



FACULDADE EVANGÉLICA DE GOIANÉSIA
CURSO DE GRADUAÇÃO EM DIREITO

**ASPECTOS JURÍDICOS DA LGPD:
UMA ANÁLISE DA APLICAÇÃO DA LEI**

LELLES WARLEY FERREIRA BORGES
ROBERT MORAIS CARBONARO

Goianésia/GO
2024

LELLES WARLEY FERREIRA BORGES

ROBERT MORAIS CARBONARO

**ASPECTOS JURÍDICOS DA LGPD:
UMA ANÁLISE DA APLICAÇÃO DA LEI**

Artigo Científico apresentado junto ao Curso de Direito da FACEG (Faculdade Evangélica de Goianésia), como exigência parcial para a obtenção do grau de Bacharel em Direito.

Orientador: Me^a Prof.^a Kleber Torres de Moura

Goianésia/GO
2024

TERMO DE RESPONSABILIDADE AUTORAL

Nós autores deste trabalho declaramos para os devidos fins, que este artigo científico é original e inédito. Foi devidamente produzido conforme Regulamento para elaboração, apresentação e avaliação do trabalho de conclusão de curso em Direito da Faculdade Evangélica de Goianésia/Goias- FACEG.

Declaramos, também, na qualidade de autores do manuscrito que participamos da construção e formação deste estudo, e assumimos a responsabilidade pública pelo conteúdo deste. Assim temos pleno conhecimento de que possamos ser responsabilizados legalmente caso infringjam tais disposições.

FOLHA DE APROVAÇÃO

ASPECTOS JURÍDICOS DA LGPD: UMA ANÁLISE DA APLICAÇÃO DA LEI

Este Artigo Científico foi julgado adequado para a obtenção do título de Bacharel em Direito e aprovado em sua forma final pela banca examinadora da Faculdade Evangélica de Goianésia/GO- FACEG.

Aprovada em, ____ de ____ de 2024.

Nota Final

Banca Examinadora:

Prof. Me. Kleber Torres de Moura
Orientador

Prof. Me. Jean Carlos Moura Mota
Professor convidado 1

Prof.^a Carolina Santana Martins
Professora convidada 2

ASPECTOS JURÍDICOS DA LGPD: UMA ANÁLISE DA APLICAÇÃO DA LEI

LEGAL ASPECTS OF THE LGPD: AN ANALYSIS OF LAW APPLICATION

LELLES WARLEY FERREIRA BORGES¹

ROBERT MORAIS CARBONARO¹

KLEBER TORRES DE MOURA²

¹Discente do curso de Direito da Faculdade Evangélica de Goianésia- e-mail: lellesferreira@gmail.com

¹Discente do curso de Direito da Faculdade Evangélica de Goianésia- e-mail: knccbrasil123@gmail.com

²Docente do curso de Direito da Faculdade Evangélica de Goianésia- e-mail: kleber.moura@yahoo.com.br

Resumo: A presente pesquisa, intitulada “Aspectos Jurídicos da LGPD: Uma análise da aplicação da Lei”. O tema abordado se justifica visando a relevância da LGPD para a sociedade, empresas e o próprio Estado. A fim de analisar a sua aplicabilidade e de se explanar a uma forma correta e consonante de aplicação da referida Lei. O objetivo geral desta pesquisa é analisar e avaliar o status da Lei Geral de Proteção de Dados (LGPD) no Brasil, tais como, os desafios e conformidade na aplicação da LGPD, bem como seu impacto jurídico no panorama da proteção de dados. Os objetivos específicos são: Entender quais e como as autoridades reguladoras estão aplicando a LGPD, qual a sua base de surgimento e inspiração para o prosseguimento, e demonstrar a que agentes se aplica e a quem tem o direito de assecuração da Lei. A metodologia utilizada foi o tipo da pesquisa descritiva, qualitativa, utilizando-se os métodos de revisão bibliográfica, com pesquisa em doutrinas e análise documental nas legislações vigentes e outros documentos relacionados à Lei Geral de Proteção de Dados. A presente pesquisa constatou que, o continuo estudo sobre a Lei de Proteção de Dados e suas possíveis mudanças para se adequar as futuras demandas, esclare os pontos significativos no quesito segurança e proteção de dados, que traz essa conformidade na atual sociedade que apresenta constante desenvolvimento no ambiente tecnológico.

Palavras-chave: LGPD; dados pessoais; proteção.

Abstract: This research, entitled “Legal Aspects of the LGPD: An analysis of the application of the Law”. The topic addressed is justified by the relevance of the LGPD for society, companies and the State itself. In order to analyze its applicability and explain a correct and consistent way of applying said Law. The general objective of this research is to analyze and evaluate the status of the General Data Protection Law (LGPD) in Brazil, such as, the challenges and compliance in applying the LGPD, as well as its legal impact on the data protection landscape.”. The specific objectives are: Understand which and how the regulatory authorities are applying the LGPD, what is its basis of emergence and inspiration for the procedure, and demonstrate to which agents it applies and who has the right to ensure the Law. The methodology used was a descriptive, qualitative type of research, using bibliographic review methods, with research into doctrines and documentary analysis of current legislation and other documents related to the General Data Protection Law. The research found that there was clarification that through the Data Protection Law, it clarifies the significant points in terms of security and data protection that brings this compliance in the current society that has developed in the technological environment.

Keywords: LGPD; personal data; protection.

INTRODUÇÃO

A pesquisa intitulada "ASPECTOS JURÍDICOS DA LGPD: UMA ANÁLISE DA APLICAÇÃO DA LEI" aborda a problemática da implementação e conformidade com a LGPD no Brasil, e o presente tema foi escolhido com o objetivo de analisar o estado atual da lei, os desafios jurídicos enfrentados pelas organizações, e o impacto dessa legislação no panorama da proteção de dados no país. O estudo busca ainda identificar os principais obstáculos e oportunidades na aplicação da LGPD, bem como, tratar a respeito das autoridades reguladoras na fiscalização e imposição de penalidades.

Assim, tem-se como justificativa demonstrar o anseio que a sociedade moderna possui em alcançar uma administração em entidades públicas e privadas transparente e ética se tratando de dados pessoais. E com base nisso, será tratado a respeito da Lei Geral de Proteção de Dados Pessoais (LGPD), sancionada em 14 de agosto de 2018 e vigente desde setembro de 2020, representando um marco histórico na regulamentação do tratamento de dados pessoais no Brasil.

Inspirada pelo Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia, a LGPD visa estabelecer diretrizes claras para a coleta, armazenamento, processamento e compartilhamento de dados pessoais, tanto por entidades públicas quanto privadas. A importância deste trabalho reside na relevância da LGPD para a proteção dos direitos individuais à privacidade e à segurança dos dados pessoais. Além disso, a lei tem implicações significativas para a economia, a competitividade das empresas e o papel do Estado na regulamentação dessas práticas.

O presente artigo desenvolveu-se através da pesquisa descritiva, qualitativa, utilizando-se os métodos de revisão bibliográfica, com pesquisa em doutrinas e análise documental nas legislações vigentes e outros documentos relacionados à Lei Geral de Proteção de Dados.

No primeiro tópico, os principais autores utilizados na busca pela compreensão da evolução histórica, e comparação com cenários internacionais, são Fernanda G. (2022) e Lima Rapôso, C. Melo de Lima, H de Oliveira Junior, W. F. Ferreira Silva, P. A. ., Elaine de Souza Barros (2019). No segundo tópico passar-se-á a explanação das

obrigações dos controladores de dados e a respeito da ANPAD, à luz do entendimento de Garrida (2023). Ademais, no terceiro tópico, analisará os desafios e os benefícios da LGPD, tendo-se Próximos (2022) e Reis (2023) como autores principais do tópico em comento.

1. LGPD: REVOLUÇÃO TECNOLÓGICA

Necessita-se destacar o surgimento da Lei 13.709/2018 para referenciar uma devida análise legal na atualidade e para demonstrarmos as batalhas que foram e que serão enfrentadas para alcançar a sua perfeita condição. Deste modo, nota-se que na sociedade atual é importante entendermos o impacto que causa uma grande lei inovadora no meio jurídico, de forma tão significativa que um simbólico marco tecnológico, aparenta o Direito não estar preparado para tantos desafios.

A Lei Geral de Proteção de Dados (LGPD) foi publicada em 14 de agosto de 2018, entretanto somente em 2020 entra em vigência, além das sanções que passam a ser validadas em 2021, demora que foi determinada pelo grande acontecimento da pandemia (COVID 19), logo, certamente podemos dizer que legalmente seus dispositivos vêm sendo aplicados apenas a mais de 03 anos. Nesse ponto, Lima Rapôso, C. Melo de Lima, H de Oliveira Junior, W. F. Ferreira Silva, P. A. ., & Elaine de Souza Barros, E. . (2019, p. 01), elucida:

RESUMO: Com a globalização e o desenvolvimento de novas tecnologias desenvolve uma competição cada vez mais voraz entre as empresas, desenvolvendo questionamentos sobre a segurança das informações corporativas e de seus clientes. Apesar de entrar em vigor no próximo ano, é evidente que se discute muito na literatura sobre a adaptabilidade da tecnologia da informação a LGPD o que traz uma insegurança jurídica de como será a aplicabilidade da lei e que atitudes devem ser tomadas visando o compliance da lei.

O que se vive hoje no âmbito jurídico e na sociedade em si, é de uma imensa adaptação virtual, onde a agilidade procede em locais de trabalho, em casa e nas ruas, contudo excede em quesitos como comunicação interpessoal criando barreiras, no que se diz respeito à presunção do consentimento diante de uma presunção e percepção de confiança ficta e principalmente questões de segurança cibernética à medida que nos tornamos mais dependentes da tecnologia.

Portanto, é inevitável que nessa vertente procure alternativas para a devida proteção de dados pessoais, e até então que não se propague desinformações que

não são relativas à realidade. Logo o surgimento da Lei 13.709/2018 é de fato para revolucionar a sociedade e sua tecnologia de forma legal. Nesse sentido, é necessário destacar os artigos que movem em face do titular, como pessoa jurídica, a sua exibição de dados pessoais para os agentes que, prosseguindo conseguem cumprir o seu papel com suas conformidades baseados na LGPD.

É notório que a Lei vem para assegurar e proteger o compartilhamento destes dados pessoais, mas também para instruir e proteger as empresas tanto públicas quanto privadas. Em seus artigos 17º e 18º, da Lei Geral de Proteção de Dados de 2018, estão previstos os direitos dos titulares, *in verbis*.

Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei.

Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

I - confirmação da existência de tratamento;

II - acesso aos dados;

III - correção de dados incompletos, inexatos ou desatualizados;

IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;

V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;

VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;

VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;

VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;

IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei (BRASIL, 2018, *online*).

Logo, podemos perceber com a leitura do artigo supracitado, que aos titulares de dados é assegurado o direito de obter do controlador, em relação aos seus dados pessoais, a confirmação da existência de tratamento e o acesso a esses dados. Em outras palavras, os titulares têm o direito de saber se suas informações pessoais estão sendo processadas e, caso estejam, têm o direito de acessar esses dados. Já, o artigo 18 estabelece o direito dos titulares de dados de solicitar a correção de dados pessoais incompletos, inexatos ou desatualizados que estejam sob tratamento do controlador, portanto, isso significa que os titulares têm o direito de garantir que suas informações pessoais sejam precisas e atualizadas.

Para adentrarmos mais neste conhecimento da Lei e do seu surgimento, é

primordial sabermos de onde vem esta análise para implementarmos na nossa sociedade, e neste caso, o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia é uma das legislações importantes que estabelecem direitos e diretrizes para a proteção de dados pessoais.

Tanto a atual legislação do Brasil quanto da União Europeia (GDPR), têm como objetivo principal o regimento do cuidado de dados pessoais, gerando através da mesma, a defesa dos direitos fundamentais das pessoas naturais. Para mais, SOLER, Fernanda G. (2022, p. 11) aduz:

A escolha do legislador seguiu o padrão europeu, que em seu regulamento (GDPR - General Data Protection Regulation - Regulamento Geral sobre a Proteção de Dados - Regulamento (UE) 2016/679), tampouco dispõe acerca dessa questão e delega a um novo normativo apreciar o tema e definir os limites e possibilidade. Trata-se de uma escolha que demandará estudo e um balanceamento de direitos, conjuntamente com uma política pública própria, aplicada ao povo de cada país, considerando sua especificidade cultural.

Desta maneira, considerando a comparação, é de suma importância trazermos seus aspectos para a devida análise. No quesito em abrangência geográfica, a GDPR aplica-se a todos os agentes que processam dados pessoais de indivíduos na União Europeia, independentemente da localização da empresa, e nesse mesmo sentido, a LGPD aplica-se a todas as operações de tratamento de dados realizadas no território brasileiro, bem como ao tratamento de dados pessoais de indivíduos localizados no Brasil, independentemente da localização da empresa.

No artigo 3º, da Lei Geral de Proteção de Dados de 2018, encontra-se positivado o texto que determina a aplicação do tratamento de dados pessoais, *in verbis*.

Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

I - a operação de tratamento seja realizada no território nacional;

II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou (Redação dada pela Lei nº 13.853, de 2019) Vigência

III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

(...) (BRASIL, 2018, *online*).

Sobre as definições de dados pessoais, ambas as leis definem dados pessoais como qualquer informação relacionada a uma pessoa física identificada ou identificável. Para os princípios de processamento de dados, ambas as leis estabelecem quesitos semelhantes, como propósito, minimização, precisão, limitação de armazenamento, integridade e confidencialidade, responsabilidade e transparência.

É preciso também ressaltar a importância do consentimento, e notamos que, ambas as leis exigem que o consentimento seja obtido de forma clara e inequívoca para o processamento de dados pessoais e o consentimento deve ser específico para cada finalidade de processamento.

Ao aprofundar nas sanções e penalidades, ambas as leis preveem multas e penalidades significativas por violações. A GDPR pode impor multas de até 20 milhões de euros ou 4% do volume de negócios anual global, o que for maior. Na LGPD, as multas podem chegar a 2% do faturamento da empresa no Brasil, limitadas a R\$ 50 milhões por infração. Portanto, embora existam diferenças específicas entre a LGPD e a GDPR, ambas refletem a crescente importância global da proteção de dados pessoais e têm como objetivo garantir que os direitos fundamentais das pessoas em relação à privacidade sejam respeitados.

2. OBRIGAÇÕES E CONFORMIDADES DA LEI

As obrigações dos controladores e operadores de dados pessoais são vastas e essenciais para a conformidade com a Lei Geral de Proteção de Dados (LGPD), estas responsabilidades são importantes para mitigar os riscos que podem ocorrer no processo de tratamento de dados, diante disto o Art. 37 da Lei Nº 13.709 de 2018 trás:

Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse (BRASIL, 2018, *online*).

A manutenção desses registros é crucial para a mitigação de riscos e a prestação de contas, conforme expresso no artigo 6º, inciso X, da lei.

Na regulamentação europeia (GDPR), há parâmetros claros para a obrigatoriedade desses registros. Empresas com mais de 250 colaboradores ou

aquelas que processam dados pessoais que possam implicar em riscos para os direitos dos titulares são obrigadas a manter registros. Isso inclui empresas que realizam processamento contínuo e não eventual de dados pessoais, tratam dados sensíveis, ou dados relacionados a condenações penais e infrações.

Diferentemente do modelo europeu, a LGPD não estabeleceu parâmetros mínimos para a obrigatoriedade do registro de atividades de tratamento de dados pessoais. Portanto, a menos que a Autoridade Nacional de Proteção de Dados (ANPD) venha a dispor sobre parâmetros objetivos mínimos, todas as empresas que realizam atividades de tratamento de dados pessoais estão obrigadas a realizar esses registros.

Adicionalmente, a LGPD reforça a necessidade de registro das operações de tratamento de dados baseadas no legítimo interesse, situação que pressupõe, além do registro, a elaboração de um relatório específico de impacto, conforme o artigo 10, § 3º, da lei. Esse relatório deve descrever os tipos de dados coletados, a metodologia utilizada para a coleta, e as medidas de segurança implementadas.

Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial. Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados. (BRASIL, 2018, online)

O artigo 38 da LGPD prevê que a ANPD pode exigir a elaboração de um relatório de impacto à proteção de dados pessoais, incluindo dados sensíveis. Esse relatório deve conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia para a coleta e segurança das informações, e a análise do controlador sobre medidas de mitigação de riscos.

Conforme o artigo 38, caberá à ANPD estabelecer as situações em que o relatório de impacto será recomendável. No entanto, a LGPD já indica a necessidade desse relatório para atividades envolvendo dados sensíveis e legítimo interesse. A estrutura do relatório de impacto será estabelecida por regulamento, mas a lei já define como documentação do controlador que descreve processos de tratamento que podem gerar riscos às liberdades civis e direitos fundamentais.

Embora similares, o registro das atividades de tratamento de dados e o relatório de impacto possuem finalidades distintas, sendo que o registro documenta os processos relacionados ao tratamento de dados, enquanto o relatório de impacto foca no mapeamento e mitigação de riscos decorrentes dessas atividades, sendo essencial para apontar riscos e orientar o controlador e o operador na mitigação desses riscos.

Empresas que já passaram pela adequação à norma ISO 27.001, que identifica dados pessoais como ativos e levantam riscos, estão próximas de cumprir o requisito do artigo 38 da LGPD. A elaboração do relatório de impacto é recomendável não apenas quando exigida por lei, mas em todas as situações que possam representar riscos aos titulares dos dados.

Se uma empresa não está certa quanto à necessidade de um relatório de impacto, a recomendação é por fazê-lo, visando mitigar riscos potenciais e responsabilidades futuras. Essa postura é segura e recomendável, especialmente em operações que envolvam avaliações sistemáticas de aspectos pessoais, tratamento de dados em grande escala, ou decisões automatizadas com efeitos significativos.

Art. 39. O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria (BRASIL, 2018, online).

Embora o operador siga as instruções do controlador, ele não é eximido de adotar medidas para conformidade com a legislação de proteção de dados e medidas de segurança. A atuação do operador é relevante, pois há a possibilidade de responsabilização solidária do controlador por falhas do operador, conforme o artigo 42 da LGPD. Portanto, ambos os agentes devem trabalhar em conjunto para assegurar a proteção dos dados pessoais.

Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais. § 1º. A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador. § 2º. As atividades do encarregado consistem em: I – aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; II – receber comunicações da autoridade nacional e adotar providências; III – orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; IV – executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares. § 3º. A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do

encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados. § 4º. (VETADO). (Incluído pela Lei nº 13.853, de 2019). (BRASIL, 2018, online)

O artigo 41 da LGPD obriga o controlador a indicar um Encarregado pelo Tratamento de Dados Pessoais, cuja identidade e informações de contato devem ser divulgadas publicamente. As atividades do encarregado incluem aceitar reclamações e comunicações dos titulares, receber comunicações da ANPD, orientar funcionários sobre práticas de proteção de dados, e executar atribuições determinadas pelo controlador ou por normas complementares.

A ANPD pode estabelecer normas complementares sobre a definição e atribuições do encarregado, incluindo hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e porte da entidade ou volume de operações de tratamento de dados. A nomeação do encarregado deve ser documentada, demonstrando a consideração de todos os fatores relevantes para essa decisão.

Ainda que a função não seja obrigatória, a empresa pode optar pela nomeação voluntária do encarregado. Nesse caso, as mesmas responsabilidades aplicáveis ao encarregado obrigatório serão também aplicáveis ao nomeado voluntariamente. A falta de designação de um encarregado não desobriga a empresa de cumprir as obrigações previstas na LGPD.

A empresa deve avaliar as funções, perfil e posição do encarregado dentro da estrutura organizacional. Entre as funções do encarregado, destacam-se a interação com os titulares de dados, a ANPD, a orientação dos colaboradores, a execução de atribuições determinadas em normas complementares, e a emissão de relatórios de impacto à proteção de dados.

O encarregado deve estar acessível aos titulares e à ANPD. Por isso, a LGPD exige a divulgação clara e objetiva dos dados de contato do encarregado. A conformidade com essas obrigações é essencial para a proteção dos direitos dos titulares de dados pessoais e para a criação de um ambiente seguro e confiável para o tratamento de informações.

O cumprimento rigoroso dessas responsabilidades é crucial para evitar sanções e manter a confiança dos titulares de dados. Portanto, a empresa deve investir em processos internos robustos, auditorias regulares, treinamento contínuo de funcionários e mecanismos eficazes de resposta a incidentes para garantir a conformidade com a LGPD.

Ademais, é extremamente relevante entender sobre a Autoridade Nacional de Proteção de Dados (ANPD), que por sua vez é uma entidade essencial no contexto da proteção de dados pessoais no Brasil, estabelecida pela Lei Geral de Proteção de Dados (LGPD). Suas estruturas e funções são desenhadas para assegurar que as práticas de tratamento de dados pessoais estejam em conformidade com a legislação vigente, sendo uma das principais competências da ANPD a aplicação e a execução da referida Lei.

A autoridade é responsável por criar normas e diretrizes complementares à LGPD, adaptando a legislação às necessidades específicas dos diversos setores da economia e da sociedade. Este papel regulatório permite que a ANPD mantenha a LGPD relevante e eficaz diante das constantes inovações tecnológicas, proporcionando segurança jurídica tanto para os titulares de dados quanto para os agentes de tratamento.

A estrutura da ANPD inclui diversas unidades organizacionais, sendo o Conselho Diretor o órgão máximo de decisão. Este conselho é composto por cinco membros, nomeados pelo Presidente da República, com mandatos de quatro anos. A função do Conselho Diretor é formular e implementar políticas de proteção de dados, assegurando que a ANPD cumpra seu papel regulador de maneira eficiente.

Art. 55-D. O Conselho Diretor da ANPD será composto de 5 (cinco) diretores, incluído o Diretor-Presidente. § 1º Os membros do Conselho Diretor da ANPD serão escolhidos pelo Presidente da República e por ele nomeados, após aprovação pelo Senado Federal, nos termos da alínea 'f' do inciso III do art. 52 da Constituição Federal, e ocuparão cargo em comissão do Grupo-Direção e Assessoramento Superiores - DAS, no mínimo, de nível 5. § 2º Os membros do Conselho Diretor serão escolhidos dentre brasileiros que tenham reputação ilibada, nível superior de educação e elevado conceito no campo de especialidade dos cargos para os quais serão nomeados. § 3º O mandato dos membros do Conselho Diretor será de 4 (quatro) anos. § 4º Os mandatos dos primeiros membros do Conselho Diretor nomeados serão de 2 (dois), de 3 (três), de 4 (quatro), de 5 (cinco) e de 6 (seis) anos, conforme estabelecido no ato de nomeação. § 5º Na hipótese de vacância do cargo no curso do mandato de membro do Conselho Diretor, o prazo remanescente será completado pelo sucessor. (BRASIL, 2018, online)

A ANPD também exerce uma função de fiscalização, e isto envolve monitorar e verificar o cumprimento das obrigações da LGPD. A autoridade pode conduzir auditorias, solicitar informações planejadas e realizar inspeções para garantir que as práticas de tratamento de dados estejam em conformidade com a lei. Em casos de descumprimento, a ANPD possui competência para aplicar sanções administrativas, que podem variar desde advertências até multas substanciais, e, em casos graves, a suspensão parcial ou total do banco de dados relacionados à infração.

Outra competência fundamental da ANPD é a promoção da conscientização sobre a proteção de dados pessoais. A autoridade realiza campanhas educativas e de divulgação, aumentando o conhecimento da sociedade sobre a importância da proteção de dados e as melhores práticas a serem adotadas. Conforme aponta Patrícia Peck Garrido em seu livro “Proteção de dados pessoais: comentários à lei n. 13.709/2018 (LGPD)”.

No que diz respeito às competências da ANPD – art. 55-J –, é possível destacar:

zelar pela proteção dos dados pessoais, nos termos da legislação;
elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade;

fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;

apreciar petições de titular contra controlador após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação;

promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança;

solicitar, a qualquer momento, às entidades do poder público que realizem operações de tratamento de dados pessoais informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento desta Lei;

realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público;

editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclararem startups ou empresas de inovação, possam adequar-se a esta Lei;

garantir que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento, nos termos desta Lei e da Lei n. 10.741, de 1º de outubro de 2003 (Estatuto do Idoso).

É relevante pontuar que o art. 55-K deixa claro que compete exclusivamente à ANPD a aplicação das sanções previstas na LGPD, e que suas competências prevalecerão, no que se refere à proteção de dados pessoais, sobre as competências correlatas de outras entidades ou órgãos da administração pública.

Em suma, a atuação da ANPD é vital para a proteção de dados pessoais no Brasil, e através de uma estrutura robusta e funções abrangentes, a ANPD assegura que a privacidade e os direitos dos titulares de dados sejam respeitados.

3. APLICAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS: DESAFIOS E BENEFÍCIOS

Com a implementação da Lei Geral de Proteção de Dados (LGPD), e para maior entendimento da mesma, é de suma importância esmiuçar as obrigações constantes na mesma. Logo, a Lei nº 13.709/2018, impõe obrigações significativas tanto para entidades públicas quanto privadas no Brasil, visando proteger a privacidade e os dados pessoais dos indivíduos. A adequação à LGPD tem sido um processo desafiador, mas crucial para garantir a conformidade legal e a proteção efetiva dos dados. Abaixo, abordamos como as entidades públicas e privadas têm se adaptado à LGPD, os desafios enfrentados e as medidas adotadas.

No tocante às entidades privadas, houveram desafios na regulamentação devido a sua complexidade, considerando a existência de diversos setores e a variedade dos dados coletados, tornando a adequação um processo complexo. Por consequência, as pequenas e médias empresas também enfrentam desafios devido aos recursos que na maioria das vezes eram limitados e havia necessidade de implementação de programas e técnicas no tocante a proteção de dados CARDOSO. R. R. C. (2022, p. 25) conceitua:

Atualmente, o único meio viável para auxiliar na implantação e cumprimento da LGPD é a terceirização desse serviço para empresas já estruturadas, contudo, mesmo essa opção ainda seria algo que acarretaria em custos extras, desta forma, a criação de ferramentas de Tecnologia da informação simples poderia servir como apoio para essas empresas usarem como base na aplicação e entendimento da LGPD, contribuindo assim para a redução de custos com mão de obra especializada e diminuiria o risco dessas instituições sofrerem sanções administrativas.

Outro desafio contínuo que é enfrentado é a cultura organizacional, que deve priorizar a privacidade e a segurança dos dados. A falta de conscientização também é um desafio, considerando que muitas empresas ainda não compreendem plenamente a importância da LGPD e as implicações de não estarem em conformidade com a lei. Isso inclui a crença equivocada de que apenas dados sensíveis necessitam de proteção especial, quando, na realidade, todos os dados pessoais coletados ou tratados precisam ser protegidos.

Um dos maiores desafios é a falta de conscientização das empresas em relação à importância da LGPD. Muitos empresários desconhecem as implicações da lei e os riscos de não fazer nada. Alguns ainda acreditam que só precisam se adequar se trabalham com dados pessoais sensíveis, o que é um grande equívoco. (REIS. R, 2023).

A LGPD é aplicável a qualquer tipo de informação pessoal, desde que seja coletada e tratada por uma empresa. Por isso, é fundamental que as empresas entendam que o cumprimento da lei é uma obrigação legal e ética e que qualquer violação pode gerar sanções legais e danos à reputação.

A ausência de treinamento de colaboradores também deve ser ressaltada, pois há uma carência de treinamento adequado para os funcionários das empresas. Sem esse treinamento, é difícil para os colaboradores entenderem a importância da proteção de dados e atuarem de acordo com as exigências da LGPD. Investir na capacitação é crucial para o sucesso da implementação da lei.

Um funcionário mal-informado pode acabar realizando um processamento inadequado dos dados pessoais sob sua responsabilidade. É fundamental que as empresas invistam na capacitação de seus colaboradores, inclusive terceirizados e temporários, para garantir o sucesso da implementação da LGPD. (REIS. R, 2023).

Nesse mesmo sentido, outro desafio é a necessidade de avaliação de processos internos, em que as empresas precisam revisar e aprimorar seus processos internos para se adequarem à LGPD. Muitas companhias possuem processos obsoletos ou baseados em tecnologias ultrapassadas, o que dificulta a conformidade com a nova legislação.

A falta de um processo adequado pode levar à vulnerabilidade e exposição de dados pessoais, o que pode ser desastroso para a empresa e para os clientes. Por isso, é necessário identificar quais são os dados que estão sendo coletados, como estão sendo armazenados, quem tem acesso a eles e como estão sendo descartados. (REIS. R, 2023).

Necessário salientar também o desafio das empresas no tocante ao investimento em cibersegurança, tendo em vista que a proteção eficaz dos dados pessoais exige investimentos substanciais em cibersegurança. No entanto, muitas

empresas ainda não destinam recursos suficientes para garantir a segurança dos dados, o que as torna vulneráveis a violações e ataques cibernéticos.

Além disso, afirmar-se que investir em cibersegurança é essencial para evitar violações e ataques cibernéticos de qualquer tipo, que podem trazer danos irreparáveis à imagem da empresa (REIS. R, 2023).

Nesta continuidade, os desafios enfrentados na esfera das entidades públicas se assemelham a das privadas, contudo, existe a complexidade na estruturação governamental, visto que existe uma vasta quantidade de dados pessoais que são tratados por diversas agências, representando o desafio.

Outro quesito que pode ser visto como um desafio é no tocante aos recursos e a capacitação, pois a escassez de recursos financeiros, aliado a escassez de pessoas especializadas em proteção de dados, geram a necessidade de capacitação dos funcionários públicos a respeito dos princípios, indo assim de encontro ao abalo financeiro. De acordo com SILVA. J. O. A. VILELA. C. VELOSO. E. G. (2022):

“A aplicação da LGPD na Administração Pública é um tema de extrema relevância, uma vez que os órgãos públicos lidam com uma enorme quantidade de informações pessoais dos cidadãos, tais como dados de identificação, informações de saúde, registros criminais, entre outros. É fundamental que essas entidades estejam em conformidade com a lei, a fim de garantir a segurança e à privacidade desses dados sensíveis.”

Feitas tais considerações, concluímos que a adequação à LGPD é um processo contínuo que exige esforço e investimento significativos tanto de entidades públicas quanto privadas. Apesar dos desafios, os benefícios em termos de proteção de dados, aumento da confiança e melhoria na segurança são substanciais. A conformidade com a LGPD não é apenas uma obrigação legal, mas também uma oportunidade para as organizações demonstrarem seu compromisso com a privacidade e a segurança dos dados pessoais, construindo um ambiente mais seguro e confiável para todos.

Conforme dito em outros tópicos, a LGPD foi promulgada com o intuito de proteção de direitos fundamentais de liberdade e de privacidade. Contudo, em que pese a notória necessidade de tal lei, grande foi o impacto da adaptação das empresas, bem como, por conseguinte, as mesmas tiveram inúmeros desafios para sua implementação, considerando a série de mudanças que as empresas enfrentariam.

Diversas adaptações foram necessárias serem seguidas nas empresas que lidavam com dados pessoais, como por exemplo em relação a adoção de políticas de privacidade, em que as empresas precisaram criar e manter políticas de privacidade que expliquem de forma clara ao usuário como os dados são coletados, compartilhados, usados e até armazenados.

Essa política de privacidade deve ser um documento de conteúdo de fácil acesso e compreensão, e que deve ser preciso em suas informações, a fim de que o usuário saiba os dados pessoais que estão sendo compartilhados, sua finalidade, qual seria a base jurídica para tal, e também é importante destacar o prazo em que os dados ficam armazenados.

Outro ponto que merece atenção é no tocante ao mapeamento de dados, em que foi necessário implementar a rotina de identificar todos os dados pessoais que seriam processados pela empresa, incluir a sua finalidade é apontar a base legal para cada processamento.

Salientar também o desafio das empresas com os direitos dos titulares, que tiveram seus dados armazenados, com a necessária implementação de um setor responsável pelo atendimento a solicitações dos usuários, pois diversas dúvidas poderiam surgir. E sempre tratar com enorme transparência, considerando a necessidade de deixar os usuários sempre cientes dos seus direitos. E com a adequação das empresas, alguns princípios tiveram que ser observados, e de acordo com SILVA. A. C. M. PRÓXIMO. R. (2022), vejamos os principais:

- a) Princípio da Finalidade - O controlador terá que informar o titular de dados pessoais sobre a finalidade de cada dado pessoal coletado.
- b) Princípio da Adequação - O controlador de dados deverá utilizar os dados apenas para as finalidades informadas ao titular dos dados pessoais, não podendo utilizar de forma diversa a apresentada.
- c) Princípio da Necessidade - Só poderão ser coletados os dados direcionados a determinada finalidade informada ao titular, devendo-se sempre observar a necessidade da coleta e excluindo coleta excessiva, dados desnecessários para o cumprimento da finalidade.
- d) Princípio do Livre Acesso - O controlador dos dados deverá garantir ao titular de dados o livre acesso a todos os seus dados e a forma como eles são tratados dentro da instituição. Ou seja, será necessário garantir ao titular, de forma clara, direta, explícita e gratuita, todo o ciclo de vida de seus dados dentro da empresa, desde a forma em que foram coletados até a forma que serão descartados.
- e) Princípio da Qualidade dos Dados - Deve o controlador garantir aos titulares de dados a exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

- f) Princípio da Transparência - O controlador deverá garantir aos titulares de dados, informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e todos os respectivos agentes de tratamento, devendo sempre observar os segredos comercial e industrial.
- g) Princípio da Segurança - O controlador é responsável por utilizar medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.
- h) Princípio da Prevenção - Deve o controlador adotar medidas de prevenção quanto a ocorrência de danos em virtude do tratamento de dados pessoais.
- i) Princípio da Não Discriminação - A lei traz que o controlador não pode realizar o tratamento de dados pessoais se estes forem para fins discriminatórios ilícitos e/ou abusivos.
- j) Princípio da Responsabilização e Prestação de Contas - É dever do controlador demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Logo, ao adequar as empresas aos princípios supracitados, os desafios foram surgindo na prática, surgindo a necessidade de constituição de bases para tratamentos de dados, nesta senda, salientam ANDRADE. J. STEPENOSKI. P. (2022):

“Diante de todos os impactos previstos com promulgação da LGPD, o fenômeno da abrangência gera preocupação, tendo em vista que a Lei tem abrangência ampla, uma vez que engloba dados de todas as espécies, que sirvam para identificar ou tornem o indivíduo identificável, ou seja, ante a abrangência do conceito legal, as empresas deverão se adequar ao texto normativo, no que concerne ao tratamento dos dados pessoais coletados no território brasileiro ou de pessoas localizadas no mesmo. Assim a necessidade premente é pela constituição de bases para tratamento de dados por parte destas, a adequação de seus sistemas para a transmissão de informações claras do que se quer e o que se pretende com aquelas informações, assim como a obtenção do consentimento explícito do usuário. Ainda, o processamento destas informações e a necessidade de renovação destas, especialmente se alterada a finalidade prévia e consentida ao longo do período desde o início daquelas informações coletadas, que já compõe a base de dados”.

Assim, na prática existiu a dificuldade de adaptação visto o alto custo de implementar sistemas que lidam com a alimentação desses dados, mas também com a sistemática de tratamento dos dados, evitando as sanções impostas na Lei de que se trata o presente. Por outro lado, em que pese ter existido pontos negativos, atualmente, após a implementação da Lei 13.709/18, inúmeros foram os benefícios, tanto para as empresas, como para os indivíduos.

Em relação aos usuários, o maior controle sobre os dados pessoais, com a possibilidade de revogar o consentimento para o uso desses dados, oferece uma autonomia aos titulares, podendo assim controlar o acesso, a correção e até mesmo a exclusão desses dados.

Portanto, os benefícios surgem para ambas as partes, tendo as empresas se beneficiando com a melhoria da governança de dados, uma maior vantagem competitiva, considerando que estar em conformidade com a LGPD indica responsabilidade e compromisso com a privacidade de seus clientes, e automaticamente, estar em conformidade com a Lei reduz riscos de vazamento de dados e incidentes relacionados à segurança, prevenindo multas e sanções, evitando prejuízos significativos.

A Lei Geral de Proteção de Dados (LGPD) do Brasil estabelece uma série de penalidades para aqueles que não cumprirem suas diretrizes. Essas penalidades foram delineadas no artigo 52 da Lei Geral de Proteção de Dados de 2018 e variam em severidade, dependendo da natureza e gravidade da infração cometida.

Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: I - advertência, com indicação de prazo para adoção de medidas corretivas; II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R\$ 50.000.000,00 (cinquenta milhões de reais) por infração; III - multa diária, observado o limite total a que se refere o inciso II; IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência; V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização; VI - eliminação dos dados pessoais a que se refere a infração; VII - (VETADO); VIII - (VETADO); X - (VETADO). X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados (BRASIL, 2018, *online*)

De acordo com o previsto na Lei em seu art. 52, § 1º, o controlador ou operador de dados somente irá receber alguma destas sanções, após o procedimento administrativo que possibilite a ampla defesa. Essas sanções previstas pelos incisos X, XI e XII só podem ser aplicadas após já ter sido imposta ao menos 1 (uma) das sanções de que tratam os incisos II, III, IV, V e VI do caput deste artigo para o mesmo caso concreto.

Ainda no § 1º, do art. 52, dispõe entre os fatores considerados na aplicação das penalidades estão a gravidade da infração, a boa-fé do infrator, a vantagem auferida, e a condição econômica do infrator. A reincidência e o grau de dano causado também são considerados, assim como a cooperação do infrator com as autoridades e a adoção de políticas de boas práticas e governança.

No caso da administração pública, as penalidades aplicáveis são limitadas a advertências, publicização da infração, bloqueio e eliminação de dados, suspensão parcial do banco de dados e suspensão do exercício da atividade de tratamento dos dados. As multas pecuniárias não se aplicam a órgãos públicos, exceto para empresas públicas e sociedades de economia mista que operam em regime de concorrência, que são tratadas como entidades privadas.

A fiscalização inclui monitoramento, orientação e ações preventivas. O monitoramento envolve a coleta de informações para apoiar a tomada de decisões, enquanto a orientação visa educar e conscientizar os agentes de tratamento e os titulares de dados. As ações preventivas buscam reconduzir os agentes de tratamento à conformidade ou evitar situações de risco.

Além das atividades de fiscalização, a ANPD pode realizar atividades repressivas, aplicando sanções através de processos administrativos sancionadores. Para aplicar uma sanção, é necessário regular a metodologia que orientará o cálculo da gravidade da violação, determinando se a infração é de baixa, média ou alta gravidade.

Em suma, as penalidades da LGPD são diversas e escalonadas, visando garantir que as infrações sejam corrigidas e que os direitos dos titulares de dados sejam protegidos. A ANPD desempenha um papel crucial na fiscalização e aplicação dessas penalidades, promovendo um ambiente de conformidade e proteção de dados no Brasil.

CONSIDERAÇÕES FINAIS

A aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil representa um marco significativo na proteção de dados e privacidade, trazendo desafios e oportunidades tanto para entidades públicas quanto privadas. A LGPD exige uma mudança cultural nas organizações, que devem se adaptar a novos processos de transparência e segurança no tratamento de dados pessoais.

Os desafios incluem a adequação às exigências legais, a criação de políticas internas robustas, e a capacitação dos colaboradores para garantir o cumprimento da lei. Além disso, a fiscalização e aplicação de penalidades pela Autoridade Nacional de Proteção de Dados (ANPD) são aspectos cruciais para assegurar a eficácia da LGPD.

Por outro lado, a LGPD oferece oportunidades para empresas que se destacam na conformidade com a lei, podendo aumentar a confiança dos consumidores e melhorar sua reputação no mercado. A proteção de dados também é essencial para a segurança cibernética e a prevenção de incidentes de vazamento de informações, que podem trazer prejuízos financeiros e de imagem.

A comparação com o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia evidencia a necessidade de uma legislação robusta e atualizada para enfrentar os desafios do mundo digital. Ambas as leis compartilham princípios semelhantes, como a minimização de dados, a transparência e a responsabilização, mas a LGPD se adapta ao contexto específico do Brasil, considerando suas particularidades culturais e econômicas.

Em conclusão, a LGPD é uma legislação fundamental para garantir a proteção dos direitos dos indivíduos em relação aos seus dados pessoais. Sua implementação eficaz depende da cooperação entre empresas, autoridades reguladoras e a sociedade em geral. A pesquisa e a análise contínua dos aspectos jurídicos da LGPD são essenciais para aprimorar sua aplicação e garantir a proteção dos dados pessoais no Brasil.

REFERÊNCIAS

Aplicação da Lei Geral de Proteção de Dados (LGPD) na Administração Pública: Um Olhar Detalhado. *Rei Advogado*, 2022. Disponível em:

<https://reyabogado.com/brasil/como-a-lgpd-se-aplica-a-administracao-publica/>. Acesso em 26 em mai. 2024.

BECKER. Rafael Reis. Os desafios da implementação da LGPD em empresas brasileiras. 31 de maio de 2023. Disponível em:

<https://www.direitoempresarial.com.br/os-desafios-da-implementacao-da-lgpd-em-empresas-brasileiras>. Acesso em 25 de mai. 2024.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Brasília, DF, 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em 20 de abril 2024.

CANEDO, F. L. O. Proteção de dados pessoais: o surgimento de um novo direito fundamental no Brasil. *Revista do Tribunal Regional Federal da 3ª Região*, [S. l.], v. 32, n. 149, p. 15–31, 2021. Disponível em:

<https://www.revista.trf3.jus.br/index.php/rtrf3/article/view/196>. Acesso em: 08 fev. 2024.

CARDOSO, Rafaella Ranniele Cândido. LGPD - Lei Geral De Proteção De Dados: o desafio do micro empreendedor individual, das micro e pequenas empresas quanto ao seu custo, adequação e implementação. Orientador: Bruno Fonseca Gurão. 2021. 29f. Trabalho de Conclusão de Curso (Bacharel em Direito) - Centro Universitário do Planalto Central Aparecido dos Santos, 2021. Disponível em:

<https://dspace.uniceplac.edu.br/handle/123456789/1689>. Acesso em 24 de mai. 2024.

DIÁRIO Oficial da União, Resolução CD/ANPD nº 2, de janeiro de 2022, publicado em 28/01/2022, Edição 20, Seção 1, Página 6. Disponível em:

<https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019#wrapper>. Acesso em 21 mai. 2024

GARRIDO, Patricia P. Proteção de dados pessoais: comentários à lei n. 13.709/2018 (LGPD). SRV Editora LTDA, 2023. E-book. ISBN 9786555599480. Disponível em:

[https://integrada.minhabiblioteca.com.br/reader/books/9786555599480/epubcfi/6/34\[%3Bvnd.vst.idref%3Dcap08.xhtml\]!/4](https://integrada.minhabiblioteca.com.br/reader/books/9786555599480/epubcfi/6/34[%3Bvnd.vst.idref%3Dcap08.xhtml]!/4) Acesso em: 14 mai. 2024.

JUSBRASIL. Artigo 55 da Lei nº 13.709 de 14 de Agosto de 2018. Disponível em: jusbrasil.com.br/topicos/200398514/artigo-55-da-lei-n-13709-de-14-de-agosto-de-2018. Acesso em: 24 de maio. 2024.

LEI Geral de Proteção de Dados Pessoais completa quatro anos com avanços e desafios. Agência Câmara de Notícias, 2022. Disponível em: <https://www.camara.leg.br/noticias/904176-lei-geral-de-protecao-de-dados-pessoais-completa-quatro-anos-com-avancos-e-desafios/>. Acesso em 22 de fev. 2024.

LGPD: Um marco na regulamentação sobre dados pessoais no Brasil. STJ. Disponível em: <https://www.stj.jus.br/sites/portalp/WebPub/NovoPortal/LGPD.aspx>. Acesso em 23 de mai. 2024.

LIMA RAPÔSO, C. F.; MELO DE LIMA, H.; DE OLIVEIRA JUNIOR, W. F.; FERREIRA SILVA, P. A. .; ELAINE DE SOUZA BARROS, E. . LGPD - LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS EM TECNOLOGIA DA INFORMAÇÃO: Revisão Sistemática. RACE - Revista de Administração do Cesmac, [S. l.], v. 4, p. 58–67, 2019. DOI: 10.3131/race.v4i0.1035. Disponível em: <https://revistas.cesmac.edu.br/administracao/article/view/1035>. Acesso em: 07 fev. 2024.

LIMA, Victtor Henrique. LGPD análise dos impactos da implementação em ambientes corporativos: estudo de caso. Pontifícia Universidade Católica de Goiás, 2020. Disponível em: <https://repositorio.pucgoias.edu.br/jspui/handle/123456789/108>. Acesso em 16 de mar. 2024.

MAFRA, Ediléia. Proteção da Privacidade no Brasil: Desafios, Oportunidades e Avaliação da efetividade da LGPD. Jus Navigandi, 2023. Disponível em: <https://jus.com.br/artigos/103414/protecao-da-privacidade-no-brasil-desafios-oportunidades-e-avaliacao-da-efetividade-da-lgpd>. Acesso em 25 de mai. 2024

PLANALTO, Lei Geral de Proteção de Dados (Lei nº 13.709, de 14 de agosto de 2018). Brasília, DF, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em 08 de mai. 2022.

PRÓXIMO, R.; SILVA. A. C. M. Impacto da LGPD nas Pequenas e Médias empresas Small and Medium Business. OAB Campinas, Disponível em: <https://oabcampinas.org.br/impacto-da-lgpd-nas-pequenas-e-medias-empresas-small-and-medium-business/>. Acesso em 15 mar. 2024.

SOLER, Fernanda G. Proteção de dados: reflexões práticas e rápidas sobre a LGPD. SRV Editora LTDA, 2022. E-book. ISBN 9786553622500. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786553622500/>. Acesso em: 26 de maio. 2024.