23

DOI: https://doi.org/10.5007/2175-8077.2023.e82226

Recebido: 14/06/2021

Aceito: 05/09/2023

Gestão de dados em micro e pequenas empresas: Conformidade com a lei geral de proteção de dados

Data management in micro and small companies: Compliance with the general data protection law

Marco Antonio Silveira

Faculdade de Campo Limpo Paulista (UNIFACCAMP)
marco.silveira@cti.gov.br
https://orcid.org/0000-0002-2436-0364

Talita da Silva Carlos Langen

Serviço Nacional de Aprendizagem Comercial (SENAC)
talitabiblio32@gmail.com
https://orcid.org/0009-0003-4928-0090

RESUMO

Para compreender o impacto dos dados pessoais em micro e pequenas empresas (MPEs), este estudo se propôs a investigar o grau de conformidade destas em relação às exigências dispostas na Lei Geral de Proteção de Dados/LGPD. O objetivo foi verificar como as MPEs estão se preparando para cumprir os requisitos da LGPD. A abordagem desta pesquisa é fenomenológica, de caráter quali-quantitativa. Das três hipóteses testadas, somente uma foi confirmada, mostrando que a proporção de não conformidades, considerando-se o fator "término do tratamento de dados pessoais", é significativamente maior do que as conformidades. Esse resultado indica a necessidade de atenção com as questões relacionadas, uma vez que os dados pessoais, na maioria das vezes, são bastante sensíveis sendo, inclusive, objetos de proteção legal. Com base nos resultados encontrados é possível afirmar que, muito embora as MPEs da amostra estudada estarem preocupadas com a proteção dos dados pessoais, o seu preparo ainda é incipiente. De maneira prática, sugere-se a adoção do Ciclo de Vida dos Dados para mapear os processos do negócio. Do ponto de vista teórico, esta pesquisa buscou abordar o *gap* das competências tecnológicas e humanas das empresas ao lidar com a complexidade do mundo digital e a sua regulação, evidenciado pelo aumento do comércio digital.

Palavras-Chave: Lei Geral de Proteção de Dados. grau de conformidade. proteção de dados. micro e pequenas empresas.

ABSTRACT

In order to understand the impact of personal data on micro and small companies (MSEs), this research aimed to investigate the degree of compliance of these in relation to the requirements set forth in the Brazilian General Data Protection Law / LGPD. The objective was to verify whether MSEs are preparing to meet the requirements of the LGPD. The approach of this research is phenomenological, of a quali-quanti character. Of the three hypotheses tested, only one was confirmed, showing that the proportion of non-compliance, considering the factor "conclusion of personal data processing", is significantly higher than compliance. Based on the results found, it is possible to state that the MSEs in the studied sample are concerned with the protection of personal data. However, their preparation is still incipient. In a practical way, it is suggested the adoption of the Data Life Cycle to map the business processes. From a theoretical point of view, this research sought to address the gap in technological and human skills of companies when dealing with the complexity of the digital world and its regulation, evidenced by the increase in digital commerce.

Key-words: General Data Protection Law. degree of compliance. data protection. micro and small companies.

1 INTRODUÇÃO

A evolução das tecnologias de informação e comunicação propiciou grandes transformações na sociedade, incluindo a forma como produzimos e consumimos dados e informações (Zeng & Yang, 2023). Atualmente, nenhuma organização pode ser eficaz sem dados de alta qualidade, pois estes são base para a tomada de decisões assertivas (Serumaga-Zake & Van Der Poll, 2021; Russa, 2021).

O incremento substancial no volume e a aceleração da taxa de geração de dados contribuem para intensificar os desafios inerentes à manipulação e à mineração de dados (*Data Administration Management Association* [DAMA], 2017). Nesse cenário, os dados pessoais dos cidadãos transformam-se em importantes elementos para essa nova economia e, as possibilidades de monetização desses dados e informações têm sido exploradas por empresas de todos os portes e de diferentes setores (Bioni, 2019; Branco, 2020).

Esse aumento da importância dos dados trouxe à baila a necessidade da segurança e da proteção dos dados, em especial, relacionados às pessoas. A esse respeito, Oliveira *et al*. (2019) ressaltam que:

> A preocupação com o tratamento de dados pessoais como desdobramento da privacidade é um efeito colateral da mudança de paradigma trazida pela "Quarta Revolução Industrial", cujo tom é dado pelo fenômeno da "informacionalização da sociedade", iniciado na década de 1970. Seus reflexos impactam diretamente tanto a atividade econômico-empresarial, quanto a atuação do próprio Estado, que, além de criar e consumir informação, controla o fluxo de informações. (Oliveira *et al*., 2019)

Martin *et al*. (2017) afirma que as boas práticas de gerenciamento de dados das empresas podem suprimir os efeitos negativos da vulnerabilidade dos dados do cliente. Um exemplo ilustrativo desse fenômeno pode ser observado no contexto internacional pois, de acordo com o *U.S. Identity Theft Resource Center*, estima-se que quase 130 milhões de registros pessoais tenham sido expostos a riscos de violações de dados (*Identity Theft Resource Center* [ITRC], 2023).

Nem todos aqueles cujos registros foram comprometidos sofrem vitimização, mas a amplitude desconhecida e a falta de controle sobre essa ameaça tornam esse tipo de vulnerabilidade especialmente preocupante para os clientes. A percepção de vulnerabilidade aumenta como resultado de uma violação de dados em uma empresa que possui os dados do cliente (empresa focal), mas também, indiretamente, com violações em concorrentes próximos (empresas rivais), pois esses eventos aumentam a saliência da crença de que violações semelhantes são possíveis (Johansen, 2023).

Muitos países têm respondido ao desafio destas questões relacionadas à privacidade, segurança e uso responsável dos dados por meio da implementação de legislações e regulamentações específicas (Chiarini & Compagnucci, 2022). Iniciativas notáveis, no contexto internacional, incluem a criação de leis de proteção de dados, como o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia, que estabeleceu um marco abrangente para o tratamento de dados pessoais e os direitos dos titulares desses dados (Ziegler *et al*., 2019).

Impulsionados por essas mudanças, o Brasil se inspirou em legislações vigentes em outros países, em especial o GDPR da União Europeia, e criou nesse contexto de regulamentação de mercado e incentivo à inovação leis que visam regulamentar novas práticas de negócios, tais como a Lei Geral de Proteção de Dados (LGPD), o Marco Civil da Internet (MCI), a Lei de Acesso à Informação (LAI) e a Lei do Cadastro Positivo (LCP). Esse conjunto de leis tem o objetivo de normatizar as novas formas de consumir, produzir e trabalhar (Bioni, 2019).

As empresas em geral enfrentam dificuldades para inovar e se adaptar às regras impostas pelas novas leis, sendo que as micro e pequenas empresas (MPEs) enfrentam dificuldades ainda maiores por falta de competência técnica, investimentos estruturais ou tecnologia (Lima e Silva, 2019). Assim, a regulação do mercado impacta diretamente os pequenos negócios, agregando mais um desafio à sobrevivência em um mercado complexo e competitivo.

Costa *et al*. (2023) afirmam que as pequenas e médias empresas, as quais representam 90% dos negócios a nível mundial, são afetadas pela transformação digital de forma diferente das grandes empresas. Isso porque, embora essas empresas tenham mais flexibilidade e agilidade para se adaptarem a novas circunstâncias, também têm recursos e capacidades

de especialização mais limitadas. Assim, as ferramentas, dimensões e variáveis para medir e investigar os impactos da transformação digital no desempenho das pequenas e medianas empresas é um tema de interesse crescente, mas o corpo de conhecimento ainda está em desenvolvimento (Costa *et al*., 2023).

Estar em conformidade com a legislação traz benefícios para os consumidores e aumenta a competitividade do negócio (Derbli, 2019; Molina & Santos, 2020). Portanto, buscar soluções inovadoras e de baixo custo são importantes para que as MPEs se mantenham ativas. e competitivas no complexo e competitivo mercado contemporâneo é um desafio imperativo (Rodrigues *et al*., 2021).

Por outro lado, a LGPD também oferece oportunidades de melhoria, permitindo às empresas fortalecerem a proteção dos titulares de dados, construindo confiança e relações sólidas com os clientes. No estudo de Sousa (2021) foi considerado o Ciclo de Vida dos Dados (CVD) nos atos praticados pelos Registros Civis para, a partir dele, descrever a sequência de ações necessárias para atingir os objetivos da Lei.

Cruz *et al*. (2021) analisaram as implicações da LGPD nas operações das empresas de contabilidade e nas adaptações necessárias decorrentes, a qual destacou a necessidade urgente de empresas de contabilidade se adaptarem à LGPD, dadas as possíveis consequências negativas caso não cumpram suas diretrizes. Além de enfrentar multas e sanções, essas empresas correm o risco de prejudicar sua reputação no mercado, especialmente se estiverem envolvidas em incidentes de segurança ou vazamento de dados.

No entanto, esse cenário de transformações tecnológicas também expôs as MPEs a desafios consideráveis, especialmente no que se refere à implementação e conformidade com regulamentações visando à proteção de dados (Kádárová *et al*., 2023). Diante dessa realidade, emergem duas questões fundamentais para nossa pesquisa: Qual é o nível de conformidade das MPEs à LGPD no que diz respeito ao tratamento e uso de dados pessoais dos clientes? Quais são as principais não conformidades relacionadas aos fatores de tratamento de dados pessoais identificadas nas MPEs, e como essas não conformidades afetam a conformidade geral com a LGPD?

Este estudo tem como objetivo geral analisar o grau de conformidade das MPEs à LGPD no que tange ao uso de dados pessoais dos clientes. Para atingir esse objetivo, se delimitaram os seguintes objetivos específicos:

- Explorar os conceitos fundamentais de gestão de dados e tecnologia da informação;
- Investigar a relação entre as práticas das MPEs e os princípios estabelecidos pela LGPD;
- Identificar e avaliar não conformidades relacionadas ao tratamento e término de dados pessoais pelas micro e pequenas empresas.

A estrutura do trabalho reflete uma abordagem abrangente para examinar as nuances da conformidade das MPEs à LGPD. Iniciando com a base de gestão de dados e tecnologia da informação, aprofundando-se na proteção de dados, e explorando os princípios da LGPD. Além disso, a análise das bases legais e do tratamento de dados sensíveis, juntamente com o papel do encarregado de dados (ou, *data protection office*-DPO, na GDPR) para prestar contas e garantir a transparência dos processos, forma um mosaico completo para avaliar como as MPEs lidam com dados pessoais dos clientes e garantem a conformidade com os padrões regulatórios.

2 REVISÃO DE LITERATURA

2.1 Gestão de dados e tecnologia da informação

Gestão de dados (GD) é o processo de coletar, armazenar, proteger e usar os dados de uma organização, sendo fundamental o papel desempenhado pelas legislações e regulamentações para estabelecer diretrizes claras e responsabilidades na coleta, tratamento e proteção dos dados. Essas regulamentações visam garantir que as organizações implementem práticas sólidas de gerenciamento de dados, promovendo a transparência, a segurança e a privacidade (Wang *et al*., 2023; Sant'Ana, 2016; Solomon & Linton, 2016).

À medida que a tecnologia da informação inova a forma como conduzimos nossas vidas, a expansão de nosso acervo de dados digitais está experimentando um rápido crescimento. Embora as tecnologias de informação e comunicação facilitem o fluxo de

dados e informações na sociedade do conhecimento, é importante repensar a forma como os dados, a informação e o conhecimento impactam as organizações (Ben-Zvi & Luftman, 2022). A relevância dessa tríade permite não apenas o ajuste na gestão e no armazenamento das organizações, podendo resultar em uma economia significativa, como também afeta diretamente a competitividade sustentável a longo prazo (Kádárová *et al*., 2023; Sant'Ana, 2016).

Diversos autores discutem a importância da tecnologia, da inovação e do empreendedorismo para as pequenas empresas (Vrontis *et al*., 2022; Cantner *et al*., 2021; Solomon & Linton, 2016). Esses autores argumentam que as pequenas empresas que são capazes de se adaptar às mudanças tecnológicas, de inovar e de gerenciar seu conhecimento de forma eficaz, estão em uma posição melhor para ter sucesso.

Desde 2020, a Comissão Europeia vem alertando que as empresas precisam ser inovadoras para sobreviver no mercado atual. Isso significa estar aberto a novas ideias, estar disposto a mudar e ser capaz de implementar novas tecnologias. As políticas públicas também precisam apoiar a inovação, fornecendo incentivos para as empresas inovarem e facilitando o fluxo de conhecimento entre as empresas.

Então as boas práticas de gestão do conhecimento podem ser influenciadas pela gestão de dados. A gestão de dados é "a função empresarial de planejar, controlar e fornecer ativos de dados e informações" (DAMA, 2017, p. 4). Este processo pode ajudar as organizações a identificar padrões e tendências que podem ser usados para melhorar a tomada de decisões, a inovação e o desempenho e a competitividade. Ele vai fornecer eficácia e eficiência nas práticas de armazenamento, análise e compartilhamento do conhecimento nas MPEs.

2.2 Ciclo de vida dos dados (CVD)

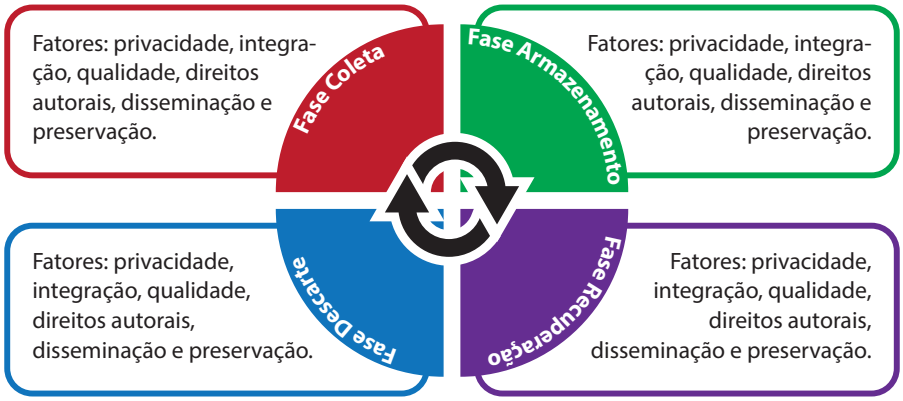
A informação precede a tecnologia, o conhecimento e a ação, por isso é tão importante gerir esse processo complexo e caótico, exigindo o desenvolvimento de competências de gestão de dados, informações e conhecimento (União Europeia, 2021).

Um dos conceitos de gestão de dados mais amplamente aceitos é a abordagem de Gestão do Ciclo de Vida dos Dados (CVD), ele abrange todo o ciclo de vida dos dados, desde sua criação ou captura até seu arquivamento ou descarte. Isso envolve vários processos, incluindo coleta de dados, armazenamento, organização, análise, compartilhamento e preservação. Esse conceito enfatiza a importância de gerenciar efetivamente os dados em cada estágio de seu ciclo de vida, garantindo qualidade, acessibilidade, segurança e conformidade com regulamentações relevantes (DAMA, 2017).

Sant'Ana (2016) apresenta o modelo do ciclo de vida dos dados, no qual apresenta quatro fases e seis fatores, conforme disposto na Figura 1. Em todas as fases estão presentes os fatores privacidade, integração, qualidade, direitos autorais, disseminação e preservação.

Uma empresa que compreender e implementar as medidas essenciais em todas as fases do CVD,

Figura 1 Ciclo de vida dos dados



Fonte: elaborado pelos autores com base em Sant'Ana (2016).

adaptando-o ao modelo de negócios e à atividade principal de cada empresa, poderá, de maneira organizada, ajustar-se às normativas e garantir conformidade com a LGPD. Assim, ao abranger as fases de coleta, armazenamento, processamento, compartilhamento e término dos dados, o CVD transforma-se em uma ferramenta para orientar as MPEs em direção à adoção de práticas seguras.

Dentro do CVD os fatores se repetem, identificados por Sant'Ana (2016). A primeira fase, denominada coleta, consiste em definir quais são as necessidades informacionais. Na segunda fase, armazenamento, deve-se pensar no conjunto de variáveis dos conteúdos armazenados. Na terceira fase, recuperação, preocupações com o *download* do conteúdo, a usabilidade, a acessibilidade e a interpretação dos dados são importantes. E, na quarta fase, é necessário planejar a eficiência do sistema que suporta os dados e avaliar o descarte.

A gestão dos dados deve estar alinhada à missão e à visão do negócio para se obter o máximo de benefícios. E o CVD pode contribuir com o mapeamento dos dados do negócio. O Governo Federal, por meio do Comitê Central de Governança de Dados, lançou em abril de 2020 um guia de boas práticas em consonância com a LGPD (Brasil, 2020), e apresenta a relação entre as fases do ciclo de vida dos dados como mostra ao Quadro 1, e as operações sobre os dados pessoais.

Quadro 1 Relação ciclo X operações de tratamento

Fase do ciclo de tratamento	Operações de tratamento - LGPD, art. 5º, X
Coleta	Coleta, produção, recepção
Retenção	Arquivamento e armazenamento
Processamento	Classificação, utilização, reprodução, processamento, avaliação ou controle da informação, extração e modificação
Compartilhamento	Transmissão, distribuição, comunicação, transferência e difusão
Eliminação	Eliminação

OBS: A operação de tratamento "acesso" (LGPD, art. 5º, X) está presente em todas as fases do ciclo de vida dos dados pessoais, pois de alguma forma é preciso realizar acesso ao dado pessoal para viabilizar sua coleta, retenção, processamento, compartilhamento ou eliminação.

Neste contexto, o Ciclo de Vida dos Dados (CVD) oferece um arcabouço conceitual que possibilita às MPEs compreender a trajetória completa dos dados pessoais, desde sua coleta até a conclusão do tratamento. Por meio deste, essas empresas podem mapear e assimilar cada etapa do procedimento de tratamento de dados, identificando eventuais vulnerabilidades e chances para assegurar a adesão à LGPD. No cenário brasileiro Alves (2020) conduziu uma análise-sucinta das várias etapas desse ciclo, bem como das alterações ocorridas em cada uma delas após a implementação da LGPD. Alves (2020) indica que a utilização de normas do conjunto ISO 27000 e outras normas de segurança da informação auxiliam na construção de boas práticas de segurança da informação. Uma exigência complexa da lei é o relatório de impacto de dados, e o ciclo de vida dos dados pode ser utilizado como base fundamental deste relatório.

Segundo Sant'Ana (2016) outros benefícios da implementação do ciclo de vida dos dados para o negócio incluem a redução dos riscos e a melhoria da qualidade dos dados, pois o CVD é utilizado para mapear tarefas ou processos com o objetivo de reduzir o gargalo de processos e dados, minimizar a redundância e melhorar a consistência dos dados, suportando empresas para adoção de políticas de acesso e uso dos dados (Rahul & Banyal, 2020). Mas, as MPEs sofrem com a falta de recursos para investir em novas tecnologias, entretanto sua flexibilidade de contornar as dificuldades são relevantes objetos de estudo.

2.3 Proteção de dados em MPEs

A proteção de dados, ou autodeterminação informativa, confere autonomia a cada cidadão para se utilizar de seus próprios dados, assim como preferir. A proteção de dados tem a intenção de regular a utilização de informações pessoais durante sua submissão em quaisquer redes, pois é necessário encontrar equilíbrio entre a garantia da privacidade e a tecnologia (Ramos & Gomes, 2019).

O debate acerca da proteção de dados inclui a preocupação com segurança da informação, área explorada pela Ciência da Computação e pelo Direito, e intrinsecamente relacionada à proteção de um grupo de informações. Portanto, são considerados princípios fundamentais a confidencialidade, a integridade e a disponibilidade da informação.

> A expressão 'tratamento de dados' da LGPD é abrangente, e, portanto, a compreensão dessa relação é relevante para a construção de processos e políticas que atendam as hipóteses previstas na lei. Os principais ativos das operações são: bases de dados, documentos, equipamentos, locais físicos, pessoas, sistemas e unidades organizacionais. A identificação desses ativos irá auxiliar nas medidas de segurança. (Bioni, 2019)

No caso das MPEs, o investimento em segurança da informação muitas vezes é deixado de lado por falta de recursos. Além disso, é mais vantajoso investir em tecnologias de prevenção, já que ações para mitigar possíveis violações ou exposição de dados são mais custosas.

A LGPD pontua a responsabilidade das organizações em incentivar boas práticas de segurança da informação, a fim de evitar possíveis violações de dados. O encarregado de dados (DPO) deve ser o profissional responsável pela proteção dos dados tratados e atuará como intermediador da comunicação entre o controlador e os titulares e a autoridade nacional. A indicação pode ser de pessoa natural ou jurídica, seja uma instituição pública ou privada (Brasil, 2018).

2.4 Lei geral de proteção de dados (LGPD)

Os princípios de proteção aos dados são fundamentais e devem ser observados de acordo com o propósito para o qual foram coletados. Bioni (2019) discute os princípios que são parte dos direitos dos titulares dos dados, e devem ser observados pelas empresas que realizarão o tratamento dos dados. Entre esses se destacam: legalidade, justiça e transparência; limitação de propósito; minimização dos dados: os dados coletados e processados devem ser os mínimos necessários ao propósito; acurácia; limitação de armazenamento: os dados devem ser mantidos somente enquanto são necessários ao propósito; integridade e confidencialidade (Bioni, 2019; Brasil, 2019).

A Lei nº 13.709/18, também conhecida como LGPD, estabelece normas para a proteção dos dados pessoais. O regramento se aplica ao uso de dados pessoais tanto *online* quanto *offline*, nos setores público e privado, visando garantir a privacidade, estabelecer regras de transparência, fomentar o desenvolvimento, padronizar e proteger o mercado, além de promover a concorrência (Machado, 2018).

Com essa legislação, todas as pessoas, físicas ou jurídicas, de direito público ou privado, devem se adaptar aos requisitos estabelecidos, que envolvem, entre outros, propósito legítimo para exigência de dados pessoais, bem como consentimento prévio para tratamento dos mesmos. Uma alteração ocorrida por meio de medida provisória de grande impacto foi a criação da ANPD (Autoridade Nacional de Proteção de Dados), cuja prerrogativa inclui edição de normas, orientações, procedimentos simplificados e diferenciados, inclusive no referente a prazos para que MPEs e *startups* possam se adaptar a ela.

A LGPD regula o tratamento dos dados relacionados apenas às pessoas físicas. Aplica-se em meios de comunicação analógico ou digital, em qualquer meio ou forma de tratamento dos dados, portanto abrange manipulação de dados dentro e fora da internet no território brasileiro.

Além disso, também é aplicada em operações de tratamento que ocorrem fora do país, quando os dados pessoais forem coletados em território brasileiro ou tenham relação a indivíduos localizados no Brasil, ou que tenham objetivo de oferta de serviços e produtos ao público brasileiro (Ramos & Gomes, 2019). Para melhor compreensão da LGPD é necessário ciência de conceitos que fundamentam a criação da lei, apresentados no Quadro 2.

Os princípios estabelecidos na LGPD impõem novas diretrizes e limitações sobre como os dados pessoais poderão ser tratados. Agentes de tratamento

Quadro 2 Conceitos fundamentais da LGPD

Conceito	Definição
Dado pessoal	É a informação relacionada a uma pessoa natural identificada ou identificável, ou seja, qualquer informação que identifique ou possa identificar uma pessoa, tais como nomes, números, códigos de identificação, endereços.
Dado pessoal sensível	É o dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião pública, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico quando vinculado a uma pessoa natural.
Tratamento	É toda a operação realizada com o dado pessoal. Por exemplo: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, controle da informação, comunicação, transferência, difusão ou extração.
Controlador	É a pessoa que tem competência para tomar decisões referentes ao tratamento de dados pessoais. Essa pessoa pode ser natural ou jurídica, de direito público ou privado.
Operador	É a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.
Agentes de tratamento	São o controlador e o operador.

Quadro 3 Princípios da LGPD

Princípios	Conceitos
Finalidade	O tratamento de dados pessoais deve ser realizado para propósitos legítimos, específicos, explícitos e informados ao titular, observadas as finalidades originárias.
Adequação	O tratamento de dados pessoais deve ser compatível com as finalidades informadas ao titular, de acordo com o contexto do tratamento.
Necessidade	O tratamento de dados pessoais deve ser limitado ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.
Livre acesso	É garantida aos titulares a consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.
Qualidade dos dados	É garantido aos titulares que seus dados sejam exatos, claros, relevantes e atualizados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.
Transparência	É garantido aos titulares o direito a informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.
Segurança	Devem ser utilizadas 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.
Prevenção	Devem ser adotadas medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais. Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.
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.

de dados devem promover revisões e adequações de políticas internas, contratos, procedimentos e atividades que envolvam a manipulação de dados pessoais, de clientes ou empregados, para que estejam alinhadas aos princípios previstos na lei. Além disso, os registros também devem ser mantidos, preferencialmente por escrito, com apresentação da adoção de medidas para adequação das operações de tratamento aos princípios estabelecidos na LGPD, como mostra o Quadro 3, independentemente do tamanho da base de dados existente.

Quando o tratamento de dados pessoais for baseado no consentimento, o controlador deve manter documentação (digital ou analógica) comprobatória da sua obtenção em conformidade com a legislação (Branco, 2020). Quando o tratamento de dados pessoais for baseado no interesse legítimo, o controlador deve adotar medidas que garantam que o tratamento aplicado seja transparente e possa ser revisado pela ANPD (Ramos & Gomes, 2019).

2.5 Consentimento e Interesse Legítimo

A LGPD estabelece que o consentimento será sempre considerado uma autorização temporária porque pode ser revogado a qualquer momento pelo titular dos dados pessoais, por procedimento gratuito e facilitado (Brasil, 2018). Caso haja mudança na finalidade para o tratamento de dados pessoais para a qual o consentimento do titular foi obtido, e desde que essa mudança não seja compatível com o consentimento originalmente dado, o controlador deverá informar previamente o titular (Ramos & Gomes, 2019).

Em caso de dados tornados manifestamente públicos pelo próprio titular, o agente fica desobrigado de obter o consentimento para tratamento de dados, observada a finalidade originária do tratamento, de modo que permaneçam vigentes os demais direitos do titular e aos princípios estabelecidos na LGPD (Branco, 2020).

O tratamento de dados pessoais necessário para atender ao interesse legítimo do controlador ou de terceiro é permitido pela LGPD, desde que tal tratamento não viole os direitos e as liberdades fundamentais do titular dos dados e que medidas para garantir a transparência de tal tratamento sejam adotadas (Brasil, 2018).

2.6 Tratamento de dados pessoais sensíveis

De acordo com a natureza de dados pessoais sensíveis, a LGPD se encarregou de diminuir as hipóteses para tratamento desses dados e impor um consentimento mais rigoroso. Para o tratamento de dados pessoais sensíveis devem ser fornecidos de forma específica e destacada (Brasil, 2018). Isto é, o agente de tratamento responsável por obter o consentimento deve se preocupar em conseguir uma autorização especial para o tratamento desse tipo de dado (Branco, 2020).

A LGPD não permite o tratamento de dados pessoais sensíveis para atender ao interesse legítimo do controlador ou de terceiros, ou proteção do crédito (Brasil, 2018). Por outro lado, permanece a possibilidade de tratar os dados pessoais sensíveis quando for indispensável para o cumprimento de obrigação legal ou regulatória pelo controlador dos dados, para o exercício regular de direitos em processo judicial, administrativo ou arbitral, ou necessário para a execução de contrato (Ramos & Gomes, 2019).

Para fins da LGPD, anonimização é um procedimento por meio do qual um dado perde a possibilidade de identificar um titular, enquanto bloqueio significa suspensão temporária de qualquer operação de tratamento de dados pessoais (Brasil, 2018).

3 MÉTODO E TÉCNICAS UTILIZADAS

O presente estudo adota uma abordagem de pesquisa qualitativa-quantitativa. Essa abordagem combina elementos de métodos qualitativos e quantitativos, permitindo uma compreensão mais abrangente e aprofundada do objeto de estudo. Especificamente, o caráter exploratório da pesquisa reflete sua intenção de investigar e descrever o objeto em questão de forma aberta e detalhada (De Sordi, 2017).

A escolha pela abordagem fenomenológica se justifica pelo seu foco em compreender a essência e a natureza dos fenômenos, tal como são percebidos pelas pessoas envolvidas, ou seja, busca capturar a perspectiva e a experiência dos participantes de forma rica e profunda. Portanto, ao adotar uma

abordagem fenomenológica dentro da estrutura de pesquisa de métodos mistos, o estudo se posiciona para capturar tanto aspectos quantificáveis quanto as complexidades subjetivas e experienciais inerentes ao objeto investigado.

Nesse caso, o fenômeno estudado é recente e, portanto, quanto mais informações houver, mais rica será a descrição do estudo (Creswell, 2010). O caráter exploratório desta pesquisa sugeriu uma abordagem qualitativa-quantitativa:

> A pesquisa do tipo quantitativo-qualitativo envolve tanto dados subjetivos quanto objetivos, mesmo que estes últimos sejam extrapolados a partir dos primeiros (interpretações que geraram quantificações). [...] A pesquisa do tipo quantitativo-qualitativo geralmente envolve mais de um tipo de lógica entre dedutiva, indutiva e abdutiva (De Sordi, 2017).

Um ponto importante no método adotado diz respeito às coletas dos dados quantitativos e qualitativos, que devem ser feitas simultaneamente, atribuindo-se pesos iguais a todos os dados. As combinações dos dados coletados devem fundir-se na etapa de análise para que a discussão apresente resultados consistentes e validados.

O levantamento bibliográfico foi realizado entre 2019 e 2020 usando a base de dados multidisciplinar *Web of Science*, com os seguintes termos (em inglês): "General Data Protection Regulation" *OR* "GDPR"; "Cycle of Data Life" *OR* "CVD" *AND* "customer sensitive data". Para os termos em português, a pesquisa bibliográfica usou o buscador de Google Acadêmico com os seguintes termos: "Lei Geral de Proteção de Dados" *OR* "LGPD" *AND* "conformidade" *OR* "adequação" *OR* "implementação" *AND* "empresas" *OR* "organizações" *OR* "negócios".

Para o levantamento dos dados, optou-se pela utilização do questionário, devido à vantagem dessa técnica relativa ao tempo. Os dados foram coletados no período de 12/jun. até 14/jul./2020, com um total de 156 respostas. A ferramenta utilizada para aplicação do questionário foi a *survey monkey*, útil na visualização da coleta de dados, e com recursos que permitem melhorar a confiabilidade das respostas coletadas.

Visando maximizar a coleta de informações em um curto período de tempo, atingindo um grande número de pessoas, optou-se por um questionário *online*, cuja facilidade de distribuição e de acesso tem o potencial de mitigar o risco da baixa taxa de resposta. Além disso, o questionário *online* permite tornar todos os campos de preenchimento obrigatório, evitando assim perguntas não respondidas.

3.1 População e amostra

O universo populacional é composto por MPEs da Aglomeração Urbana de Jundiaí (AUJ), que, devido ao seu relacionamento com clientes, fazem uso de dados pessoais. Uma amostra piloto, por conveniência, de 97 empresas mostrou que seis (6,25%) fazem coleta de dados pessoais, o que proporcionalmente corresponderia a cerca de 1.512 MPEs que fazem parte da população estudada.

O tamanho da amostra, tendo em conta o tamanho da população, é de 61 respondentes, com um nível de confiança de 90% e margem de erro de 5%, considerando o percentual de 6% de MPEs que realizam a coleta de dados pessoais dos seus clientes e funcionários.

3.2 Tabulação dos dados

Os dados tabulados estão estratificados em função das principais partes do processo requerido pela LGPD, tais como: informações gerais; tratamento de dados pessoais; término do tratamento de dados pessoais; direitos dos titulares; deveres do controlador e do operador; boas práticas; funcionários; incidentes de dados pessoais; e jurídico/contratos. A tabulação e análise dos dados foram feitas utilizando-se o software Excel.

4 ANÁLISE DOS RESULTADOS

Devido à pandemia do COVID-19, a coleta de dados foi exclusivamente *online*, para evitar contato físico conforme recomendação da Organização Mundial de Saúde (OMS) e do Ministério da Saúde. Foram obtidas 156 respostas no total. Para que fosse possível filtrar os participantes, foram inseridas duas perguntas classificadoras. Com esse filtro, a amostra foi reduzida para 67 respostas completas.

4.1 Questionário

O público-alvo desta pesquisa são MPEs que trabalham com dados pessoais. O respondente que indicasse ter mais do que 20 funcionários ou que alegasse não trabalhar com dados era automaticamente direcionado a uma página de agradecimento e desclassificação. A pergunta 1, refere-se ao porte da empresa; a pergunta 8 refere-se aos dados pessoais utilizados pela empresa. Com esses critérios, 59 respondentes estão fora do perfil desejado para esta pesquisa.

Para o filtro 2, foi utilizado um conceito base da pesquisa, o uso de dados pessoais. Perguntou-se ao respondente de quais públicos a empresa coleta dados pessoais. Dezenove empresas afirmaram não coletar nenhum dado pessoal, e 12 não sabem se coletam dados pessoais, indicando desconhecimento sobre o que são dados pessoais. Sendo este um conceito base para responder a pesquisa, os mencionados 12 respondentes foram desclassificados e direcionados para uma página de agradecimento.

Houve também o abandono do preenchimento do questionário por 9 respondentes. Isso pode indicar a dificuldade do participante em responder questões de cunho mais específico.

Entre os respondentes predominam indivíduos da geração Y, também conhecida como 'Millennials'. Segundo Oliveira e Saraiva (2019), pessoas dessa geração nasceram entre 1980 e 2000 e, portanto, se originaram na era da informação e dos avanços tecnológicos. Portanto, a geração Y é familiarizada com o uso das tecnologias, pois cresceu juntamente com a inserção das tecnologias de informação e comunicação no dia a dia. Do ponto de vista da mudança das práticas da privacidade, essa geração vivenciou parte dela tanto na modalidade analógica como na digital.

A maior parte da amostra é composta por respondentes do gênero masculino, havendo uma diferença de quase 20% em relação ao gênero feminino, sendo que a maior parte dos respondentes possui formação superior e pós-graduação. Os respondentes com formação média e técnica são minoria, representando, respectivamente, 9,1% e 6,5%. A maioria dos respondentes é dono ou sócio das MPE. Portanto, pode-se inferir que os principais processos dos negócios são conhecidos pelo respondente, o que aumenta a confiabilidade dos dados obtidos na pesquisa.

O principal tipo de cliente dos respondentes é o consumidor final, ou seja, pessoas físicas. Isso indica uma intenção por parte da empresa de procurar coletar dados pessoais, o que tende a diminuir no caso de *Business to Business* (B2B), em que os clientes são outras empresas.

Os resultados apresentados indicam que a coleta de dados pessoais restrita aos funcionários da própria empresa é de apenas 11,84%. O maior percentual (44,74%) é o de coleta de dados pessoais dos clientes, indicando a atenção da empresa com a gestão dos seus clientes. Grande parte dos respondentes (79,22%) atua nos ramos de comércio ou de serviços. Esse resultado está alinhado à crescente personalização do consumo, a qual induz os setores de comércio e de serviços a buscarem uma maior coleta de dados.

As MPEs pesquisadas, em sua maioria, não estão fortemente ligadas a associações. Esse resultado sugere uma possível dificuldade de acesso às informações normalmente fornecidas por tais organizações. Isso tende a diminuir o conhecimento de legislações como a LGPD e outras de interesse para esta pesquisa.

Portanto, com base nos dados apresentados na Seção 1, o perfil predominante do respondente é formado por homens de 25 a 44 anos, com ensino superior e pós-graduação, em sua maioria donos ou sócios do negócio, com atuação no ramo de serviços, trabalhando direto com o consumidor final, isso é, em negócios do tipo B2C.

Os resultados apresentados na Seção 2 do questionário revelam que as empresas pesquisadas utilizam uma gama de dados pessoais em seus negócios, tanto ligados aos seus colaboradores, como aos seus clientes. A ênfase em dados dos clientes deriva do fato de a maioria atuar em negócios do tipo B2C.

Poucos respondentes afirmaram trabalhar com dados sensíveis. Isso, no entanto, parece mais um desconhecimento da criticidade das informações sob seu poder, haja vista a existência de dados sensíveis em processos tais como, contratação de serviços contábeis ou de recrutamento e seleção, externos ao negócio. Em linha com isso, constatou-se que ações e políticas de proteção de dados ainda não são comuns a todos os respondentes.

Do total, 26 empresas (38,2% da amostra pesquisada) informaram que seus funcionários têm ciência da política de proteção de dados. A convergência de respostas nessas três questões sugere haver uma atenção efetiva com a segurança de informação nessas empresas. Já o número de empresas que alega entender a necessidade de um relatório de impacto à proteção de dados aumenta para trinta e duas (47,1% do total). Trata-se de um requisito importante tratado na LGPD, o qual é desconhecido por pelo menos 13 das empresas respondentes (19,1% do total).

Por outro lado, o número de empresas que fornece informações para os seus titulares acerca das finalidades do tratamento de dados diminui em quase 5% (de 38,2% para 33,8%). Essa queda sugere que, apesar de o contrato estar de acordo com a LGPD, nem todas as etapas dos tratamentos de dados estão em conformidade com a legislação.

Outros 20 respondentes afirmaram ter identificado as bases legais para tratamento dos dados. Portanto, a maioria dos respondentes (quase 70%) não possui justificativa, conforme indicada na LGPD, para tratar os dados pessoais: 36 afirmaram não identificar as bases legais para tratamento dos dados, e 12 responderam não saber do que se trata.

Apenas nove empresas da amostra possuem um DPO. Somado ao fato do descumprimento de um requisito importante da LGPD, esse resultado revela uma fragilidade na gestão do sistema de informações da empresa, elemento de destaque em empresas inseridas em mercados competitivos e dinâmicos, que caracterizam o momento atual. Assim, esta pesquisa revela lacunas não só em termos de requisitos legais, como também em fundamentos da moderna gestão empresarial.

Os dados apresentados referem-se ao monitoramento que a empresa faz de sua própria conformidade com as políticas de proteção de dados, bem como se é feita uma análise regular da eficácia dos controles de manipulação e segurança de dados. Apenas 29,4% das empresas responderam afirmativamente (20 respondentes). Trata-se de um número significativamente menor dos que os 32 participantes que sinalizaram positivamente, indicando que as políticas de segurança dos respondentes não estão atualizadas conforme previsto na LGPD.

A maioria das empresas respondentes não gerencia o consentimento, requisito solicitado pela lei para atender um direito fundamental do titular dos dados. Os dados apresentados mostram que apenas 35,3% das empresas responderam afirmativamente a essa questão. Os resultados apresentados em comparação revelam uma pequena diferença entre os respondentes que gerenciam consentimento e os que possuem processo de descarte de dados. O descarte é parte do término do tratamento dos dados previstos na LGPD.

Nesta seção do questionário, os dados analisados apontaram a existência de preocupações respeito à proteção de dados pessoais, mas com pouca/nenhuma ação ou processo formalizado para tratar essa questão. Conforme já mencionado, o perfil predominante dos respondentes é o de pessoas com acesso e familiaridade à tecnologia, mas com conhecimentos básicos de segurança da informação. Ou seja, existe a preocupação com a proteção de dados, mas pouca formalização na proteção dos dados pessoais de seus colaboradores e clientes. A comparação dos requisitos da LGPD com os dados analisados revela a necessidade de se traduzir os requisitos da lei em processos e ações no dia a dia dos negócios.

4.2 Hipótese Ha

Uma não conformidade é uma prescrição da LGPD não atendida pelo usuário, sendo que tanto as conformidades como as não conformidades foram abordadas nas questões 17, 20, 21, 23, 24, 25, 26, 27, 28, 29, 30, 31 e 32. Essas questões estão exibidas na Tabela 1.

Na Tabela 1 são apresentadas as estatísticas descritivas das variáveis que serviram para testar a hipótese Ha para as 13 questões relacionadas na Tabela 2, a qual está assim formulada:

Ha*: Ao nível de significância de 0,05, a proporção de não conformidades na mediana de todos os respondentes é significativamente maior do que as conformidades.*

Em termos percentuais, a mediana das conformidades representou 57,35% e as não conformidades, 42,65%. Para testar-se a proporção de não conformidades de todos os respondentes é significativamente maior do que as conformidades utilizou-se o teste

Tabela 1 Conformidade e não conformidades dos respondentes segundo a LGPD

Questões	Conf	NãoC	Conf%	NãoC%
17. A empresa possui políticas de segurança da informação documentadas (por exemplo: manuais, memorandos, termos)?	37	31	54,41	45,59
20. Quais mecanismos de segurança da informação a empresa utiliza em seu ambiente?	68	0	100,00	0,00
21. Sua empresa realiza backup dos dados cópia de segurança)? Se sim, indique o modo como os backups são armazenados.	59	9	86,76	13,24
23. Os contratos da sua empresa estão adequados com a LGPD?	54	14	79,41	20,59
24. Sua empresa documentou/mapeou quais dados pessoais possuem (armazenam), de onde vieram (como foram coletados), com quem você os compartilha e o que fazem com eles?	35	33	51,47	48,53
25. Os funcionários da sua empresa estão cientes da política de proteção de dados adotada?	68	0	100,00	0,00
26. Sua empresa entende quando um relatório de impacto à proteção de dados é necessário?	45	23	66,18	33,82
27. Sua empresa fornece informações sobre as finalidades do tratamento de cada dado pessoal coletado para os seus titulares?	40	28	58,82	41,18
28. Sua empresa identificou suas bases legais para processamento e tratamento de dados pessoais e as documentou?	32	36	47,06	52,94
29. Sua empresa já nomeou o encarregado de dados ou data protection officer (DPO)?	21	47	30,88	69,12
30. Sua empresa monitora sua própria conformidade com as políticas de proteção de dados e analisa regularmente a eficácia dos controles de manipulação e segurança de dados?	35	33	51,47	48,53
31. Sua empresa possui sistemas para registrar e gerenciar os consentimentos dados, assim como para possibilitar a revogação de consentimento?	37	31	54,41	45,59
32. Sua empresa possui um processo para descartar com segurança dados pessoais que não são mais necessários ou aqueles os quais o usuário solicitou a exclusão?	39	29	57,35	42,65
MEDIANA	**39**	**29**	**57,35**	**42,65**

Legenda: Conf = resposta em conformidade com a LGPD; NãoC = resposta não conforme a LGPD.
% indicam valores percentuais

Tabela 2 Estatísticas descritivas das variáveis da hipótese Ha

Descriptive Statistics: Conf; NãoC; Conf%; NãoC%
Total

Variable	Count	Minimum	Q1	Median	Q3	Maximum	Range
Conf	13	21.00	35.00	39.00	56.50	68.00	47.00
NãoC	13	0.00	11.50	29.00	33.00	47.00	47.00
Conf%	13	30.88	51.47	57.35	83.09	100.00	69.12
NãoC%	13	0.00	16.91	42.65	48.53	69.12	69.12

Tabela 3 Conformidade e não conformidade - hipótese Hb

Questões	Conf	NãoC	Conf%	NãoC%
31. Sua empresa possui sistemas para registrar e gerenciar os consentimentos dados, assim como para possibilitar a revogação de consentimento?	37	31	54,41	45,59
32. Sua empresa possui um processo para descartar com segurança dados pessoais que não são mais necessários ou aqueles os quais o usuário solicitou a exclusão?	39	29	57,35	42,65
17. A empresa possui políticas de segurança da informação documentadas (por exemplo: manuais, memorandos, termos)?	37	31	54,41	45,59
20. Quais mecanismos de segurança da informação a empresa utiliza em seu ambiente?	68	0	100,00	0,00
21. Sua empresa realiza backup dos dados cópia de segurança)? Se sim, indique o modo como os backups são armazenados.	59	9	86,76	13,24
23. Os contratos da sua empresa estão adequados com a LGPD?	54	14	79,41	20,59
24. Sua empresa documentou/mapeou quais dados pessoais possuem (armazenam), de onde vieram (como foram coletados), com quem você os compartilha e o que fazem com eles?	35	33	51,47	48,53
25. Os funcionários da sua empresa estão cientes da política de proteção de dados adotada?	68	0	100,00	0,00
26. Sua empresa entende quando um relatório de impacto à proteção de dados é necessário?	45	23	66,18	33,82
27. Sua empresa fornece informações sobre as finalidades do tratamento de cada dado pessoal coletado para os seus titulares?	40	28	58,82	41,18
28. Sua empresa identificou suas bases legais para processamento e tratamento de dados pessoais e as documentou?	68	0	100,00	0,00
29. Sua empresa já nomeou o encarregado de dados ou data protection officer (DPO)?	21	47	30,88	69,12
30. Sua empresa monitora sua própria conformidade com as políticas de proteção de dados e analisa regularmente a eficácia dos controles de manipulação e segurança de dados?	35	33	51,47	48,53
Mediana	**40,00**	**28,00**	**58,82**	**41,18**

Legenda: Conf = resposta em conformidade com a LGPD; NãoC = resposta não conforme a LGPD.
% indicam valores percentuais

Tabela 4 Conformidade e não conformidade - hipótese Hc

Questões	Conf	NãoC	Conf%	NãoC%
17. A empresa possui políticas de segurança da informação documentadas (por exemplo: manuais, memorandos, termos)?	37	31	54,4	45,6
18. É permitido que os colaboradores utilizem dispositivos pessoais para realizar suas atividades de trabalho ou que levem dispositivos da empresa para locais externos?	45	23	66,2	33,8
20. Quais mecanismos de segurança da informação a empresa utiliza em seu ambiente?	68	0	100,0	0,0
21. Sua empresa realiza backup dos dados cópia de segurança)? Se sim, indique o modo como os backups são armazenados.	59	9	86,8	13,2
25. Os funcionários da sua empresa estão cientes da política de proteção de dados adotada?	68	0	100,0	0,0
28. Sua empresa identificou suas bases legais para processamento e tratamento de dados pessoais e as documentou?	32	36	47,1	52,9
Mediana	**52**	**16**	**76,47**	**23,529**

Legenda: Conf = resposta em conformidade com a LGPD; NãoC = resposta não conforme a LGPD.
% indicam valores percentuais

não paramétrico da mediana. O resultado do teste mostra que a diferença é significativa ao nível de significância de 0,01.

Com base nesses resultados, rejeita-se a hipótese Ha, dado que ao nível de significância de 0,05, a proporção de não conformidades à LGPD na mediana de todos os respondentes não é significativamente maior do que as conformidades (teste da mediana, p-value = 0,0017).

Para testar se a proporção de não conformidades de todos os respondentes considerando o fator tratamento de dados é significativamente maior do que as conformidades utilizou-se o teste não paramétrico binomial de duas proporções. O resultado do teste mostra que não é encontrada significância entre as respostas obtidas ao nível de significância de 0,04. Assim, com um p-valor (unilateral) de 0,04 não foi encontrada significância na análise comparativa.

4.3 Hipótese Hb

A hipótese Hb está assim formulada:

Hb: *Ao nível de significância de 0,05, a proporção de não conformidades, considerando-se o fator término do tratamento de dados pessoais, é significativamente maior do que as conformidades.*

As questões que serviram para testar a hipótese Hb em termos percentuais, a mediana das conformidades representou 56% e as não conformidades, 43%, conforme apresentado na Tabela 3.

Para testar se a proporção de não conformidades considerando o fator término de tratamento de dados pessoais é significativamente maior do que as conformidades, utilizou-se o teste não paramétrico de proporção binomial. O resultado do teste mostra que a diferença é significativa ao nível de 0,3, confirmando a hipótese Hb.

4.4 Hipótese Hc

A hipótese Hc está assim formulada:

Hc: *Ao nível de significância de 0,05, a proporção de não conformidades não é significativamente diferente em função do fator proteção de dados.*

A Tabela 4 mostra as questões que serviram para testar a hipótese Hc. Em termos percentuais a mediana das conformidades representou 87%; e as não conformidades de 34%.

4.5 Testes de hipóteses considerados

Das três hipóteses testadas, somente a hipótese Hb foi confirmada, ou seja, no nível de significância considerado, a proporção de não conformidades, considerando-se o fator Término do tratamento de dados pessoais, é significativamente maior do que as conformidades. Esse resultado indica a necessidade de atenção com as questões relacionadas, uma vez que os dados pessoais, na maioria das vezes, são bastante sensíveis sendo, inclusive, objetos de proteção legal.

As hipóteses Ha e Hc foram rejeitadas, indicando que as empresas pesquisadas já dedicam um nível de atenção significativo à proteção dos seus dados. Portanto, já há um nível de dedicação e alocação de recursos às questões de proteção de dados, sendo necessário agora, portanto, suprir as lacunas encontradas.

5 CONCLUSÃO

No Brasil, a proteção de dados tem sido debatida atualmente nas esferas pública e privada. Nesse sentido, com a sanção da LGPD em 2020 o Brasil, ao avançar na discussão, alcança um marco importante ao se juntar ao grupo de mais de 120 países que possuem legislação voltada para a proteção de dados pessoais (Ramos & Gomes, 2019) e coloca empresas brasileiras em um patamar competitivo frente às exigências internacionais.

Um exemplo particularmente ilustrativo do impacto decisivo das leis de proteção de dados pode ser encontrado no caso *Schrems I*: trata-se do caso levado ao Tribunal de Justiça Europeu, afirmando que as informações reveladas ao público por Edward Snowden, mostram que empresas norte-americanas não podiam garantir a proteção adequada dos dados pessoais. Embora a LGPD possa não estar diretamente relacionada ao caso *Schrems I*, ela exemplifica o movimento global em direção a medidas rigorosas de proteção de dados (Parlamento Europeu, 2020). Essas

situações destacam a necessidade de as empresas se adaptarem às regulamentações de proteção de dados, independentemente de sua localização ou porte, à medida que a proteção dos dados pessoais se torna uma questão de importância fundamental no mundo interconectado de hoje.

Diante desse cenário, este estudo propôs como objetivo geral analisar o grau de conformidade à LGPD das MPEs localizadas no AUJ, no que tange ao uso de dados pessoais dos clientes. Para atingir esse objetivo, foram definidos três objetivos específicos: explorar os conceitos fundamentais de gestão de dados e tecnologia da informação; investigar a relação entre as práticas das MPEs e os princípios estabelecidos pela LGPD; identificar e avaliar não conformidades relacionadas ao tratamento e término de dados pessoais pelas empresas.

Esses objetivos se justificam, pois, a introdução da LGPD transformou a maneira como as MPEs devem tratar seus dados. Apesar dos desafios enfrentados pelas MPEs devido a recursos limitados, investir em segurança da informação e orientação por parte de seu DPO é crucial para atingir a conformidade com os princípios da LGPD, aumentando a confiança dos clientes.

A maioria das MPEs que afirmou tratar dados pessoais foi representada por seus gestores. Cerca de 60% desses gestores são homens, com idades entre 25 e 44 anos, que pertencem à chamada geração Y, isto é, possuem familiaridade com as tecnologias de informação e comunicação, com grau de instrução de nível superior (40%) e pós-graduação (46%). Isso sugere a importância da formação escolar e da prática no uso das tecnologias da informação para compreender a importância da proteção dos dados.

Foi constatado também que 75% dos respondentes afirmam não possuir certificações ISO ou similares em suas empresas; ou seja, há uma baixa adesão de certificações. Trata-se de um aspecto negativo, visto que a revisão bibliográfica mostrou que há certificações ABNT e ISO que tratam da proteção de dados, as quais podem ser úteis na construção de uma governança dos dados.

As MPEs da amostra possuem baixa associação às entidades representativas. Isso parece sugerir que essas MPEs não possuem uma fonte de informação segura para orientá-las sobre a LGPD, já que tais entidades associativas usualmente são fontes disseminadoras de ações em respeito às normas e leis aplicáveis.

Os resultados apresentados relativos à Seção 2 do questionário revelaram também que as empresas pesquisadas utilizam dados pessoais de seus colaboradores e clientes, já que a maioria atua em negócios do tipo B2C. Poucos respondentes afirmaram trabalhar com dados sensíveis, o que indica desconhecimento desse conceito, haja visto o compartilhamento de dados sensíveis em processos de terceirização de serviços. Constatou-se, também, que ações e políticas de proteção de dados ainda não são comuns à maioria dos respondentes.

Apesar de os dados indicarem a adoção de algum tipo de solução tecnológica a respeito da segurança dos dados, identificou-se o desconhecimento das exigências da LGPD e, por consequência, o não cumprimento das mesmas. Por exemplo, 41% dos respondentes não sabem dizer se os contratos da empresa estão adequados à lei e, também, 41% das empresas estudadas não informam a finalidade dos dados coletados. Como a LGPD possibilita que os clientes se tornem uma peça fundamental na cobrança de conformidade das empresas, a MPE é passível de ser fiscalizada não apenas por órgãos governamentais, mas por todos os cidadãos.

A pandemia do COVID-19 provocou mudanças no comportamento social, com reflexos na política e na economia. Um dos seus efeitos foi a migração de produtos e serviços para plataformas digitais de negócios a fim de garantir a sobrevivência das MPEs. Com o consequente aumento do comércio digital, ficou ainda mais evidente o gap das competências tecnológicas e humanas das empresas em lidar com a complexidade do mundo digital e sua regulação.

Uma das limitações desta pesquisa foi ter sido realizada anteriormente ao início da vigência da LGPD. Portanto, há diversos pontos que não foram abordados, visto que a aprovação da lei previa a criação da Agência Nacional de Proteção de dados, mas que não tinha sido discutida, além da definição de como seriam aplicadas as multas, entre outros aspectos que podem ser explorados com maior profundidade. Outra limitação encontrada foi a postergação da data de início do vigor da lei, que não diminuiu a discussão acerca da proteção de dados. Pelo contrário, a exposição indevida de dados sensíveis da saúde dos

cidadãos contaminados durante a pandemia do COVID-18 mostrou que a privacidade e a proteção dos dados de cidadãos, empresas e governos são assuntos de interesse público, apesar da superficialidade no debate público.

Recomenda-se, portanto, que em estudos futuros sejam feitas pesquisas sobre os impactos do aumento do uso das tecnologias digitais pelas MPEs. Em especial, que se procure entender como esse segmento empresarial está lidando com o aumento de dados sensíveis, visando sua proteção e gestão adequada.

REFERÊNCIAS

Alves, G. (2020). Ciclo de Vida dos Dados e LGPD. *Xpositum: Consultoria empresarial*. https://www.xpositum.com.br/ciclo-de-vida-dos-dados-e-lgpd.

Ben-Zvi, T., & Luftman, J. (2022). Post-Pandemic IT: Digital Transformation and Sustainability. *Sustainability*, *14*(22), 15275. https://doi.org/10.3390/su142215275

Bezerra, M. R. B. (2019). Autoridade nacional de proteção de dados pessoais: a importância do modelo institucional independente para a efetividade da lei. *Caderno Virtual, 2*(44), 1-95.

Bioni, B. R. (2019). *Proteção de dados pessoais*: a função e os limites do consentimento. Rio de Janeiro: Editora Forense.

Branco, S. (2020). As hipóteses de aplicação da LGPD e as definições legais. *In*: Mulhollan, C. (org). *A LGPD é o novo marco normativo no Brasil*. São Paulo: Editora Arquipélago.

Brasil (2019). *Decreto nº 9.936, de 24 de julho de 2019*. Regulamenta a Lei nº 12.414, de 9 de junho de 2011, que disciplina a formação e a consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Brasília. http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D9936.htm

Brasil (2020). *Lei Geral de Proteção de Dados*: Guia de boas práticas para implementação na administração pública federal. https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-lgpd.pdf

Brasil (2018). Lei nº. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília. http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm

Cantner, U., Cunningham, J. A., Lehmann, E. E., & Menter, M. (2021). Entrepreneurial ecosystems: a dynamic lifecycle model. *Small Bus Econ,* 57, 407-423. https://doi.org/10.1007/s11187-020-00316-0

Cavalcanti, N. P., & Santos, L. M. S. B. (2018). A lei geral de proteção de dados do Brasil na era do big data. In *Tecnologia Jurídica e Direito Digital - II Congresso Internacional de Direito, Governo e Tecnologia, 2*. Belo Horizonte: Fórum, 1, 351-366.

Chiarini, A., & Compagnucci, L. (2022). Blockchain, Data Protection and P2P Energy Trading: A Review on Legal and Economic Challenges. *Sustainability, 14*(23), 16305. https://doi.org/10.3390/su142316305

Choo, C. W. (2003). *A organização do conhecimento: como as organizações usam a informação para criar significado, construir conhecimento e tomar decisões.* São Paulo: ed. SENAC São Paulo.

Costa, I.M., Alves Junior, P. N., Queiroz, G. A., Yushimito, W., & Pereira, J. (2023). Do We Consider Sustainability When We Measure Small and Medium Enterprises' (SMEs') Performance Passing through Digital Transformation? *Sustainability*, *15*(6), 4917. https://doi.org/10.3390/su15064917

Creswell, J. W. (2010). *Projeto de pesquisa: métodos qualitativo, quantitativo e misto.* (3. ed.) Porto Alegre: Artmed.

Da Cruz, U. L., Passaroto, M., Junior, N. T. (2021). O impacto da Lei Geral de Proteção de Dados Pessoais (LGPD) nos escritórios de contabilidade. *ConTexto - Contabilidade em Texto, 21*(49), 30-39. https://seer.ufrgs.br/index.pHc/ConTexto/article/view/112561

DAMA-Data Administration Management Association. (2010). *The DAMA guide to the data management body of knowledge: DAMA-DMBOK guide*. Bradley Beach, NJ.: Technics Publications, LLC.

De Sordi, J.O. (2017). *Desenvolvimento de projeto de pesquisa.* São Paulo: Saraiva.

Derbli, L.S. (2019). O transplante jurídico do regulamento geral de proteção de dados da União Europeia ("GDPR") para o direito brasileiro. *E-legis*, 30, 181-193. https://doi.org/10.51206/e-legis.v12i30.500

Doneda, D. (2011). A proteção dos dados pessoais como um direito fundamental. *Espaço Jurídico, 12*(2), 91-108.

Gil, A.C. (2017). *Como elaborar projetos de pesquisa*. (6 ed.). São Paulo: Atlas.

ITRC. (2023). Identity Theft Resource Center's 2022 Annual Data Breach Report Reveals Near-Record Number of Compromises. https://www.idtheftcenter.org/post/2022-annual-data-breach-report-reveals--near-record-number-compromises/

Johansen, J. (2023). Expert opinions on making GDPR usable. *Human Factors in Privacy Research* (p. 137-152). Springer Book. https://doi.org/10.48550/arXiv.2308.08287

Kádárová, J., Lachvajderová, L., & Sukopová, D. (2023). Impact of Digitalization on SME Performance of the EU27: Panel Data Analysis. *Sustainability*, 15, 9973. https://doi.org/10.3390/su15139973

Kumara, I., Kayes, A., Mundt, P., & Schneider, R. (2023). Data Governance. Data Science for Entrepreneurship, 37-62. https://doi.org/10.1007/978-3-031-19554-9_3

Lima, J. F.; Silva, G. (2019). Desafios para inovar na micro e pequena empresa. *Revista da Micro e Pequena Empresa,13*(2), 85-97. https://doi.org/10.21714/19-82-25372019v13n2p8597

Machado, H. P. V. (2018). Configuração de estudos sobre gestão do conhecimento em pequenas empresas no brasil. *Perspectivas em Gestão & Conhecimento, 8*(3), 209-227. https://doi.org/10.21714/2236-417X2018v8n3p209

Marconi, M. A., & Lakatos, E. M. (2017). *Fundamentos de metodologia científica.* (8. ed.) São Paulo: Atlas.

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data Privacy: Effects on Customer and Firm Performance. *Journal of Marketing, (81)*, 1. 36-58. http://dx.doi.org/10.1509/jm.15.0497

Molina, L. G., & Santos, J.C. (2020). Gestão da informação e a 4a Revolução Industrial. *AtoZ: novas práticas em informação e conhecimento, 8* (2), p. 39-48. http://dx.doi.org/10.5380/atoz.v8i2.65784

Oliveira, A.P., Zanetti, D., Lima, F. S. & Sampaio, T. O. (2019). A LGPD brasileira na prática empresarial. *Revista Jurídica da Escola Superior de Advocacia da OAB-PR, ano 4*(1), 172-200.

Oliveira, T. P. P., & Saraiva, P.M. (2019) A influência do marketing digital no perfil de consumo da geração y. Id on Line Revista Multidisciplinar e de Psicologia, *13* (44), 589-600. https://doi.org/10.22533/at.ed.16719060720

Parlamento Europeu. (2020). *The CJEU judgment in the Schrems II case*. https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf

Pelloso Piurcosky, F., Aparecido Costa, M., Frogeri, R. F., & Leal Calegario, C. L. (2019). A LGPD pessoais em empresas brasileiras: uma análise de múltiplos casos. *Suma de negócios, 10*(23), 89-99. https://doi.org/10.14349/sumneg/2019.v10.n23.a2

Rahul, K., & Banyal, R. K. (2020). Data life cycle management in big data analytics. *Procedia Computer Science, 173*, 364-371. https://doi.org/10.1016/j.procs.2020.06.042

Ramos, L. C. P., & Gomes, A.V.M. (2019). Lei geral de proteção de dados pessoais e seus reflexos nas relações de trabalho. *Scientia Iuris*, *23*(2), 127-146. https://doi.org/10.5433/2178-8189.2019v23n2p127

Rodrigues, M., Franco, M., Silva, R., & Oliveira, C. (2021). Success Factors of SMEs: Empirical Study Guided by Dynamic Capabilities and Resources-Based View. Sustainability, *13*, 12301. https://doi.org/10.3390/su132112301

Russ, M. (2021). Knowledge Management for Sustainable Development in the Era of Continuously Accelerating Technological Revolutions: A Framework and Models. *Sustainability*, 13, 3353. https://doi.org/10.3390/su13063353

Sant'Ana, R. C. G. (2016). Ciclo de vida dos dados: uma perspectiva a partir da ciência da informação. *Informação & Informação*, *21*(2), 116-142. https://doi.org/10.5433/1981-8920.2016v21n2p116

Serumaga-Zake, J. M., & Van Der Poll, J. A. (2021). Addressing the Impact of Fourth Industrial Revolution on South African Manufacturing Small and Medium Enterprises (SMEs). *Sustainability*, 13, 11703. https://doi.org/10.3390/su132111703

Silveira, M. A., & Becaro, T. C. (org). (2014). *Competitividade com qualidade de vida: o capital humano como fator de produção*. Campinas: ed. CEDET.

Solomon, G. T., & Linton, J. D. (2016). Standing at the crossroad of knowledge: Technology, innovation, entrepreneurship and the small business management - Policy perspectives. *Technovation,* 57–58, 1-3. https://doi.org/10.1016/j.technovation.2016.08.003

União Europeia. (2021). Proteção de dados na UE. https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_pt

Vieira, S. (2011). Estatística básica. Rio de Janeiro: ed. Cengage.

Vrontis, D., Chaudhuri, R., & Chatterjee, S. (2022). Adoption of Digital Technologies by SMEs for Sustainability and Value Creation: Moderating Role of Entrepreneurial Orientation. *Sustainability*, *14*(13). https://doi.org/10.3390/su14137949

Wang, Z., Lin, S., Chen, Y., Lyulyov, O., & Pimonenko, T. (2023). Digitalization Effect on Business Performance: Role of Business Model Innovation. *Sustainability*, *15*(11). https://doi.org/10.3390/su1511902

Zeng, S. & Yang, H. (2023).A Bibliometric and Visualization Analysis of Knowledge Mapping in Digital Economy Research, 1992–2022. *Sustainability* , 15, 6565. https://doi.org/10.3390/su15086565

Ziegler, S., Evequoz, E., & Huamani, A. M. P. (2019). The impact of the European General Data Protection Regulation (GDPR) on future data business models: Toward a new paradigm and business opportunities. *In*: Aagaard, A. (ed.). B2B *Digital business models*. Palgrave Macmillan, Cham, Gewerbestrasse, Switzerland. https://doi.org/10.1007/978-3-030-13005-3_9