiva das autoridades de proteção de dados da União Europeia podem servir de inspiração para a ANPD. **Revista do Programa de Direito da União Europeia,** v.2, 2023. Disponível em: <https://periodicos.fgv.br/rpdue/article/view/90004/84453>. Acesso em: 30 jul. 2024.

LORENZON, Laila Neves. Análise comparada entre regulamentações de dados pessoais no Brasil e na União Europeia (LGPD e GDPR) e seus respectivos instrumentos de enforcement. **Revista do Programa de Direito da União Europeia,** v. 1, 2021. Disponível em: <https://periodicos.fgv.br/rpdue/article/view/83423/79192>. Acesso em: 30 jul. 2024.

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

RODRIGUEZ, Daniel Piñeiro. **O Direito Fundamental à proteção de dados:** vigilância, privacidade e regulação. Rio de Janeiro, Lumen Juris, 2021.

SARLET, Gabrielle Bezerra Sales; RODRIGUEZ, Daniel Piñeiro. A Autoridade Nacional de Proteção de Dados (ANPD) e os desafios tecnológicos: alternativas para uma estruturação responsiva na era da governança digital. **Rev. direitos fundam. democ.**, v. 27, n. 3, p. 217-253, set./dez. 2022. Disponível em: <https://revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/article/view/2285/760>. Acesso em: 30 jul. 2024.

SRNICEK, Nick. **Capitalismo de plataformas.** Buenos Aires: Caja Negra, 2018.

TEFFÉ, Chiara Spadaccini de. **Dados pessoais sensíveis:** qualificação, tratamento e boas práticas. São Paulo: Foco, 2022.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.** Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: < https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:02016R0679-20160504#tocId68>. Acesso em: 30 jul. 2024.

ZUBOFF, Shoshana. **A Era do capitalismo de vigilância:** a luta por um futuro humano na nova fronteira do poder. Rio de Janeiro: Intrínseca, 2019.