XXX CONGRESSO NACIONAL DO CONPEDI FORTALEZA - CE

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS I

CARLOS MARDEN CABRAL COUTINHO

JOSÉ RENATO GAZIERO CELLA

YURI NATHAN DA COSTA LANNES

D597

Direito, Governança e novas tecnologias I [Recurso eletrônico on-line] Organização CONPEDI

Coordenadores: Carlos Marden Cabral Coutinho; José Renato Gaziero Cella; Yuri Nathan da Costa Lannes. – Florianópolis: CONPEDI, 2023.

Inclui bibliografia
ISBN: 978-65-5648-813-4
Modo de acesso: www.conpedi.org.br em publicações
Tema: Saúde: Acesso à justiça, Solução de litígios e Desenvolvimento

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direito. 3. Governança e novas tecnologias. XXX Congresso Nacional do CONPEDI Fortaleza - Ceará (3; 2023; Florianópolis, Brasil).

CDU: 34

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

XXX CONGRESSO NACIONAL DO CONPEDI FORTALEZA - CE

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS I

Apresentação

No XXX Congresso Nacional do CONPEDI, realizado nos dias 15, 16 e 17 de novembro de 2023, o Grupo de Trabalho - GT "Direito, Governança e Novas Tecnologias I", que teve lugar na tarde de 15 de novembro de 2023, destacou-se no evento não apenas pela qualidade dos trabalhos apresentados, mas pelos autores dos artigos, que são professores pesquisadores acompanhados de seus alunos pós-graduandos. Foram apresentados 23 (vinte e três) artigos objeto de um intenso debate presidido pelos coordenadores e acompanhado pela participação instigante do público presente na Faculdade de Direito do Centro Universitário Christus - UNICHRISTUS.

Esse fato demonstra a inquietude que os temas debatidos despertam na seara jurídica. Cientes desse fato, os programas de pós-graduação em direito empreendem um diálogo que suscita a interdisciplinaridade na pesquisa e se propõe a enfrentar os desafios que as novas tecnologias impõem ao direito. Para apresentar e discutir os trabalhos produzidos sob essa perspectiva, os coordenadores do grupo de trabalho dividiram os artigos em cinco blocos, quais sejam a) temas de inteligência artificial; b) temas de liberdade de expressão e fake news; c) temas de proteção de dados pessoais; d) temas de cidadania, democracia, constituição e direitos; e e) temas de regulação.

Os artigos que ora são apresentados ao público têm a finalidade de fomentar a pesquisa e fortalecer o diálogo interdisciplinar em torno do tema "Direito, Governança e Novas Tecnologias". Trazem consigo, ainda, a expectativa de contribuir para os avanços do estudo desse tema no âmbito da pós-graduação em direito, apresentando respostas para uma realidade que se mostra em constante transformação.

Os Coordenadores

Prof. Dr. Carlos Marden Cabral Coutinho - Centro Universitário Christus

Prof. Dr. José Renato Gaziero Cella - Atitus Educação

Prof. Dr. Yuri Nathan da Costa Lannes - Faculdade de Direito de Franca

O PAPEL DO DATA PROTECTION OFFICER NA GESTÃO DE VAZAMENTOS DE DADOS E OS DESAFIOS DA LGPD E DA ANPD

THE ROLE OF THE DATA PROTECTION OFFICER IN THE MANAGEMENT OF DATA LEAKS AND THE CHALLENGES OF LGPD AND ANPD

Adriana Rossini
Fernanda Lemos Zanatta
Natalia Maria Ventura da Silva Alfaya

Resumo

Este artigo investiga o papel do DPO na gestão de vazamento de dados e os desafios na implementação da LGPD e no trabalho da ANPD em aplicar as sanções administrativas previstas. A hipótese central questiona se a presença de um DPO bem treinado e com autoridade adequada é um fator determinante na redução da ocorrência e do impacto dos vazamentos de dados em uma organização. Analisa o impacto do DPO na gestão de vazamentos de dados, analisa as perspectivas futuras e os desafios da LGPD e da ANPD, bem como suas atribuições, incluindo a aplicação de sanções administrativas, a orientação às organizações e a promoção da conscientização sobre proteção de dados. O objetivo principal da pesquisa é avaliar os papeis do DPO e da ANPD na mitigação de riscos. Os objetivos específicos incluem a definição e descrição das responsabilidades do DPO, os desafios enfrentados na gestão de vazamentos de dados e a identificação das melhores práticas recomendadas para o DPO, compreender o impacto dessas regulamentações na proteção de dados pessoais, explorando os desafios enfrentados pelas organizações na adaptação às exigências da LGPD e na conformidade com as orientações da ANPD. A metodologia utilizada será hipotético-dedutiva, com base em revisão bibliográfica e análise documental. A pesquisa buscará embasar suas conclusões em evidências e referências científicas, proporcionando uma análise confiável do tema.

Palavras-chave: Encarregado de proteção de dados pessoais, Lgpd, Vazamento de dados, Autoridade nacional de proteção de dados, Sanções administrativas e dosimetria

Abstract/Resumen/Résumé

This article investigates the role of the DPO in managing data leaks and the challenges in implementing the LGPD and the work of the ANPD in applying the expected administrative sanctions. The central hypothesis questions whether the presence of a well-trained DPO with adequate authority is a determining factor in reducing the occurrence and impact of data leaks in an organization. Analyzes the impact of the DPO on the management of data leaks, analyzes the future perspectives and challenges of the LGPD and the ANPD, as well as its duties, including the application of administrative sanctions, guidance to organizations and the promotion of awareness about data protection . The main objective of the research is to evaluate the roles of the DPO and ANPD in mitigating risks. Specific objectives include

defining and describing the responsibilities of the DPO, the challenges faced in managing data breaches and identifying best practices recommended for the DPO, understanding the impact of these regulations on the protection of personal data, exploring the challenges faced by organizations in adapting to the requirements of the LGPD and in compliance with the ANPD guidelines. The methodology used will be hypothetical-deductive, based on a bibliographic review and documentary analysis. The research will seek to base its conclusions on scientific evidence and references, providing a reliable analysis of the topic.

Keywords/Palabras-claves/Mots-clés: Personal data protection officer, Lgpd, Data leak, National data protection authority, Administrative sanctions and dosimetry

1 INTRODUÇÃO

Nos últimos anos, temos testemunhado um aumento exponencial no número de vazamentos de dados, resultando em graves consequências para as organizações e indivíduos afetados. A proteção da privacidade e segurança das informações se tornou uma preocupação primordial na era digital, exigindo abordagens proativas e especializadas para enfrentar esses desafios. Nesse contexto, o papel do *Data Protection Officer* (DPO) ou, Encarregado de Proteção de Dados, emergiu como uma figura fundamental na gestão eficaz de vazamentos de dados e no cumprimento das regulamentações de proteção de dados.

Por outro lado, em um cenário digital que está em constante evolução, a proteção de dados pessoais tornou-se uma preocupação primordial. Em resposta a essa necessidade premente, o governo brasileiro estabeleceu a Autoridade Nacional de Proteção de Dados (ANPD) como a autoridade reguladora responsável por supervisionar e fazer cumprir as disposições da Lei Geral de Proteção de Dados Pessoais (LGPD). Essa legislação inovadora visa salvaguardar a privacidade e os direitos dos indivíduos, fornecendo um arcabouço abrangente para a coleta, uso e processamento de dados pessoais de todos.

Compreender o papel e as responsabilidades da ANPD é fundamental. A ANPD foi criada para atuar como uma vigilante atenta, garantindo a conformidade com a LGPD por meio de mecanismos robustos de fiscalização e aplicação de sanções administrativas. Além disso, a autoridade desempenha um papel crucial na orientação das organizações sobre as melhores práticas de proteção de dados e na promoção da conscientização sobre a importância da proteção da privacidade.

O DPO é um profissional altamente qualificado e responsável por garantir a conformidade com as leis e regulamentos de proteção de dados, bem como por promover uma cultura de segurança da informação dentro de uma organização. Sua atuação abrange uma série de responsabilidades e funções essenciais, desde a interface com a alta administração até o monitoramento e implementação de políticas de privacidade e segurança de dados.

Neste artigo científico, investigaremos em detalhes o papel do DPO na gestão de vazamento de dados, analisando suas responsabilidades e funções-chave. Exploraremos a importância da interface entre o DPO e a alta administração, destacando a necessidade de uma colaboração efetiva para garantir a proteção adequada dos dados. Além disso, examinaremos o monitoramento e implementação de políticas de privacidade e segurança de dados, discutindo as melhores práticas para garantir a conformidade e mitigar os riscos de vazamento. Avaliar e

mitigar os riscos de vazamento de dados é uma tarefa complexa e desafiadora, considerando a constante evolução das ameaças cibernéticas e técnicas utilizadas pelos invasores. Portanto, iremos analisar as estratégias e abordagens adotadas pelo DPO para identificar e reduzir os riscos de vazamento, levando em consideração a natureza dinâmica desse ambiente de segurança.

Além disso, exploraremos a resposta a incidentes de segurança e o desenvolvimento de planos de ação eficazes. A rápida identificação e resposta a um vazamento de dados são cruciais para minimizar seu impacto e mitigar danos adicionais. Portanto, analisaremos as melhores práticas para garantir uma resposta ágil e coordenada, envolvendo todas as partes interessadas relevantes.

Através desta análise abrangente do papel do DPO na gestão de vazamento de dados, nosso objetivo é oferecer informações valiosas para profissionais da área, pesquisadores e organizações que buscam aprimorar suas estratégias de proteção de dados. Ao explorar as responsabilidades e funções do DPO, sua interação com a alta administração, o monitoramento de políticas, a avaliação de riscos, a resposta a incidentes e os planos de ação, pretendemos contribuir para o fortalecimento da segurança da informação e garantir a conformidade com as regulamentações de proteção de dados.

Adicionalmente, é de suma importância refletir sobre as perspectivas futuras e os desafios emergentes na aplicação da LGPD e no trabalho contínuo da ANPD. Diante do constante avanço tecnológico e das mudanças de paradigma na proteção de dados, novas questões e demandas surgem constantemente. Portanto, identificar possíveis melhorias e aprimoramentos na LGPD e na atuação da ANPD, baseando-se em experiências internacionais e nas necessidades locais, assume uma tarefa de extrema relevância para aprimorar ainda mais a proteção de dados pessoais no contexto brasileiro.

A investigação minuciosa das sanções administrativas previstas na Lei Geral de Proteção de Dados (LGPD) e a forma como a Autoridade Nacional de Proteção de Dados (ANPD) as aplica diante de violações tornam-se de suma importância neste estudo científico. Além disso, é imperativo realizar uma análise aprofundada do impacto da LGPD e da atuação da ANPD nas organizações e na sociedade como um todo. Esse exame minucioso permitirá avaliar os desafios enfrentados pelas organizações ao se adequarem às exigências da LGPD e às orientações da ANPD, bem como os efeitos benéficos da LGPD e do trabalho da autoridade reguladora na proteção da privacidade dos indivíduos e no fortalecimento de uma cultura de proteção de dados no Brasil. Destaca-se que, recentemente, no dia 27 de fevereiro de 2023, foi publicado o Regulamento de Dosimetria e Aplicação de Sanções Administrativas pela

Autoridade Nacional de Proteção de Dados. A chamada “norma de dosimetria” foi bastante esperada pela sociedade, por tratar da atuação sancionadora da ANPD, proporcionando, assim, o devido reforço à atuação fiscalizatória da Autoridade. A aprovação aconteceu em deliberação eletrônica do Conselho Diretor da ANPD e trouxe, também, alteração da Resolução ANPD nº 1, que trata das regras para o processo de fiscalização e para o processo administrativo sancionador da Autoridade, sendo que, a sanção administrativa é apenas uma das ferramentas que a Autoridade possui para reconduzir o agente de tratamento de dados pessoais à conformidade com a Lei Geral de Proteção de Dados Pessoais - LGPD.

Neste contexto, este estudo visa lançar luz sobre as complexidades do cenário atual de proteção de dados e o papel essencial do DPO e da ANPD na mitigação de riscos, promoção da conformidade e defesa da privacidade na era digital. Como a proteção de dados tornou-se uma prioridade inegável, a colaboração eficaz entre profissionais, organizações e autoridades reguladoras é fundamental para enfrentar os desafios emergentes e garantir um futuro mais seguro para as informações pessoais.

2 DA SEGURANÇA E PROTEÇÃO DE DADOS: O PAPEL DO ENCARREGADO DE DADOS

A dignidade inerente à pessoa humana, entendida como o valor intrínseco que identifica cada indivíduo como ser humano (SARLET, 2006, p. 40), amplia sua abrangência e, consequentemente, exige maior proteção jurídica. É indubitável que a dignidade humana está intrinsecamente ligada aos direitos fundamentais.

Diante dessa compreensão abrangente da dignidade da pessoa humana, emerge um debate crucial sobre a inclusão dos dados pessoais nesse conceito e, portanto, sua conexão com os direitos fundamentais. Tal pressuposto se faz necessário para garantir, sob o amparo jurídico, a proteção adequada desses dados.

No âmbito do ordenamento jurídico brasileiro, a Constituição Federal de 1988 estabelece diversos direitos e garantias fundamentais, sendo alguns deles diretamente relacionados à proteção de dados pessoais. O artigo 5º, inciso XII, assegura a inviolabilidade do sigilo da correspondência, comunicações telegráficas, de dados e comunicações telefônicas, exceto em casos de persecução penal. Além disso, o inciso LXXII do mesmo artigo prevê o habeas data, que permite o acesso a informações constantes de registros ou bancos de dados de entidades governamentais ou públicas, bem como a retificação desses dados. A Constituição

também protege a intimidade, a vida privada, a honra e a imagem das pessoas, considerando-as invioláveis conforme o artigo 5º, inciso X. No entanto, a garantia constitucional da privacidade, embora importante, não é suficiente para abranger integralmente a disciplina da proteção de dados pessoais, o que pode limitar sua abrangência. No contexto da era da informação, algumas decisões judiciais têm se destacado na preocupação de garantir a proteção dos dados pessoais dos indivíduos. Entre elas, mencionam-se as decisões proferidas pelo Supremo Tribunal Federal (STF) em casos como a ADI nº 6387, 6389, 6390 e 633, a ADPF nº 695 e os Recursos Extraordinários nº 1055941 e nº 9738379, que abordaram questões relevantes relacionadas ao compartilhamento de dados e à proteção dos direitos individuais (Gesta Leal, 2023).

Essas manifestações jurisprudenciais evidenciam que políticas públicas envolvendo a coleta, armazenamento, tratamento e compartilhamento de dados já estão sendo implementadas no Brasil, com tendência de expansão. Nesse sentido, a proteção de dados não se restringe apenas à segurança dos dados em si, mas também abrange a proteção contra os efeitos das informações contidas nesses dados para seus titulares. Portanto, a regulamentação da proteção de dados no setor público deve considerar os legítimos interesses individuais e os impactos desejados pelo Estado no tratamento de dados pessoais.

Diante da relevância do tema acerca da proteção de dados pessoais, no Brasil, é promulgada a então chamada Lei Geral de Proteção de Dados Pessoais (LGPD), instituída através do nº13.709 de 14 de agosto de 2018, que teve como base o Regulamento Geral de Proteção de Dados da União Europeia (RGPD).

Apesar de representar um avanço na legislação brasileira para garantir o direito fundamental à proteção de dados pessoais, a Lei Geral de Proteção de Dados (LGPD) possui exceções em sua aplicabilidade. O artigo 4º, inciso III, da LGPD estabelece que a lei não se aplica ao tratamento de dados pessoais exclusivamente para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de crimes. Além disso, o §1º do mesmo artigo ressalta que o tratamento desses dados pessoais mencionados no inciso III deve ser regulado por legislação específica, resultando em uma lacuna normativa sobre o tema (Gesta Leal, 2023).

Diante da ausência de regulamentação específica no âmbito da proteção de dados na segurança pública no ordenamento jurídico brasileiro, juntamente com a crescente utilização de tecnologias avançadas para fins de investigação e repressão penal, foi instituída, por meio de um Ato do Presidente da Câmara dos Deputados em 26 de novembro de 2019, uma Comissão de Juristas com o propósito de realizar estudos e elaborar um anteprojeto de lei que preencha essa

lacuna legal. Essa iniciativa visa estabelecer a regulamentação adequada e o controle legislativo desses processos, garantindo a proteção dos direitos fundamentais envolvidos.

A Comissão de Juristas encaminhou à Câmara dos Deputados o Anteprojeto de Lei de Proteção de Dados para Segurança Pública e Persecução Penal (LGPD Penal), acompanhado de uma exposição de motivos que busca apresentar a necessidade, a estrutura e os principais conceitos da proposta legislativa destinada a regular o tratamento de dados no âmbito da segurança pública e das atividades de investigação e repressão de infrações penais. É imprescindível destacar que tanto a Lei Geral de Proteção de Dados Pessoais (LGPD) brasileira quanto o projeto de lei em análise, que trata da proteção de dados no contexto da segurança pública e persecução penal, possuem aplicabilidade no tratamento de dados. Essa abrangência engloba todas as operações realizadas em dados pessoais ou conjuntos de dados, independentemente do uso de meios automatizados, incluindo coleta, armazenamento, organização, modificação, avaliação, entre outros, ao longo de todo o ciclo de vida desses dados.

O projeto de lei em questão tem como objetivo estabelecer normas claras para o tratamento de dados pessoais conduzido por autoridades competentes nas atividades de segurança pública e persecução penal. Essa regulamentação busca salvaguardar os direitos fundamentais de liberdade, privacidade e livre desenvolvimento da personalidade das pessoas naturais, de maneira consistente e coerente (Brasil, 2018).

O controle estrito por parte da sociedade e dos órgãos de controle é essencial diante da implementação de políticas públicas que envolvem o acesso e manipulação de dados para fins de interesse público. Isso se torna ainda mais importante quando regulamentos específicos estão em jogo, pois podem apresentar fragilidades normativas e estruturais. O projeto, de forma simplificada, busca atribuir responsabilidades às autoridades de investigação no tratamento de dados, abrangendo princípios, finalidades, acesso, e descarte de dados. Além disso, requer autorização judicial para o compartilhamento de dados, mesmo entre autoridades. O projeto de lei demonstrou acerto ao estabelecer uma espécie de “cadeia de custódia” para as operações de tratamento de dados pessoais, regulamentada nos artigos 32 a 34. Essa abordagem busca garantir, pelo menos em termos formais, procedimentos e protocolos uniformes para o registro dessas operações, proporcionando segurança a todos os envolvidos no acesso e manipulação de dados pessoais.

No que se refere à segurança e sigilo dos dados pessoais abordados pelo projeto, o artigo 36 estipula que os agentes de tratamento devem adotar medidas técnicas e administrativas de segurança capazes de proteger os dados pessoais contra acesso não autorizado e situações

acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. Além disso, impõe aos órgãos públicos a adoção de políticas, protocolos e procedimentos adequados e eficientes para essa finalidade, sob pena de responsabilização pelos danos decorrentes. No entanto, é importante ressaltar que a implementação dessas medidas de segurança requer recursos consideráveis, como orçamentários, logísticos, tecnológicos, pessoal e infra estruturais. Isso ocorre porque os repositórios de dados envolvidos são igualmente vastos, tanto em termos físicos quanto virtuais, e abrangem diversas naturezas de informações (como origem facial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dados relacionados à saúde ou à vida sexual, dados genéticos ou biométricos, situação socioeconômica, entre outros).

No que se refere à segurança e sigilo dos dados pessoais abordados pelo projeto, o artigo 36 estipula que os agentes de tratamento devem adotar medidas técnicas e administrativas de segurança capazes de proteger os dados pessoais contra acesso não autorizado e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. Além disso, impõe aos órgãos públicos a adoção de políticas, protocolos e procedimentos adequados e eficientes para essa finalidade, sob pena de responsabilização pelos danos decorrentes.

No entanto, é importante ressaltar que a implementação dessas medidas de segurança requer recursos consideráveis, como orçamentários, logísticos, tecnológicos, pessoal e infra estruturais. Isso ocorre porque os repositórios de dados envolvidos são igualmente vastos, tanto em termos físicos quanto virtuais, e abrangem diversas naturezas de informações (como origem facial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dados relacionados à saúde ou à vida sexual, dados genéticos ou biométricos, situação socioeconômica, entre outros).

De acordo com Danilo Doneda e Laura Mendes (2018, p. 469), a Lei Geral de Proteção de Dados apresenta cinco elementos centrais que sustentam a proteção dos direitos dos titulares de dados: i) aplicação unificada e abrangente da lei; ii) legitimidade para o tratamento de dados (situações autorizativas); iii) princípios e direitos do titular; iv) obrigações dos agentes de tratamento de dados; v) responsabilização dos agentes envolvidos (Mendes, 2018). A partir desses elementos, inicialmente poderíamos inferir que a Lei Geral de Proteção de Dados se aplicaria também à jurisdição penal, devido à sua abrangência e universalidade, ou seja, seria uma lei geral. No entanto, essa possibilidade não se concretiza ao analisarmos o artigo 4º, III,

que exclui expressamente as atividades de tratamento de dados pessoais relacionadas à segurança pública, defesa nacional, segurança do Estado ou investigação e repressão de crimes.

Um dos principais problemas surge quando examinamos além do artigo 4º, o artigo 33, III, que estabelece que a transferência internacional de dados pessoais só é permitida quando necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, investigação e persecução, de acordo com os instrumentos do direito internacional (Brasil, 2018). Em outras palavras, enquanto a lei não é aplicável às investigações criminais nacionais, ela trata da possível cooperação internacional entre as autoridades estrangeiras e as brasileiras. Diante desse cenário, surge a questão se a Lei Geral de Proteção de Dados agiu corretamente ao abordar o assunto dessa forma, ou se uma oportunidade importante de regulamentação foi perdida.

A legislação para a proteção a dados pessoais na sociedade informatizada é uma preocupação que remonta, pelo menos, a 1981, quando foi concluída a Convenção do Conselho da Europa para a proteção das pessoas relativamente ao tratamento automatizado de dados de caráter pessoal.

Considerando as estreitas relações econômicas, culturais e jurídicas que o Brasil mantém com a Europa, outros países também seguiram o exemplo europeu ao implementar uma legislação abrangente de proteção de dados. Nesse contexto, o Brasil não poderia deixar de estabelecer um conjunto de direitos e obrigações relacionados a esse tema em sua legislação nacional. Assim, em 2018, o Congresso Nacional aprovou a Lei Geral de Proteção de Dados (Lei n. 13.709/2018), que foi fortemente influenciada pelo Regulamento Geral de Proteção de Dados (GDPR) da União Europeia. No entanto, os legisladores brasileiros optaram por adiar a regulamentação da proteção de dados pessoais no contexto da segurança pública e da persecução penal (Brasil, 2018).

3 O PAPEL DO DPO NA GESTÃO DE VAZAMENTO DE DADOS

No atual contexto, em que incidentes de segurança envolvendo dados pessoais se tornaram cada vez mais frequentes, compreender o papel do *Data Protection Officer* (DPO) na gestão dessas violações é de suma importância. O DPO desempenha uma função fundamental na mitigação de riscos e na garantia da conformidade com as leis e regulamentações vigentes, atuando como o guardião dos dados pessoais e assegurando a implementação das melhores práticas de proteção de dados.

As responsabilidades e funções do DPO abrangem diversas áreas-chave, sendo crucial para o sucesso da organização. Ele é o responsável por assegurar que medidas de segurança adequadas sejam adotadas para proteger os dados pessoais contra acessos não autorizados, alterações indevidas ou qualquer forma de tratamento inadequado ou ilícito. Além disso, o DPO atua como ponto focal de contato entre a organização, os titulares dos dados e as autoridades de proteção de dados, facilitando a comunicação e garantindo o cumprimento das obrigações legais.

No entanto, a gestão de vazamento de dados apresenta desafios significativos que exigem um constante aprimoramento das práticas e uma adaptação às novas demandas. A evolução contínua das ameaças cibernéticas requer uma atualização constante das melhores práticas de segurança por parte do DPO. Além disso, a complexidade das leis e regulamentações de proteção de dados pode representar um obstáculo para as organizações, exigindo um conhecimento especializado por parte do DPO. Nesse sentido, a colaboração e cooperação com outras áreas da organização, como TI, jurídico e comunicação, são fundamentais para garantir a eficácia das medidas de proteção de dados.

Para enfrentar esses desafios, é essencial que o DPO adote as melhores práticas disponíveis. A educação e o treinamento contínuos são fundamentais para manter-se atualizado sobre as últimas ameaças e soluções de segurança, capacitando o DPO a tomar decisões informadas e implementar medidas eficazes de proteção. Além disso, o uso de medidas de segurança adequadas e tecnologias avançadas, como criptografia e autenticação em dois fatores, auxilia na proteção dos dados contra acessos não autorizados. O desenvolvimento de planos de resposta a incidentes bem estruturados e a colaboração com equipes multidisciplinares permitem uma resposta eficaz em caso de vazamentos de dados, minimizando o impacto causado aos titulares dos dados afetados e garantindo a recuperação segura das informações.

O advento da Lei Geral de Proteção de Dados (LGPD) no Brasil introduziu diversos aspectos jurídicos, sendo um dos principais o papel do DPO (Encarregado de Dados). O DPO é responsável por zelar pela proteção de dados dentro de uma empresa, visando garantir a segurança das informações dos clientes e da própria instituição, conforme estabelecido em lei. Sua atuação não se limita apenas a empresas privadas, mas também pode abranger órgãos públicos, desde que haja a necessidade de alguém responsável pelo tratamento e processamento de dados pessoais. As regras e diretrizes desse profissional são baseadas em regulamentos aprovados na Europa.

O papel do DPO na gestão de vazamento de dados é de extrema importância para garantir a proteção dos dados pessoais e a segurança das informações. Por meio da

implementação das melhores práticas, como a busca por educação contínua, a utilização de medidas de segurança apropriadas e o desenvolvimento de planos de resposta a incidentes, o DPO contribui para a construção de uma cultura sólida de proteção de dados e para a promoção da conformidade legal. A cooperação com outras áreas da organização e a colaboração com equipes multidisciplinares fortalecem a abordagem holística necessária para enfrentar os desafios atuais de segurança da informação.

É imprescindível que o DPO assuma suas responsabilidades com integridade e comprometimento, buscando constantemente aprimorar suas habilidades e conhecimentos. A compreensão aprofundada das leis e regulamentações relacionadas à proteção de dados é essencial para garantir a conformidade em todas as atividades relacionadas ao tratamento de dados pessoais. Além disso, a interação próxima com outras áreas da organização, como jurídico, TI e comunicação, proporciona uma troca de expertise e experiência, permitindo uma implementação mais eficaz das práticas de proteção de dados.

A colaboração com equipes multidisciplinares é uma estratégia valiosa para enfrentar os desafios da gestão de vazamento de dados. O DPO deve trabalhar em conjunto com profissionais de diferentes áreas, aproveitando suas perspectivas e conhecimentos específicos para desenvolver planos de resposta a incidentes abrangentes e eficazes. Esses planos devem abordar aspectos cruciais, como a identificação e notificação rápidas de vazamentos, a minimização do impacto aos titulares dos dados afetados e a recuperação segura das informações.

Ao adotar abordagens proativas, o DPO pode desempenhar um papel fundamental na proteção dos dados pessoais, garantindo a privacidade e a segurança das informações. A busca por educação e treinamento contínuos é fundamental para se manter atualizado sobre as ameaças em constante evolução e as soluções de segurança mais eficazes. Além disso, o uso de medidas de segurança adequadas, como criptografia e autenticação robusta, auxilia na prevenção de acessos não autorizados.

Outro ponto importante a se ressaltar é a proatividade de que se reveste a função do DPO. A responsabilidade proativa na proteção de dados pessoais implica em uma abordagem preventiva e antecipatória por parte das empresas e do DPO. Isso significa que, ao invés de apenas cumprir com as exigências legais e regulatórias, é necessário agir de forma a prevenir riscos e violações à privacidade dos dados pessoais.

Essa abordagem proativa traz consigo importantes implicações legais e éticas. Primeiramente, as empresas devem garantir o cumprimento das leis e regulamentações aplicáveis à proteção de dados pessoais. Além disso, é fundamental que elas ajam com cautela para evitar

invasões à privacidade dos titulares dos dados e o uso inadequado das informações pessoais. No contexto da responsabilidade proativa na proteção de dados pessoais, a ética desempenha um papel crucial. Isso envolve manter uma preocupação constante com a privacidade das pessoas e a proteção de suas informações pessoais. Portanto, as empresas e o DPO devem trabalhar continuamente para promover uma cultura de privacidade e conscientização sobre a importância da proteção de dados pessoais.

É importante ressaltar que não abordaremos aqui as questões de responsabilidade subjetiva ou objetiva do DPO, uma vez que nosso foco é a responsabilidade proativa dessa função. Embora a LGPD tenha ampliado o escopo dos dados pessoais sensíveis, abrangendo aspectos existenciais e sociais, é irrelevante para o DPO a discriminação entre dados sensíveis ou não. O objetivo central é estabelecer uma política ética dentro das organizações. A proibição do tratamento discriminatório e abusivo é o ponto-chave para estabelecer limites ao uso de dados, independentemente de serem sensíveis ou não. Conforme enfatizado por Doneda, "um dado em si não é perigoso ou discriminatório, mas o uso que se faz dele pode ser" (Doneda, 2006).

Ao discutir as implicações legais e éticas da responsabilidade proativa na proteção de dados pessoais, é importante destacar que as empresas que não estão em conformidade com as leis e regulamentações de proteção de dados podem enfrentar penalidades significativas. Portanto, é essencial que as empresas adotem medidas proativas para garantir a segurança e a privacidade dos dados pessoais, como a nomeação de um DPO qualificado e a implementação de políticas abrangentes e sólidas de proteção de dados. A responsabilidade proativa desempenha um papel fundamental na promoção de uma cultura de proteção de dados mais robusta e eficaz tanto em termos legais quanto éticos.

Em conclusão, o papel do DPO na gestão de vazamento de dados é complexo e exige um profundo conhecimento das melhores práticas, leis e regulamentações. Através de sua atuação comprometida e colaborativa, o DPO desempenha um papel crucial na proteção dos dados pessoais, promovendo uma cultura de segurança da informação e assegurando a conformidade com as regulamentações vigentes. Ao enfrentar os desafios com resiliência e adotar medidas de segurança adequadas, o DPO contribui para a construção de um ambiente confiável, no qual a proteção dos dados é uma prioridade central em todas as operações organizacionais.

3.1 Desafios na Gestão de Vazamento de Dados

A gestão de vazamento de dados é uma questão complexa e desafiadora que requer uma abordagem abrangente e estratégica. Ela envolve a consideração de várias áreas-chave que estão intrinsecamente ligadas à proteção dos dados pessoais em um ambiente digital em constante evolução.

Um dos principais desafios é a evolução das ameaças cibernéticas. Os avanços tecnológicos têm proporcionado às organizações uma série de benefícios, mas também têm dado origem a uma ampla gama de ameaças virtuais. Atacantes cada vez mais sofisticados e técnicas avançadas estão em constante desenvolvimento, exigindo das empresas uma compreensão contínua das táticas empregadas pelos invasores e a adoção de contramedidas adequadas. A gestão de vazamento de dados deve, portanto, estar constantemente atualizada sobre as ameaças emergentes, a fim de responder efetivamente a ataques como *ransomware*, *phishing* e engenharia social (Barcelos, 2021).

Além disso, a complexidade das leis e regulamentações relacionadas à proteção de dados representa um desafio significativo. Regulamentações como a Lei Geral de Proteção de Dados (LGPD) no Brasil e o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia são abrangentes e detalhadas. A interpretação e aplicação adequadas dessas regulamentações requerem um profundo conhecimento especializado e a capacidade de adaptar-se a diferentes contextos organizacionais. A conformidade com essas leis é fundamental para garantir a privacidade e a segurança dos dados pessoais.

A manutenção das melhores práticas de segurança é outro desafio importante. À medida que as ameaças evoluem, as melhores práticas também se desenvolvem. As organizações devem estar atualizadas e adaptadas às tecnologias emergentes, além de desenvolver políticas e procedimentos eficazes para proteger os dados pessoais. Isso requer uma abordagem proativa e uma constante atualização das medidas de segurança adotadas pela organização.

A colaboração com outras áreas da organização é essencial para a gestão de vazamento de dados. Equipes multidisciplinares, como TI, jurídico, comunicação e recursos humanos, devem trabalhar em conjunto para identificar, responder e mitigar incidentes de segurança de forma eficaz. A coordenação adequada entre essas equipes é crucial para garantir uma abordagem integrada e coerente na proteção dos dados, maximizando os recursos e conhecimentos disponíveis em toda a organização.

A comunicação e a transparência desempenham um papel fundamental na gestão de vazamento de dados. Comunicar adequadamente os incidentes de vazamento de dados para as partes interessadas internas e externas é essencial para preservar a confiança e a reputação da

organização. Isso requer uma divulgação transparente das violações, fornecendo informações precisas sobre a natureza do incidente, as medidas tomadas para mitigá-lo e os possíveis impactos aos titulares dos dados. A comunicação eficaz demonstra comprometimento com a proteção dos dados e permite que as partes interessadas tomem as medidas apropriadas para proteger seus próprios interesses.

Para enfrentar esses desafios, a gestão de vazamento de dados deve ser encarada como uma responsabilidade de toda a organização, desde a alta administração até os colaboradores em todos os níveis. É necessário estabelecer uma cultura de segurança da informação que promova a conscientização, a responsabilidade e a colaboração entre os membros da equipe. Somente por meio de uma abordagem abrangente, um planejamento estratégico e uma cooperação eficaz é possível proteger os dados pessoais contra vazamentos e violações indesejadas, garantindo assim a segurança e a confiança dos clientes e parceiros comerciais.

4 REGULAMENTAÇÃO DE DOSIMETRIA E APLICAÇÃO DE SANÇÕES ADMINISTRATIVAS PELA ANPD

No Brasil, a Lei Geral de Proteção de Dados (LGPD), estabelece as regras para o tratamento de dados pessoais pelas empresas e busca garantir a privacidade e a segurança dessas informações. A LGPD também estabelece direitos aos cidadãos em relação aos seus dados pessoais e penalidades para empresas que não estiverem em conformidade com a lei.

A finalidade primordial da Lei Geral de Proteção de Dados (LGPD) reside na proteção dos dados pessoais, impondo responsabilidades às empresas que não aderem às diretrizes estabelecidas. No cenário atual, é crucial a aplicação efetiva dessa lei, especialmente no que se refere à salvaguarda dos interesses das pessoas físicas. Infelizmente, temos presenciado situações em que dados que deveriam ser confidenciais e possuir finalidade específica são indevidamente expostos. Nesse contexto, as empresas precisam se adequar às formalidades e exigências impostas, uma vez que a negligência em relação ao consentimento claro do titular dos dados pode acarretar em multas significativas.

A LGPD não se limita a ações de reparação civil, abrangendo também processos administrativos e penais. Ela concede aos consumidores controle sobre seus dados e a capacidade de responsabilizar aqueles que utilizam indevidamente suas informações. Embora não introduza novos crimes, a LGPD desempenha um papel crucial na avaliação das ações dos administradores em incidentes de proteção de dados. Portanto, sua implementação adequada é fundamental para

proteger a segurança e privacidade dos dados pessoais, estabelecendo parâmetros para a responsabilidade das empresas no ambiente digital.

As sanções administrativas estão previstas na LGPD, em seu capítulo VII nos artigos 52 e 54 (Brasil, 2018). Por meio da Medida Provisória 869/18, surgiu a Agência Nacional de Proteção de Dados (ANPD), entidade responsável por supervisionar o cumprimento da LGPD. A agência desempenha um papel crucial ao fiscalizar o cumprimento da lei, elaborar diretrizes para o Plano Nacional de Proteção de Dados e aplicar sanções administrativas às empresas que não aderirem às disposições da LGPD. No entanto, as punições só seriam efetivas a partir de 1º de agosto de 2021, conforme estabelecido pela legislação (De Lucca e Mota, 2018).

A Lei Geral de Proteção de Dados Pessoais (Lei 13.709/18) foi proativa ao incluir disposições que responsabilizam os agentes envolvidos. De acordo com o artigo 42, o controlador ou operador que, no exercício de atividades de tratamento de dados pessoais, causar danos patrimoniais, morais, individuais ou coletivos em violação às leis de proteção de dados pessoais, é obrigado a repará-los. Essa responsabilização estabelecida pela lei é essencial para garantir a proteção adequada dos direitos dos indivíduos.

A LGPD se concentra em medidas sancionatórias administrativas, mas a manipulação inadequada de dados pessoais pode levar a infrações criminais. Portanto, é essencial considerar a possibilidade de sanções criminais quando a manipulação de dados viola a lei. A LGPD regula as infrações administrativas relacionadas à proteção de dados por meio de uma abordagem de responsabilidade objetiva. No entanto, é crucial destacar que a LGPD não abrange a responsabilização por condutas criminosas. Caso seja identificada uma conduta criminosa no âmbito da manipulação e tratamento de dados pessoais, a análise da responsabilidade subjetiva do agente criminoso deve ser realizada pelo Direito Penal.

Na LGPD, a responsabilidade penal de um administrador ocorre quando ele causa danos em violação às leis de proteção de dados pessoais. As sanções criminais buscam garantir a segurança dos dados e o sigilo, considerando as normas do Direito Penal. A causalidade entre a conduta do agente e o resultado do crime é fundamental, de acordo com o Código Penal Brasileiro.

4.1 Dosimetria e Metodologia para Aplicação

A norma de Dosimetria, com seus objetivos claros e fundamentais, desempenha um papel crucial no contexto da Lei Geral de Proteção de Dados Pessoais (LGPD).

Em primeiro lugar, a norma busca regulamentar de forma precisa e abrangente os artigos 52 e 53 da LGPD, estabelecendo critérios e parâmetros que serão aplicados pela Autoridade Nacional de Proteção de Dados (ANPD) no momento de impor sanções pecuniárias e não pecuniárias. Além disso, ela visa definir as formas e dosimetrias adequadas para o cálculo do valor-base das multas, trazendo clareza e consistência ao processo sancionador. Por segundo, a norma tem o propósito de promover alterações nos artigos 32, 55 e 62 da Resolução nº 1º CD/ANPD. Essas modificações têm como objetivo aprimorar o processo administrativo sancionador e de fiscalização conduzido pela ANPD, permitindo que a instituição avance em sua atividade repressiva, sempre respeitando os princípios do devido processo legal e do contraditório. Com isso, busca-se proporcionar segurança jurídica e transparência a todos os envolvidos nesse processo, estabelecendo uma base sólida para a atuação da ANPD.

A elaboração do regulamento de dosimetria, conforme estabelecido pelo artigo 53 da LGPD, é essencial para viabilizar a aplicação das sanções previstas na legislação. Esse regulamento tem como objetivo definir os critérios e parâmetros para as multas pecuniárias e não pecuniárias pela Autoridade Nacional de Proteção de Dados (ANPD), além de aprimorar o processo administrativo sancionador e de fiscalização.

Por meio desse instrumento normativo, serão estabelecidos os parâmetros que nortearão as decisões da ANPD em relação às sanções, garantindo maior clareza, previsibilidade e segurança jurídica para todas as partes envolvidas. A dosimetria das sanções considerará diversos aspectos relevantes, como a gravidade e natureza das infrações, o impacto nos direitos pessoais afetados, a boa-fé do infrator, a vantagem auferida ou pretendida, a condição econômica, a reincidência, o grau do dano, a cooperação do infrator, a adoção de mecanismos de minimização de danos, políticas de boas práticas e governança, a pronta adoção de medidas corretivas e a proporcionalidade entre a falta cometida e a sanção aplicada.

Essa abordagem da dosimetria das sanções busca garantir a efetividade da LGPD, proporcionando um ambiente de conformidade com a proteção de dados pessoais e promovendo a segurança e o respeito aos direitos dos titulares de dados no Brasil. Outrossim, é importante ressaltar que a divulgação da infração surge como uma possível consequência, na qual a autoridade responsável pela aplicação das sanções pode disseminar informações sobre a violação cometida pela organização, o que pode acarretar repercussões significativas em sua imagem e reputação. Em circunstâncias mais graves, a autoridade competente pode deliberar pelo bloqueio ou eliminação dos dados pessoais tratados de forma indevida, com o intuito primordial de salvaguardar os direitos dos titulares. Em cenários extremos, há inclusive a possibilidade de

suspensão parcial ou integral do direito da organização de conduzir atividades relacionadas ao tratamento de dados.

Neste diapasão, torna-se imprescindível que a dosimetria das sanções seja conduzida de maneira proporcional, respeitando os princípios da legalidade, culpabilidade e individualização da pena. A autoridade competente deve considerar todas as circunstâncias pertinentes para determinar a sanção mais adequada em cada caso, com o objetivo de salvaguardar os direitos dos titulares de dados pessoais e promover uma cultura de respeito à privacidade e à segurança dos dados.

A regulamentação da dosimetria tem como objetivo assegurar a adequação da sanção imposta à gravidade da conduta do agente, ao mesmo tempo em que busca proporcionar segurança jurídica aos processos de fiscalização e garantir os princípios fundamentais do devido processo legal e do contraditório. Por meio dessa abordagem, busca-se estabelecer uma maior correspondência entre o objetivo a ser alcançado e o meio utilizado, de forma a garantir a justiça e a equidade nas sanções aplicadas. A criação do regulamento de dosimetria foi prevista no artigo 53 da LGPD e constitui um requisito fundamental para a aplicação de multas pela Autoridade. Sua aprovação desempenha um papel crucial ao promover uma maior efetividade nos processos de fiscalização, que podem resultar em sanções administrativas.

A Lei Geral de Proteção de Dados Pessoais (LGPD) estabelece uma série de sanções que podem ser aplicadas em casos de violação das disposições da lei. Essas sanções visam garantir a conformidade com as normas de proteção de dados e salvaguardar os direitos dos indivíduos afetados.

Dentre as sanções previstas na LGPD, destacam-se a advertência, que serve como uma notificação inicial para orientar as organizações sobre a necessidade de se adequarem às exigências legais. Além disso, multas podem ser impostas, tanto na forma simples quanto na forma diária, podendo alcançar até 2% do faturamento da empresa infratora ou um valor total limitado a R$ 50.000.000,00. Além das multas, outras sanções podem ser aplicadas com o intuito de coibir práticas irregulares. A publicização da infração é uma dessas medidas, que envolve a divulgação pública da violação cometida pela organização. Adicionalmente, é possível determinar o bloqueio ou a eliminação dos dados pessoais tratados de forma inadequada. Em casos mais graves, é viável suspender parcialmente as atividades do banco de dados por até seis meses, com possibilidade de prorrogação pelo mesmo período, até que a situação seja regularizada. A suspensão do exercício da atividade de tratamento de dados pessoais também

pode ser imposta pelo mesmo período. Em circunstâncias excepcionais, é possível até mesmo proibir parcial ou totalmente a realização de atividades relacionadas ao tratamento de dados.

Cabe ressaltar que, com exceção das multas, todas as demais sanções podem ser aplicadas também ao Poder Público. A Autoridade responsável pela aplicação das sanções tem o poder de impor punições severas aos infratores que não estejam em conformidade com as disposições da LGPD, incluindo o bloqueio ou a eliminação definitiva dos dados pessoais tratados de forma irregular. Essas sanções visam promover a segurança e a conformidade no tratamento de dados, garantindo a proteção dos direitos dos titulares de dados pessoais.

A aplicação das sanções previstas pela Lei Geral de Proteção de Dados Pessoais (LGPD) ocorre após análise em processo administrativo individual, garantindo a ampla defesa e considerando critérios como a gravidade da infração, a boa-fé do infrator, a vantagem auferida, a condição econômica, a reincidência, o grau do dano, a cooperação, a adoção de mecanismos internos de minimização de danos, política de boas práticas e governança, adoção de medidas corretivas e a proporcionalidade entre a infração e a sanção.

O regulamento de dosimetria desempenha um papel crucial ao assegurar a proporção entre a sanção aplicada e a gravidade da conduta do agente, proporcionando segurança jurídica aos processos fiscalizatórios e garantindo o devido processo legal e o contraditório. As sanções previstas na LGPD são complementares à abordagem repressiva da Autoridade Nacional de Proteção de Dados (ANPD) e têm o propósito de incentivar a conformidade com a lei. Além das multas, podem ser aplicadas outras medidas, como a publicização da infração, o bloqueio e a eliminação de dados pessoais, a suspensão parcial do funcionamento do banco de dados, a suspensão do exercício da atividade de tratamento de dados e até mesmo a proibição parcial ou total de atividades relacionadas ao tratamento de dados.

A ANPD adota um modelo de fiscalização responsivo, que busca não apenas aplicar sanções, mas também adotar medidas orientativas e preventivas para conduzir as entidades de tratamento de dados à conformidade com a LGPD. Com a entrada em vigor do regulamento de dosimetria, a ANPD tem critérios claros para a aplicação das sanções administrativas, fortalecendo sua atuação regulatória. Essas medidas visam garantir cada vez mais a proteção dos direitos fundamentais dos cidadãos em relação à privacidade e proteção de dados pessoais, ao mesmo tempo em que o Brasil se alinha às melhores práticas para melhorar o ambiente de negócios.

5 CONSIDERAÇÕES FINAIS

Considerando os argumentos apresentados e a análise dos dados disponíveis, podemos concluir que a presença de um *Data Protection Officer* (DPO) com treinamento adequado e autoridade efetiva é, de fato, um fator determinante na redução da ocorrência e do impacto dos vazamentos de dados em uma organização. O DPO desempenha um papel crucial na proteção da privacidade e segurança das informações, garantindo a conformidade com as regulamentações de proteção de dados e promovendo uma cultura de segurança da informação.

Através da definição e implementação de políticas de privacidade e segurança, da avaliação e mitigação de riscos, da resposta eficaz a incidentes de segurança e do desenvolvimento de planos de ação apropriados, o DPO assume uma função central na prevenção de vazamentos de dados. Ademais, sua abordagem proativa ao antecipar riscos e buscar conformidade ética e responsável evidencia um compromisso constante com a proteção dos dados pessoais.

É fundamental reconhecer que os desafios no âmbito da proteção de dados estão em constante evolução, com ameaças cibernéticas cada vez mais sofisticadas e leis e regulamentos que se alteram continuamente. Nesse contexto, é imperativo que os DPOs se beneficiem de educação e treinamento contínuos em segurança da informação, implementem medidas de segurança apropriadas e promovam a colaboração com equipes multidisciplinares.

Ao adotar essas melhores práticas, o DPO contribui para construir uma cultura de segurança da informação sólida e sustentável dentro da organização, o que, por sua vez, fortalece a confiança de clientes e partes interessadas. Portanto, a presença de um DPO devidamente treinado e com autoridade é essencial para mitigar os riscos de vazamentos de dados, prevenir violações de privacidade e preservar a reputação e a integridade da organização.

No entanto, é importante destacar que a regulamentação, embora busque garantir segurança jurídica e previsibilidade nos processos administrativos sancionadores da Autoridade Nacional de Proteção de Dados (ANPD), apresenta alguns pontos de controvérsia. Por exemplo, a discricionariedade da ANPD para afastar a metodologia de dosimetria em casos específicos e a aplicação retroativa do regulamento a processos administrativos em andamento geram preocupações legítimas.

Em conclusão, esta pesquisa fornece evidências e argumentos sólidos que respaldam a hipótese de que a presença de um *Data Protection Officer* devidamente treinado e com autoridade é um fator crucial na redução da ocorrência e do impacto dos vazamentos de dados em uma organização. Recomenda-se enfaticamente que as organizações reconheçam a importância desse

papel e invistam na formação de seus DPOs, garantindo que eles possuam os conhecimentos, competências e autoridade necessários para cumprir suas funções de maneira eficaz. Somente dessa forma poderemos enfrentar os desafios em constante mutação na proteção de dados e garantir a privacidade e a segurança das informações em um mundo cada vez mais digitalizado.

A preservação da confiança é a espinha dorsal de nossa jornada rumo a um futuro mais seguro para a proteção de dados, onde a transparência, a clareza dos critérios e o devido processo legal são os pilares inabaláveis que sustentam nosso compromisso com uma cultura de privacidade resiliente. Em um mundo onde os dados são o alicerce de nossa era digital, a confiança é o alicerce que sustenta nosso progresso e nosso compromisso com a proteção de dados. Unidos, somos os guardiões dos dados e, juntos, moldamos um futuro de confiança e segurança digital. Este é nosso imperativo, nossa herança e nossa promessa à sociedade.

Nossa jornada rumo a um futuro mais seguro para a proteção de dados é delineada por essas descobertas, e a transparência, a clareza dos critérios e a devida garantia do processo legal emergem como os pilares inalienáveis que sustentam nossa busca por uma cultura sólida de privacidade. Nesse contexto, avançamos, cientes de que a proteção dos direitos dos titulares de dados e a segurança jurídica para os agentes de tratamento estão inextricavelmente ligadas em nossa trajetória em direção a um ambiente digital mais confiável. Em um mundo onde os dados são o cerne de nossa era digital, a confiança é o fundamento que sustenta nossos avanços. Portanto, é nossa responsabilidade coletiva proteger essa confiança, pois, afinal, somos os guardiões dos dados e, unidos, moldamos o futuro da privacidade e segurança da informação. Este é o nosso imperativo, nosso legado e nossa promessa à sociedade.

REFERÊNCIAS

BRASIL. Lei n. 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de dados pessoais. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 10 agosto de 2023.

BOTELHO, Marcos César. A proteção de dados pessoais enquanto direito fundamental: considerações sobre a Lei Geral de Proteção de Dados. Argumenta Journal Law, Jacarezinho – PR, n. 32, p. 191-207, 2020. Disponível em: http://seer.uenp.edu.br/index.php/argumenta/article/view/1840/pdf. Acesso em: 10 agosto de 2023.

BARCELOS, Ana Karollina *et al*. A LEI GERAL DE PROTEÇÃO DE DADOS E O PAPEL DO DPO. Revista Projetos Extensionistas, v. 1, n. 2, p. 87-92, 2021.

Disponível em: https://periodicos.fapam.edu.br/index.php/RPE/article/view/455. Acesso em: 10 agosto de 2023.

DE LUCCA, Newton. MACIEL, Renata Mota. A lei n. 13.709, de 14 de agosto de 2018: a disciplina normativa que faltava. In: In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de; MACIEL, Renata Mota (Coord.). Direito & internet IV: sistema de proteção de dados pessoais. São Paulo: Quartier Latin, 2019. p. 21-50.

DONEDA, Danilo. Da privacidade à proteção de dados. Rio de Janeiro, Editora Renovar, 2006. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://acervo-digital.espm.br/CAP%C3%8DTULOS%20DE%20LIVROS/2020/382770.pdf. Acesso em: 10 agosto de 2023.

GESTA LEAL, R. A PROTEÇÃO DE DADOS NO BRASIL EM FACE DAS DEMANDAS DE SEGURANÇA PÚBLICA E PERSECUÇÃO PENAL: LIMITES E POSSIBILIDADES: DATA PROTECTION IN BRAZIL IN THE FACE OF PUBLIC SAFETY DEMANDS AND CRIMINAL PERSECUTION: LIMITS AND POSSIBILITIES. Cadernos de Dereito Actual, [S. l.], n. 20, p. 221–245, 2023. Disponível em: https://www.cadernosdedereitoactual.es/ojs/index.php/cadernos/article/view/927. Acesso em: 10 agosto de 2023.

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. Revista de Direito do Consumidor. 2018. Disponível em: https://revistadedireitodoconsumidor.emnuvens.com.br/rdc/article/view/1116. Acesso em: 10 agosto de 2023.

MALDONADO, L. B..; SOTERO, A. L. E.. APLICABILIDADE DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS LEI 13.709/18 — SANÇÕES ADMINISTRATIVAS E CRIMINAIS. Revista Ibero-Americana de Humanidades, Ciências e Educação, [S. l.], v. 7, n. 3, p. 221–229, 2021. DOI: 10.51891/rease.v7i3.771. Disponível em: https://periodicorease.pro.br/rease/article/view/771. Acesso em: 10 agosto de 2023.