UNIVERSIDADE ESTADUAL DA PARAÍBA
CAMPUS V – JOÃO PESSOA
CENTRO DE CIÊNCIAS BIOLÓGICAS E SOCIAIS APLICADAS
CURSO DE PÓS-GRADUAÇÃO LATU SENSU EM GESTÃO EM ADMINISTRAÇÃO PÚBLICA

ANTONIO IZIDRO DOS SANTOS NETO

A APLICAÇÃO DA LGPD NA ADMINISTRAÇÃO PÚBLICA, AS SUAS CONSEQUÊNCIAS E PENAS APLICADAS PELO SEU DESCUMPRIMENTO

JOÃO PESSOA
2024

ANTONIO IZIDRO DOS SANTOS NETO

A APLICAÇÃO DA LGPD NA ADMINISTRAÇÃO PÚBLICA, AS SUAS CONSEQUÊNCIAS E PENAS APLICADAS PELO SEU DESCUMPRIMENTO

Trabalho de Conclusão de Curso apresentado à Coordenação do Curso de Especialização em Gestão em Administração Pública da Universidade Estadual da Paraíba em parceria com a Escola de Serviço Público do Estado da Paraíba, como requisito para a obtenção do título de Especialista em Gestão em Administração Pública.

Orientadora: Profª. Dra. Julyana de Lira Fernandes

JOÃO PESSOA
2024

S237a Santos Neto, Antônio Izidro dos.

A aplicação da LGPD na administração pública, as suas consequências e penas aplicadas pelo seu descumprimento [manuscrito] / Antonio Izidro dos Santos Neto. - 2024.

19 p.

Digitado.

Monografia (Especialização Gestão em Administração Pública) - Universidade Estadual da Paraíba, Centro de Ciências Biológicas e Sociais Aplicadas, 2024.

"Orientação : Profa. Dra. Julyana de Lira Fernandes , Especialização em Gestão em Administração Pública - UEPB/ESPEP. "

1. Administração pública. 2. Lei Geral de Proteção de Dados - LGPD. 3. Penalidades. I. Título

21. ed. CDD 351

Elaborada por Elesbao S. Neto - CRB - 15/347 BSC5/UEPB

ANTONIO IZIDRO DOS SANTOS NETO

A APLICAÇÃO DA LGPD NA ADMINISTRAÇÃO PÚBLICA, AS SUAS CONSEQUÊNCIAS E PENAS APLICADAS PELO SEU DESCUMPRIMENTO

Trabalho de Conclusão de Curso apresentado à Coordenação do Curso de Especialização em Gestão em Administração Pública da Universidade Estadual da Paraíba em parceria com a Escola de Serviço Público do Estado da Paraíba, como requisito para a obtenção do título de Especialista em Gestão em Administração Pública.

Aprovado em: 04/07/2024.

BANCA EXAMINADORA

gov.br Documento assinado digitalmente
JULYANA DE LIRA FERNANDES
Data: 17/07/2024 16:12:40-0300
Verifique em https://validar.iti.gov.br

Profa. Dra. Julyana de Lira Fernandes (Orientadora)
Escola do Serviço Público do Estado da Paraíba (ESPEP)

Prof. Dr. José Glaucio Ferreira de Figueiredo
Escola do Serviço Público do Estado da Paraíba (ESPEP)

gov.br Documento assinado digitalmente
MICHELLI LIMA DOS SANTOS FERRARI
Data: 17/07/2024 16:26:18-0300
Verifique em https://validar.iti.gov.br

Profa. Ma. Michelli Lima dos Santos Ferrari
Escola do Serviço Público do Estado da Paraíba (ESPEP)

À minha esposa Lívia Emmily, pelo apoio, dedicação e companheirismo, DEDICO.

SUMÁRIO

A APLICAÇÃO DA LGPD NA ADMINISTRAÇÃO PÚBLICA, AS SUAS CONSEQUÊNCIAS E PENAS APLICADAS PELO SEU DESCUMPRIMENTO

Antonio Izidro dos Santos Neto
Julyana de Lira Fernandes*

RESUMO

O presente estudo aborda a aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) na administração pública, suas consequências e as penas pelo descumprimento. O objetivo geral é analisar a eficiência da aplicação da LGPD no setor público e seus efeitos jurídicos. Os objetivos específicos incluem: apresentar a aplicação da LGPD nas empresas públicas; explanar a importância das penalidades da LGPD pelo seu descumprimento; promover o discernimento da aplicação de sentenças através de casos concretos da LGPD; e demonstrar o fortalecimento da segurança virtual pela lei. Este estudo, realizado por meio de pesquisa qualitativa, descritiva e analítica, com coleta e análise de dados bibliográficos, revela que a implementação da LGPD na administração pública é um desafio. As instituições precisam adaptar seus processos e políticas internas para garantir conformidade com a legislação, reestruturando sistemas de informação, promovendo a conscientização e treinamento dos funcionários, e estabelecendo novas práticas de governança de dados para assegurar a privacidade e proteção dos dados pessoais. Na esfera pública, isso implica maior transparência no tratamento de dados dos cidadãos, ajustando práticas para garantir a proteção da privacidade. O cumprimento da LGPD fortalece a confiança pública e contribui para um ambiente digital mais ético e seguro. A pesquisa também destaca a necessidade urgente de medidas robustas de proteção de dados para prevenir e mitigar os impactos dos vazamentos de informações pessoais, evidenciada pelo aumento significativo de credenciais vazadas na internet em 2021. Conclui-se que a aplicação da LGPD na administração pública não só é necessária para a conformidade legal, mas também crucial para a manutenção da segurança e privacidade dos dados no contexto da digitalização crescente dos serviços públicos.

Palavras-Chave: LGPD; Administração Pública; Conformidade; Penalidades.

* Policial Penal de carreira no Estado da Paraíba, Gestor de Segurança Pública, Graduado em Administração Pública (UEPB), Pós-graduado em Direito Penal e em Auditoria. izidro@gmail.com.
** Doutora e Mestra em Educação (FCU). Pós-graduada em Educação Global, Inteligências Humanas e Construção da Cidadania (FESP), Graduada em Serviço Social (UFPB).

THE APPLICATION OF THE LGPD IN PUBLIC ADMINISTRATION, ITS CONSEQUENCES, AND PENALTIES FOR NON-COMPLIANCE

Antonio Izidro dos Santos Neto
Julyana de Lira Fernandes*

ABSTRACT

The present study addresses the application of the General Data Protection Law (LGPD) in public administration, its consequences, and penalties for non-compliance. The general objective is to analyze the efficiency of LGPD implementation in the public sector and its legal effects. The specific objectives include: presenting the application of LGPD in public companies; explaining the importance of LGPD penalties for non-compliance; promoting the understanding of the application of sentences through concrete cases of LGPD; and demonstrating the strengthening of virtual security by the law. This study, conducted through qualitative, descriptive, and analytical research, with the collection and analysis of bibliographic data, reveals that the implementation of LGPD in public administration is a challenge. Institutions need to adapt their processes and internal policies to ensure compliance with the legislation, restructuring information systems, promoting employee awareness and training, and establishing new data governance practices to ensure the privacy and protection of personal data. In the public sphere, this implies greater transparency in handling citizens' data, adjusting practices to guarantee privacy protection. Compliance with LGPD strengthens public trust and contributes to a more ethical and secure digital environment. The research also highlights the urgent need for robust data protection measures to prevent and mitigate the impacts of personal information leaks, as evidenced by the significant increase in leaked credentials on the internet in 2021. It is concluded that the application of LGPD in public administration is not only necessary for legal compliance but also crucial for maintaining data security and privacy in the context of the growing digitalization of public services.

Keywords: LGPD; Public Administration; Compliance; Penalties.

* Career Penal Police Officer in the State of Paraíba, Public Security Manager, Graduated in Public Administration (UEPB), Postgraduate in Criminal Law and Auditing. izidro@gmail.com
** Ph.D. and Master's in Education (FCU). Postgraduate in Global Education, Human Intelligences, and Citizenship Building (FESP), Graduated in Social Work (UFPB)

1 INTRODUÇÃO

A Lei Geral de Proteção de Dados Pessoais (LGPD) é uma legislação que entrou em vigor no Brasil com o objetivo de estabelecer regras e diretrizes para a coleta, armazenamento, uso e compartilhamento de dados por pessoas jurídicas de Direito Público e Privado, bem como pessoas físicas que tratam dados pessoais com fins econômicos. Dessa forma, pontua-se que o presente trabalho abordará sobre a aplicação da LGPD na administração pública, as suas consequências e penas aplicadas pelo seu descumprimento.

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) estabelece, em seu artigo 6º, os princípios que devem orientar o tratamento de dados pessoais, tais como a finalidade, a adequação, a necessidade, o livre acesso, a qualidade dos dados, a transparência, a segurança, a prevenção, a não discriminação e a responsabilização e a prestação de contas. O artigo 52 prevê as sanções administrativas que podem ser aplicadas pela Autoridade Nacional de Proteção de Dados (ANPD) em casos de descumprimento, incluindo advertência, multa simples ou diária, publicização da infração, bloqueio e eliminação dos dados pessoais envolvidos.

No cenário contemporâneo, a implementação da Lei Geral de Proteção de Dados Pessoais (LGPD) tem desencadeado mudanças significativas na forma como a administração pública lida com informações pessoais. A legislação, que visa assegurar a privacidade e a segurança dos dados dos cidadãos, estabelece uma série de normas e diretrizes a serem seguidas. Contudo, a relevância da LGPD não se limita apenas ao estabelecimento de direitos e deveres, pois a lei também prevê penalidades específicas para o descumprimento de suas disposições. Diante desse contexto, pontua-se que este trabalho visa responder à seguinte questão problema: Quais as penalidades que são aplicadas por meio da Lei Geral de Proteção de Dados Pessoais na administração pública e quais são os efeitos de sua implantação?

Segundo o relatório da empresa de segurança digital Axur, revelou-se que, apenas no primeiro semestre de 2021, houve um aumento de 493% no número de credenciais vazadas na internet em comparação com o ano anterior. Esses dados sublinham a urgência da aplicação rigorosa da LGPD, destacando a necessidade de medidas robustas de proteção de dados na administração pública para prevenir e mitigar os impactos dos vazamentos de informações pessoais. A inclusão dessas estatísticas na pesquisa oferece um panorama concreto da magnitude dos desafios enfrentados

e reforça a importância de um estudo detalhado sobre a eficácia e a aplicação da LGPD.

Assim, a primeira hipótese a ser levantada é que com o advento da Lei Geral de Proteção de Dados Pessoais houve um aparato jurídico mais fortalecido após a sua vigência a partir de setembro de 2020, em que se conseguiu o deslumbramento de uma segurança jurídica. A segunda hipótese é que a recepção da Lei Geral de Proteção de Dados Pessoais foi bem aceita nas empresas públicas, que devem de forma constante se atualizarem como uma forma de proteção dos dados pessoais dos cidadãos, funcionários e usuários.

A terceira hipótese é que a eficiência da aplicabilidade dessa LGPD resulta em pontos positivos para a sociedade, pois a partir da Lei Carolina Dieckmann ocasionou uma segurança virtual para a sociedade, que por muitas das vezes não tem certeza se os seus dados disponibilizados estão realmente seguros. A quarta hipótese é sobre as decisões judiciais mais recentes e impactantes que a LGPD oportunizou para vítimas no mundo virtual em relação a sua segurança de dados e a sua confiabilidade nos órgãos ou empresas privadas.

Também é imprescindível pontuar que o objetivo geral do trabalho consiste em analisar a eficiência da aplicação da LGPD nas empresas públicas e os efeitos de sua implantação. Os objetivos específicos são: apresentar a aplicação da LGPD nas empresas públicas; explanar a importância das penalidades da LGPD pelo seu descumprimento; promover o discernimento da aplicação de sentenças por meio de casos concretos da LGPD e demonstrar o aparato do fortalecimento da segurança virtual através da LGPD.

Logo, a realização de um trabalho acadêmico sobre a aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) na administração pública, bem como suas consequências e penas pelo seu descumprimento, revela-se fundamental diante do atual contexto, caracterizado pela crescente digitalização de serviços e processos, e que a quantidade de dados pessoais coletados, armazenados e processados aumentou exponencialmente. Com a proliferação de dispositivos conectados e o avanço das tecnologias da informação, a proteção da privacidade e da segurança dos dados tornou-se uma prioridade crucial para garantir a confiança e a segurança dos cidadãos. Em primeiro lugar, a LGPD representa um marco normativo que redefine as relações entre as instituições e os indivíduos no que diz respeito à coleta, tratamento e armazenamento de dados pessoais. Investigar como essa legislação é implementada na

esfera pública possibilita uma compreensão mais aprofundada das práticas adotadas por organizações e governos para garantir a conformidade com os preceitos legais.

Além disso, a análise das consequências e penas previstas pela LGPD auxilia na criação de mecanismos de responsabilização. Este aspecto ganha relevância diante do crescente volume de informações sensíveis compartilhadas no ambiente digital, exigindo um exame minucioso das estratégias adotadas pelas organizações para evitar violações e, consequentemente, as penalidades associadas. Compreender as nuances das sanções estabelecidas pela legislação é crucial para avaliar a eficácia do seu cumprimento e identificar áreas passíveis de aprimoramento.

Por fim, a investigação sobre as consequências da LGPD na sociedade permite explorar os impactos mais amplos dessas regulamentações, incluindo a proteção efetiva da privacidade dos cidadãos e a promoção de uma cultura de transparência e responsabilidade. Ao examinar de que maneira as mudanças legais afetam a relação entre as instituições e os cidadãos, é possível formular análises críticas sobre os avanços e desafios na proteção de dados, contribuindo assim para o desenvolvimento de estratégias mais robustas e éticas no tratamento das informações pessoais.

Para o autor, esta obra será um diferencial para sua vida pessoal e profissional, pois ajudará na aquisição de conhecimentos, habilidades e competências, contribuindo diretamente para o ganho de experiência e a utilização correta das ferramentas disponíveis na literatura. Dessa forma, cabe ressaltar que este trabalho também contribuirá para a comunidade acadêmica, pois servirá de referência para pesquisas futuras, principalmente na área de direito e LGPD.

A relevância desta pesquisa do ponto de vista social reside na proteção dos direitos fundamentais dos cidadãos em um ambiente digital cada vez mais intrusivo. A aplicação eficaz da LGPD na administração pública garante que informações pessoais sensíveis sejam tratadas com o devido respeito à privacidade e segurança, prevenindo abusos e violações que podem ter consequências devastadoras para os indivíduos. Além disso, ao promover a transparência e a responsabilidade nas práticas de gestão de dados, a pesquisa contribui para o fortalecimento da confiança da população nas instituições públicas. Isso, por sua vez, fomenta uma cultura de respeito aos direitos de privacidade e encoraja comportamentos mais éticos e responsáveis no trato das informações pessoais, beneficiando a sociedade como um todo ao assegurar que os dados dos cidadãos sejam protegidos de maneira adequada e justa.

2 REFERENCIAL TEÓRICO

2.1 ADMINISTRAÇÃO PÚBLICA E A LGPD

A segurança da informação tornou-se uma questão central na era digital, impulsionada pela rápida expansão da tecnologia e pela crescente quantidade de dados pessoais gerados diariamente. A Lei Geral de Proteção de Dados Pessoais surge como uma ferramenta à necessidade urgente de proteger a privacidade e a confidencialidade das informações, impondo ao setor público a responsabilidade de adotar medidas rigorosas nesse sentido (Montolli, 2020).

Na Administração Pública, a LGPD exige uma abordagem proativa para garantir a segurança dos dados pessoais sob sua custódia. Ambos os setores, embora distintos em suas operações, compartilham a responsabilidade de implementar políticas robustas de segurança cibernética. Essas políticas não se limitam apenas à proteção contra ameaças externas, mas também à conscientização interna, ao treinamento de pessoal e à criação de uma cultura organizacional que valorize a segurança da informação (Magacho; Trento, 2021).

Dessa forma, no âmbito da Administração Pública, agências governamentais lidam com uma variedade de dados sensíveis, desde informações fiscais até dados relacionados à saúde e segurança nacional. A implementação eficaz da segurança da informação nesse setor requer não apenas a adoção de tecnologias avançadas de proteção, mas também a atualização constante de protocolos de segurança para enfrentar ameaças em constante evolução. Além disso, é crucial envolver os funcionários em programas de treinamento para que compreendam a importância de práticas seguras e estejam cientes das últimas ameaças cibernéticas.

A LGPD impõe a necessidade de uma avaliação criteriosa dos riscos associados ao tratamento de dados pessoais, incentivando a implementação de medidas proporcionais a esses riscos. Isso inclui a criptografia de dados, controles de acesso rigorosos, monitoramento constante de sistemas e a incorporação de práticas de segurança desde o design de novos produtos ou serviços (Montolli, 2020).

A realização de avaliações de riscos é uma etapa crucial para a Administração Pública. Identificar potenciais vulnerabilidades nos sistemas e processos é essencial para desenvolver estratégias de mitigação eficazes. Essas avaliações devem ser realizadas regularmente, dada a dinâmica do cenário de ameaças cibernéticas, e devem

levar em consideração não apenas os aspectos técnicos, mas também os fatores humanos e organizacionais que podem influenciar a segurança da informação (Magacho; Trento, 2021).

Outro ponto vital é a pronta resposta a incidentes de segurança. A LGPD exige que organizações estejam preparadas para identificar, conter e notificar incidentes de violação de dados. A rapidez na resposta pode minimizar os danos e preservar a confiança dos usuários afetados. Isso requer a implementação de planos de resposta a incidentes, testes regulares desses planos e a cooperação com órgãos reguladores e autoridades competentes (Lima et al. 2019).

Neste sentido, a implementação eficaz da segurança da informação não é apenas uma questão técnica, mas também uma questão cultural. Evidencia-se a necessidade de criar uma cultura organizacional que promova a conscientização sobre segurança, incentivando práticas responsáveis no manuseio de dados pessoais. Isso envolve não apenas a alta administração, mas todos os níveis da organização (Montolli, 2020).

Ressalta-se ainda que a transparência e prestação de contas emergem como pilares fundamentais na era da informação, ganhando ainda mais destaque com a implementação da Lei Geral de Proteção de Dados Pessoais (LGPD). Tanto na Administração Pública quanto na iniciativa privada, a necessidade de comunicar de maneira clara e eficaz como os dados pessoais são tratados representa não apenas uma obrigação legal, mas um compromisso ético com a privacidade e a confiança dos indivíduos (Magacho; Trento, 2021).

A LGPD, ao destacar a importância da transparência no tratamento de dados pessoais, busca assegurar que os cidadãos compreendam plenamente como suas informações são coletadas, processadas e armazenadas. Esse requisito vai além de simplesmente divulgar políticas de privacidade; exige uma comunicação acessível e compreensível, garantindo que mesmo os leigos em questões tecnológicas possam entender o destino de suas informações pessoais (Lima et al. 2019).

Na Administração Pública, a transparência no tratamento de dados torna-se ainda mais crucial, dada a natureza sensível das informações muitas vezes sob custódia do governo. Os cidadãos têm o direito de saber como suas informações são utilizadas pelos órgãos públicos, seja para a prestação de serviços, formulação de políticas ou outros propósitos. Os governos devem adotar práticas transparentes que

incluam a divulgação ativa de informações sobre o tratamento de dados, promovendo assim uma relação mais aberta e confiável com os cidadãos (Montolli, 2020).

Além da transparência, a LGPD também destaca a necessidade de prestação de contas por parte das organizações. Isso implica que as entidades devem estar preparadas para prestarem contas às autoridades reguladoras, em caso de questionamentos sobre a conformidade com a legislação de proteção de dados. A prestação de contas não é apenas uma resposta a possíveis violações, mas também uma demonstração proativa de responsabilidade e compromisso com a privacidade (Lima et al. 2019).

A implementação eficaz desses princípios requer a criação de políticas claras e procedimentos internos, e também o desenvolvimento de uma cultura organizacional que valorize a transparência e a responsabilidade no tratamento de dados. Princípios fundamentais da LGPD, como o princípio da finalidade, que determina que o tratamento de dados deve ser feito para propósitos legítimos, específicos e explícitos; o princípio da adequação, que exige que os dados sejam limitados ao mínimo necessário para a realização de suas finalidades; e o princípio da transparência, que assegura que os titulares sejam informados de forma clara e acessível sobre o tratamento de seus dados, são essenciais para orientar a elaboração dessas políticas. Além disso, o princípio da responsabilização implica que as organizações devem ser capazes de demonstrar conformidade com a LGPD, adotando medidas técnicas e organizacionais que garantam a proteção adequada dos dados pessoais sob sua responsabilidade. Portanto, a criação de uma cultura organizacional que promova a transparência e a responsabilidade no tratamento de dados não apenas fortalece a conformidade com a LGPD, mas também contribui para a construção de um ambiente confiável e ético no cenário digital.

3 MATERIAL E MÉTODOS

Esta revisão bibliográfica foi realizada por meio de uma pesquisa qualitativa, de caráter analítico e descritivo, com o objetivo de analisar a aplicabilidade da Lei Geral de Proteção de Dados Pessoais no âmbito da administração pública e sobre as consequências e penalidades pelo seu descumprimento. Ressalta-se ainda que foi realizada uma revisão de literatura para ampliar ainda mais as informações para contextualizar a proposta. Autores como Alencar (2023), em seu trabalho sobre a Lei Geral

de Proteção de Dados – LGPD e segurança na internet; Kremer (2020) que discute os agentes de tratamento de dados pessoais e o novo marco normativo do Brasil; e Magacho e Trento (2021) em seu estudo sobre LGPD e compliance na Administração Pública, contribuíram significativamente para embasar teoricamente esta pesquisa.

Assim, a pesquisa bibliográfica utiliza várias concepções teóricas como base para a obtenção de respostas, com o objetivo de adquirir um embasamento suficiente para sustentar a pesquisa e explicitar os diferentes pontos de vista dos atores que já escreveram ou argumentaram algum tópico sobre o assunto.

Para o desenvolvimento dessa pesquisa foram usados artigos, livros, revistas, resumos e e-Books. Contudo, ressalta-se que visando aumentar o número de dados e informações captados para melhor compreensão acerca do tema foram utilizadas as bases de dados de fontes documentais e bibliográficas, além da base de dados do Poder Executivo Federal, proporcionando maiores informações e aprofundamento do objeto de estudo.

Também é de suma importância pontuar que durante as pesquisas e buscas nos periódicos foram consideradas as palavras relacionadas ao tema como palavras-chave, como por exemplo: LGPD, administração pública e penas, dessa forma houve uma otimização do tempo na busca dos artigos, bem como uma facilitação na busca dos periódicos que serão de suma importância para o desenvolvimento do trabalho e o alcance dos objetivos propostos inicialmente.

4 RESULTADOS E DISCUSSÃO

4.1 PENAS APLICADAS PARA O DESCUMPRIMENTO DA LGPD

No contexto da Lei Geral de Proteção de Dados Pessoais (LGPD), as sanções impostas pela Autoridade Nacional de Proteção de Dados (ANPD) desempenham um papel crucial na promoção da conformidade e na garantia da proteção dos dados pessoais. A advertência, como primeira medida punitiva, representa um alerta inicial para as organizações que não estão em conformidade com as normas estabelecidas pela legislação (Santos; Duarte, 2022).

A advertência, mencionada no primeiro estágio de descumprimento da LGPD, atua como um sinal de que práticas ou processos específicos da organização estão em desacordo com as normas de proteção de dados. Esse alerta tem como objetivo

não apenas identificar as irregularidades, mas também instigar a empresa a tomar as medidas necessárias para ajustar seus procedimentos internos, adequando-se às exigências legais. Nesse estágio, a ANPD busca promover a conscientização sobre a importância da conformidade com a LGPD, oferecendo à organização a oportunidade de corrigir suas práticas antes que medidas mais severas sejam aplicadas (Kremer, 2020).

No caso de infrações menos graves, a LGPD prevê a aplicação de multas simples, que podem chegar a 2% do faturamento da empresa, com um limite de R$ 50 milhões por infração, representando uma penalidade financeira significativa. A imposição de multas simples visa não apenas punir a organização infratora, mas também dissuadir outras empresas de cometerem violações semelhantes. Além disso, as multas simples servem como uma forma de compensação pelo dano causado e como um incentivo para que as organizações invistam em práticas que estejam em conformidade com a LGPD (Alencar, 2023).

No estágio seguinte, a ANPD adota uma abordagem mais intensiva em casos de descumprimento continuado da legislação. Essas multas diárias são aplicadas até que a organização demonstre a implementação de medidas corretivas eficazes. Essa medida visa garantir que a empresa não apenas corrija as irregularidades, mas também estabeleça práticas sustentáveis a longo prazo que estejam alinhadas com os requisitos da LGPD. A imposição de multas diárias destaca a importância da celeridade na correção de falhas e na implementação de medidas efetivas de conformidade (Santos; Duarte, 2022).

Dentro do arcabouço da Lei Geral de Proteção de Dados Pessoais (LGPD), as medidas punitivas da ANPD assumem uma importância crucial para assegurar a conformidade das organizações com os padrões rigorosos de proteção de dados pessoais. No contexto da LGPD, a suspensão do tratamento de dados é uma das medidas que pode ser determinada em resposta a infrações cometidas por uma empresa (Kremer, 2020).

A suspensão temporária do tratamento de dados pessoais representa uma intervenção mais severa por parte da ANPD. Essa medida é acionada quando a gravidade das irregularidades demanda uma pausa imediata nas operações de tratamento de dados da organização infratora. O propósito central da suspensão é proteger os titulares dos dados, interrompendo temporariamente qualquer atividade que possa comprometer a privacidade e a segurança das informações pessoais. Essa pausa no

tratamento fornece à empresa o tempo necessário para tomar as medidas corretivas essenciais e que se possa alinhar totalmente aos requisitos estabelecidos pela LGPD (Alencar, 2023).

Outra medida que pode ser adotada pela ANPD é o bloqueio dos dados pessoais relacionados à infração, restringindo o acesso, impedindo qualquer manipulação ou utilização dessas informações enquanto a situação é investigada e corrigida. Embora os dados permaneçam armazenados, a intervenção da ANPD, por meio do bloqueio, assegura que nenhum dado adicional seja processado, garantindo uma pausa efetiva nas atividades que levaram à infração. Essa medida não apenas protege os titulares dos dados, mas também viabiliza uma análise aprofundada da situação, contribuindo para uma resolução adequada do problema (Santos; Duarte, 2022).

No entanto, em situações mais graves de descumprimento da LGPD, a ANPD pode determinar a eliminação dos dados pessoais relacionados à infração. Essa medida extrema é aplicada quando a continuidade do tratamento representa um risco significativo à privacidade dos titulares dos dados. A eliminação dos dados é uma resposta assertiva a violações graves, visando interromper imediatamente qualquer tratamento que possa resultar em danos irreparáveis à privacidade dos indivíduos. Essa medida serve como uma advertência enfática e como uma salvaguarda para proteger os direitos dos titulares dos dados (Kremer, 2020).

No universo complexo da Lei Geral de Proteção de Dados Pessoais (LGPD), a publicização da infração surge como uma ferramenta estratégica nas mãos da Autoridade Nacional de Proteção de Dados para reforçar a importância da conformidade com as normas estabelecidas. Essa medida, quando aplicada, permite que a ANPD torne pública a infração cometida por uma empresa, juntamente com as medidas adotadas para corrigir as violações da LGPD. A essência por trás desse mecanismo é clara: informar o público sobre violações significativas e promover a transparência no tratamento de dados (Alencar, 2023).

Ao tornar a infração pública, a ANPD não apenas expõe as práticas inadequadas de uma organização, mas também busca conscientizar a sociedade sobre a seriedade das questões relacionadas à proteção de dados. A publicização age como um instrumento educativo, incentivando empresas e indivíduos a compreenderem as implicações de não seguir os protocolos adequados estabelecidos pela LGPD. Além

disso, a exposição pública tem o potencial de influenciar a reputação da empresa infratora, proporcionando uma motivação adicional para que outras organizações evitem cair nas mesmas práticas não conformes (Santos; Duarte, 2022).

No contexto da LGPD, o conceito de responsabilização civil refere-se à capacidade dos titulares de dados pessoais de buscar reparação por danos morais e materiais decorrentes do tratamento inadequado de suas informações. A legislação estabelece que os titulares têm o direito de exigir indenização caso sofram prejuízos em virtude do descumprimento das normas de proteção de dados. Isso inclui situações em que ocorre o vazamento de informações pessoais sensíveis, acesso não autorizado a dados, uso indevido de informações para fins diferentes dos especificados ou qualquer outra prática que comprometa a segurança e a privacidade dos dados dos indivíduos.

Por exemplo, se uma empresa sofre um incidente de segurança de dados devido à falta de medidas adequadas de proteção, resultando na exposição de dados pessoais de seus clientes, esses clientes têm o direito de buscar compensação por eventuais danos emocionais ou financeiros sofridos. Além disso, violações como a coleta excessiva de informações sem consentimento adequado, o não fornecimento de informações claras sobre como os dados serão utilizados ou compartilhados, ou o não cumprimento de direitos garantidos aos titulares (como o direito de acesso, correção e exclusão de dados) também podem levar à responsabilização civil.

Portanto, a responsabilização civil prevista na LGPD não apenas visa punir as empresas infratoras com penalidades financeiras, mas também proteger os direitos dos indivíduos afetados, proporcionando uma via eficaz para a reparação de danos e incentivando a conformidade com as normas de proteção de dados pessoais.

Além das penalidades administrativas e da responsabilização civil, a LGPD estabelece a responsabilização criminal. Essa disposição é aplicada a condutas mais graves, incluindo situações de má-fé em que a obtenção não autorizada de dados pessoais é realizada com a intenção de obter vantagem indevida. A responsabilização criminal implica consequências mais sérias, como processos judiciais e sanções criminais, visando desencorajar comportamentos deliberadamente prejudiciais relacionados à manipulação inadequada de dados pessoais (Alencar, 2023).

Por fim, é crucial destacar que as penalidades podem variar em conformidade com a gravidade da infração, o impacto sobre os titulares dos dados e as circunstân-

cias específicas de cada caso. A LGPD visa assegurar que as sanções sejam proporcionais às violações, fomentando, assim, a conformidade e a efetiva proteção dos dados pessoais.

5 CONSIDERAÇÕES FINAIS

Primeiramente, destaca-se que o objetivo geral e os objetivos específicos do trabalho foram alcançados, ou seja, por meio da pesquisa de revisão bibliográfica foi possível analisar a eficiência da aplicação da LGPD no setor público e os efeitos de sua implantação, bem como apresentar a aplicação da LGPD; explanar a importância das penalidades da LGPD pelo seu descumprimento; promover o discernimento da aplicação de sentenças por meio de casos concretos da LGPD e demonstrar o aparato do fortalecimento da segurança virtual através da LGPD.

No cenário digital em constante evolução, os desafios da cibersegurança no Brasil são cada vez mais relevantes. A crescente digitalização de dados acarreta ameaças significativas, como ataques cibernéticos e vazamentos de informações sensíveis. A proteção contra essas ameaças exige investimentos em tecnologias avançadas, capacitação de profissionais e estratégias abrangentes para proteger organizações e indivíduos.

Assim, com base na pesquisa, analisa-se que a Lei Geral de Proteção de Dados Pessoais representa um marco normativo significativo no Brasil, estabelecendo diretrizes claras para o tratamento de dados pessoais, conferindo aos cidadãos maior controle sobre seus dados. Suas disposições impactam empresas, órgãos públicos e demais entidades que lidam com dados, exigindo a implementação de práticas transparentes e seguras.

Dessa forma, ressalta-se que com a LGPD, o tratamento de dados adquire uma dimensão crucial, impondo às organizações a responsabilidade de assegurar a conformidade com as normas de privacidade. A legislação (Lei Geral de Proteção de Dados - Lei nº 13.709/2018) destaca a necessidade de consentimento claro e informado, além de medidas robustas de segurança. A responsabilização torna-se um princípio fundamental, exigindo que empresas e entidades sejam capazes de comprovar a adequação de suas práticas, sob pena de sanções administrativas e outras penalidades caso descumpram as disposições legais.

A capacitação dos colaboradores, a criação de mecanismos de auditoria interna e a realização de revisões regulares são elementos-chave para garantir a conformidade contínua e aprimorar as práticas de transparência e prestação de contas ao longo do tempo (Montolli, 2020).

Neste sentido, a implementação da LGPD no setor público apresenta desafios significativos. É necessário adaptar os processos e políticas internas para garantir total conformidade com as exigências rigorosas estabelecidas pela legislação. Isso implica em promover maior transparência no tratamento dos dados dos cidadãos, assegurando que sejam utilizados de maneira ética e segura. O cumprimento da LGPD não apenas visa atender aos requisitos legais, mas também fortalecer a confiança da população e promover um ambiente digital mais seguro e ético no serviço público.

Por fim, averígua-se que a Lei Geral de Proteção de Dados Pessoais estabelece um conjunto de medidas punitivas para assegurar a conformidade no tratamento de dados pessoais. A ANPD pode iniciar com advertências, alertando organizações sobre a necessidade de adequação. Multas simples, aplicáveis a infrações menos graves, podem chegar a 2% do faturamento da empresa. Em casos de descumprimento prolongado, multas diárias incentivam a implementação ágil de correções. Medidas mais drásticas incluem a suspensão temporária do tratamento de dados e o bloqueio, com eliminação dos dados em situações graves. A publicização de infrações promove a transparência, enquanto a LGPD também prevê responsabilização civil e criminal, garantindo uma abordagem abrangente na proteção dos dados.

REFERÊNCIAS

BRASIL, Presidência da República. **Lei nº 13.709 de 14 de Agosto de 2018**. Lei Geral de Proteção de Dados Pessoais. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm#art65 . Acesso em: 24 de abril de 2024.

ALENCAR, Larissa. (2023). LEI GERAL DE PROTEÇÃO DE DADOS – LGPD E SEGURANÇA NA INTERNET. **Revista Judicial Brasileira**. 3. 429-447

KREMER, Bianca. **Os agentes de tratamento de dados pessoais.** A LGPD e o novo marco normativo do Brasil. Porto Alegre: Arquipélago, p. 289-318, 2020.

LIMA, Rapôso, C. F., Melo de Lima, H., de Oliveira Junior, W. F., Ferreira Silva, P. A. ., Elaine de Souza Barros, E. . (2019). LGPD - LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS EM TECNOLOGIA DA INFORMAÇÃO: **Revisão Sistemática**. RACE - Revista De Administração Do Cesmac, 4, 58–67.

MAGACHO, Bruna Toledo Piza; TRENTO, Melissa. LGPD e compliance na Administração Pública: O Brasil está preparado para um cenário em transformação contínua dando segurança aos dados da população? É possível mensurar os impactos das adequações necessárias no setor público. **Revista Brasileira de Pesquisas Jurídicas**, v. 2, n. 2, p. 7-26, 2021.

MONTOLLI, Carolina Ângelo. Segurança da informação e da transparência e a proteção de dados na Administração Pública: LGPD, ACESSO À INFORMAÇÃO E OS INCENTIVOS À INOVAÇÃO E À PESQUISA CIENTÍFICA E TECNOLÓGICA NO ÂMBITO DO ESTADO DE MINAS GERAIS. **REVISTA ELETRÔNICA DA PGE-RJ**, v. 3, n. 3, 2020.

PINHEIRO, Patricia Peck. **Proteção de dados pessoais**: comentários à Lei n. 13.709/2018 (LGPD). – São Paulo: Saraiva Educação, 2018.

RELATÓRIO Vazamentos de Dados no Brasil. [S. l.]: Axur, 2021. Disponível em: https://pt.scribd.com/document/583084387/Relato-rio-de-Q1-2021-Vazamentos-de-Dados-no-Brasil. Acesso em: 24 abr. 2024.

SANTOS, Andreia Xavier da Silva; DUARTE, Icaro de Souza. A LEI GERAL DA PROTEÇÃO DE DADOS (LGPD) E SUA APLICAÇÃO NA RELAÇÃO DE TRABALHO. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, v. 8, n. 5, p. 2671-2690, 2022.

TORNAGO, Alessandro. Notícias e artigos. **O que a LGPD tem a ver com o empoderamento digital?** Disponível em: https://www.serpro.gov.br/lgpd/noticias/2020/lgpd-e-empoderamento-digital. Acesso em: 24 abr. 2024.