Revista Científica UNAR (ISSN 1982-4920), Araras (SP), v.23, n.1, p.118-132, 2023.
DOI: 10.18762/1982-4920.20230008

LGPD NAS MICROEMPRESAS: IMPACTOS EM DECORRÊNCIA DA NOVA LEI

Osni Ribeiro dos Santos, Leonardo Costa Evangelista, André Luiz Oliveira

RESUMO

Este trabalho teve como objetivo apresentar os impactos da Lei Geral de Proteção de Dados (LGPD) na estrutura de microempresas. A implementação da LGPD foi fundamental para garantir a privacidade e proteção dos dados pessoais de clientes e colaboradores, além de evitar possíveis sanções e multas. Ao longo do trabalho, foram abordados temas como a importância da implementação da lei, os custos oriundos do processo de adequação e as causas de não ter estado em conformidade com as normas. Além disso, foi apresentada a importância da segurança da informação nas microempresas, destacando a necessidade de proteger os dados pessoais e evitar o vazamento ou perda de informações sensíveis. Foi abordado também o conceito da LGPD e as dificuldades que as microempresas enfrentaram para se adequarem a essa nova legislação. Foram levantados os principais riscos de não adesão à LGPD, tais como danos financeiros e de imagem, e as possíveis consequências legais. Por fim, foi definido o que é compliance e como ele está diretamente ligado à LGPD. A adequação à LGPD exigiu a adoção de medidas de aderência, que garantem a conformidade com as normas de proteção de dados pessoais. Assim, este trabalho teve como propósito contribuir para uma melhor compreensão dos desafios enfrentados pelas microempresas na adesão à LGPD e como a implementação da lei pode ter impactado na estrutura e funcionamento do negócio.

Palavras-chave: LGPD; COMPLIANCE; MICROEMPRESAS.

ABSTRACT

This work aimed to present the impacts of the General Data Protection Law (LGPD) on the structure of micro-enterprises. The implementation of the LGPD was crucial to ensure the privacy and protection of personal data of customers and employees, as well as to avoid possible sanctions and fines. Throughout the work, topics such as the importance of implementing the law, the costs arising from the adaptation process, and the reasons for not complying with the regulations were addressed. In addition, the importance of information security in micro-enterprises was presented, highlighting the need to protect personal data and prevent leakage or loss of sensitive information. The concept of the LGPD and the difficulties that micro-enterprises faced in adapting to this new legislation were also addressed. The main risks of non-compliance with the LGPD, such as financial and reputational damages, and possible legal consequences were raised. Finally, compliance was defined and how it is directly linked to the LGPD.

Compliance with the LGPD required the adoption of adherence measures, which ensure compliance with personal data protection rules. Thus, this work aimed to contribute to a better understanding of the challenges faced by micro-enterprises in adhering to the LGPD and how the implementation of the law may have impacted the structure and functioning of the business.

Keywords: LGPD; COMPLICE; MICRO-ENTERPRISES.

1. INTRODUÇÃO

Com o passar dos anos e com o avanço da tecnologia, ocorreu a popularização da internet, que se constituiu nas mais diversas ferramentas. Atualmente, podemos nos conectar com o outro lado do mundo com muita facilidade, empresários conseguem armazenar informações em bancos de dados com um simples click, o que tempos atrás parecia quase impossível. Em decorrência deste progresso, surgiu a necessidade de se preocupar com as informações que são introduzidas neste espaço virtual, principalmente se formos analisar as consequências financeiras que a perca ou o vazamento destes elementos poderiam acarretar a um empreendimento de pequeno porte.

De acordo com o Instituto Nacional de Padrões e Tecnologia (NIST) dos Estados Unidos, a segurança da informação é baseada em três pilares fundamentais: disponibilidade, confiabilidade e integridade, que são utilizados para proteger dados e mitigar possíveis danos (NIST, 2023). Este conceito de proteção tem um principal objetivo, que é a gestão de pessoas, onde se procura conscientizar os usuários sobre os riscos da utilização da tecnologia e como proceder em relação à segurança de dados. Além disso, segundo o artigo 46 da Lei nº 13.709, de 14 de agosto de 2018 (LGPD), que estabelece a obrigação de garantir a segurança dos dados pessoais, a segurança da informação também é importante pelo fato de ser um requisito exigido pela Lei Geral de Proteção de Dados Pessoais.

A respeito da LGPD, o artigo 7º, item I, estabelece que toda empresa que capture dados dos usuários deve possuir um fluxo seguro e apropriado para utilizá-los. Isso significa que os dados só podem ser coletados com permissão do usuário e usados apenas com seu consentimento. Essa prática surgiu primeiramente na Alemanha, após uma grande exposição de dados, originando as futuras leis mundiais de proteção de dados. A primeira geração dessas legislações abrangeu até a instauração da Bundesdatenschutzgesetz, a lei federal da República Federativa da Alemanha sobre

proteção de dados pessoais, em 1977. Várias leis relacionadas à proteção de dados foram criadas na Alemanha nessa época, como é explicado por Gasiola:

> [...] são reações a projetos estatais para implementar bancos de dados centralizados sobre a população, em meio à euforia tecnológica que marcou o pós-guerra. O choque entre a recente lembrança (ou presença) dos governos autoritários e a iminência de tais projetos levou ao reconhecimento expresso da proteção de dados perante as pretensões públicas de aumentar seu poder informacional. O objetivo dessas leis era, acima de tudo, estabelecer limites e garantir a transparência na criação de bancos de dados. (GASIOLA,2019[1])

No Brasil a Autoridade Nacional de Proteção de Dados (ANPD) da Presidência da República aprovou o Regulamento de aplicação da Lei nº 13.709, de 14/08/2018, Lei Geral de Proteção de Dados Pessoais, para agentes de tratamento de pequeno porte – microempresas, empresas de pequeno porte, startups[2] e pessoas jurídicas de direito privado, inclusive sem fins lucrativos. Apesar de parecer burocrática, a lei prevê mais segurança para o usuário e para a vida financeira dos negócios.

Portanto, o presente artigo é estruturado a partir de um cenário, para analisar e compreender a influência que a LGPD ocasiona aos micros empreendimentos, bem como as consequências a que estão sujeitos os empresários que não se adequarem a esta legislação.

2. REFERENCIAL TEÓRICO

Nesta seção, a pesquisa aborda os principais conceitos teóricos relativos ao estudo através de revisão bibliográfica, oportunizando apresentar o estado da arte com relação ao tema central - a LGPD.

2.1 Segurança da informação

De acordo com Vilaça e De Araújo (2016), a informação vem se tornando cada vez mais importante na sociedade, se moldando conforme a evolução da tecnologia e sendo também um recurso crítico para realização do negócio e execução da missão

[1] https://www.jota.info/opiniao-e-analise/artigos/criacao-e-desenvolvimento-da-protecao-de-dados-na-alemanha-29052019. Acesso em 10 abril 2023.

[2] Startups: empresa que nasce em torno de uma ideia diferente, escalável e em condições de extrema incerteza.

organizacional. A informação é um recurso que agrega valor para a organização e deve ser bem gerenciado e utilizado, tendo em vista que é necessário garantir que ela esteja sendo disponibilizada apenas para aqueles que necessitam dela em um determinado momento. Assim a análise da informação deve ser realizada como um conjunto de dados que podem gerar informações tornando-se assim um ativo valioso para a organização.

Segundo (SUDRÉ,2018 apud DA SILVA e MISAGHI,2021,p.3), a proteção de dados é a combinação dos três elementos, que incluem: instrumentos, restrições e diretrizes de segurança. A salvaguarda de dados é marcada pelo impedimento de três características fundamentais da informação, quais sejam: sigilo, acessibilidade e autenticidade.

1. Confidencialidade: Essa expressão descreve a asseguração de que as informações estão sendo manuseadas com sigilo e sem compartilhamento não autorizado, iniciando na coleta, seguindo pela retenção e processamento até o instante em que elas sejam eliminadas ou passem para outro custodiante.(HINTZBERGEN et al., 2018);
2. Disponibilidade: Tem sua finalidade vinculada ao prover de entrada a uma informação no instante solicitado. Em outras palavras, é a característica de que os dados estejam prontamente disponíveis e utilizáveis mediante pedido por um indivíduo ou determinado sistema, instituição ou organização no momento em que tenha sido requisitado, sendo aplicável para qualquer espécie de informação ou modo de acesso, desde que autorizado para tanto. (SUDRÉ,2018 apud DA SILVA e MISAGHI,2021,p.3);
3. Integridade: De acordo com (SUDRÉ,2018 apud DA SILVA e MISAGHI,2021,p.3), pode ser definida como um meio de assegurar que as informações não sejam manipuladas ou violadas indevidamente. Desse modo, almeja-se que a informação seja disponibilizada integralmente e sem qualquer tipo de alteração, conforme indicado. (HINTZBERGEN et al. 2018)

2.2 Lei geral de proteção de dados (lgpd)

A Lei Geral de Proteção de Dados Pessoais (LGPD), que entrou em vigor no Brasil em setembro de 2020 (BRASIL,2018), tem como objetivo regular o tratamento

de dados pessoais por empresas públicas e privadas. Ela foi criada em 2018 com a motivação de proteger a privacidade dos cidadãos diante do avanço da tecnologia e do aumento do armazenamento e compartilhamento de informações pessoais online. O rápido desenvolvimento tecnológico tornou necessária a criação de normas para proteger os direitos fundamentais das pessoas e garantir o controle dos indivíduos sobre seus dados pessoais, diante dos constantes vazamentos e escândalos envolvendo o uso indevido dessas informações (CÂMARA DOS DEPUTADOS DO BRASIL, 2023).

A lei impacta na gestão de dados pessoais pelas empresas em todos os setores, fazendo com que as empresas implementem ou adequem novos procedimentos ou criem setores para alinhamento às novas normas (POHLMANN, 2019). Esta lei representa um novo marco no ordenamento jurídico brasileiro, tendo em vista que trata da proteção de dados pessoais independente do meio em que sejam adquiridos e independente de se referir à pessoa física ou jurídica.

A LGPD está dividida em 10 capítulos e composta por 65 artigos, e alguns deles ainda precisam ser complementados pela Autoridade Nacional de Proteção de Dados (ANPD) que está em processo de criação, sendo este o órgão o responsável pela fiscalização, regulação e punição das instituições que não seguirem a legislação (BRASIL, 2018).

2.2.1 As atribuiçoes do *data protection officer* - (dpo) perante a lgpd

A figura do Data Protection Offícer - DPO é oriunda da lei de proteção de dados da Europa, General Data Protection Regulation - GDPR, sancionada em 2016. No Brasil, o DPO é intitulado como “encarregado”, este deve ser designado com base em suas qualidades profissionais, mais especificamente em seu conhecimento jurídico-regulatório.

Apesar de a LGPD não fazer nenhuma exigência explícita para a qualificação específica do Encarregado, o que constituiria para o legislador uma limitação ao livre exercício profissional (direito este fundamental previsto na Constituição Federal em seu art. 5º, XIII), é imprescindível que a figura do DPO seja apta a compreender o ordenamento jurídico local, sobretudo regulatório, bem como tenha um vasto conhecimento das legislações internacionais sobre proteção de dados, tendo em vista

que tratará diretamente das informações dos titulares, os quais terão fluxo entre países diversos (GIBSON, 2003, p.5).

Além disso, é salutar também que o DPO tenha conhecimento sobre tecnologia e segurança da informação, a fim de que compreenda os riscos que circundam os softwares e programas da empresa. O art. 37 do GDPR dispõe o seguinte:

> O encarregado da proteção de dados é designado com base nas suas qualidades profissionais e, em especial, nos seus conhecimentos especializados no domínio do direito e das práticas de proteção de dados, bem como na sua capacidade para desempenhar as funções referidas no artigo 39. (GDPR, 2018[3]).

O art. 41 da LGPD determina que o encarregado será indicado pelo controlador da proteção de dados. Ainda que o DPO não seja o responsável pela palavra final no processo de tratamento de dados (armazenagem, coleta, produção, transferência, eliminação, etc), papel este de incumbência do controlador, a sua escolha deve ser criteriosa pois será o encarregado o responsável por educar, avaliar e ponderar a adequação do trabalho desenvolvido pela empresa com as normas vigentes de proteção das informações dos titulares.

Importante lembrar que, o DPO deve sempre estar acessível, de preferência falar fluentemente a língua portuguesa e residir no Brasil, tendo em vista a sua função de elo de comunicação entre os titulares de dados, a Autoridade Nacional de Proteção de Dados - ANPD e o controlador, cuja atribuição está prevista no art. 5º, VII, da Lei n° 13.709/18.

Tal função tem ligação direta com o disposto no art. 18, da LGPD, nos seguintes termos:

> 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 [...]" (BRASIL, 2018).

Embora a referida atribuição pertença ao controlador, o Encarregado enquanto ponte entre os titulares e os operadores do tratamento, deve também estar acessível para prestar esclarecimentos a estes quando solicitado. O DPO deverá aceitar as

[3] https://gdpr-info.eu/. Acesso em: 01 de Maio de 2023.

reclamações e comunicações dos titulares, bem como adotar providências, conforme art. 41, §2°, da Lei de Proteção de Dados (BRASIL, 2018)."

Frisa-se que a LGPD em seu art. 20, traz a possibilidade de o titular requerer a revisão das decisões tomadas com fundamento no tratamento automatizado de dados pessoais que afetem seus interesses, principalmente decisões que repercutem diretamente na formação de seu perfil, seja ele profissional ou pessoal, na análise e aceitação de crédito ou nos aspectos de sua personalidade (BRASIL, 2018).

Diante desse cenário, sugere-se que o responsável seja uma entidade corporativa, levando em conta a complexidade e a exigência rigorosa que seria requerer de um indivíduo orgânico possuir todo esse acervo de saberes de áreas pluridisciplinares e restringir, de certa maneira, a prática profissional. No entanto, destaca-se que essa escolha fica a critério da companhia contratante, podendo ela selecionar livremente quem assumirá a posição de DPO

2.3 Responsabilidade civil no âmbito da proteção de dados

A obrigação de reparação de danos civis decorrentes da proteção de dados é uma responsabilidade que surge de outra relação em que um equívoco primário foi cometido. Isso implica que as empresas precisam frequentemente revisar seus termos de consentimento, cumprindo com os requisitos de informação, que podem gerar a obrigação de indenização perante a lei, conforme Maldonado (2019).

Esse contexto exige que as empresas não apenas se adaptem à legislação, mas também mantenham seus programas de conformidade funcionando adequadamente, revisando constantemente os processos e investindo em treinamento e políticas de segurança da informação para evitar incidentes como vazamentos de dados.

2.4 ISO 27002 e ISO 27001

A implementação das normas ISO 27001 e ISO 27002 é de extrema importância para as organizações que buscam estabelecer um Sistema de Gestão da Segurança da Informação (SGSI) em conformidade com os requisitos da LGPD. De acordo com o Portal GSTI (2023), a ISO/IEC 27001 é a norma que define os requisitos para um SGSI, enquanto a ISO/IEC 27002 consiste em um código de práticas com um conjunto completo de controles que auxiliam na aplicação do SGSI.

A ISO/IEC 27001, como citado pelo Portal GSTI, é considerada a principal norma utilizada por organizações para obter a certificação empresarial em gestão da segurança da informação. Ela estabelece os requisitos necessários para um SGSI, que é parte integrante do sistema de gestão global da organização. O SGSI é baseado em uma abordagem de risco do negócio e engloba a estrutura organizacional, políticas, atividades de planejamento, responsabilidades, práticas, procedimentos, processos e recursos. A ISO 27001 é amplamente reconhecida e estudada, inclusive por candidatos em concursos de TI.

De acordo com a GSTI, a ISO/IEC 27002 fornece um conjunto completo de controles e boas práticas para a aplicação do SGSI. Embora seja recomendável utilizá-la em conjunto com a ISO 27001, a norma pode ser consultada de forma independente para adoção das boas práticas em segurança da informação.

2.5 Microempresas

Segundo o Livro Lei Geral da Microempresa e da Empresa de Pequeno Porte (2022), microempresa (ME) é um porte de empresa, ou seja, uma classificação de seu tamanho e que possui as seguintes características:

• Rendimento bruto de até R$ 360 mil por ano;

• Opção de escolha do regime tributário entre Simples Nacional, Lucro Presumido e Lucro Real;

• Opção de escolha de natureza jurídica como: Microempresário Individual (MEI), para faturamentos até 81 mil reais ao ano, Empresário Individual, Sociedade Limitada Unipessoal ou Sociedade Limitada com sócios e Sociedade Simples

De acordo com a Contabilizei (2023), “Uma característica muito importante das MEs, e que acaba sendo uma grande vantagem, é o fato delas se enquadrarem na Lei Geral das Microempresas e Empresas de Pequeno Porte”. Graças a essa legislação, que foi instituída em 2006 com o objetivo de regulamentar as atividades, as Microempresas (ME) e Empresas de Pequeno Porte (EPP) são protegidas e até mesmo favorecidas de modo a usufruir de certas importantes vantagens, como pagar menos impostos.

2.6 Panorama LGPD em Santa Catarina

Em janeiro de 2021, o SEBRAE Santa Catarina, em seu artigo "Panorama LGPD em Santa Catarina", realizou uma pesquisa por telefone para identificar o nível de conhecimento e adequação à nova Lei Geral de Proteção de Dados – LGPD, com intervalo de confiança de 95%. A amostragem é estratificada, composta por 810 (oitocentos e dez) entrevistas distribuídas por cotas representativas ao número de MEI, ME e PE, assim como por setor de atividade nas regiões Foz do Itajaí, Grande Florianópolis, Extremo Oeste, Meio Oeste, Oeste, Norte, Serra, Sul e Vale do Itajaí. Os resultados gerais são ponderados por região do estado.

Em um trecho retirado da pesquisa o Sebrae cita o seguinte: “Cerca de 7 em cada 10 empresários ouviu falar da LGPD” também é complementado por “...que o empresário se sente desconfortável em afirmar que não está adequado à lei, indicando que o percentual de empresas que não estão em conformidade com a LGPD tende a ser maior”. Citando as microempresas 74% têm conhecimento sobre a lei, entretanto o nível de adequação está em 27%, das que não estão adequadas somam 30% e as que estão em fase de adequação 42%.

2.7 Desafios na adequação da LGPD segundo pesquisa da RD Station

Segundo a pesquisa retirada de Resultados Digitais que foi realizada em 2021 pela RD Station em parceria com a Manar Soluções em Pesquisa e Eduardo Dorfmann Aranovich e Cia Advogados, somente 35% das microempresas dizem não ter política estabelecida de segurança de dados e afirmam que vão ter que começar do zero. Um dos pontos citados na pesquisa é:

> [...] A pesquisa revela a existência de uma pulverização de gargalos, com destaque para os principais pontos: complexidade das medidas, ausência de pessoas especializadas e ausência do conhecimento necessário. (MANAR,2021[4]).

Manar (2021) ainda cita que cerca de 28% planejam alocar menos de R$ 10 mil, enquanto quase 40% das companhias pesquisadas ainda não sabem responder o quanto deverão desembolsar. Ainda com números 14% dizem não ter problemas para se adequar até o momento, 30% reclamam da complexidade das medidas e

[4] https://d335luupugsy2.cloudfront.net/cms%2Ffiles%2F2%2F1628275980relatorio-adequacao-lgpd-rd-manar.pdf. Acesso em: 01 de maio de 2023.

volume de trabalho necessário, 27% relatam a inexistência de uma área dedicada à informação e tratamento de dados na companhia, 26% da falta de conhecimento suficiente sobre a LGPD, 17% têm pouco tempo disponível para se dedicar à Lei, 13% informam da falta de verba para a contratação de uma consultoria especializada e 20% não souberam informar.

2.8 Desafios na adequação da LGPD segundo a Techcompliance

Como apontado pela Tech Compliance, o artigo “Principais desafios das empresas na jornada de adequação à LGPD” redigido por Paola Luongo Lorenzetti e Heloísa Helena de Paula Cunha, as multas em razão do descumprimento da LGPD podem chegar a 2% da receita da empresa, até o limite de R$ 50 milhões, sem contar os danos reputacionais que uma penalidade ou eventual vazamento de dados podem causar à imagem da empresa.

Conforme observado o artigo da Tech Compliance, foi realizado uma entrevista com 366 empresas (em diferentes estágios de crescimento e de setores diversos), apenas 9,8% consideram já ter atendido de 81% a 100% dos requisitos legais da LGPD.

Um dos pontos citados na pesquisa é a falta de entendimento dos aspectos da lei que é um dos principais desafios das empresas com a LGPD. Isso porque, a maioria sequer sabe se realiza atividade de tratamento de dados pessoais ou não. Ocorre que, de acordo com o disposto na LGPD, salvo raras exceções, tratamento é qualquer atividade realizada com um dado pessoal, que por sua vez, é qualquer dado que identifica, direta ou indiretamente, uma pessoa. Em outro trecho é citado a falta de Recursos Financeiros, porém com contrapartidas:

> Embora a falta de recursos financeiros tenha sido apontada pelas empresas como um dos principais desafios para a adequação, os benefícios percebidos pelas organizações que já se adequaram se sobrepõem, inclusive financeiramente, já que, com a organização dos dados, a empresa tem uma melhora significativa em sua administração geral, conforme apontou o SEBRAE em 2020. (Tech Compliance,2022[5]).

[5] https://techcompliance.org/desafios-das-empresas-com-a-lgpd/. Acesso em: 10 de setembro de 2022

A pesquisa também cita a ausência de cultura de proteção de dados:

> [...]é essencial o envolvimento de todos os funcionários e prestadores de serviços, que deverão estar cientes de todas as práticas adotadas pela empresa para assegurar que a privacidade e os dados pessoais dos titulares de dados estão sendo devidamente tutelados (Tech Compliance,2022).

3 METODOLOGIA

Com a finalidade de alcançar os objetivos propostos neste trabalho, foi desenvolvida a metodologia de pesquisa exploratória bibliográfica que consiste na pesquisa, que envolveu a verificação de materiais bibliográficos pertinentes, visando fundamentar toda a contextualização inicial, bem como o desfecho ao final deste estudo.

A pesquisa bibliográfica teve foco na leitura de material digital, em segmentos acadêmicos e industriais, onde os autores possuem referência no assunto. Ademais, foram analisados índices de integração de microempresas a LGPD, com o intuito de entender a demanda de adesão e o que isto impactou na vigência da lei.

4 RESULTADOS E DISCUSSÃO

A partir da pesquisa realizada no presente artigo, é possível observar que a Lei Geral de Proteção de Dados (LGPD) representa um desafio significativo para as empresas, especialmente as microempresas. As pesquisas realizadas pelo SEBRAE Santa Catarina (2021)[6], Resultados Digitais em parceria com a Manar Soluções em Pesquisa e Eduardo Dorfmann Aranovich e Cia Advogados, e Tech Compliance evidenciam a necessidade de maior conhecimento e adequação por parte das organizações em relação à LGPD.

Os resultados das pesquisas de Manar, R. D. (2021), revelam que uma grande parcela dos entrevistados, mais precisamente 93%, tem conhecimento sobre a existência da lei ou pelo menos já ouviram falar dela, já a pesquisa do SEBRAE Santa Catarina, esse número cai para 67.7%, lembrando que ambas as pesquisas foram feitas em 2021.

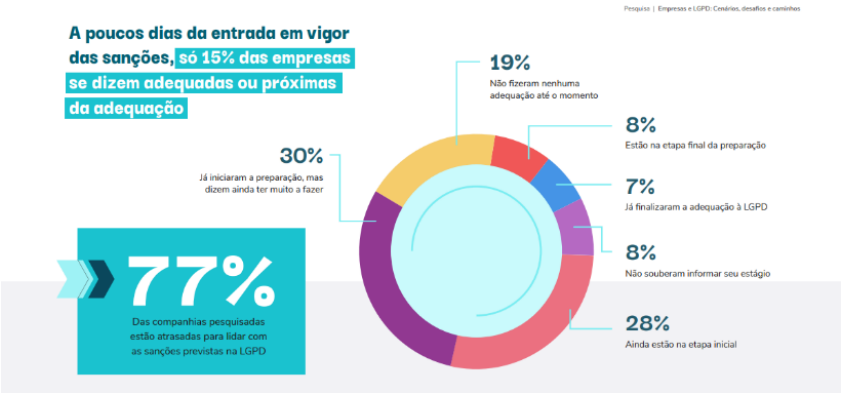
[6] https://atendimento.sebrae-sc.com.br/panorama-lgpd-em-santa-catarina/ Acessado em: 15 maio 2023.

Figura 1: - Empresas e LGPD: Cenários, desafios e caminhos

Fonte: Manar, R. D. (2021, pág. 10)

Ainda sobre Manar, R. D. (2021), a pesquisa mostra que 77% das companhias estão atrasadas no processo de adequação; apenas 15% já terminaram ou estão na reta final de sua adaptação, além disso, a complexidade das medidas, a ausência de pessoas especializadas, a falta de recursos financeiros e o desconhecimento sobre aspectos específicos da lei foram identificados como os principais desafios enfrentados pelas empresas em sua jornada de adequação à LGPD. De acordo com os números do levantamento, 69% não possuem ou estão em processo de construção de políticas de proteção aos dados dos clientes – uma etapa fundamental para implantação dos padrões demandados pela LGDP. Mais preocupante ainda: umas porções consideráveis ainda não iniciaram sequer a primeira etapa. Mais de um quinto – 22% – das companhias nacionais não adotam nenhum tipo de medida de segurança relativa às informações pessoais da clientela.

Figura 2: Empresas e LGPD



Fonte: Manar, R. D. (2021, pag. 14)

É importante ressaltar que segundo os dados obtidos da Tech Compliance, o descumprimento da LGPD pode acarretar multas significativas e danos reputacionais para as empresas. As penalidades podem chegar a 2% da receita da organização, com um limite máximo de R$ 50 milhões. Portanto, é fundamental que as empresas estejam cientes dos riscos envolvidos e adotem as medidas necessárias para garantir a proteção dos dados pessoais.

Ao olharmos as pesquisas realizadas em 2021, ambas citam pontos similares tais como, não saberem informar qual área lidera a adequação às normas da LGPD ou informaram na pesquisa que não possuem a figura do encarregado de proteção de dados (DPO) contratado. É citado ainda uma falta de investimento e de capacitação dos profissionais, sendo outra barreira para a adoção das novas regras, a maior parte das companhias não sabem o quanto terão que investir outra parte não pretende investir.

Em resumo, não há uma única razão principal para o retardamento das empresas brasileiras em se ajustarem às normas da LGPD. As pesquisas revelam a existência de uma pulverização de gargalos, com destaque para os principais pontos: complexidade das medidas, ausência de pessoas especializadas, ausência do conhecimento necessário, falta de Recursos Financeiros e ausência de Cultura de Proteção de Dados.

5 CONSIDERAÇÕES FINAIS

Através dos estudos efetuado, contatou-se a importância da LGPD, mediante os desafios enfrentados pelas empresas, sendo esta crucial que as organizações

invistam em capacitação, recursos e infraestrutura adequados para garantir a conformidade com a legislação. A conscientização sobre a proteção de dados deve ser disseminada em todos os níveis da organização, promovendo uma cultura de privacidade e segurança.

Apesar dos desafios, as pesquisas também destacam os benefícios percebidos pelas organizações que já se adequaram à LGPD. Além do cumprimento das exigências legais, a organização dos dados proporciona melhorias significativas na administração geral das empresas. A implementação de práticas de proteção de dados também contribui para o fortalecimento da cultura de privacidade e segurança da informação, envolvendo todos os funcionários e prestadores de serviços.

Além disso, é fundamental que as empresas compreendam a importância da LGPD não apenas como uma exigência legal, mas também como uma oportunidade de fortalecer a confiança dos clientes, proteger a reputação da empresa e estabelecer uma vantagem competitiva no mercado atual, cada vez mais consciente da proteção dos dados pessoais.

REFERÊNCIAS

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais**. Brasília, DF: Presidência da República, 2018. Disponível em: https://www2.camara.leg.br/legin/fed/lei/2018/lei-13709-14-agosto-2018-787077-publicacaooriginal-156212-pl.html. Acesso em: 19 de setembro de 2022.

CÂMARA DOS DEPUTADOS DO BRASIL. Avulso - PL 4060/2012. **Código do teor 1663865.** Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=FA5C1BA8CBEC7AB3417FF184C2FCBED3.proposicoesWebExterno2?codteor=1663865&filename=Avulso+-PL+4060%2F2012. Acesso em 14 de maio de 2023.

CONTABILIZEI. **O que é microempresa e qual a diferença com outros tipos?** Disponível em: https://www.contabilizei.com.br/contabilidade-online/o-que-e-microempresa-e-qual-a-diferenca-com-outros-tipos/. Acesso em: 14 mai. 2023.

DA SILVA, Milton Machado Pereira; MISAGHI, Dr.Mehran. **ESTUDO DE CASO SOBRE A APLICAÇÃO DA LGPD NA ÁREA DA PSICOLOGIA CLÍNICA.** Unisociesc, Joinvile,SC,2021.

GASIOLA, Gustavo Gil. **Criação e desenvolvimento da proteção de dados na Alemanha**. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/criacao-e-desenvolvimento-da-protecao-de-dados-na-alemanha-29052019. Acesso em 10 abril 2023.

GDPR. **Regulamento Geral de Proteção de Dados.** Disponível em: https://gdpr-info.eu/. Acesso em: 01 de maio de 2023.

GIBSON, Willian. **Neuromancer**. São Paulo: Aleph, 2003.

HINTZBERGEN, Jule et al. **Fundamentos de Segurança da Informação:** com base na iso 27001 e na iso 27002. 2. ed. Rio de Janeiro: Brasport, 2018.

Instituto Nacional de Padrões e Tecnologia (NIST). **Controles e Práticas de Segurança da Informação para Sistemas de Informação e Organizações (NIST SP 800-53).** Disponível em: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf. Acesso em: 14 de maio de 2023.

MALDONADO, Viviane Nóbrega. LGPD – **Lei geral de proteção de dados – Manual de implementação**. 3ª ed. Revista dos Tribunais, 2019.

Manar, R. D. (2021). **Empresas e LGPD: Cenários, desafios e caminhos**. Recuperado de https://d335luupugsy2.cloudfront.net/cms%2Ffiles%2F2%2F1628275980relatorio-adequacao-lgpd-rd-manar.pdf. Acesso em: 01 de maio de 2023.

POHLMANN, S. LGPD Ninja: Entendend**o e implementando a Lei Geral de Proteção de Dados na Empresa.** Rio de Janeiro: Fross, 2019.

PORTAL GSTI. Sobre a ISO 27001 e ISO 27002. **Portal GSTI, [S.l.], [2023].** Disponível em: https://www.portalgsti.com.br/iso-27001-iso-27002/sobre/. Acesso em: 15 maio 2023.

Revista Sebrae: **Lei Geral 3 Anos da Lei Geral da Micro e Pequena**. Disponível em: https://sebrae.com.br/sites/PortalSebrae/artigos/lei-geral-da-micro-e-pequena-empresa,46b1494aed4bd710VgnVCM100000d701210aRCRD. Acesso em: 10 de setembro de 2022.

Resultados Digitais. **Pesquisa de Empresas e a LGPD.** Disponível em: https://resultadosdigitais.com.br/marketing/pesquisa-empresas-e-lgpd/. Acesso em: 01 de maio de 2023.

SEBRAE Santa Catarina. **Panorama LGPD em Santa Catarina**. SEBRAE Santa Catarina, 2021. Disponível em: https://atendimento.sebrae-sc.com.br/panorama-lgpd-em-santa-catarina/ Acessado em: 15 maio 2023.

VILAÇA, Maurício; DE ARAÚJO, Fábio. **Gestão da informação e do conhecimento:** abordagens, conceitos e práticas. 3. ed. São Paulo: Saraiva, 2016.

Tech Compliance: **Principais desafios das empresas na jornada de adequação à LGPD**. Disponível em: https://techcompliance.org/desafios-das-empresas-com-a-lgpd/. Acesso em: 10 de setembro de 2022.