



REVISTA ARTE, CIÊNCIA E TECNOLOGIA DA FACULDADE CET

A PROTEÇÃO E O TRATAMENTO DOS DADOS PESSOAIS DA PREVIDÊNCIA SOCIAL: UMA ANÁLISE DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

THE PROTECTION AND PROCESSING OF SOCIAL SECURITY PERSONAL DATA: AN ANALYSIS OF THE GENERAL DATA PROTECTION LAW (LGPD)

MEIRELES FILHO, Mário Rodrigues Gomes¹
MEIRELES, Joelma Danniely Cavalcanti²

RESUMO

O Instituto Nacional do Seguro Social – INSS, autarquia federal criada pela lei 8029/90, vinculado ao Ministério da Economia, que para a realização de suas prestações de serviços públicos, tem a necessidade de coletar, tratar dados pessoais, tendo ainda a necessidade de distribuição de informações a diversos entes públicos e privados para o atendimento das ações públicas necessárias. Nesse contexto, e com o vigor da Lei 13709/18 conhecida como Lei Geral de Proteção de Dados – LGPD, que tem como objetivo a proteção dos dados pessoais coletados em território nacional. O INSS teve que se adequar com o objetivo de alcançar a transformação cultural ao tratamento de dados pessoais dos cidadãos exigidos na nova legislação, sendo apresentado nesse trabalho quais as alterações necessárias e suas normatizações aplicadas para a concretização dessas alterações.

Palavras-Chaves: Lei Geral de Proteção de Dados, Previdência Social, Dados Pessoais

ABSTRACT

The National Institute of Social Security - INSS, a federal agency created by law 8029/90, linked to the Ministry of Economy, which, in order to carry out its public service provision, has the need to collect and process personal data, also having the need to distribution of information to various public and private entities to meet the necessary public actions. In this context, and with the enactment of Law 13709/18 known as the General Data Protection Law - LGPD, which aims to protect personal data collected in the national territory. The INSS had to adapt with the objective of achieving the cultural transformation to the processing of personal data of citizens required in the new legislation, being presented in this work what are the necessary alterations and their applied normalization for the accomplishment of these alterations.

Keywords: General Data Protection Law, social security, personal data

¹ Mestre em Engenharia Elétrica pela UFPI, Especialista em Tecnologia da Informação pela UFC, Bacharelado em Direito da Faculdade CET e Tecnólogo em Processamento de dados pela UESPI, Professor Faculdade CET nos cursos de Medicina na disciplina Informática Médica e na Pós-graduação em Penal na disciplina de Crimes Digitais, Coordenador dos Cursos de Tecnolôgias em Sistemas para internet da Faculdade CET marorgmfilho@hotmail.com;

²Mestranda em Direito pela Universidade Católica de Brasília (UCB). Especialista em Contabilidade Tributária Físico Contábil pelo Centro de Ensino Superior do Vale do Parnaíba (CESVALE). Graduada em Ciências Contábeis pela Universidade Federal do Piauí. Graduada em Direito. Coordenadora da Pós-graduação em Direito Previdenciário e Prática Previdenciária (CET/PI). Professora Faculdade CET. E Mail: joelmameireles@hotmail.com



REVISTA ARTE, CIÊNCIA E TECNOLOGIA DA FACULDADE CET**Introdução**

Com o avanço tecnológico e o surgimento de uma sociedade convergente às relações (profissionais ou sociais) interpessoais, torna as pessoas mais vulneráveis à exposição de suas informações pessoais (ASTELLS, 2016).

Essas novas tecnologias trouxeram o que podemos chamar de “sociedade da informação”, está formada por indivíduos hiper conectados a diferentes tecnologias, que tem uma necessidade cada vez maior de consumir informação (CONI JR. e PAMPLONA FILHO, 2020).

Ao tempo que essas novas sociedades consomem cada vez mais informações, dela também é cobrado uma massiva coleta de dados pessoais, sendo estes considerados a matéria prima dos tempos atuais (CONI JR. e PAMPLONA FILHO, 2020).

Essa nova matéria prima, podemos considerar, a informação como o elemento central da economia, tornando dessa forma necessário buscar meios que permitam uma maior segurança e proteção à privacidade e a intimidade das informações pessoais (CONI JR., 2019) (BERTOTTI, 2022).

Nesse contexto de colheita de informações, o mundo globalizado formou-se ao longo das últimas décadas, das informações extraídas principalmente em sítios de internet, de aplicativos de comunicação. Sendo essas informações, reunidas e processadas em estruturas tecnológicas denominadas *BIG DATA*, que permitem o desenvolvimento de ativos comerciais (informações de negócios) a partir de informações pessoais (LOUREIRO, 2020).

(LOUREIRO, 2020), destaca que:

Destaca-se que a coleta de informações pessoais não é consequência da sociedade da informação, e sim uma prática milenar, mas a sua relevância e preocupação jurídica atual são devido à grande agilidade da manipulação, notadamente pelo fato de que, na maioria das vezes, o cidadão não tem conhecimento do funcionamento e processamento dessa atividade, bem como da sua extensão e destino, tornando-a uma invasão.

Desta forma, a busca pela privacidade dos dados pessoais utilizados pela necessidade de circulação dessas informações de contexto íntimo e pessoal, faz-se cada vez mais necessária, buscando-se assim, a garantia dos direitos à segurança jurídica dessa informação. Nesse contexto, a Legislação brasileira vem nos últimos anos sendo trabalhada de forma a buscar garantir o bem jurídico mais precioso para o cidadão, ou seja, seus dados pessoais.

Após a criação de diversas leis, que tem como objetivo a proteção das informações em sistemas eletrônicos como Lei 12.527/2011, conhecida como a “Lei de Acesso à Informação –LAI”, que regula o acesso a informações previsto no inciso XXXIII do art. 5º da Constituição Federal; a Lei 12.737/2012, também conhecida como “Lei Carolina Dieckmann”, que tipificou os crimes de invasão de equipamentos eletrônicos; a Lei 12.965/2014, conhecida como “Lei do Marco Civil da Internet”, determinou os serviços e as responsabilidades dos serviços oferecidos na internet; e em agosto de 2018, foi promulgada a Lei 13.709/2018, conhecida como a “Lei Geral de Proteção de Dados Pessoais (LGPD)”, com o intuito de proteção aos direitos fundamentais de privacidade e liberdade das informações pessoais.



REVISTA ARTE, CIÊNCIA E TECNOLOGIA DA FACULDADE CET

O Instituto Nacional do Seguro Social (INSS) teve autorização de criação dada pela Lei nº 8.029/1990, sendo ele uma autarquia federal, hoje vinculada ao Ministério da Economia por decreto de número 9.660/2019. Sendo que atualmente tem como principal função, gerenciar o plano de serviços e benefícios do Regime Geral de Previdência Social (RGPS) (GOVERNO FEDERAL, 2020).

Além de seu atendimento pessoal e pela central “Atendimento 135”, os serviços oferecidos pelo INSS, encontram-se também disponíveis pela internet no serviço “Portal do INSS”, permitindo através dele realizar diversos atendimentos ao cidadão (GOVERNO FEDERAL, 2020).

Desta forma, a LGPD, atribui ao INSS, assim como a toda a administração pública um conjunto de responsabilidades e deveres sobre a forma de proteção e uso dos dados pessoais dos cidadãos atendidos pelo ente público (BARROS, SCHIMDT e SILVA, 2019).

Neste sentido esse trabalho tem como objeto principal a apresentação da necessidade legal da proteção dos dados do INSS, através da análise dos dispositivos legais exigidos pela LGPD, bem como apresentar conceitos de proteção, privacidade de dados pessoais e como isso poderá ser aplicado às informações do INSS conforme é exigido pela LGPD

Este trabalho está estruturado em seções, que inicialmente temos as notas introdutórias. Na segunda seção apresentamos as legislações aplicadas à Lei Geral de Proteção de Dados, suas características, a evolução legislativa de proteção de dados e sua aplicação nos entes públicos, a legislação que rege a coleta e os serviços disponibilizados pelo INSS. Na terceira seção descrevemos como os conceitos da LGPD estão sendo aplicados pelo INSS na coleta e tratamento de dados de seus segurados, seguido das considerações finais.

A transformação digital e a privacidade

Quando falamos em transformação digital, nos referimos às mudanças decorrentes da adoção de tecnologias digitais em diversas áreas da sociedade, incluindo o setor empresarial e governamental. Tendo o potencial de melhorar a eficiência e a qualidade dos serviços, mas também trazendo consigo desafios relacionados à privacidade e à segurança dos dados (RUSSELL, O'RAGHALLAIGH, *et al.*, 2018).

Para a sociedade brasileira e internacional, a segurança dos dados pessoais é um assunto crítico, uma vez que a coleta e o uso indevido de informações pessoais podem ter consequências graves. A falta de segurança adequada dessas informações pode levar a vazamentos de dados, fraude, roubo de identidade e outros crimes cibernéticos que podem afetar negativamente a vida dos cidadãos, incluindo a perda de privacidade, a violação de direitos fundamentais, o roubo de identidade e o crime financeiro (ASTELLS, 2016).

Nesse sentido, a privacidade dos dados pessoais é um direito fundamental que deve ser protegido, cabendo a toda sociedade e entes públicos, o trabalho de garantir a segurança da informação, sendo essencial que as informações sejam protegidas de maneira adequada.

Conforme já mencionado, para os entes públicos a segurança da informação é extremamente importante, entre eles podemos destacar o Instituto Nacional do Seguro Social



REVISTA ARTE, CIÊNCIA E TECNOLOGIA DA FACULDADE CET

(INSS), que é responsável por lidar com informações confidenciais de milhões de cidadãos, como informações de previdência social, dados financeiros e informações pessoais. Sendo vital para ele, manter esses dados seguros para evitar qualquer tipo de violação de privacidade, fraude ou roubo de identidade (SOUZA, BARRANCOS e MAIA, 2019).

Informação X Dados

Em um mundo em constante transformação digital, a informação é uma ferramenta econômica de grande importância, podendo definir a evolução de produtos e serviços oferecidos pelas instituições privadas ou públicas (CALAZANS, 2014).

Ela mostra-se ainda com uma importância essencial para a tomada de decisão, gerenciamento de processos e criação de novas inovações através de seus dados armazenados. E no meio desse conjunto de dados e informações importantes, encontramos também os Dados Pessoais (SOUZA, BARRANCOS e MAIA, 2019).

Em LYRA (2015), informação é definida como um conjunto de dados organizados e tratados, que representam um significado, um sentido, em um contexto específico, passando a informação a ter valor próprio.

A legislação brasileira conceitua informação no Inciso I do artigo 4º da Lei 12.527/2011 (LAI). Ela também conceitua termos como: informações pessoais. Informações sigilosas, documentos, tratamento da informação, disponibilidade de informação, autenticidade da informação, integridade da informação e a primariedade da informação (BRASIL, 2011).

Art. 4º ..

I - Informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

II - Documento: unidade de registro de informações, qualquer que seja o suporte ou formato;

III - Informação sigilosa: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado;

IV - Informação pessoal: aquela relacionada à pessoa natural identificada ou identificável;

V - Tratamento da informação: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação;

VI - Disponibilidade: qualidade da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados;

VII - autenticidade: qualidade da informação que tenha sido produzida, expedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema;

VIII - integridade: qualidade da informação não modificada, inclusive quanto à origem, trânsito e destino;

IX - Primariedade: qualidade da informação coletada na fonte, com o máximo de detalhamento possível, sem modificações.

REVISTA ARTE, CIÊNCIA E TECNOLOGIA DA FACULDADE CET

PIURCOSKY *et al.*(2019), apresentam que, os princípios da Segurança da Informação (SI), tem como objetivo, garantir a proteção, confiabilidade, a disponibilidade, a integridade da informação para os seus devidos fins, a qual foi projetada.

Em Souza, 2019 é apresentado sobre o panorama de acesso aos dados (informações) públicos, a necessidade da proteção pessoal e da privacidade, sendo considerado, o consentimento, como requisito essencial para garantia dos direitos dos dados pessoais, conforme legislação brasileira. Este trabalho examinou o tratamento dos dados pessoais realizado pelo poder público considerando a Lei de Acesso à Informação em relação aos prazos e procedimentos aplicados para garantir a proteção pessoal.

Neste contexto podemos considerar a proteção de dados, material ou digital, como fundamental para a proteção dos direitos das pessoas, sendo esta segurança, elevada ao *status* de direito constitucional fundamental pela EC 115/2022, que alterou os artigos 5º, 21 e 22 da Constituição Federal (CF) de 1988, e acrescentou o inciso LXXIX no artigo 5º, “LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.”, alterou o inciso XXVI do artigo 21, “XXVI - organizar e fiscalizar a proteção e o tratamento de dados pessoais, nos termos da lei.” (NR)” e acrescentou o inciso XXX no artigo 22 “XXX - proteção e tratamento de dados pessoais.” (BRASIL, 2022).

A Lei geral de Proteção de dados

A lei 13.709/2018, também conhecida como Lei Geral de Proteção de Dados (LGPD), é considerada o primeiro instrumento jurídico brasileiro dedicado exclusivamente a regulamentar o tratamento de dados pessoais, tendo como principal objetivo a proteção dos direitos fundamentais de liberdade, de privacidade, e o desenvolvimento da personalidade da pessoa natural. Ela também explana como os dados pessoais são tratados, sendo por meios físicos ou digitais, em sua utilização por pessoa física ou jurídica de direito público ou privado (BARROS, SCHIMDT e SILVA, 2019).

Internacionalmente a LGPD, vem trazer uma segurança jurídica ao tratamento de dados pessoais, estabelecendo regras para coleta, armazenamento e tratamento das informações de cidadãos brasileiros, como também de estrangeiros em território brasileiro; por ser ela semelhante a *General Data Protection Regulation* (GDPR) da União Europeia, que entrou em vigor em maio de 2018 (PIURCOSKY, COSTA, *et al.*, 2019)

Segundo PIURCOSKY *et al.*(2019), a GDPR, assim como a LGPD, tem como objetivo obter mais segurança para as pessoas em relação ao armazenamento e tratamento de seus dados pessoais. Ambas apresentam que os titulares da informação, têm todo o direito sobre seus dados, ao tempo que desenvolvem uma maior responsabilidade sobre os responsáveis por guardar e tratar a informação.

O trabalho de PIURCOSKY *et al.*(2019), destaca que a LGPD busca adequar o Brasil a era digital, onde dados são transmitidos, tratados e até mesmo comercializados, sem o devido consentimento de seu titular, cerceando assim o princípio da liberdade e privacidade pessoal.

REVISTA ARTE, CIÊNCIA E TECNOLOGIA DA FACULDADE CET

Para PIURCOSKY *et al.*(2019), impor regras sobre as formas de coleta e manutenção de dados de cidadãos brasileiros ou de estrangeiros em território nacional, devem ser feitos sempre com o consentimento dos usuários, salvo em situações de garantia da ordem pública ou mandado de segurança, criando-se assim um cenário de segurança jurídica conforme os parâmetros internacionais existentes.

Desta forma, a compreensão de conceitos como “dados pessoal” e “tratamento de dados”, em termos jurídicos, passa a ter uma relevância para o legislador, tanto que a LGPD, traz consigo esses conceitos em seu artigo 5ª, onde em seu inciso primeiro conceitua dados pessoais como a: informação relacionada a pessoa natural identificada ou identificável.

Ainda no artigo 5º da LGPD encontramos as definições de quem são, a quem pertence os dados pessoais e quais dados devem ser protegidos conforme citado abaixo.

Dado pessoal sensível são os dados pessoais sobre os seguintes assuntos: origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, desde que esses dados estejam ligados a uma pessoa natural, Artigo 5º, II da Lei 13.709/2018.

O Titular é a pessoa natural a quem se referem os dados pessoais a serem tratados, Artigo 5º, V da Lei 13.709/2018.

No artigo 5ª ainda se apresentam as definições de quem são os responsáveis pela coleta, armazenamento e processamento de dados, conforme conceituados abaixo.

O controlador é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais, conforme Artigo 5º, VI da Lei 13.709/2018.

O operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador, conforme Artigo 5º, VII da Lei 13.709/2018

O encarregado é a pessoa indicada para a comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), conforme Artigo 5º, VIII da Lei 13.709/2018 alterada pela redação da Lei nº 13.853, de 2019.

Os agentes de tratamento dos dados são apenas o controlador e o operador, conforme Artigo 5º, IX da Lei 13.709/2018.

Os órgãos de pesquisa são as entidades da administração pública direta ou indireta ou a pessoa jurídica de direito privado sem fins lucrativos, com sede e foro no Brasil, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter: histórico, científico, tecnológico ou estatístico, conforme Artigo 5º, XVIII da Lei 13.709/2018, alterada pela redação da Lei nº 13.853, de 2019.

E a autoridade nacional é o órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional, conforme Artigo 5º, XIX da Lei 13.709/2018 alterada pela redação da Lei nº 13.853, de 2019.

Ainda no Artigo 5ª encontramos as definições das ações a serem realizados pelos agentes de tratamentos, os quais podemos destacar:

REVISTA ARTE, CIÊNCIA E TECNOLOGIA DA FACULDADE CET

O tratamento: o qual se destina a toda operação realizada com dados pessoais (coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração) conforme Artigo 5º, X da Lei 13.709/2018;

A anonimização que é a utilização de meios no momento do tratamento, os quais permite que um dado perca a possibilidade de associação, direta ou indireta, a um indivíduo, conforme Artigo 5º, XI da Lei 13709/2018;

O compartilhamento de dados, que é a comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados, conforme Artigo 5º, XVI da Lei 13.709/2018;

A aplicabilidade da LGPD

A aplicabilidade da lei é apresentada em seu Art. 3, §2º, e abrange todas as atividades que envolvem o tratamento de dados pessoais, tanto por parte de empresas quanto de órgãos públicos (TAMBOSI, 2021).

Sendo ela aplicada a todas as empresas e instituições que atuam no Brasil, independentemente de seu tamanho ou setor de atuação. Aplicando-se ainda a empresas estrangeiras que tratam dados pessoais de brasileiros, mesmo que não tenham presença física no país (BARROS, SCHIMDT e SILVA, 2019).

Como responsável pelo pagamento de benefícios previdenciários, como aposentadorias, pensões e auxílios, o INSS trata um grande volume de dados pessoais, como informações de identificação dos segurados, dados de contribuição previdenciária, histórico de benefícios concedidos, entre outros. Dessa forma, é necessário que o INSS esteja em conformidade com as disposições da LGPD (BERTOTTI, 2022).

Aplicabilidade da LGPD na Administração Pública e no INSS

A LGPD, impõe à administração pública brasileira, um conjunto de responsabilidades sobre os dados sensíveis coletados pelos entes públicos, principalmente os dados coletados no setor de saúde e previdência, tendo essas coletas um impacto direto na esfera do SUS e do INSS, como também nas organizações públicas que trabalham com conectadas as informações da seguridade social, como hospitais e clínicas, secretarias municipais e estaduais de saúde, entidades filantrópicas e assistenciais entre outras (GOVERNO FEDERAL, 2020).

Em seu artigo 7º a LGPD, fornece ao Governo a autorização, em alguns casos, de utilizar os dados pessoais sem o consentimento do cidadão, desde que se enquadre nos incisos II ao inciso X.



REVISTA ARTE, CIÊNCIA E TECNOLOGIA DA FACULDADE CET

No entanto quando tratar-se de dados sensíveis (CPF, de doenças – CID etc.) deverão ser respeitados as hipóteses previstas em seu Art. 11 e em seu art. 13, quando tratar-se dos casos de fornecimento de dados de saúde, da previdência social, entre outros, com a finalidade de realização de estudos por universidades e outras instituições de pesquisa de âmbito públicas ou privadas (BERTOTTI, 2022).

A LGPD em seu artigo 26 determina as limitações do poder público ao compartilhamento dos dados, limitando-se a atender as necessidades específicas da execução de políticas públicas e atribuições legais do órgão.

A responsabilidade da gestão e do tratamento de dados do INSS

Conforme já mencionado o INSS tem como principal função, gerenciar o plano de serviços e benefícios do RGPS, conforme art. 5, da Lei 11.457/2007, tendo ele a competência para conceder, revisar e negar os benefícios e serviços previdenciários em favor dos seus segurados e seus dependentes.

O INSS, necessita também coletar os dados dos agentes públicos, estagiários e terceirizados que prestam serviços à instituição atendendo as obrigações legais referente à lei nº 8.112/1990 e a lei nº 11.788/2008.

O decreto 10.047/2019 oficializou que a gestão, o tratamento e a proteção dos dados, do Cadastro Nacional de Informações Sociais – CNIS e da previdência, fossem de responsabilidade do INSS.

Para o cumprimento dessas leis e de outras leis esparsas que atribuem funções e serviços ao INSS, a exemplo da Lei nº 9.876/99, que dispõe sobre a contribuição previdenciária do contribuinte individual, e da Lei nº 10.666/2003, que dispõe sobre a concessão da aposentadoria especial ao cooperado de cooperativa de trabalho ou de produção e dá outras providências, é necessário a coleta e o tratamento de dados pessoais e de informações sensíveis, como sexo, CPF, doenças, entre outras.

Além desses dados, é necessário também ao INSS a realizar o cadastro e o tratamento das informações coletadas das pessoas que acessam as dependências das Unidades do INSS, ou mesmos dos sistemas online que permitem o acesso dos seus beneficiários pela internet ou telefone, de forma a garantir a identificação e a segurança dos usuários de seus serviços.

O CNIS contempla as informações cadastrais, previdenciárias, trabalhistas e sociais dos cidadãos, e tem por finalidade agregar as informações oriundas de diversas fontes governamentais, que alimentam o banco de dados que permitem a execução de políticas públicas.

Desta forma, o INSS hoje possui o cadastro consolidado das remunerações para o armazenamento dessas informações de todos os empregados formais desde 1975, utilizando para o armazenamento dessas informações, o compartilhamento de seus dados com outras instituições como a DATAPREVE.

REVISTA ARTE, CIÊNCIA E TECNOLOGIA DA FACULDADE CET

Como forma da disponibilidade desses de seus dados, o INSS permite aos seus segurados a consulta e alteração de suas informações através de serviços em seu portal na internet (<https://meuinss.gov.br>), e pessoalmente em suas agências.

A aplicabilidade da LGPD nos serviços prestados pelo INSS

Quando se trata da relação previdenciária, o papel de controlador é do INSS ou do Regime Próprio de Previdência Social, e o papel do operador é do servidor público responsável pela gestão dos dados.

Desta forma, para o atendimento da LGPD pelo INSS, foi necessária sua adequação ao processo de governança corporativa, através da implementação de programas de compliance, onde foi possível o levantamento dos dados a serem tratados, a análise das especificações dos consentimentos de dados pelos seus titulares; o desenvolvimento do mapa de risco e elaboração do plano de ação, entre outros elementos previsto nos art. 7º ao 10º da LGPD.

O INSS por ter a responsabilidade e conceder, negar e revisar os benefícios e serviços do RGPS (Regime Geral de Previdência Social) de seus segurados e dependentes, trata os dados pessoais de seus filiados (segurados obrigatórios ou facultativos) e não filiados (não contribuintes), analisa apenas os dados referentes às finalidades inerentes e indispensáveis a sua prestação de serviço.

Desta forma, para o tratamento compartilhado de dados pessoais sensíveis destinados ao atendimento necessários pela administração pública e cumprimento de obrigações legais, dispensa-se o consentimento do titular dos dados, conforme incisos II e III do art. 7º e alíneas “a” e “b” do inciso II do art. 11 da LGPD.

Já os dados que não se enquadrem na categoria acima, são tratados como exceção e necessitam de autorização de seu titular, como por exemplo os dados dos visitantes da instituição que devem ser informados a finalidade para o tratamento de dados conforme os princípios existentes no artigo 6º da LGPD.

A LGPD, garante em seu art. 18º os direitos dos titulares sobre os seus dados, entre eles pode-se destacar o direito ao acesso aos dados que se encontram no inciso II do referido artigo. Para essa demanda, o INSS através do sítio³ eletrônico “<https://meu.inss.gov.br>” ou aplicativo para celular, disponibiliza as informações aos segurados. Além das informações, é possível ainda no portal solicitar diversos serviços, entre eles a solicitação de alterações dos dados pessoais.

E referente aos dados do CNIS, conforme § 1º do art. 19 do Decreto nº 3.048/1999, com redação dada pelo Decreto nº 10.410/2020, o segurado poderá solicitar, a qualquer momento, a inclusão, exclusão ou retificação de informações constantes do CNIS, atendendo dessa forma o

³ Sítios (domínio e páginas armazenadas) (Res 23610/19 Art. 37º X) hospedado diretamente em provedor de internet estabelecido no país: aquele cujo endereço (URL *Uniform Resource Locator*) é registrado no organismo regulador da internet no Brasil e cujo conteúdo é mantido pelo provedor de hospedagem em servidor instalado em solo brasileiro;

REVISTA ARTE, CIÊNCIA E TECNOLOGIA DA FACULDADE CET

inciso III do artigo 18, da Lei 13.709/2018, que dá direito ao Titular a correção de dados incompletos, inexatos ou desatualizados.

A comunicação dos dados entre os diversos órgãos públicos é tratada através do Decreto nº 10.046, de 2019, o qual estabelece as normas e as diretrizes para o compartilhamento de informações entre órgãos, entidades da administração pública, autarquias e os demais Poderes da União.

Esse decreto busca garantir a qualidade e a eficiência na operacionalidade da transmissão dos dados. Atendendo dessa forma os princípios apresentados na LGPD, em seu artigo 6º no inciso V, que trata sobre a qualidade dos dados, inciso VI, que trata da transparência dos dados e do inciso VII, que trata da segurança dos dados.

Ainda tratando de segurança da Informação, encontra-se em vigor no INSS a Política de Segurança da Informação do Instituto Nacional do Seguro Social (POSIN-INSS), bem como a Norma de Controle de Acesso Lógico (NCAL/INSS), aprovadas, respectivamente, pelas Resoluções 9 e 10/CEGOV/INSS, de agosto/2020, que assegura o acesso aos sistemas do INSS pelos seus servidores.

O POSIN-INSS ainda assegura aos servidores as obrigações de manter o devido sigilo quanto às informações obtidas por meio do acesso concedido; assegura ainda a proteção dos dados pessoais armazenados ou tratados no exercício de suas atribuições, além de comunicar ao responsável pela administração do sistema quaisquer violações ou incidentes referentes à proteção dos dados, conforme solicitado pela LGPD.

Da responsabilidade Civil pelo vazamento de dados do INSS

Apesar da LGPD, Lei 13.709/2018 e a Lei de Acesso à Informação (LAI), Lei 12.527/2011, vedarem ao poder público transferir a entidades privadas os dados pessoais constantes em suas bases de dados, com exceção aos casos previstos em Lei. Ainda ocorrem vazamentos dessas informações ou por erro humano, ou por falhas sistêmicas, sendo em ambos os casos uma afronta à privacidade das informações pessoais.

Para estes tipos de erros, onde não existe motivos para o compartilhamento de dados pessoais entre o INSS e terceiros, sem a devida autorização do titular dos dados, ou não atendendo aos itens do artigo 4º da LGPD, será possível a propositura de ação contra o INSS, o terceiro que teve acesso aos dados

Nestes casos, caberá ao judiciário aplicar as medidas jurídicas cabíveis, como ocorrido recentemente no processo Civil de N º 5000086-03.2021.4.03.6345 – TRF 3ª Região, onde a 12ª Turma Recursal do Juizado Especial Federal de São Paulo condenou o INSS a indenizar uma senhora pela divulgação de seus dados pessoais para uma instituição financeira sem autorização. Dessa forma, o judiciário demonstra sua atenção aos descumprimentos das determinações da LGPD, aplicando-se assim, condenações decorrentes aos danos causados

REVISTA ARTE, CIÊNCIA E TECNOLOGIA DA FACULDADE CET**CONSIDERAÇÕES FINAIS**

Neste trabalho, percorremos sobre a Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709, de 14 de agosto de 2018), conhecendo um pouco de sua origem, e as atividades afetadas por ela, e como o ente público é afetado na realização de suas atividades quando necessário o armazenamento, manipulação e transferências de informações entre os diversos setores públicos e privados.

Dentre os diversos entes públicos existentes, o presente trabalho, focou apenas no Instituto Nacional de Seguro Social – INSS, buscando conhecer através de pesquisas bibliográficas como ele se adequou para atender a LGPD, na prestação de seus serviços e atendimento ao cidadão.

Pode-se destacar que a segurança da informação é extremamente importante para o INSS, que é responsável por lidar com informações confidenciais de milhões de cidadãos, como informações de previdência social, dados financeiros e informações pessoais. Sendo vital que ele mantenha esses dados seguros para evitar qualquer tipo de violação de privacidade, fraude ou roubo de identidade. E que o tratamento de dados pessoais pelo INSS é regulado pela Lei Geral de Proteção de Dados Pessoais (LGPD) e pela Lei de Acesso à Informação (LAI).

Na pesquisa foi apresentado que, para o exercício do papel de controlador de dados, o INSS teve que passar por um processo de governança corporativa, que permitiu a implantação do programa de compliance, possibilitando o estudo dos dados a serem tratados, a criação de mapas de riscos e elaboração de plano de ações, a fim de se adequar a legislação referente ao tratamento de dados previstos dos artigos 7º ao 10º da LGPD.

Foi explanado ainda, as legislações utilizadas pelo INSS que permite assegurar o cumprimento das normas solicitadas pela LGPD para a garantia dos dados de seus segurados, dos entes públicos e dos entes privados com os quais são compartilhados dados.

Que os dados pessoais dos segurados são coletados para fins de concessão, manutenção ou revisão de benefícios previdenciários. Sendo que ele só armazena os dados que são estritamente necessários para o desempenho de suas funções e que são autorizados pela lei. Adotando ainda medidas de segurança para protegê-los e evitar o acesso não autorizado ou o uso indevido dessas informações.

Os segurados têm direito a acessar, retificar, atualizar, portar ou excluir seus dados pessoais que estão sob responsabilidade do INSS, conforme previsto na LGPD e na LAI. Sendo que ele também é obrigado a fornecer informações sobre o tratamento de dados pessoais aos segurados, sempre que solicitado.

Por fim, ficou demonstrado que, apesar de todas as ações desenvolvidas pelo INSS, ainda podem ocorrer falhas de segurança ocasionadas por erro humano ou de sistemas, expondo de forma culposa ou dolosa informações contidas em sua base de dados. Dessa forma o titular dos dados tem o direito de reclamar e apresentar denúncias aos órgãos competentes, como a Autoridade Nacional de Proteção de Dados (ANPD) e o Ministério Público. Diante disso, caberá

REVISTA ARTE, CIÊNCIA E TECNOLOGIA DA FACULDADE CET

ações judiciais em desfavor do próprio INSS e a terceiros que venha adquirir as informações sem a conformidade da LGPD.

Referências

ASTELLS, M. A sociedade em rede. A era da informação: economia, sociedade e cultura. **Paz e Terra**, são Paulo, 2016. 96.

BARROS, G.; SCHIMDT, C. SILVA, Documentos públicos e dados pessoais: o acesso sob a ótica da Lei Geral de Proteção de Dados Pessoais e da Lei de Acesso à Informação Pública. **Researchgate**, 5, 2019. 22,39.

BERTOTTI, P. S. D. S. E. A. **Gestão dos documentos e os aspectos da privacidade e proteção de dados pessoais de crianças e adolescentes: um estudo de caso no INSS**. [S.l.]. 2022.

BRASIL. Lei Nº 12.527, DE 18 DE NOVEMBRO DE 2011, Lei de Acesso à Informação - LAI. **planalto**, 2011. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 05 jan. 2023.

BRASIL. Lei Nº 13.709, DE 14 DE AGOSTO DE 2018. **Planalto**, 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 2023 jan. 03.

BRASIL. EMENDA CONSTITUCIONAL Nº 115, DE 10 DE FEVEREIRO DE 2022. **Planalto.gov.br**, 2022. Disponível em: <https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm>. Acesso em: 03 jan. 2023.

CALAZANS, A. T. S. Qualidade da informação: conceitos e aplicações. **Epub**, 20, 2014. 99.

CONI JR., V. V. A cibercidadania como consequência de um novo modelo de governança da gestão de políticas públicas. **Empório e direito**, Florianópolis, 2019. 117.

CONI JR., V. V.; PAMPLONA FILHO, R. A Lei Geral de Proteção de Dados Pessoais e seus impactos no direito do. **Revista Direito UNIFACS**, Salvador, 2020. 249-254.

GOVERNO FEDERAL. A LGPD E O INSS, 2020. Disponível em: <<https://www.gov.br/inss/pt-br/centrais-de-conteudo/publicacoes/apresentacoes/SaibaMaisLGPDINSS.pdf>>. Acesso em: 26 dez. 2022.

LOUREIRO, M. A. V. A Lei Geral de Proteção de Dados e seus reflexos no Direito do Trabalho. **Conteúdo Jurídico**, 2020.

LYRA, M. R. Governança da segurança da informação, Brasília, 2015. n,d.

PAMPLONA FILHO, R.; CONI JUNIOR, V. V. A Lei Geral de Proteção de Dados Pessoais e seus impactos no Direito do Trabalho. **Direito UNIFACS–Debate Virtual**, 2020.

PIURCOSKY, F. P. et al. A Lei geral de proteção de dados pessoais em empresas brasileiras: uma análise de múltiplos casos. **Suma de Negócios**, 2019. 88-99.

RUSSELL, K. D. et al. Digital privacy GDPR: a proposed digital transformation framework. **Association for Information Systems**, p. 1-10, 2018.

REVISTA ARTE, CIÊNCIA E TECNOLOGIA DA FACULDADE CET

SOUZA, R. P. M. D.; BARRANCOS, E. E.; MAIA, M. E. ACESSO A INFORMAÇÃO E AO TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO. **Informação & Sociedade**, 2019.

TAMBOSI, P. V. P. E. A. **Responsabilidade civil pelo tratamento de dados pessoais conforme a Lei Geral de Proteção de Dados (LGPD): subjetiva ou objetiva?** [S.l.]. 2021.

