UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE DIREITO

JEAN CARLOS DA COSTA LIMA DE OLIVEIRA

IMPLEMENTAÇÃO DE PROTEÇÃO DE DADOS PARA PEQUENAS E MÉDIAS EMPRESAS

Uberlândia - MG
2023

JEAN CARLOS DA COSTA LIMA DE OLIVEIRA

IMPLEMENTAÇÃO DE PROTEÇÃO DE DADOS PARA PEQUENAS E MÉDIAS EMPRESAS

Trabalho de conclusão de curso apresentado à graduação em Direito da Faculdade de Direito da Universidade Federal de Uberlândia, como requisito para obtenção do título de Bacharel em Direito.

Orientador: Prof. Dr. Almir Garcia Fernandes

Uberlândia - MG
2023

IMPLEMENTAÇÃO DE PROTEÇÃO DE DADOS PARA PEQUENAS E MÉDIAS EMPRESAS

Trabalho de Conclusão de Curso apresentado como exigência parcial para obtenção do título de Bacharel em Direito à Universidade Federal de Uberlândia pela banca examinadora formada por:

Uberlândia, 30 de outubro de 2023.

_____

Dr. Almir Garcia Fernandes
Universidade Federal de Uberlândia

_____

Dr. Ricardo Padovini Pleti Ferreira
Universidade Federal de Uberlândia

_____

Mestrando José Henrique de Oliveira Couto
Universidade Federal de Uberlândia

Dedico este trabalho de conclusão de curso acima de tudo a Deus, a toda a minha família, principalmente a minha mãe que sempre me incentivou e me encorajou e a minha noiva que nos dias mais difíceis me deu todo suporte necessário para que eu os vencesse.

IMPLEMENTAÇÃO DE PROTEÇÃO DE DADOS PARA PEQUENAS E MÉDIAS EMPRESAS

Jean Carlos da Costa Lima de Oliveira[1]

RESUMO

O presente artigo tem como objetivo analisar a implementação da Lei Geral de Proteção de Dados (LGPD) no contexto de pequenas e médias empresas (PMEs). Enquanto é amplamente reconhecido o valor da proteção de dados para grandes empresas, este estudo visa compreender como as PMEs podem se beneficiar ou ser prejudicadas ao adotar práticas de conformidade com a LGPD. Considerando que as PMEs geralmente possuem menos pessoal, processos, informações e recursos, exploraremos as oportunidades e desafios que surgem durante a implementação da LGPD no dia a dia dessas empresas.

Palavras-chave: Lei de Proteção de Dados; Implementação; pequenas e médias empresas.

[1] Graduando em Direito pela Universidade Federal de Uberlândia.

ABSTRACT

This article aims to analyze the implementation of the General Data Protection Law (LGPD) in the context of small and medium-sized enterprises (SMEs). While the value of data protection for large companies is widely recognized, this study seeks to understand how SMEs can benefit from or be adversely affected by adopting LGPD compliance practices. Considering that SMEs typically have fewer personnel, processes, information, and resources, we will explore the opportunities and challenges that arise during the day-to-day implementation of LGPD in these companies.

Keywords: Data Protection Law; Implementation; Small and Medium-sized enterprises.

SUMÁRIO

Introdução

A proteção de dados pessoais tornou-se um desafio crucial na era digital, impulsionada pelo rápido avanço da tecnologia e pela crescente preocupação com a privacidade dos indivíduos. Nesse contexto, a Lei Geral de Proteção de Dados (LGPD)[2] foi promulgada no Brasil, estabelecendo diretrizes e requisitos para o tratamento adequado dos dados pessoais por todos aqueles que possuem acesso aos dados de terceiros. Embora a importância da proteção de dados seja amplamente reconhecida para grandes empresas, a adoção e implementação da LGPD podem ser um desafio particularmente complexo para as pequenas e médias empresas.

As PMEs representam uma parcela significativa do setor empresarial e desempenham um papel crucial na economia. No entanto, elas geralmente enfrentam recursos limitados, tanto financeiros quanto humanos, o que pode dificultar a implementação de práticas adequadas de proteção de dados. Além disso, grande parte destas empresas podem ter menos familiaridade com as implicações jurídicas e operacionais da LGPD, tornando o processo de conformidade ainda mais desafiador.

Compreender como a implementação da LGPD afeta as PMEs é de extrema importância, pois essas empresas lidam diariamente com dados pessoais de clientes, funcionários e parceiros de negócios. A LGPD não apenas impõe obrigações específicas às PMEs, mas também apresenta oportunidades significativas para melhorar a confiança dos clientes, a reputação da marca e a competitividade no mercado.

O presente artigo tem como objetivo uma análise minuciosa sobre a implementação da Lei Geral de Proteção de Dados (LGPD), no contexto das Pequenas e Médias Empresas. Serão examinadas as oportunidades e desafios emergentes durante o processo de conformidade, levando em consideração as limitações e peculiaridades inerentes a essas organizações. Pretende-se discutir estratégias práticas que possam ser adotadas pelas PMEs para enfrentar esse desafio, com o propósito de auxiliá-las na proteção adequada dos dados pessoais e no cumprimento das exigências legais.

---

[2] Lei nº 13.709, de 14 de agosto de 2018.

Surge, então, a pertinente indagação: as exigências delineadas na legislação são aplicáveis à realidade das pequenas e médias empresas? Considerando que a conformidade legal pode se configurar como um processo dispendioso capaz de ameaçar a continuidade de suas operações.

No decorrer deste estudo, serão abordados aspectos cruciais da LGPD, tais como os direitos dos titulares dos dados, as obrigações das PMEs, as medidas de segurança necessárias e as penalidades decorrentes da não conformidade. Serão apresentadas também estratégias práticas para a implementação da LGPD, levando em consideração os recursos e as características destas empresas.

Em resumo, esta pesquisa almeja contribuir para a compreensão dos desafios e das oportunidades enfrentados pelas PMEs ao implementar a LGPD. Espera-se que este texto ofereça insights valiosos para gestores, profissionais de tecnologia e demais interessados na proteção de dados pessoais no âmbito das PMEs, fornecendo auxílio e direcionamento.

No âmbito metodológico, optou-se pelo método de pesquisa dedutivo, um enfoque que busca validar constatações gerais e transformá-las em soluções aplicáveis a casos específicos. Este método se revela apropriado para investigar a aplicabilidade das normas e diretrizes da LGPD no contexto das PMEs. A abordagem dedutiva possibilita a formulação de hipóteses a partir de princípios estabelecidos na legislação. Além disso, permite a análise crítica das estratégias práticas propostas para a implementação da norma legal, levando em consideração os recursos e particularidades das pequenas e médias empresas.

Para alcançar os objetivos da pesquisa, serão utilizadas pesquisas bibliográficas que são fundamentais para aprofundar o conhecimento sobre a LGPD, compreendendo suas nuances, diretrizes e implicações. A análise documental permitirá uma investigação detalhada das normativas relacionadas à proteção de dados e das informações provenientes de órgãos regulatórios. O estudo dogmático jurídico possibilitará uma análise crítica da legislação, considerando a interpretação doutrinária. A abordagem qualitativa será adotada para compreender as percepções

e experiências das PMEs na implementação da LGPD, destacando desafios e possíveis estratégias de conformidade.

Esse conjunto de abordagens metodológicas visam proporcionar uma análise abrangente e aprofundada da implementação da LGPD, fornecendo subsídios para a compreensão das questões legais, técnicas e operacionais envolvidas. A integração dessas metodologias oferecerá uma visão ampla e embasada, permitindo a identificação de melhores práticas e o desenvolvimento de recomendações para facilitar a conformidade das PMEs com as exigências da LGPD.

1. LEI GERAL DE PROTEÇÃO DE DADOS: ASPECTOS GERAIS

1.1. Evolução Histórica da LGPD

De acordo com Pinheiro (2018, p. 13), com o avanço acelerado da internet e os desafios que surgiram, o debate sobre a privacidade e proteção de dados pessoais ganhou destaque a partir dos anos 1990, impulsionado pelo crescimento da economia digital e a necessidade de regular os fluxos de informações pessoais em âmbito global. Essa preocupação está diretamente relacionada à garantia dos direitos fundamentais, incluindo o direito à privacidade, consagrado na Declaração Universal dos Direitos Humanos e recentemente tal proteção ganhou maior notoriedade com a sua inclusão no Art. 5º da Constituição Federal de 1.988, no inciso LXXIX[3].

O marco inicial desse debate ocorreu na União Europeia (UE), com a aprovação do Regulamento Geral de Proteção de Dados Pessoais (GDPR)[4] em abril de 2016. As leis de proteção de dados pessoais se caracterizam por princípios

[3] Art. 5º, LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.

[4] REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO. 4 maio 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN. Acesso em: 16 de julhode 2023.

fundamentais e indicadores técnicos que permitem avaliar o cumprimento desses princípios.

O GDPR estabeleceu regras rigorosas para a proteção de dados pessoais e a livre circulação desses dados, exigindo sua implementação até maio de 2018. Conforme, Pinheiro (2018, p. 14), a adoção do GDPR pela UE teve um efeito dominó, pois passou a exigir que outros países e empresas que tivessem relações comerciais com a UE também adotassem uma legislação de proteção de dados equivalente E como penalidade aqueles que não aderissem à conformidade poderia resultar em barreiras econômicas ou dificuldades nas relações comerciais.

Diante dessa realidade, a maioria dos países, especialmente os da América Latina, precisou se adequar às exigências do GDPR. No contexto brasileiro, a Lei Geral de Proteção de Dados (LGPD) foi promulgada em 2018, inspirada no GDPR europeu.

A LGPD visa assegurar a proteção dos direitos fundamentais em relação ao tratamento de seus dados pessoais, seja por pessoa natural, seja por pessoa jurídica. Ela estabelece princípios, direitos dos titulares dos dados, obrigações para as organizações que coletam e processam dados, além de medidas de segurança e penalidades por não conformidade.

De acordo com o art. 1º da LGPD pode-se perceber que ela tem como objetivo proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Logo, busca resgatar a dignidade dos titulares de dados e seus direitos básicos relacionados à autodeterminação informativa.

A partir do comentário da autora Patrícia Peck Pinheiro, depreende-se que o texto legal considera como tratamento de dados:

> Toda operação realizada com algum tipo de manuseio de dados pessoais: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, edição, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (2018, p.109).

Representa um marco regulatório importante para o Brasil, pois reforça a proteção da privacidade e a importância da transparência no tratamento de dados pessoais. Sua implementação impacta não apenas grandes empresas, mas também as pequenas e médias empresas (PMEs), que enfrentam desafios específicos devido a suas limitações de recursos e conhecimento. Representa um marco regulatório importante para o Brasil.

Vale salientar ainda que a legislação de proteção de dados busca estimular a aplicação de seus dispositivos em caráter preventivo ao exigir que o tratamento dos dados pessoais atenda aos requisitos legais, em caso de descumprimento incorre a aplicação de sanções administrativas que podem chegar a uma multa diária de 2% do faturamento, limitado a R$50 milhões de reais, além da suspensão das atividades relacionadas ao tratamento dos dados pessoais, regra estipulada no art. 52 da LGPD.

1.2. Aplicabilidade da LGPD às Empresas de Pequeno e Médio Porte

Para compreender plenamente os aspectos da aplicação da Lei Geral de Proteção de Dados (LGPD), é essencial ter em mente que o conceito de Pequenas e Médias Empresas (PMEs) se baseia em critérios como o número de funcionários, o faturamento anual e o ativo total da empresa. No Brasil, a Lei Complementar nº 123 de 2006, em seu art. 3º, estabelece critérios com base no faturamento anual para classificar as empresas: microempresas (ME)[5] com faturamento bruto anual de até R$ 360 mil, empresas de pequeno porte (EPP) [6] com faturamento entre R$ 360 mil e R$ 4,8 milhões, e médias empresas com faturamento entre R$ 4,8 milhões e R$ 300 milhões.

[5] I - no caso da microempresa, aufira, em cada ano-calendário, receita bruta igual ou inferior a R$ 360.000,00 (trezentos e sessenta mil reais);

[6] II - no caso de empresa de pequeno porte, aufira, em cada ano-calendário, receita bruta superior a R$ 360.000,00 (trezentos e sessenta mil reais) e igual ou inferior a R$ 4.800.000,00 (quatro milhões e oitocentos mil reais).

Deste modo, as PMEs se destacam por sua estrutura enxuta e escala operacional menor em comparação com as grandes empresas. Geralmente possuem menos funcionários, recursos financeiros limitados, estruturas organizacionais simplificadas e menor capacidade de investimento em tecnologia. Essas empresas estão presentes em diversos setores, como comércio, serviços, indústria e tecnologia.

Dentre os diversos agentes de apoio aos empreendedores brasileiros destaca-se o SEBRAE – Serviço Brasileiro de Apoio às Micro e Pequenas Empresas. Segundo dados do SEBRAE, as pequenas e médias empresas respondem por mais de um quarto do Produto Interno Bruto (PIB) brasileiro, representando 27% do PIB e gerando uma produção de R$ 599 bilhões em 2011. Além disso, essas empresas são responsáveis por 52% dos empregos formais e 40% da massa salarial do país[7].

No contexto da Lei Geral de Proteção de Dados (LGPD), essas informações ressaltam a necessidade premente de que as pequenas e médias empresas (PMEs) observem e implementem as etapas de tratamento dos dados previstas na norma. A coleta, armazenamento e processamento de dados pessoais devem seguir diretrizes claras e adequadas para garantir a segurança e a privacidade das informações, tanto para os consumidores quanto para as próprias empresas.

Outrossim, é importante observar que a responsabilidade acarretada por um incidente é objetiva, com exceção das situações previstas nos artigos 43[8] e 44[9] da

---

[7] SEBRAE, Micro e Pequenas empresas geram 27% do PIB do Brasil. 2011. Disponível em: https://sebrae.com.br/sites/PortalSebrae/ufs/mt/noticias/micro-e-pequenas-empresas-geram-27-do-pib-do-brasil,ad0fc70646467410VgnVCM2000003c74010aRCRD#:~:text=As%20micro%20e%20pequenas%20empresas,empresas%20(24%2C5%25). Acesso em: 01 de outubro de 2023.

[8] Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem: I - que não realizaram o tratamento de dados pessoais que lhes é atribuído; II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou, III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiros.

[9] Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais: I - o modo pelo qual é realizado; II - o resultado e os riscos que razoavelmente dele se esperam; III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado Parágrafo único. Responde pelos danos decorrentes da violação da segurança

legislação em vigor que abordam a isenção dos agentes de tratamento de dados e estabelecem o conceito de tratamento irregular Contudo, a responsabilidade dos agentes de tratamento de pequeno porte, como foram intitulados pela ANPD na resolução de nº 2 de janeiro de 2022, foi flexibilizada para que estas categorias de empresas tenham maior facilidade em se adequarem as regras[10].

Logo, torna-se perceptível que a responsabilização será afastada mediante a comprovação, pelos agentes, da ausência de tratamento de dados pessoais, da inexistência de violação das normas de proteção de dados ou da ocorrência de danos exclusivamente por culpa do titular dos dados pessoais ou de terceiros.

Portanto, caso os agentes não consigam demonstrar a adoção dessas medidas, estarão sujeitos à responsabilidade. Considerando que a simples desconformidade com a legislação já resultará em responsabilidade para o agente de tratamento, evidencia-se a possível adoção de uma teoria de responsabilidade civil objetiva, a qual não exige a comprovação de culpa para sua aplicação (Novakoski e Naspolini, 2020, p. 162-163).

Ademais, Maria Celina Bodin de Moraes aponta que a LGPD incorpora uma abordagem chamada "responsabilidade proativa" (ou *accountability*em inglês). Esse princípio significa que as organizações são responsáveis por adotar medidas proativas para garantir a conformidade com a lei e a proteção dos dados pessoais que estão sob sua responsabilidade, no qual o eixo axiológico do instituto se deslocaria da reparação do dano para sua prevenção de forma eficaz:

> Trata-se do conceito de “prestação de contas”. Esse novo sistema de responsabilidade, que vem sendo chamado de “responsabilização ativa” ou “proativa”, encontra-se indicado no inciso X do art. 6º, que determina às empresas não ser suficiente cumprir os artigos da lei; será necessário também “demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de

dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano.

[10]Art. 6º A dispensa ou flexibilização das obrigações dispostas neste regulamento não isenta os agentes de tratamento de pequeno porte do cumprimento dos demais dispositivos da LGPD, inclusive das bases legais e dos princípios, de outras disposições legais, regulamentares e contratuais relativas à proteção de dados pessoais, bem como direitos dos titulares.

> dados pessoais e, inclusive, a eficácia dessas medidas". Portanto, não descumprir a lei não é mais suficiente; é preciso "proativamente" prevenir a ocorrência de danos (MORAES, 2019, p. 5)

Ademais, há também o dever de indenização decorrente da violação das normas técnicas estabelecidas pela Autoridade Nacional de Proteção de Dados (ANPD), conforme expresso no artigo 44, parágrafo único[11] da Lei Geral de Proteção de Dados (LGPD).

Dessa forma, conforme evidenciado pelos dispositivos legais mencionados, não se faz necessária a comprovação de culpa por parte do agente, pois a mera falta de adoção de práticas adequadas de segurança de dados já é suficiente para ensejar a responsabilidade por eventuais vazamentos de dados pessoais. Na mesma esteira, decidiu a 17ª câmara do Tribunal de Justiça de Minas Gerais:

> MENTA: APELAÇÃO CÍVEL. AÇÃO DECLARATÓRIA DE INEXIGIBILIDADE DE DÉBITOS. PRELIMINARES. OFENSA AO PRINCÍPIO DA DIALETICIDADE. NÃO CONSTATADA. AUSÊNCIA DE INTERESSE DE AGIR. NÃO CONFIGURADA. ILEGITIMIDADE PASSIVA AD CAUSAM. REJEITADA. MÉRITO. "GOLPE DO MOTOBOY". RESPONSABILIDADE CIVIL OBJETIVA. FALHA NA PRESTAÇÃO DOS SERVIÇOS. **VAZAMENTO DE DADOS PESSOAIS DO CORRENTISTA. DANOS MATERIAIS CONFIGURADOS. DANOS MORAIS**. MINORAÇÃO. IMPOSSIILIDADE. MULTA POR DESCUMPRIMENTO DA LIMINAR. CABIMENTO.
> - Não há que se falar em ofensa ao princípio da dialeticidade se a parte recorrente, nas razões recursais abordou quantum satis, os fundamentos da sentença vergastada, declinando os motivos do pedido de sua revisão.
> - Há interesse de agir sempre que a tutela jurisdicional pleiteada é necessária para a obtenção do bem ou do direito almejado e adequado para proporcionar o resultado pretendido.
> - A legitimidade passiva "ad causam" deve ser aferida com base na Teoria da Asserção, à luz do disposto na causa de pedir constante da petição inicial, sem adentrar na análise probatória.
> - **O banco deve ser responsabilizado pelos danos oriundos da fraude da qual o autor foi vítima, uma vez que o imbróglio**

[11] Art.44, Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano.

> **somente se aperfeiçoou em razão da violação de dados pessoais e bancários do consumidor, em decorrência de falha dos serviços administrativos do banco.**
> - Os transtornos, dissabores e constrangimentos impostos ao consumidor em decorrência da cobrança indevida de compras realizadas em seu cartão de crédito, por estelionatários, são causas suficientes para gerar a obrigação de indenizar por danos morais.
> - O valor da indenização por dano moral deve ser arbitrado em consonância com os princípios da razoabilidade e da proporcionalidade, observado o caráter pedagógico, punitivo e reparatório da indenização.
> - Havendo fixação de astreinte e evidenciado o descumprimento da ordem judicial que lhe deu origem, a condenação da parte inadimplente, ao seu pagamento, é medida que se impõe. (TJMG - Apelação Cível 1.0000.21.237391-4/002, Relator(a): Des.(a) Aparecida Grossi , 17ª CÂMARA CÍVEL, julgamento em 30/08/2023, publicação da súmula em 31/08/2023).

Portanto, as PMEs devem estar cientes das responsabilidades e obrigações estabelecidas pela LGPD em relação à coleta, armazenamento e processamento de dados pessoais. A adoção de práticas adequadas. A ausência de práticas em conformidade com a Lei de Proteção de Dados pode expor as pequenas e médias empresas a diversos riscos que podem afetar negativamente o seu funcionamento e reputação.

Em suma, a observância da LGPD e a implementação de boas práticas no tratamento de dados são essenciais para assegurar a continuidade e o crescimento das PMEs, contribuindo significativamente para o desenvolvimento econômico do Brasil. Ao abraçar as exigências de privacidade de dados, as PMEs estão não apenas cumprindo uma obrigação legal, mas também promovendo a confiança e o respeito dos consumidores, elementos-chave para um sucesso sustentável nos mercados atuais e futuros.

2. DA AVALIAÇÃO DE IMPACTOS E MAPEAMENTO DE DADOS

2.1. Avaliação de Impactos

A avaliação de impacto sobre a proteção de dados, também conhecida como AIPD ou DPIA (Avaliação de Impacto Sobre Proteção de Dados ou Data Protection Impact Assessment), é uma etapa essencial para garantir a conformidade com a LGPD. Esta obrigação é prevista no artigo 35º[12] do RGPD - Regulamento Geral Sobre a Proteção de Dados, qual seja:

> Quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento procede, antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais. Se um conjunto de operações de tratamento que apresentar riscos elevados semelhantes, pode ser analisado numa única avaliação.

Ela envolve a análise e a identificação dos riscos e impactos que determinado tratamento de dados pode ter sobre a privacidade dos indivíduos. De acordo com Frazão; Oliva; Abilio na obra Lei Geral de Proteção de Dados e suas repercussões no Direito Brasileiro: As regras vinculativas serão, portanto, derivadas da coerência na aplicação do RGPD. Esse objetivo visa a trazer uma normalização técnica e jurídica em relação à aplicação do regulamento na União Europeia.

Além disso, o RGPD determina que para que a avaliação de impactos dos dados seja aplicada com segurança é necessário a observação de quatro aspectos para o tratamento destes dos dados, descritos no art. 35º do RGPD[13]:

I. Uma descrição sistemática das operações de tratamento previstas e a finalidade do tratamento, inclusive, se for caso disso, os interesses legítimos do responsável pelo tratamento;
II. Uma avaliação da necessidade e proporcionalidade das operações de tratamento em relação aos objetivos;
III. Uma avaliação dos riscos para os direitos e liberdades dos titulares dos direitos a que se refere o n. 1º; e;
IV. As medidas previstas para fazer face aos riscos, incluindo as garantias, medidas de segurança e procedimentos destinados a assegurar a

[12] UI-COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS. CNPD. Disponível em: <https://www.cnpd.pt/organizacoes/obrigacoes/avaliacao-de-impacto/>. Acesso em: 16 jul. 2023.

[13] Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN>. Acesso em: 16 jul. 2023.

> proteção dos dados pessoais e a demonstrar a conformidade com o presente regulamento, tendo em conta os direitos e os legítimos interesses dos titulares dos dados e de outras pessoas em causa.

Deste modo, para a correta aplicação do RGPD é necessário levar em conta as características dos diferentes setores de tratamento e as necessidades específicas das micro, pequenas e médias empresas.

Por isso, a AIPD, conforme estabelecido no artigo 5º, inciso VI da LGPD, é um processo de análise e identificação dos riscos e impactos que o tratamento de dados pessoais pode ter sobre a privacidade dos indivíduos. Para as PMEs, é essencial compreender que a AIPD é uma medida proativa e preventiva, permitindo identificar e mitigar riscos antes que se tornem problemas reais (Frazão; Olivia; Abilio, 2020, p. 555).

2.2 Mapeamento de Dados

O mapeamento de dados, também é conhecido como inventário de dados, *data mapping* ou *data flow ,* essa etapa no tratamento dos dados é umas das etapa de maior relevância de todo o controle. Por isso, foi previsto no artigo 23º da LGPD[14], que as PMEs devem mapear suas atividades de tratamento de dados, identificando quais dados são coletados, como são armazenados, processados e compartilhados.

Aqui os dados passam a serem coletados e catalogados, incluindo todos os processos e procedimentos em que os dados transitam, assim como as bases legais que permitem à empresa realizar o tratamento de todos os dados da maneira correta,

---

[14] Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:

I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos;

aqueles com maior nível de sensibilidade possuem maior rigor do que os dados mais seguros (Pinheiro, 2018, p. 72-74).

O mapeamento de dados visa a garantia da proteção dos direitos dos titulares dos dados pessoais, como o objetivo de garantir a efetivação do direito de transparência, elencado no art. 6º, X[15] da LGPD, pautado na indicação de princípios relativos ao tratamento de dados pessoais, cuja ação deve respeitar os limites dos direitos fundamentais (Pinheiro, 2018, p. 45).

O principal objetivo do mapeamento de dados é gerar um diagnóstico de como a empresa lida com a privacidade e a segurança de seus clientes, colaboradores, fornecedores e parceiros. Tal exigência é prevista no art. 37[16] da LGPD.

Esse mapeamento permite uma visão clara do fluxo de dados e ajuda a identificar potenciais riscos e vulnerabilidades no tratamento dessas informações.

Ao realizar o mapeamento, é possível classificar, catalogar e organizar os dados de acordo com suas categorias, tais como cadastrais, transacionais, especiais, sensíveis e trabalhistas, além de compreender o volume e a frequência do tráfego dessas informações. Nesse processo, é fundamental descrever detalhadamente as etapas[17] de tratamento do fluxo, incluindo coleta, armazenagem, sanitização, enriquecimento, processamento, segmentação, inferências, transferências e descarte.

De acordo com Patrícia Peck Pinheiro na obra "Proteção de Dados Pessoais: Comentários à Lei Nº13.709/2018", é fundamental mapear as principais tecnologias empregadas no tratamento de dados, bem como os locais de coleta, armazenamento,

---

[15] X – responsabilização e prestação de contas: demonstração, pelo agente, da 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.

[16] 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.

[17] BRANDAO, G. Mapeamento de Dados: O que é e como fazer data mapping. BL Consultoria Digital, 27 Feb. 2020. Disponível em: <https://blconsultoriadigital.com.br/mapeamento-de-dados/>. Acesso em: 22 jul. 2023

processamento e origem dos dados, além dos u compartilhamentos. Essa análise abrange também a verificação de transferências internacionais.

A convergência da legislação brasileira, conforme preconizada pelo GDPR, implica na necessidade de regulação dos fluxos transfronteiriços de dados, exigindo que os países envolvidos garantam a proteção dos dados em conformidade com a LGPD. Dessa forma, o Brasil adere ao movimento global de padronização, assegurando o desenvolvimento tecnológico e econômico sem comprometer direitos e garantias fundamentais (Pinheiro, 2018, p.70 - 71).

Outro aspecto essencial é a base legal para o tratamento dos dados, garantindo que o fluxo esteja de acordo com os direitos dos titulares, incluindo menores de idade (18 anos incompletos), que devem ter seus dados coletados de forma adequada e com a devida permissão (Pinheiro, 2018, p. 56).

Após o mapeamento, é necessário avaliar os riscos e impactos associados a cada atividade de tratamento de dados. A LGPD estabelece princípios como finalidade, adequação, necessidade, transparência e responsabilização, que devem guiar o tratamento. Essa avaliação deve considerar possíveis consequências negativas para a privacidade dos titulares dos dados e possibilitar a adoção de medidas para mitigar e minimizar esses riscos (Pinheiro, 2018, p. 25 - 26).

Nesse sentido, a implementação de medidas de segurança técnicas e organizacionais, como criptografia, controle de acesso e monitoramento, é fundamental para garantir a proteção adequada dos dados pessoais. É preciso agir de forma proativa para proteger as informações coletadas, armazenadas, processadas, compartilhadas e transferidas.

Além disso, a empresa deve documentar todo o processo de mapeamento de dados e avaliação de riscos, incluindo as medidas adotadas e as justificativas para suas decisões. Essa documentação é essencial para comprovar a conformidade com a legislação e criar um histórico que evidencie o comprometimento da empresa com a privacidade e a segurança dos dados.

Dessa forma, ao realizar o mapeamento de dados, avaliar os riscos e impactos, adotar medidas de mitigação e minimização, e documentar todo o processo, as

pequenas e médias empresas estarão bem preparadas para implementar a LGPD de forma efetiva, garantindo a proteção dos dados pessoais e o cumprimento das exigências legais.

3. Medidas de Segurança e Boas Práticas para a Proteção de Dados em PMEs

3.1 Medidas de Segurança

As medidas de segurança de dados é um dos principais eixos da Lei Geral de Proteção de Dados (LGPD), em seu art. 46[18] é enfática em delegar a responsabilidade aos controladores e operadores, como agentes de tratamento, devem aplicar medidas de segurança, técnicas e administrativas, capazes de proteger os dados pessoais dos de acessos não autorizados e de situações acidentais ou ilícitas que possam causar dano aos seus titulares (COTS, Márcio; OLIVEIRA, Ricardo, 2019, p. 186).

A proteção dos dados pessoais é um aspecto de suma importância na LGPD, sendo enfatizada pelas medidas de segurança e sigilo dos dados, conforme estabelecido no art. 46 da referida lei, que preconiza a proteção dos dados pessoais contra acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Um dos pilares para promover a segurança da informação é a observância dos requisitos aplicados ao tratamento de dados pessoais, conforme demonstrado na influência do Regulamento Geral sobre a Proteção de Dados (GDPR) na criação da legislação brasileira.

A LGPD enfatiza que o tratamento de dados pessoais deve ser norteado pela boa-fé, possuir finalidade e limites bem definidos, incluir prestação de contas e garantir

[18] Art. 46. Os agentes de tratamento devem adotar medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito.

a segurança por meio de técnicas e medidas adequadas, bem como transparência e a possibilidade de consulta pelos titulares (Pinheiro, 2018, p. 79).

Ademais, o texto normativo, no §1º do art. 46[19], define que a Autoridade Nacional de Proteção de Dados poderá definir padrões técnicos mínimos para que a própria ANPD possa fiscalizar seu devido cumprimento com base em critérios objetivos. Contudo, a Autoridade Nacional de Proteção de Dados, ainda não definiu quais os padrões técnicos mínimos as empresas deverão cumprir, por isso, as boas práticas são fundamentais neste momento de desenvolvimento dos mecanismos de proteção dos dados.

De acordo com Fabio Correa Xavier, em artigo publicado pela MIT Technology Review[20], a falta de definição dos padrões técnicos mínimos cria uma lacuna que pode ser preenchida com as boas práticas do mercado. As organizações são encorajadas a adotar as melhores práticas disponíveis e seguir os princípios e diretrizes da LGPD, mesmo na ausência de orientações específicas da ANPD. O uso de boas práticas do mercado é uma abordagem prudente para garantir o cumprimento da LGPD e demonstrar compromisso com a proteção de dados pessoais, enquanto aguarda as diretrizes mais detalhadas da ANPD.

3.2 Boas Práticas para a Proteção de Dados em PMEs

No contexto das pequenas e médias empresas (PMEs), a proteção de dados pessoais assume um papel fundamental em conformidade com a LGPD. Nesse sentido, é vital a implementação de medidas de segurança e a adoção de boas práticas para resguardar os dados pessoais que manipulam.

---

[19] § 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.

[20] XAVIER, Fabio Correa, MIT Technology Reveiw, 2021, **Quais São os Padrões Técnicos Mínimos Exigidos Pela LGPD.** Disponível em: https://mittechreview.com.br/quais-sao-os-padroes-tecnicos-minimos-exigidos-pela-lgpd/ , acesso em: 13 de outubro de 2023.

Percebe-se que assegurar a segurança da informação é uma tarefa que deve ser considerada desde a concepção do produto ou serviço até sua execução. Ao incorporar a privacidade desde o estágio inicial de desenvolvimento, em vez de ajustes posteriores, a proteção de dados torna-se mais eficaz. Por exemplo, a aplicação de criptografia de ponta a ponta garante que os dados permaneçam protegidos durante sua transmissão entre sistemas.

Ao abordar as boas práticas de proteção de dados, na obra Lei Geral de Proteção de Dados Pessoais: e Suas Repercussões no Direito Brasileiro, Gustavo Tepedino, Ana Frazão e Milena Donato Oliva, em 2020[21], esclarece que o conceito *privacy by design,* é um dos pilares da proatividade e prevenção, almejada pelo texto da lei. Este Conceito reforça a importância de que a privacidade deve ser integrada como princípio desde o início do desenvolvimento de instrumentos tecnológicos ou modelos de negócios.

A implementação de um sistema de controle de acesso é essencial para restringir o acesso aos dados pessoais apenas a pessoas autorizadas. As PMEs devem estabelecer políticas de acesso baseadas em níveis de permissão, garantindo que somente os funcionários que precisam acessar determinados dados possam fazê-lo. Além disso, é fundamental monitorar e revisar regularmente os privilégios de acesso (Pinheiro, 2018, p. 38).

A conscientização dos funcionários desempenha um papel fundamental na proteção de dados em uma PME. Por meio de treinamentos e workshops sobre segurança da informação e boas práticas de proteção de dados, os funcionários podem compreender a importância da privacidade e segurança dos dados pessoais. A definição de políticas internas que incentivem o cumprimento das práticas de proteção de dados também é relevante nesse contexto.

Manter os sistemas e *softwares* atualizados é crucial para garantir a segurança dos dados. As PMEs devem adotar práticas de atualização regular de sistemas

[21] TEPEDINO, G.; OLIVA, A. F. E. M. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. Thomson Reuters Brasil, 2020. P. 302 - 303.

operacionais, aplicativos e softwares de segurança, além de aplicar patches de segurança fornecidos pelos fabricantes. Isso contribui para corrigir vulnerabilidades conhecidas e minimizar os riscos de ataques cibernéticos (Atheniense, 2019, p. 28).

A realização de *backups* regulares dos dados é uma prática fundamental para assegurar a disponibilidade e integridade das informações. As PMEs devem implementar um plano de backup que garanta a cópia segura e periódica dos dados, armazenando-os em locais separados e protegidos. Isso possibilita a recuperação dos dados em caso de perda devido a incidentes (Brandão, BL Consultoria, 2020).

Portanto, elaborar uma política de privacidade clara e transparente, juntamente com termos de uso, é uma prática recomendada. Esses documentos devem informar aos usuários como seus dados serão coletados, armazenados, processados e compartilhados, estabelecendo uma relação de confiança entre a empresa e os titulares dos dados.

Dessa forma, ao seguir essas orientações e implementar as medidas de segurança apropriadas, as PMEs estarão mais bem preparadas para proteger os dados pessoais que manipulam, garantindo a conformidade com a LGPD e o respeito à privacidade de seus clientes e colaboradores.

4. Consentimento e Direitos dos Titulares de Dados na LGPD: Garantindo a Privacidade nas PMEs

4.1 Consentimento

O consentimento é uma das principais hipóteses para a realização do tratamento de dados pessoais, conforme estabelecido na Lei Geral de Proteção de Dados (LGPD). Tal consentimento deve ser obtido de forma livre, informada e inequívoca, podendo ser manifestado por escrito ou por outros meios que demonstrem a vontade do titular. É imprescindível que o consentimento seja preservado e

inequívoco, sendo inteligível e compreensível, especialmente perante as esferas judiciais, e que esteja adequadamente vinculado aos termos do tratamento de dados.

A demonstração do consentimento pode se dar de diferentes formas, incluindo autenticação por e-mail ou *login*, SMS, registro de áudio, entre outros métodos. No entanto, é fundamental que a manifestação de vontade esteja claramente associada à finalidade específica do tratamento dos dados, de forma a comprovar que o consentimento foi concedido para aquela finalidade em particular, outrossim ele deve ser obtido antes da coleta dos dados, com base no art. 8º da lei. Cabe ao controlador a responsabilidade de provar que o consentimento foi obtido em conformidade com as disposições da LGPD, caso contrário, o consentimento será considerado inválido.

Segundo Cots e Oliveira[22], relevante que a manifestação de vontade seja:

I. Preservada e inequívoca;
II. Seja inteligível, ou seja, deve ser compreensível caso precise ser comprovada, especialmente perante as esferas judiciais; e;
III. Esteja adequadamente atrelada aos termos do tratamento de dados, isto é, é necessário comprovar que determinado consentimento se deu sobre determinado tratamento.

Ressalta-se que, cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto na Lei (LGPD). Dessa forma, caso não seja observado o modelo estabelecido em lei para a coleta da manifestação de vontade, será inválido o consentimento.

Ademais, a lei estabelece que o tratamento de dados pessoais de acesso público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização. Por exemplo, se uma pessoa torna público seu interesse em adquirir um imóvel em determinada região, divulgando dados pessoais de contato, é possível que os dados sejam tratados para oferecer imóveis naquela região, mas não para outros fins, como oferecer serviços de telefonia ou recolocação profissional.

[22] COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Pessoais Comentada**. 2. ed. São Paulo: Thomson Reuters Brasil, 2019, p. 86.

Nessa esteira, o Tribunal de Justiça do Paraná, decidiu a favor da autora, que teve seus dados vazados e utilizados indevidamente por falsários para realizarem compras não autorizadas, eis a ementa:

> RECURSO INOMINADO. RESIDUAL. COMPRA DESCONHECIDA E NÃO AUTORIZADA. USO INDEVIDO DE DADOS PESSOAIS DA CONSUMIDORA. ALTERAÇÃO NÃO CONSENTIDA DAS INFORMAÇÕES CADASTRAIS. FALHA NO TRATAMENTO DOS DADOS. SEGURANÇA E PREVENÇÃO NÃO OBSERVADAS. VIOLAÇÃO À LGPD. INDENIZAÇÃO POR DANO MORAL MAJORADA. ADOÇÃO DO MÉTODO BIFÁSICO. PRECEDENTE DO STJ. ADEQUAÇÃO AOS PARÂMETROS DA TURMA RECURSAL E ÀS CIRCUNSTÂNCIAS DO CASO. RECURSO CONHECIDO E PROVIDO.
> (TJPR - 2ª Turma Recursal - 0008309-97.2021.8.16.0019 - Rel.: JUIZ DE DIREITO SUBSTITUTO MAURÍCIO PEREIRA DOUTOR - J. 10.06.2022)
> 3.1.4.2. **Todos aqueles que realizam tratamento de dados pessoais – dentre os quais está a ré – devem ter como princípios regentes da atividade a segurança e a prevenção. Estabelece o art. 6º da Lei Geral de Proteção de Dados – LGPD**: "As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: VII – segurança: utilização de 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; VIII – prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais".
> 3.1.4.4. Ademais, não se pode perder de vista que **a violação de dados pessoais pode ultrapassar a esfera de uma simples compra não autorizada.** Ao permitir o acesso de desconhecidos aos dados da autora, a ré a colocou em situação de risco, deixando-a à mercê da ocorrência de novas fraudes e golpes.
> 3.1.4.5. Nesse contexto, entende-se por majorar a indenização por dano moral fixada na sentença recorrida para R$ 4.000,00, quantia que se revela adequada do ponto de vista compensatório, sem, contudo, causar enriquecimento ilícito da autora.

Em suma, o consentimento e os direitos dos titulares de dados assumem um papel fundamental para a proteção de dados pessoais nas Pequenas e Médias Empresas (PMEs) em conformidade com a LGPD. A obtenção de consentimento adequado e o respeito aos direitos dos titulares são essenciais para garantir a privacidade e segurança dos dados pessoais nas atividades dessas empresas.

4.2 Direitos dos Titulares de Dados na LGPD

Existem alguns direitos dos titulares dos dados estabelecidos pela LGPD, dentre eles, destaca-se o direito de acesso, conforme art. 17º[23] do texto legal, que permite aos titulares solicitar informações sobre os dados que estão sendo tratados pelas PMEs. As empresas devem disponibilizar meios para que os titulares exerçam esse direito de forma simples e eficiente, fornecendo detalhes sobre a coleta, processamento e compartilhamento dos dados.

Outro direito importante é o direito de retificação, de acordo com o art. 18º[24] da lei, que permite aos titulares solicitar a correção de dados pessoais que estejam incompletos, inexatos ou desatualizados. No comentário à LGPD da autora Patrícia Peck Pinheiro, em 2018, às páginas 60 e 61, é asseverado que:

> O direito dos titulares dos dados de livre acesso às informações relativas ao tratamento é reiterado de maneira enumerativa no art. 18, cuja preocupação é garantir que o titular possa assegurar que seus dados estão sendo tratados de forma segura, verídica e cumprindo a sua finalidade.
> Da mesma forma, a liberdade de revogar o consentimento e requerer o apagamento dos dados é reafirmada como reflexo da liberdade de escolha da pessoa, de forma que – assim como o consentimento – a revogação deve ser expressa. Novamente, o texto da lei reitera que os dados anonimizados não recebem o direito ao mesmo tratamento dos dados pessoais.

O direito de exclusão, ou direito ao esquecimento, também é assegurado pela LGPD. Os titulares têm o direito de solicitar a exclusão de seus dados pessoais, desde que sejam respeitados os prazos de retenção estabelecidos por lei. As PMEs devem desenvolver mecanismos para atender a essas solicitações e garantir a efetiva remoção dos dados pessoais.

---

[23] 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.

[24] 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.

Ainda, o direito à portabilidade de dados permite que os titulares solicitem a transferência de seus dados pessoais para outro prestador de serviço ou fornecedor, de forma estruturada e legível, previsto no artigo 20º[25] da LGPD. As PMEs devem facilitar o exercício desse direito, assegurando que os dados sejam transferidos de maneira segura e conforme as exigências legais (Pinheiro, 2018, p. 42-43).

É importante ressaltar que o respeito ao consentimento e aos direitos dos titulares não apenas assegura a conformidade com a LGPD, mas também fortalece a confiança dos clientes e usuários, estabelecendo uma relação de transparência e responsabilidade entre as PMEs e seus públicos. Por meio da adequada obtenção de consentimento e do cumprimento dos direitos dos titulares, as empresas demonstram seu compromisso com a proteção da privacidade e da segurança dos dados pessoais.

5. Consequências da Não Conformidade com a LGPD: Responsabilidades e Sanções

5.1 Responsabilidade Civil na LGPD

O texto legal da LGPD estabelece um conjunto de direitos e obrigações para o tratamento de dados pessoais no Brasil. É fundamental que as empresas, independentemente do porte, estejam em conformidade com a LGPD para evitar consequências legais e danos à reputação. A imputação de sanções administrativas demonstra que o texto normativo foi criado para estimular a aplicação dos dispositivos com caráter preventivo, sendo as sanções aplicadas de forma corretiva aos danos.

É imperioso destacar que por conta da omissão legal em definir expressamente qual a teoria da responsabilidade civil seria adotada se subjetiva ou objetiva não existe

[25] Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

um consenso doutrinário na Lei Geral de Proteção de Dados (LGPD). Nem mesmo a foi mencionada a necessidade da imputação da culpa para a responsabilização.

Nessa esteira a não conformidade com a LGPD pode levar à responsabilidade civil das empresas. Diante dos artigos 42 e 43, é necessário concluir que o regime de responsabilidade civil centrado no ilícito geral decorrente de um tratamento irregular define uma responsabilidade objetiva especial. No entanto, o texto não vincula a aplicação da norma com a existência ou não de culpa, mas com a ruptura do nexo de causalidade, hipóteses descritas nos incisos I e III do art. 43[26].

Adiante, o artigo 42º[27] da LGPD, orienta a teoria subjetiva, ao estabelecer que o titular dos dados pessoais tem o direito de ser indenizado por danos materiais ou morais decorrentes do tratamento inadequado de seus dados. Caso a empresa não cumpra com as obrigações da lei e cause prejuízos aos titulares, ela poderá ser responsabilizada e obrigada a reparar os danos causados.

Ademais, o art. 43 apresenta hipóteses em que se admite a exceção da responsabilidade dos agentes de tratamento, sendo afastada quando provado que o dado apresentado não foi tratado pelo agente, que embora tenha sido tratado o dado não tenha ocorrido nenhuma violação à legislação de proteção dos dados; e que o dano tenha ocorrido por culpa exclusiva do titular dos dados ou de terceiros.

Nessa mesma esteira, o texto normativo no art. 44, parágrafo único[28], corrobora com a teoria da responsabilidade objetiva especial. Pois, a responsabilidade civil, nesses termos, não adota a forma da responsabilidade civil subjetiva centrada na culpa, nem a forma da responsabilidade civil objetiva centrada no risco, mas uma nova

---

[26] Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem: I - que não realizaram o tratamento de dados pessoais que lhes é atribuído; II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou, III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiros.

[27] Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

[28] Art. 44. Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano.

e especial forma de responsabilidade civil objetiva, centrada na garantia da segurança no tratamento de dados pessoais[29].

Além disso, ao definir que em caso de danos decorrentes da violação da segurança de dados o ônus da prova será direcionado ao controlador ou ao operador, quando estes deixarem de observar as medidas de segurança previstas no art. 46[30] da Lei, e como resultado, essa negligência der causa ao dano.

Contudo, considerando a responsabilidade em sentido amplo no âmbito da LGPD, Maria Celina Bodin de Moraes[31] denomina o modelo lato sensu adotado como "proativo", que baseia-se em um sistema de prestação de contas, no qual o eixo axiológico do instituto se deslocaria da reparação do dano para a sua prevenção, esclarece:

> Trata-se do conceito de — prestação de contas. Esse novo sistema de responsabilidade, que vem sendo chamado de — responsabilização ativa ou — proativa, encontra-se indicado no inciso X do art. 6º, que determina às empresas não ser suficiente cumprir os artigos da lei; será necessário também — demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, a eficácia dessas medidas. Portanto, não descumprir a lei não é mais suficiente; é preciso — proativamente prevenir a ocorrência de danos.

A compreensão da autora Maria Celina Bodin de Moraes, decorre da natureza interdisciplinar do instituto da responsabilidade civil. No qual, o campo de abrangência da norma deixa de ser apenas de natureza reparatória (no âmbito jurídico) e passa a incidir antecipadamente (preventiva em sentido lato sensu), instituindo mecanismos e

---

[29] DRESCH, Rafael, **A Especial Responsabilidade Civil na Lei Geral de Proteção de Dados,** Migalhas, 2020. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/330019/a-especial-responsabilidade-civil-na-lei-geral-de-protecao-de-dados. Acesso em 30 de outubro de 2023.

[30] Art. 46. Os agentes de tratamento devem adotar medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito.

[31] MORAES, Maria Celina Bodin de**. LGPD: um novo regime de responsabilização civil dito — proativo**. Revista Civilistica, ano 8, n. 3, Rio de Janeiro, 2019. Disponível em: http://civilistica.com/lgpd-um-novo-regime/. Acesso: 16 de outubro de 2023.

obrigação que levem a impedir a causação do dano, denominada responsabilidade preventiva[32].

Portanto, fica claro que a LGPD busca garantir a proteção dos direitos dos titulares de dados pessoais e impor responsabilidade preventiva às empresas que não cumprirem com suas obrigações legais. Ao adotar a teoria da responsabilidade ativa ou proativa, a lei reforça a importância do tratamento adequado dos dados e a necessidade de medidas preventivas para evitar prejuízos aos titulares. As empresas devem estar atentas às exigências da LGPD e investir em práticas seguras de tratamento de dados, priorizando a proteção da privacidade e dos direitos dos indivíduos.

5.2 Sanções a Não Conformidade da LGPD

A LGPD prevê a aplicação de sanções administrativas em caso de descumprimento das disposições da lei. O artigo 52º[33] estabelece as sanções que podem ser impostas pela Autoridade Nacional de Proteção de Dados (ANPD). Entre as sanções previstas estão advertências, multas de até 2% do faturamento da empresa, limitadas a R$ 50 milhões por infração, publicização da infração após devidamente apurada e a suspensão parcial ou total das atividades relacionadas ao tratamento de dados pessoais.

Com base na proteção garantida pelo art. 52º da LGPD o Tribunal de Justiça do Estado de Minas Gerais, decidiu a favor do autor, a seguir:

> EMENTA: APELAÇÃO CÍVEL - AÇÃO ANULATÓRIA DE DÉBITO C/C INDENIZAÇÃO POR DANOS MORAIS - INEXISTÊNCIA DE PROVA DA CONTRATAÇÃO E EFETIVAÇÃO DE DESCONTOS INDEVIDOS DE PARCELAS DE EMPRÉSTIMO - TEMAS INCONTROVERSOS -

[32] LOPEZ, Tereza Ancona. **Responsabilidade civil na sociedade do risco**. Revista da Faculdade de Direito da Universidade de São Paulo, v. 105, São Paulo, jan./dez. 2010. p. 1220-1234.

[33] Art. 52. 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;

> REPARAÇÃO IMATERIAL - PREJUÍZO CONFIGURADO - INDENIZAÇÃO - CRITÉRIOS DE ARBITRAMENTO - MULTA PREVISTA NO ART. 52, II, DA LGPD - SANÇÃO ADMINISTRATIVA.
> - Não havendo insurgência das partes em relação aos tópicos da Sentença que reconheceram a inexistência de comprovação da contratação voluntária de mútuo consignado, bem como a efetivação de subtrações irregulares sobre os rendimentos do Autor, tais temas se tornaram incontroversos.
> - Segundo os critérios de proporcionalidade e razoabilidade, o valor reparatório não pode servir como fonte de enriquecimento do ofendido, nem consubstanciar incentivo à reincidência do responsável pela prática do ilícito. A indenização por danos morais também deve ser arbitrada de acordo com os parâmetros consolidados pela Jurisprudência e com observância aos conteúdos dos arts. 141 e 492, ambos do CPC/2015.
> - A penalidade prevista no art. 52, II, da Lei nº 13.907/2018, é de competência da Autoridade Nacional de Proteção de Dados (ANPD), aplicável em processo administrativo. (TJMG - Apelação Cível 1.0000.22.185189-2/001, Relator(a): Des.(a) Roberto Vasconcellos , 17ª CÂMARA CÍVEL, julgamento em 14/09/2022, publicação da súmula em 15/09/2022).

A não conformidade com a LGPD pode resultar em danos significativos à reputação da empresa. A falta de proteção adequada dos dados pessoais pode levar à perda de confiança dos clientes, que podem optar por não utilizar mais os serviços ou produtos oferecidos pela empresa. O artigo 43º da LGPD destaca a importância da transparência e do cumprimento das obrigações da lei para manter a confiança dos titulares de dados.

A literatura jurídica também segue na mesma direção do tribunal mineiro na obra Lei Geral de Proteção de Dados Pessoais: e Suas Repercussões no Direito Brasileiro, Gustavo Tepedino, Ana Frazão e Milena Donato Oliva[34], defendem que caso a empresa não esteja em conformidade com a LGPD, pode ser exigida a exclusão dos dados pessoais que foram coletados sem o consentimento adequado ou em desacordo com a lei. Prerrogativa garantida no artigo 18º da LGPD que

[34] TEPEDINO, G.; OLIVA, A. F. E. M. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. Thomson Reuters Brasil, 2020. P. 175-180.

assegura o direito do titular dos dados de solicitar a exclusão de seus dados pessoais da base de dados da organização.

A não conformidade com a LGPD pode acarretar sérias consequências para as empresas, incluindo responsabilidade civil, sanções administrativas, danos à reputação e perda de clientes. É essencial que as empresas estejam cientes de suas obrigações legais, adotem medidas adequadas de proteção de dados e implementem políticas e práticas em conformidade com a LGPD. Dessa forma, poderão evitar as consequências negativas decorrentes da não conformidade e garantir a proteção dos dados de clientes, colaboradores e fornecedores.

6. A INTERSEÇÃO DA LGPD NAS RELAÇÕES DE CONSUMO

6.1. Diálogo entre o Código de Defesa do Consumidor e a Lei de Proteção de Dados

Há uma forte interseção entre a proteção de dados dos seus titulares e as relações de consumo, com o objetivo de garantir a abrangência legal o artigo 45[35] da Lei Geral de Proteção de Dados (LGPD) estabelece uma conexão importante entre o microssistema de proteção e defesa do consumidor[36] presente na legislação brasileira e as disposições relativas à responsabilidade no âmbito da proteção de dados. Isso sinaliza que o regime de proteção ao consumidor no Brasil se aplica à LGPD, especialmente quando se trata das regras de responsabilidade (Pinheiro, 2018, p. 77).

[35] Art. 45. As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente.

[36] Art. 2° Consumidor é toda pessoa física ou jurídica que adquire ou utiliza produto ou serviço como destinatário final.
Parágrafo único. Equipara-se a consumidor a coletividade de pessoas, ainda que indetermináveis, que haja intervindo nas relações de consumo.

O principal ponto para essa relação é o conceito de consumidor expresso no Artigo 2º do Código de Proteção e Defesa do Consumidor[37]. Foi definido que consumidor é toda pessoa física ou jurídica que adquire ou utiliza um produto ou serviço como destinatário final. Isso significa que sempre que um titular de dados pessoais sofre um dano causado por um vazamento ao adquirir um produto ou serviço como destinatário final, poderá invocar o sistema de responsabilização previsto no e na legislação correlata (Maldonado; Blum, 2019, p. 264).

Na literatura consumerista, o autor Felipe Peixoto Braga Neto, na obra Manual de Direito do Consumidor, em 2015, 10ª edição, às páginas 132 -133, discorre sobre a figura do consumidor por equiparação. Portanto, isso inclui as vítimas de eventos danosos que, embora não tenham consumido diretamente o produto ou serviço defeituoso (acidente de consumo), sofreram danos em decorrência deles. O Artigo 17 do CDC esclarece que para os efeitos desta Seção, equiparam-se aos consumidores todas as vítimas do evento. Isso amplia o escopo da proteção do consumidor para abranger um grupo mais amplo de pessoas afetadas por incidentes.

Além disso, argumenta Braga Neto:

> A doutrina, interpretando o dispositivo, pondera que tal artigo "é norma que eleve ser entendida como aplicável não apenas ao consumidor, destinatário final do produto, já protegido pela responsabilidade objetiva do Código de Defesa do Consumidor, mas também a quaisquer vítimas dos danos derivados do produto, ainda que participantes da própria cadeia de fornecimento, como o transportador, o armazenador, o comerciante, etc.

No que diz respeito à aplicabilidade da legislação consumerista, vale ressaltar que casuisticamente há possibilidade de responsabilização objetiva do controlador e/ou operador de dados, além da inversão do ônus da prova[38]. Isso significa que, em casos de violações dos dados, os causadores do dano podem ser considerados responsáveis sem a necessidade de comprovar sua culpa, de acordo com a legislação

---

[37] Ibidem.

[38] MALDONADO, Viviane Nóbrega. BLUM, Renato Opice, LGPD, Lei Geral de Proteção de Dados: Comentada, 2ª edição, 2019, p. 264.

consumerista, tornando mais eficaz a proteção dos direitos dos titulares de dados (Neto, 2015, p. 159).

Ademais, na seção VI do Código de Defesa do Consumidor, no artigo 43, fica evidente a interseção entre a LGPD e o CDC destaca-se a importância de proteger os direitos dos consumidores em relação à proteção de dados pessoais[39]. Ela proporciona um ambiente jurídico sólido que promove a responsabilidade e a prestação de contas por parte das organizações que lidam com informações pessoais e, ao mesmo tempo, assegura que as vítimas de incidentes danosos tenham garantia que seus direitos serão devidamente protegidos.[40]

É importante ressaltar que a LGPD e o CDC não operam de forma isolada[41]. Em muitos casos, um agente de tratamento pode estar sujeito a ambos os regulamentos, o que implica em uma atuação fiscalizatória dúplice. Por exemplo, se uma violação de dados também violar o CDC, o agente de tratamento estará sujeito à fiscalização tanto pela ANPD quanto pelos diversos órgãos de defesa do consumidor[42].

Por fim, entende-se que a interseção entre a LGPD e as relações de consumo cria um cenário complexo, no qual os titulares de dados têm mais controle sobre suas informações pessoais, e, esse é um grande avanço legislativo. Por outro lado, é bem verdade que um sistema mais protetivo a princípio possa gerar um aumento nas disputas por danos causados por vazamento de dados. Apesar disso, o sistema de justiça brasileiro enfrenta o desafio de desenvolver um sistema de justiça que possa

---

[39] Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.

[40] MALDONADO, Viviane Nóbrega. BLUM, Renato Opice, LGPD, Lei Geral de Proteção de Dados: Comentada, 2ª edição, 2019, p. 303.

[41] TEPEDINO, G.; OLIVA, A. F. E. M. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. Thomson Reuters Brasil, 2020. p. 118-119.

[42] SENACON, **Sistema Nacional de Defesa do Consumidor - SNDC,** consumidor.gov.br, 1.990, Disponível em: https://www.consumidor.gov.br/pages/conteudo/publico/6#:~:text=O%20Sistema%20Nacional%20de%20Defesa,Nacional%20do%20Consumidor%20(Senacon).

lidar com essa nova realidade de forma eficaz e equitativa, equilibrando a proteção dos direitos dos consumidores e a privacidade dos dados pessoais (Bottino, Perrone, Carneiro, Heringer, Viola, 2020, p. 6-14).

6.2. Aumento de Demandas na Seara do Direito do Consumidor

É imperioso o entendimento que a proteção de dados abrange de forma global as relações cotidianas, devido ao alto grau de compartilhamento de dados[43]. Adiante, tal problemática foi trabalhada pelos autores Celina Bottino; Christian Perrone; Giovana Carneiro; Leonardo Heringer e Mario Viola, Lei Geral de Proteção de Dados Pessoais e Resolução de Conflitos: Experiências Internacionais e perspectivas para o Brasil, em 2020, 1ª edição, às páginas 5-14, devido a abertura que a LGPD da a diversas autoridades, incluindo a ANPD, os Ministérios Públicos Federal e Estaduais, associações de consumidores e proteção de dados, para lidar com a proteção de dados.

Isso pode levar a um aumento nas disputas relacionadas à privacidade e proteção de dados[44]. Além disso, o sistema de proteção dos consumidores e a proteção de dados têm semelhanças marcantes, o que reforça a defesa dos direitos dos titulares de dados. O advento da Lei Geral de Proteção de Dados (LGPD) no cenário brasileiro trouxe consigo uma multiplicidade de atores que podem estar envolvidos na sua aplicação[45].

---

[43] TEPEDINO, G.; OLIVA, A. F. E. M. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. Thomson Reuters Brasil, 2020. p. 461.

[44] MARTINS, Patrícia Helena Martins; MONTEIRO, Celso. **Proteção de dados pessoais em 2020**. Valor Econômico, janeiro de 2020. Disponível em: <https://valor.globo.com/legislacao/coluna/protecao-de-dados-pessoais-em2020.ghtml>, acesso em 28 de outubro de 2020.

[45] SENACON, **Sistema Nacional de Defesa do Consumidor - SNDC,** consumidor.gov.br, 1.990, Disponível em: https://www.consumidor.gov.br/pages/conteudo/publico/6#:~:text=O%20Sistema%20Nacional%20de%20Defesa,Nacional%20do%20Consumidor%20(Senacon).

Entre os atores, destacam-se a Secretaria Nacional do Consumidor (SENACON), os Ministérios Públicos Federal e Estaduais, as associações de defesa do consumidor, associações dedicadas à proteção de dados e, é claro, a própria Autoridade Nacional de Proteção de Dados (ANPD) criada pela LGPD[46]. Todos esses atores, juntamente com os indivíduos, podem estar envolvidos em disputas relacionadas à proteção de dados. Além disso, alguns deles têm capacidade postulatória para iniciar ações visando a responsabilização de controladores e operadores de dados[47].

Uma característica notável do Brasil que pode contribuir para o aumento do número de disputas relacionadas à LGPD é a forte cultura de proteção dos direitos do consumidor. Essa cultura apresenta muita similitude com a estrutura de proteção de dados pessoais. Em essência, a proteção de dados se encaixa na mesma lógica de criação de direitos legais para que os indivíduos possam exercê-los diretamente perante entidades públicas e privadas. A perspectiva é muito próxima, e a defesa dos consumidores complementa a proteção dos titulares de dados (Bottino; Perrone; Carneiro; Heringer; Viola, 2020, p. 10).

A SENACON motivou a Nota Técnica de número 4/2019/GAB-SENACON/SENACON/MJ, de abril de 2019[48], colaciona-se a seguir trecho da nota:

> No caso da LGPD, grande parte dos bancos de dados pessoais são constituídos por dados de consumo, originados de relações de consumo, matéria essa de atuação da SENACON. Exemplo dos reflexos consumeristas da proteção de dados podem ser constatados, inclusive, a partir das investigações conduzidas pela SENACON que versam de forma correlata (indireta ou mesmo direta) à LGPD.

---

[46] PINHEIRO, Guilherme Pereira; SOUTO, Gabriel Araújo; MORAES, Thiago Guimarães. **ANPD: uma necessidade de convergência entre CADE, Anatel e Senacon**. Jota, outubro de 2019. Disponível em https://www.jota.info/opiniao-e-analise/artigos/anpd-uma-necessidade-de-convergencia-entre-cade-anatel-e-senacon-20102019, acesso em 29 de outubro de 2023.

[47] TEPEDINO, G.; OLIVA, A. F. E. M. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. Thomson Reuters Brasil, 2020. p. 469.

[48] BRASIL, Ministério da Justiça e Segurança Pública, **Nota Técnica n.º 4/2019/GAB-SENACON/SENACON/MJ**. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/collective-nitf-content-1555356484.15/nota-tecnica-senacon.pdf, acesso em: 30 de outubro de 2023.

Portanto, fica demonstrado a interligação entre a proteção de dados e a defesa do consumidor, pois as investigações da SENACON podem estar relacionadas, direta ou indiretamente, à LGPD.

Além disso, a jurisprudência brasileira já começa a reconhecer a importância da proteção de dados pessoais. No julgamento do Recurso Especial nº 1.758.799, o Superior Tribunal de Justiça (STJ) reconheceu a ocorrência de dano moral in re ipsa devido a um tratamento irregular de dados pessoais. Isso significa que, independentemente da demonstração de dano, o tratamento irregular de dados pessoais pode resultar em uma obrigação de indenizar por parte do controlador de dados.

Eis parte da ementa:

> RECURSO ESPECIAL. FUNDAMENTO NÃO IMPUGNADO. SÚM. 283/ STF. AÇÃO DE COMPENSAÇÃO DE DANO MORAL. BANCO DE DADOS. COMPARTILHAMENTO DE INFORMAÇÕES PESSOAIS. DEVER DE INFORMAÇÃO. VIOLAÇÃO. DANO MORAL IN RE IPSA. JULGAMENTO: CPC/15. [...] 6. O consumidor tem o direito de tomar conhecimento de que informações a seu respeito estão sendo arquivadas/comercializadas por terceiro, sem a sua autorização, porque desse direito decorrem outros dois que lhe são assegurados pelo ordenamento jurídico: o direito de acesso aos dados armazenados e o direito à retificação das informações incorretas. 7. A inobservância dos deveres associados ao tratamento (que inclui a coleta, o armazenamento e a transferência a terceiros) dos dados do consumidor – dentre os quais se inclui o dever de informar – faz nascer para este a pretensão de indenização pelos danos causados e a de fazer cessar, imediatamente, a ofensa aos direitos da personalidade. [...] 11. Hipótese em que se configura o dano moral in re ipsa. (sem grifos no original)

Cabe também destacar as seguintes passagens do voto condutor do acórdão:

> Isso porque, em qualquer das circunstâncias, tem o consumidor o direito de tomar conhecimento de que informações a seu respeito estão sendo arquivadas/comercializadas por terceiro, sem a sua autorização, porque desse direito decorrem outros dois que lhe são assegurados

> pelo ordenamento jurídico: o direito de acesso aos dados armazenados e o direito à retificação das informações incorretas.
> […]
> Assim, a inobservância de qualquer dos deveres associados ao tratamento (que inclui a coleta, o armazenamento e a transferência a terceiros) dos dados do consumidor – dentre os quais se inclui o dever de informar – faz nascer para este a pretensão de indenização pelos danos causados e a de fazer cessar, imediatamente, a ofensa aos direitos da personalidade.

Esta decisão do STJ sinaliza o potencial de violações das normas da LGPD resultarem em ações judiciais mais acessíveis aos titulares de dados, diminuindo a barreira de acesso à indenização.

Em síntese, a LGPD pode contribuir para o desenvolvimento de um contencioso de massa semelhante ao que ocorre na área de defesa do consumidor. Para lidar com essa demanda potencial, é essencial pensar em alternativas adequadas que possam atender a esse enorme volume de ações judiciais. A interseção entre a proteção de dados e a defesa do consumidor representa um desafio e uma oportunidade para o sistema legal brasileiro[49].

7. Recursos e Suporte para Pequenas e Médias Empresas na Adequação à LGPD.

A adequação às exigências impostas pela LGPD pode parecer desafiadora para as PME's, mas é um passo essencial para garantir a privacidade e segurança dos dados de seus clientes e colaboradores. Felizmente, existem recursos e suportes disponíveis para ajudá-las a alcançar a conformidade com a lei.

A Autoridade Nacional de Proteção de Dados (ANPD), criada pela LGPD, desempenha um papel crucial no fornecimento de orientações e diretrizes para a aplicação da lei. As PMEs podem acessar o site da ANPD, onde encontram materiais

[49] BOTTINO, Celina; PERRONE, Christian; CARNEIRO, Giovana; HERINGER, Leonardo; VIOLA Mario. Lei Geral de Proteção de Dados Pessoais e Resolução de Conflitos: Experiências internacionais e perspectivas para o Brasil. 2020, Instituto de Tecnologia & Sociedade do Rio, p. 10-12.

informativos, guias práticos[50] e documentos explicativos que ajudam a compreender os requisitos e as melhores práticas para a conformidade com a LGPD. Esses recursos fornecem um excelente ponto de partida para as PMEs no processo de adequação e possibilitam uma compreensão mais aprofundada dos desafios e oportunidades que a LGPD apresenta.

A capacitação dos profissionais envolvidos no tratamento de dados pessoais é um requisito fundamental da LGPD. Nesse sentido, diversas organizações e empresas oferecem treinamentos e cursos especializados em proteção de dados e conformidade com a LGPD. Esses programas educacionais capacitam os funcionários das PMEs com o conhecimento necessário para implementar medidas adequadas de proteção de dados, proporcionando um ambiente seguro e em conformidade com a lei (Tepedino; Frazão; Oliva, 2020, p. 488).

Para as empresas que buscam suporte mais especializado e adaptado às suas necessidades, existem diversas empresas de consultoria que oferecem serviços de assessoria[51] e apoio na implementação da LGPD Além de poderem contratarem consultores aptos a auxiliar na avaliação de riscos, na criação de políticas internas, na elaboração de contratos e no desenvolvimento de medidas de segurança e boas práticas específicas para cada empresa. Com a orientação adequada, as PMEs podem superar os desafios inerentes à conformidade com a LGPD de forma eficiente e eficaz.

Outra possibilidade mais informal de suporte é o compartilhamento de experiências com outras empresas que também estão em processo de adequação à LGPD. Participar de fóruns, grupos de discussão ou eventos relacionados à proteção de dados possibilita que as empresas compartilhem desafios, estratégias e soluções encontradas durante sua jornada de adequação.

---

[50] ANPD. **Segurança da Informação Para Agentes de Tratamento de Pequeno Porte.** Brasília: Governo Federal, 2021. Páginas 21.Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf . Acesso em: 17 de outubro de 2023.

[51] SEBRAE; Datablock; Get Privacy; Grupo Assaf.

Outrossim, diversas organizações, incluindo a ANPD[52], desenvolveram guias e manuais de implementação da LGPD, fornecendo orientações detalhadas sobre as etapas e os requisitos para a conformidade. Os sites da ANPD, associações empresariais e consultorias especializadas disponibilizam esses guias gratuitamente ou por um custo acessível, facilitando o acesso a informações confiáveis e atualizadas sobre a LGPD.

Percebe-se que a proteção de dados pessoais é essencial para as empresas, exigindo conscientização e ações efetivas para garantir segurança. Isso inclui o uso de controles de segurança nos sistemas de TI e medidas preventivas contra incidentes de segurança. Manter documentos físicos com dados pessoais protegidos é fundamental, evitando compartilhamento indevido de informações[53].

Além disso, é crucial gerenciar contratos de forma a incluir termos de confidencialidade e cláusulas de segurança da informação. O controle de acesso aos dados é igualmente vital, com a implementação de sistemas de permissão e o armazenamento seguro de dados. A comunicação interna e externa deve ser protegida com protocolos seguros e medidas como firewalls e ferramentas AntiSpam (Pinheiro, 2018, p. 71).

A segurança dos softwares e hardwares utilizados também é prioridade. Manter os programas atualizados e adotar medidas de proteção, como autenticação multifator e criptografia, é essencial. A segurança em serviços em nuvem oferece uma camada adicional de proteção. Escolher provedores que atendam aos requisitos das PMEs e exigir medidas de segurança são práticas recomendadas.

Em resumo, a LGPD apresenta desafios para as PMEs, mas também oferece suporte para conformidade com a lei. Com orientações e medidas adequadas, é

---

[52] ANPD. **Segurança da Informação Para Agentes de Tratamento de Pequeno Porte.** Brasília: Governo Federal, 2021. Páginas 21. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf>. Acesso em: 18 de outubro de 2023.

[53] TEPEDINO, G.; OLIVA, A. F. E. M. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. Thomson Reuters Brasil, 2020. P. 485-487.

possível proteger os dados pessoais de clientes e colaboradores, garantindo segurança e privacidade num ambiente digital seguro.

CONCLUSÃO

Nos dias atuais um dos ativos de maior valor é o dado[54], e, principalmente os dados de Pessoas Físicas ou Jurídicas. São eles um dos principais responsáveis pelo desenvolvimento da nossa sociedade. Além disso, sendo as Pequenas e Médias Empresas à principal fonte de empregabilidade no país é de suma importância a abordagem do presente trabalho que busca aproximar o texto legal da realidade destas instituições tão importantes para a economia nacional.

Portanto, é fundamental que as PMEs compreendam que o processo de adequação à LGPD não é um desafio intransponível, nem mesmo que apenas as grandes corporações devam cumprir. A segurança dos dados dos seus clientes, fornecedores e colaboradores, é fundamental para a manutenção de relacionamentos duradouros e prósperos.

Para isso, a LGPD estabeleceu critérios indispensáveis para que as empresas juntamente com seus agentes de controle e tratamento possam garantir o correto manuseio dos dados. Antes da obtenção dos dados é necessário o consentimento por parte do titular dos dados, para que estes possam ser tratados pela empresa.

Deste modo, a seguir deve ser feita a avaliação de impactos, nessa etapa os dados serão classificados, pois, quanto mais sensível o dado maior será o rigor no seu tratamento. A seguir o mapeamento dos dados tem como finalidade de identificar quais são os caminhos que os dados farão ao serem coletados.

Logo, é imperioso que as medidas de segurança e de boas práticas sejam adotadas, pois, são sobre estas etapas que a responsabilização das empresas e de

---

[54] CAPPRA, Ricardo, MIT Technology Reveiw, 2020, **O Mercado dos Dados Pessoais.** Disponível em: https://mittechreview.com.br/o-mercado-dos-dados-pessoais/, acesso em: 17 de outubro de 2023.

seus controladores e operadores é imputada. A legislação foi clara em exigir que além de cumprir o que foi previsto em lei para a devida proteção dos dados fossem adotadas medidas de boas práticas que previnam danos aos titulares, sob pena de sanções.

Nesse sentido, com o intuito de criar recursos e suporte as PMEs a LGPD criou a Autoridade Nacional de Proteção de Dados (ANPD), para desempenhar um papel crucial no fornecimento de orientações e criação de diretrizes para a aplicação da lei.

Com base no que foi apresentado, busca-se compreender as implicações da criação da nova lei e apresentar um caminho para a adequação das empresas de pequeno e médio porte à LGPD. Deste modo, prevenir dano aos titulares, por vazamento de dados. Assim como, proteger os agentes controladores ou mesmo atenuar as sanções devido o enquadramento legal, em caso de vazamento.

REFERÊNCIAS

ATHENIENSE, Alexandre. **LGPD Para Empresas.** Belo Horizonte: 2019. *E-book*. Página 28. Disponível em: https://www.alexandreatheniense.com.br/wp-content/uploads/2019/07/ebook_guia_LGPD_para_empresas_impressao_baixa.pdf, acesso em: 15 de outubro de 2023.

ANPD. **Segurança da Informação Para Agentes de Tratamento de Pequeno Porte.** Brasília: Governo Federal, 2021. Páginas 21. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf>. Acesso em: 26 jul. 2023.

ANPD. **Tratamento de Dados Pessoais Pelo Poder Público.** Brasília: Governo Federal, 2023. Páginas 52. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf>. Acesso em: 26 de julho de 2023.

BRANDAO, G. **Mapeamento de Dados: O que é e como fazer data mapping. BL Consultoria Digital**, 27 Feb. 2020. Disponível em: <https://blconsultoriadigital.com.br/mapeamento-de-dados/>. Acesso em: 22 jul. 2023 em: 22 jul. 2023

BRASIL. Constituição Federal (1988). **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal, 1988.

BRASIL. Lei Complementar nº 123 (2006). **Estatuto Nacional da Microempresa e da Empresa de Pequeno Porte**.

BRASIL. **Lei Geral de Proteção de Dados** (2018). LGPD. Brasília, DF: Executivo, 2018.

COTS, Márcio; OLIVEIRA, Ricardo**. Lei Geral de Proteção de Dados Pessoais Comentada**. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

CAPPRA, Ricardo, MIT Technology Reveiw, 2020, **O Mercado dos Dados Pessoais.** Disponível em: https://mittechreview.com.br/o-mercado-dos-dados-pessoais/, acesso em: 17 de outubro de 2023.

LIMA, Ana Paula Moraes Canto de. **LGPD Aplicada**. São Paulo: Atlas, 2020.

LOPEZ, Tereza Ancona. **Responsabilidade civil na sociedade do risco**. Revista da Faculdade de Direito da Universidade de São Paulo, v. 105, São Paulo, jan./dez. 2010. p. 1223-1234.

MORAES, Maria Celina Bodin de**. LGPD: um novo regime de responsabilização civil dito —proativo**. Revista Civilistica, ano 8, n. 3, Rio de Janeiro, 2019. Disponível em: http://civilistica.com/lgpd-um-novo-regime/. Acesso: 15 de agosto de 2023.

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

REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO. 4 de maio de 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN. Acesso em: 19 out. 2023.

SEBRAE, **Micro e Pequenas empresas geram 27% do PIB do Brasil**. 2011. Disponível em: https://sebrae.com.br/sites/PortalSebrae/ufs/mt/noticias/micro-e-pequenas-empresas-geram-27-do-pib-do-brasil,ad0fc70646467410VgnVCM2000003c74010aRCRD#:~:text=As%20micro%20e%20pequenas%20empresas,empresas%20(24%2C5%25). Acesso em: 01 de outubro de 2023.

TEPEDINO, G.; OLIVA, A. F. E. M. (coordenadores) **Lei Geral de Proteção de Dados Pessoais e suas repercuções no Direito Brasileiro**. Av. Dr. Cardoso de Melo, 1855 – 13º andar - Vila Olímpia CEP 04548-005, São Paulo, SP, Brasil: Thomson Reuters Brasil, 2020.