TALITA DA SILVA CARLOS LANGEN

LEI GERAL DE PROTEÇÃO DE DADOS: DIAGNÓSTICO DO GRAU DE CONFORMIDADE DE MICRO E PEQUENAS EMPRESAS

CAMPO LIMPO PAULISTA

2020

CENTRO UNIVERSITÁRIO CAMPO LIMPO PAULISTA

MESTRADO PROFISSIONAL EM ADMINISTRAÇÃO DAS MICRO E PEQUENAS EMPRESAS

TALITA DA SILVA CARLOS LANGEN

Lei Geral de Proteção de Dados: Diagnóstico do grau de conformidade de micro e pequenas empresas

Dissertação de mestrado apresentada ao Programa de Mestrado em Administração das Micro e Pequenas Empresas do Centro Universitário Campo Limpo Paulista para obtenção do título de Mestre em Administração.

Orientador: Prof. Dr. Marco Antonio Silveira.

Linha de Pesquisa: Dinâmica das micro e pequenas empresas (MPEs).

CAMPO LIMPO PAULISTA
2020

Ficha catalográfica

LANGEN, Talita da Silva Carlos.
LEI GERAL DE PROTEÇÃO DE DADOS: Diagnóstico do grau de conformidade em Micro e pequenas empresas / Talita da Silva Carlos Langen; Campo Limpo Paulista - SP: UNIFACCAMP, 2020 (Dissertação de mestrado)

Orientador: Prof. Dr. Marco Antonio Silveira

1.Lei geral de proteção de dados (LGPD) 2. Proteção de dados 3. *Compliance* 4. Micro e pequenas empresas. 5. Grau de conformidade.

CDD: 658.406

CAMPO LIMPO PAULISTA

TALITA DA SILVA CARLOS LANGEN

Lei Geral de Proteção de Dados:
Diagnóstico do grau de conformidade em micro e pequenas empresas

Dissertação de Mestrado aprovada em 03/07/2020

BANCA EXAMINADORA

_____

Prof. Dr. Marco Antonio Silveira
Unifaccamp

_____

Profa. Dra. Cida Sanches
Unifaccamp

_____

Prof. Dr. Guilherme Ataíde Dias
Universidade Federal da Paraíba (UFPB)

DEDICATÓRIA

Dedico à minha família, os Carlos, que foram minha base para chegar aqui. Dedico também a todas as pessoas que me incentivaram a dar pequenos passos para concluir essa jornada incrível.

AGRADECIMENTOS

Agradeço a todas as pessoas que cruzaram a minha jornada. Agradeço aos professores deste programa, em especial ao Dr. Marco Antonio Silveira, meu orientador, à Professora Cida, que me instigou a procurar uma versão melhor de mim, e ao Professor Meireles, por não ter desistido de me ensinar estatística com tanto amor.

Agradeço ao Professor e amigo querido Samuel Ferreira Junior, sem você seria impossível terminar esta etapa. Ao Professor Aleixo, pela ajuda. Ao amigo José Carlos por renovar minha fé, aos amigos de sala que compartilharam momentos de café e conhecimentos.

Agradeço ao Senac, representado na pessoa do Mauro de Nardi, por ter me apoiado com a bolsa de estudos e por acreditar no meu desenvolvimento ao longo desses anos. Às minhas companheiras de trabalho Tania e Tereza, pelo companheirismo.

Agradeço à minha esposa Eugenia Langen, por apoiar meus projetos e segurar minha mão. Josie Lucas pela amizade e amor. E agradeço ao meu parceiro e irmão Hugo Carlos por todo incentivo e amor.

Agradeço a todos as pessoas que me ajudaram direta ou indiretamente.

EPÍGRAFE

Vamos pegar nossos livros e canetas. Eles são nossas armas mais poderosas. Uma criança, um professor, uma caneta e um livro podem mudar o mundo. A educação é a única solução.

Malala Yousafzai

RESUMO ESTRUTURADO

Contextualização: A evolução das tecnologias de informação e comunicação propiciaram grandes transformações na sociedade, incluindo a forma como se produz e consome dados e informações. Nesse cenário, os dados pessoais transformam-se em elementos substanciais, cujas possibilidades de monetização têm sido exploradas por empresas de todos os portes e de diferentes setores. Visando compreender o impacto dos dados pessoais em micro e pequenas empresas (MPEs), esta pesquisa se propôs a investigar o grau de conformidade destas em relação às exigências dispostas na Lei Geral de Proteção de Dados/LGPD.

Objetivos: Elaborar uma revisão teórica sobre gestão de dados em organizações, sua proteção e leis relacionadas; verificar se as MPEs estão se preparando para cumprir os requisitos da LGPD, especialmente no que se refere à proteção de dados; verificar o nível de não conformidades relacionadas aos fatores “tratamento de dados pessoas” e “término de tratamento de dados pessoais”; e sugerir caminhos possíveis conforme o grau de conformidade identificado nas MPES.

Abordagem metodológica: A abordagem desta pesquisa é fenomenológica, de caráter qualitativa e quantitativa. Para coleta de dados, foi utilizado um questionário diagnóstico para investigar MPEs do Aglomerado Urbano de Jundiaí - São Paulo. Para análise dos dados qualitativos do questionário, foram realizadas inferências a fim de relacionar a literatura com os dados apresentados. Para análise quantitativa dos dados foram aplicados testes estatísticos de mediana para as hipóteses levantadas.

Resultados alcançados: Com base nos resultados encontrados é possível afirmar que as MPEs da amostra estudada estão preocupadas com a proteção dos dados pessoais. No entanto, o preparo delas ainda é incipiente, visto que a compreensão dos princípios e hipóteses previstos na LGPD é ampla, exigindo um conjunto de conhecimentos específicos para mapear o fluxo dos dados dentro do negócio.

Implicações práticas: Do ponto de vista prático, sugere-se a adoção do Ciclo de Vida dos Dados como solução para mapear os processos do negócio, relacionando às

fases de tratamento dos dados dispostas na LGPD, uma vez que a lei não obriga o uso de uma tecnologia específica, apenas a transparência dos processos adotados. Outra recomendação inclui a adoção das normas ABNT e ISO de proteção de dados, junto ao Ciclo de Vida dos Dados, para a construção da governança de dados em *compliance* com a lei.

Contribuições teóricas: 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 o aumento do comércio digital.

Palavras-chave: lei geral de proteção de dados; LGPD; grau de conformidade; proteção de dados; micro e pequenas empresas.

General data protection law: Micro and small businesses compliance diagnostic

ABSTRACT

Contextualization: The evolution of information and communication technologies has led to major transformations in society, including how data and information are produced and consumed. In this scenario, personal data is transformed into substantial elements, whose monetization possibilities have been explored by companies of all sizes and from different sectors. To understand the impact of personal data on micro and small businesses (MSBs), this research investigated the degree of compliance of MSBs with the requirements outlined in the General Data Protection Act.

Objectives: To develop a theoretical review on data management in organizations, their protection, and related laws; to verify whether MSBs are preparing to meet the requirements of the General Data Protection Act, especially concerning data protection; to verify the level of non-compliance related to the factors "processing of personal data" and "termination of processing of personal data"; and to suggest possible ways in which MSBs can improve their degree of compliance with the LGPD.

Methodological approach: The approach of this research is phenomenological, qualitative, and quantitative. For data collection, the author utilized a diagnostic questionnaire to investigate micro and small businesses in the urban agglomeration of Jundiaí - São Paulo. To analyze the qualitative data of the questionnaire, inferences were made to relate the literature with the data presented. For quantitative analysis of the data, statistical tests of median were applied for the hypotheses raised.

Results achieved: Based on the results found, it is possible to state that the sample MSBs are concerned with the protection of personal data. However, their preparation is still incipient, since the understanding of the principles and hypotheses foreseen in the LGPD is broad, requiring a set of specific knowledge to map the data flow within the business.

Practical implications: From a practical point of view, it is suggested to adopt the Data Life Cycle as a solution to map the business processes, relating to the data treatment phases provided in the LGPD, since the law does not require the use of a specific technology, only the transparency of the adopted processes. Another recommendation includes the adoption of ABNT and ISO data protection standards, along with the Data Life Cycle, to build data governance in compliance with the law.

Theoretical contributions: 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.

Keywords: general data protection law; LGPD; degree of compliance; data protection; micro and small businesses.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABES	Associação Brasileira de Empresas de *Software*
ABNT	Associação Brasileira de Normas Técnicas
ANPD	Agência Nacional de Proteção de Dados
AUJ	Aglomerado Urbano de Jundiaí
CVD	Ciclo de Vida dos Dados
DPO	*Data Protection Officer*
GC	Gestão do Conhecimento
GDPR	*General Data Protection Regulamentation*
INPI	Instituto Nacional da Propriedade Industrial
ISO	*International Organization for Standardization* ou Organização Internacional de Normalização
LAI	Lei de Acesso à Informação
LGPD	Lei Geral de Proteção de Dados
MPEs	Micro e Pequenas Empresas
PLC	Projeto de Lei da Câmara
SEBRAE	Serviço Brasileiro de Apoio às Micro e Pequenas Empresas
YAMM	*Yet Another Mail Merge*

SUMÁRIO

1. INTRODUÇÃO

A evolução das tecnologias de informação e comunicação propiciaram grandes transformações na sociedade, incluindo a forma como produzimos e consumimos dados e informações. Com a chegada da Quarta Revolução Industrial, a economia deslocou seu foco da produção para o consumo. Uma economia focada no consumo exige que os negócios se adaptem e se reinventem para garantir níveis competitivos e globais.

Boff, Fortes e Freitas. (2018, p. 13) 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.

Nesse cenário, os dados pessoais dos cidadãos transformam-se em elementos substanciais 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).

> A 4ª Revolução, marcada pela convergência de tecnologias digitais, físicas e biológicas, afetará o mercado, pois os homens terão que se adaptar às transformações, que certamente serão complexas, pois estarão ligadas diretamente à velocidade, ao alcance e aos impactos, portanto, as Organizações devem estar aptas para evoluir e inovar (MOLINA; SANTOS, 2020, p.40).

O volume e a velocidade da geração de dados são cada vez maiores, ampliando os desafios da manipulação e da mineração dos dados. O debate sobre a privacidade e a proteção de dados é cada vez mais comum no dia a dia de pessoas e negócios. Derbli (2019) pontua que, com os avanços da sociedade e o desenvolvimento da economia digital, torna-se urgente leis que regulamentem esse mercado a fim de garantir maior transparência no processo de coleta e tratamento desses dados pessoais, e assegurar a proteção da privacidade dos indivíduos.

Impulsionados por essas mudanças, o Brasil se inspirou em legislações vigentes em outros países, em especial o Regulamento Geral de Proteção de Dados

(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, a Lei de Acesso à Informação (LAI), e a Lei do Cadastro Positivo. Esse conjunto de leis tem o objetivo de normatizar as novas formas de consumir, produzir e trabalhar (BIONI, 2019).

De modo geral, empresas enfrentam dificuldades para inovar e se adaptar às regras impostas pelas novas leis. No entanto, micro e pequenas empresas (MPEs) enfrentam dificuldades ainda maiores por falta de competência técnica, ou investimentos estruturais e tecnológicos (LIMA; SILVA, 2019).

No Brasil, as MPEs são responsáveis pela maior parte da renda da população. De acordo com o SEBRAE (2019), 99% dos 6,4 milhões de estabelecimentos são considerados microempresa ou empresa de pequeno porte, e respondem por 52% dos empregos com carteira assinada no setor privado.

As MPEs desempenham também uma função social ao gerar renda para parte da população. Assim, desenvolver estudos que auxiliem a sobrevivência dessas empresas é também garantir bem-estar à população e promover uma sociedade mais sustentável.

> As MPEs são responsáveis pela maior parte do trabalho e da renda dos brasileiros, cumprindo seu papel social e contribuindo com a economia, por ser tão relevante é importante que as MPEs cresçam. E o conhecimento representa não só uma oportunidade de sobrevivência, mas também de crescimento (MACHADO, 2018, p. 211).

As MPEs, ao exercerem sua função social, são um dos principais meios de reduzir a desigualdade social, aumentar a distribuição de renda, além de ser um espaço para exercício de direitos e deveres.

A regulação do mercado impacta diretamente os pequenos negócios, agregando mais um desafio à sobrevivência em um mercado complexo e competitivo. Buscar soluções inovadoras e de baixo custo são importantes para que as MPEs se mantenham ativas. Estar em conformidade com a legislação traz benefícios para os consumidores e aumenta a competitividade do negócio (DERBLI, 2019; MOLINA, SANTOS; 2020).

Diante disso, dada a importância das MPEs para a economia brasileira, o desenvolvimento de pesquisas que auxiliem a sobrevivência dessas organizações torna-se fundamental para garantir o desenvolvimento econômico e social do país.

Em linha com o propósito acima mencionado, esta pesquisa buscou compreender o grau de conformidade das MPEs em relação à LGPD. Uma vez que o GDPR lançou bases jurídicas importantes na Europa, impactando negócios em escala mundial, o Brasil criou a LGPD, a fim de regulamentar a manipulação de dados pessoais por parte das empresas e estabelecer níveis competitivos com o mercado globalizado.

Dessa forma, buscou-se, através do levantamento da literatura, entender e relatar a história da proteção dos dados no Brasil e no mundo e a gestão de dados em MPEs, com o objetivo de fundamentar a construção de uma ferramenta adequada para a coleta dos dados. Com a pesquisa, esperou-se obter um diagnóstico do grau de conformidade das MPEs às determinações da LGPD. A partir de tais considerações, indagou-se: **qual o nível de conformidade das MPEs em relação aos requisitos da LGPD?**

O objetivo geral proposto para esta pesquisa foi investigar o grau de conformidade das MPEs em relação às exigências dispostas na LGPD.

Para a execução do objetivo geral acima descrito, este foi desdobrado em quatro objetivos específicos:

a) Elaborar uma revisão teórica sobre gestão de dados em organizações, sua proteção e leis relacionadas.
b) Verificar se as MPEs estão se preparando para cumprir os requisitos da LGPD, especialmente no que se refere à proteção de dados.
c) Verificar o nível de não conformidades relacionadas aos fatores “tratamento de dados pessoais” e “término de tratamento de dados pessoais”.
d) Propor caminhos possíveis conforme com o grau de conformidade identificado nas MPEs.

1.1 Gestão de dados, informações e conhecimentos

Diversas ciências têm como objeto de estudo o dado, a informação e o conhecimento, cada qual com uma perspectiva. Sendo assim, é possível encontrar

diferentes definições para esses termos. Para esta dissertação, serão utilizados significados advindos da ciência da administração. No Quadro 1 são apresentadas as definições norteadoras da pesquisa, com base em De Sordi (2015):

Quadro 1 - Definições de dado, informação e conhecimento

Dados	Dados são coleções de evidências relevantes sobre um fato observado.
Informação	Informação é a interpretação de um conjunto de dados segundo um propósito relevante e de consenso para o público-alvo (leitor).
Conhecimento	Conhecimento é o novo saber, resultante de análises e reflexões sobre informações segundo os valores e o modelo mental daquele que o desenvolve, proporcionando-lhe melhor capacidade adaptativa às circunstâncias do mundo real.

Fonte: Elaborado pela autora com base em De Sordi, 2015

As tecnologias de informação e comunicação facilitam o fluxo de dados e informações na sociedade do conhecimento, por isso é importante repensar a forma como os dados, a informação e o conhecimento impactam as organizações. 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.

“A organização que for capaz de integrar eficientemente os processos de criação de significado, construção do conhecimento e tomada de decisões pode ser considerada uma organização do conhecimento” (CHOO, 2003, p. 30).

Dessa forma, compreende-se que, em um ambiente constantemente desafiador e com o crescente volume de dados disponíveis, a gestão estratégica dessa tríade é fundamental para que as organizações impulsionem a criação de conhecimento, inovação e competitividade:

> Criar novos conhecimentos é fundamental para a geração da inovação, esta que possui origem no ser humano, de forma intrínseca, pois, as organizações aprendem através dos indivíduos que aprendem. A aprendizagem individual não é garantia para que ocorra a aprendizagem organizacional, mas sem ela não é possível que a organização aprenda (SILVEIRA, 2014, p. 35).

Ao explorar as dimensões de dados e informações por meio do uso de tecnologias de informação e comunicação, as organizações propiciam condições para que indivíduos criem, aprendam, gerem, compartilhem e socializem conhecimento.

Choo (2003) afirma que a organização do conhecimento liga três processos de uso estratégico da informação: a criação de significado, a construção do conhecimento e a tomada de decisões.

O gerenciamento de dados é o desenvolvimento e a implementação de políticas, planos e processos que gerenciam tais dados para manter a integridade de segurança e de sua utilização.

Para Silveira (2014, p. 34):

> Preocupações com a gestão do conhecimento tendem a incentivar e potencializar o desenvolvimento de relações cooperativas no âmbito organizacional; assim como o estímulo à criação de relações cooperativas auxilia uma maior “aderência” (aceitação e uso) dos esforços na implementação das ferramentas que dão suporte à gestão do conhecimento.

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.

1.2 Gestão de dados em micro e pequenas empresas

O processo de implantação da gestão do conhecimento (GC) em MPEs deve levar em consideração a dinâmica e a estrutura dessas empresas, uma vez que compreender essas diferenças é importante para o sucesso da GC. Características como a proximidade entre o dirigente dos negócios e os empregados, clientes, e fornecedores aproxima também as decisões estratégicas, administrativas e operacionais.

A proximidade é uma característica importante para o fortalecimento do pequeno negócio, juntamente à flexibilidade e à capacidade de aprendizagem contínua. Ela favorece o espaço compartilhado, os encontros constantes, as conversas e as discussões, possibilitando trocas a respeito do trabalho entre a equipe normalmente pequena, com cargos e tarefas pouco definidos, o que favorece o esquema de rodízio entre as funções. E essa condição é favorável para a aprendizagem por meio de narrativas, já que trabalhadores podem compartilhar suas impressões, habilidades e críticas.

Dessa forma, as MPEs apresentam uma estrutura flexível, com poucos níveis hierárquicos, podendo ser totalmente integradas e dependentes do seu dirigente, que

possui tarefas pouco delineadas, assim como sua equipe. Os gestores de MPEs são polivalentes e utilizam mais a intuição do que o planejamento formal. Seus processos tendem a apresentar baixo grau de padronização e de formalização (MENEZES; OLAVE, 2016).

O conhecimento em pequenas empresas pode ser observado a partir de três pilares: recursos, fatores e processos. Os recursos são compostos por humanos, capital e propriedade intelectual. Os fatores consistem em cultura, liderança, infraestrutura organizacional e estratégia. Em processos, o conhecimento consiste em: aquisição, criação ou geração, aplicação/utilização, codificação/armazenamento, e transferência/compartilhamento de conhecimento (MEDEIROS *et al*., 2013).

A Gestão do Conhecimento não se trata apenas da estratégia adotada pela organização, mas também do exercício contínuo de mapeamento de competências e conhecimentos, e de aprendizagem organizacional. Do ponto de vista estratégico, ela visa à identificação dos conhecimentos necessários para desenvolver as competências essenciais, além do mapeamento de tais competências, já que busca identificar os conhecimentos e as capacidades que a organização possui. Em relação à aprendizagem organizacional, a GC vai tentar assimilar os saberes que a empresa não sabe, mas necessita (MENEZES; OLAVE, 2016; DE SORDI, 2015).

Nesse processo, além do investimento em tecnologia, é necessário investir no humano, elemento fundamental, pois somente a tecnologia não é capaz de atribuir significado ao conhecimento. Organizações criadoras de conhecimento impulsionam o conhecimento dos trabalhadores em benefício do desempenho do negócio e consequentemente contribuem para o desenvolvimento de seus profissionais e da sociedade.

As MPEs que adotam estratégias de gestão do conhecimento visando a expansão de suas bases de saberes devem promover ações de monitoramento do ambiente tanto tecnológico, como mercadológico.

As MPEs que aprendem incorporam a aprendizagem e o conhecimento em suas estratégias, criando uma cultura do aprendizado compreendida por dimensões estratégicas dos indivíduos, dos processos e da infraestrutura. Para Machado (2018, p. 210):

> A MPE aprendiz incorpora conhecimento e aprendizado em suas estratégias, refinando os meios de coleta e utilização destes dados e informações,

> propiciando à MPE o autoquestionamento para que a mesma avance na construção de novos conhecimentos e desenvolva uma “dimensão'' identitária para se desenvolver e sobreviver. [...]. Deste modo, o conhecimento na MPE constitui um fator relevante para o crescimento e para a sobrevivência.

A gestão de dados tem se tornado um desafio cada vez maior. Não só o aumento da velocidade da geração de dados e informações, mas também o volume resultante dessa aceleração impossibilitam o consumo humano de toda essa informação.

O conhecimento organizacional é gerado a partir de estágios inter-relacionados do ciclo do conhecimento envolvendo obtenção, captura, criação, codificação, compartilhamento, armazenamento, utilização e reutilização de conhecimento. Pesquisas sobre ciclos de conhecimento resultaram em diferentes explicações e modelos.

Para De Sordi (2017b), a criação do conhecimento é um processo complexo, que deriva da identificação de informações que precisam ser conectadas para gerar conceitos e conhecimento explícito. Além de projetar o compartilhamento, o armazenamento é importante para solidificar o conhecimento explícito e a memória organizacional, que pode ser de forma física ou digital. Repositórios e intranets são mecanismos utilizados para armazenamento, como também manuais, relatórios, normativas e outros.

O armazenamento requer atualização, dinamicidade e estrutura, capaz de permitir aos indivíduos, entre outros aspectos, relacionar conteúdos e garantir proteção dos dados. Entende-se que o conhecimento armazenado seja utilizado e reutilizado. A utilização e reutilização do conhecimento estão fortemente associadas às tecnologias de informação e comunicação.

O montante de dados armazenados em bancos de dados em todos os setores da economia é alimentado pelo próprio indivíduo, em troca da utilização de um produto ou serviço público ou privado. Como resultado da demanda gerada pelo volume de dados, houve um crescimento da oferta de empresas no ramo da exploração de dados, sistematização da informação e formação de bancos de dados pessoais (DE SORDI, 2015; MACHADO, 2018; MENEZES; OLAVE, 2016).

Os dados pessoais identificam ações e preferências do indivíduo, podendo até prever o comportamento de consumo, por exemplo. O conjunto de dados tratados

fornecem informações valiosas para as organizações, e a MPE também está passando por essa transformação para se apropriar da nova “moeda”.

O uso de tecnologias de informação e comunicação, ao mesmo tempo em que facilita o fluxo de dados, também aumenta o risco da sua exposição. Desse modo, surgem novos desafios relacionados sobretudo à preservação de direitos humanos básicos, como a dignidade da pessoa e a proteção de sua privacidade. Para lidar com esse cenário, o desenvolvimento de competências relacionadas à gestão de dados passa a ser um elemento fundamental para a sobrevivência das organizações (BEZERRA, 2019).

1.3 Proteção de dados em micro e pequenas empresas

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 refere-se 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 a segurança da informação, área explorada pela Ciência informação, 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 (DONEDA, 2011).

A confidencialidade tem por objetivo garantir que o acesso à informação seja exclusivo à pessoa designada a acessá-la. A integridade tem o intuito de garantir que a informação esteja correta e íntegra. Já a disponibilidade visa garantir que a informação possa ser recuperada quando necessário e de forma integra. Moraes (2010, p. 37), ao conceituar segurança da informação, afirma que “toda e qualquer informação deve ser correta, precisa e estar disponível, a fim de ser armazenada, recuperada, manipulada ou processada, além de poder ser trocada de forma segura e confiável”.

Dos princípios apresentados, o que gera a privacidade é a confidencialidade. Sendo assim, a garantia para que esses três pilares se mantenham preservados é

uma tarefa árdua, uma vez que novas tecnologias, acompanhadas de novos riscos, surgem a todo momento (DONEDA, 2011; PIURCOSKY *et al*., 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 cultura organizacional também é um fator relevante para o aumento das ameaças, pois muitas vezes os funcionários compartilham senhas, equipamentos e até mesmo misturam o uso de *smartphones* pessoais com o negócio.

A LGPD pontua a responsabilidade das organizações em incentivar boas práticas de segurança da informação, a fim de evitar possíveis violações de dados. Nesse caso, surge a figura do encarregado de dados, ou *data protection office* na GDPR, para prestar contas e garantir a transparência dos processos.

> A LGPD trouxe uma gama de obrigações para as empresas, que terão de se adaptar e adotar medidas técnicas, administrativas e de segurança com vistas à proteção dos dados pessoais e sensíveis obtidos em decorrência das relações de trabalho (RAMOS; GOMES, 2019, p.143).

As MPEs necessitam verificar se todos os seus contratos estão em consonância com a lei, seja entre empresas e prestadores de serviços, como nos contratos entre empresa e seu cliente final.

Um ponto relevante para a MPE é avaliar se os colaboradores sabem que são responsáveis pelas informações, para evitar incidentes com os dados do negócio. Especialistas afirmam que as MPEs devem se adequar por meio de consultorias especializadas em segurança da informação, a fim de evitar penalidades administrativas ou ações de responsabilização civil por eventuais danos causados (RAMOS; GOMES, 2019).

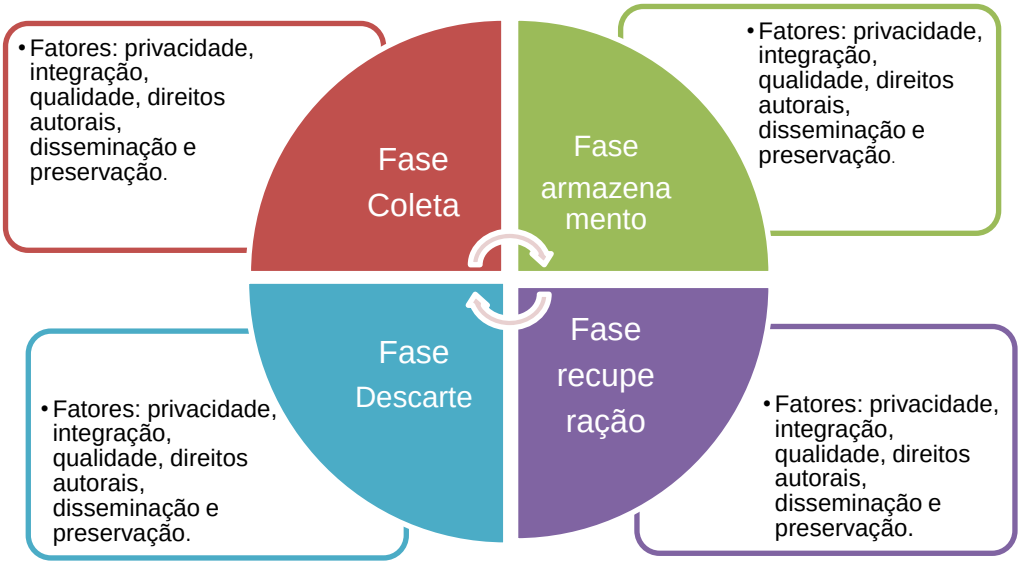
1.4 Ciclo de vida dos dados

A LGPD possui exigências específicas no que se refere ao tratamento dos dados. Dessa maneira, compreender os processos e classificar os dados corretamente é fundamental para estar em conformidade com a lei. Nesse sentido, é necessário pensar em práticas que possam auxiliar o cumprimento da lei.

A implementação de uma gestão voltada para o ciclo de vida dos dados pode trazer muitos benefícios para o negócio, uma vez que a gestão do ciclo de vida dos dados visa administrar a forma de coleta, de processamento, de análise, de armazenamento, de compartilhamento, de reuso e de eliminação dos dados.

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.

Figura 1 - Ciclo de vida dos dados



Fonte: Elaborada pela autora com base em Sant'Ana, 2016

Dentro do ciclo de vida dos dados os fatores se repetem, identificados por Sant'Ana (2016). A primeira fase, denominada coleta, consiste em definir quais são as necessidades informacionais. Nessa etapa, a proposta é pensar quais serão os dados úteis ao negócio, podendo ser um projeto ou processo. São discutidos nessa fase a privacidade, a integração, o direito autoral, a disseminação e a preservação dos dados.

Na segunda fase, armazenamento, deve-se pensar no conjunto de variáveis dos conteúdos armazenados: qual estrutura será utilizada para armazenar, quem serão as pessoas autorizadas a acessar determinados dados e como serão acessados, quais os formatos ou padrões adotados, e onde estarão armazenados.

Na terceira fase, recuperação, preocupações com o *download* do conteúdo, a usabilidade, a acessibilidade e a interpretação dos dados são importantes.

Na quarta fase, descarte, 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 ciclo de vida dos dados, ou 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, e apresenta a relação entre as fases do ciclo de vida dos dados e as operações sobre os dados pessoais (Quadro 2).

Quadro 2 - 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.	

Fonte: Elaborado pela autora com base na Lei Geral de Proteção de Dados, 2020

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.

O guia de boas práticas (LEI GERAL DE PROTEÇÃO DE DADOS, 2020), apesar de ser voltado para a administração pública, pode ser útil ao relacionar os

requisitos da LGPD com processos aplicados a qualquer negócio. Recomenda-se a consulta das normas técnicas para a construção do ciclo de vida dos dados.

- ABNT NBR ISO/IEC 27001 – Tecnologia da informação – Técnicas de segurança – Sistemas de gestão da segurança da informação – Requisitos;
- ABNT NBR ISO/IEC 27002 – Código de Prática para controles de segurança da informação;
- ABNT NBR ISO/IEC 27701 Técnicas de segurança – Extensão da ABNT NBR ISO/ IEC 27001; e
- ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação – Requisitos e diretrizes.

A utilização dessas normas auxilia 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 desse relatório.

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).

1.5 Hipóteses

A pesquisa buscou investigar até que ponto as MPEs estão considerando as exigências da LGPD no que concerne àquelas que tratam e utilizam dados pessoais de seus clientes, e isso foi observado considerando-se os diversos fatores sob os quais a LGPD pode ser analisada: 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.

Dessa forma, a hipótese substantiva ou principal da pesquisa é a seguinte:

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.

Com relação ao questionário diagnóstico, ao considerar a mediana das respondentes como representando a amostra, formulou-se as seguintes hipóteses:

Hb: Aplicando-se o questionário diagnóstico, o nível de conformidade dos respondentes, considerando a mediana das respostas, não é superior a 20%.

Hc: Ao nível de significância de 0,05, a proporção de não conformidades, considerando-se o fator Tratamento de Dados Pessoais, é significativamente maior do que as conformidades.

Hd: 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.

He: Ao nível de significância de 0,05, a proporção de não conformidades, considerando-se o fator Direito dos Titulares, é significativamente maior do que as conformidades.

Hf: Ao nível de significância de 0,05, a proporção de não conformidades, considerando-se o fator Deveres do Controlador e do Operador, é significativamente maior do que as conformidades.

Hg: Ao nível de significância de 0,05, a proporção de não conformidades, considerando-se o fator Boas Práticas, é significativamente maior do que as conformidades.

Hh: Ao nível de significância de 0,05, a proporção de não conformidades, considerando-se o fator Funcionários, é significativamente maior do que as conformidades.

Hi: Ao nível de significância de 0,05, a proporção de não conformidades, considerando-se o fator Incidentes de Dados Pessoais, é significativamente maior do que as conformidades.

Hj: Ao nível de significância de 0,05, a proporção de não conformidades, considerando-se o fator Contratos, é significativamente maior do que as conformidades.

Hk: Ao nível de significância de 0,05, a proporção de não conformidades não é significativamente diferente em função do gênero do respondente.

Hl: Ao nível de significância de 0,05, a proporção de não conformidades não é significativamente diferente em função da faixa etária do respondente.

Hm: Ao nível de significância de 0,05, a proporção de não conformidades não é significativamente diferente em função do grau de instrução do respondente.

Hn: Ao nível de significância de 0,05, a proporção de não conformidades não é significativamente diferente em função do setor econômico da empresa.

Ho: Ao nível de significância de 0,05, a proporção de não conformidades não é significativamente diferente em função da associação a uma entidade.

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

2. LEIS SUBSIDIÁRIAS

A discussão em torno do panorama geral das leis de proteção de dados pessoais na Europa mostra o quão avançado estão em comparação aos demais países do mundo.

A globalização do comércio e as transformações no mundo do trabalho trazem como consequência a necessidade de legislar sobre as novas formas de consumir, trabalhar e se relacionar. 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.

No Brasil, a discussão da proteção de dados surgiu de forma tímida no final dos anos 80. Nos anos 90, foi criada a primeira lei que tratava do direito do proprietário dos dados. Anos depois, criou-se a Lei de patentes, momento este em que a internet se expandia e a necessidade de patentes industriais para proteger empresas se fortaleceu.

> Diante dessa transformação exsurge a necessidade de regulamentar o uso dos dados, fenômeno que vem inspirando a edição de leis e regulamentações específicas sobre a matéria a nível global (OLIVEIRA *et al*., 2019, p. 175).

Com o amadurecimento do direito de propriedade intelectual e a convenção de Berna, o Brasil promulgou a Lei de direitos autorais (Lei Nº 9.610, de 1998). Após 12 anos de intervalo, criou-se a Lei de acesso à informação, visando a transparência de dados gerados pelo e para o governo brasileiro. Em seguida, para regulamentar a internet, surgiu o Marco civil da internet (Lei n° 12.965 de 2014), fomentando a discussão sobre a proteção de dados.

Nesse contexto, o congresso aprovou a Lei do cadastro positivo (Lei Nº 12.414 de 2011), que utiliza os dados de pagamentos a fim de alimentar o *score* dos cidadãos para empréstimos e financiamentos. Seguido do debate mundial de proteção de dados, impulsionado pela GDPR, o Brasil criou a LGPD (Lei nº 13.709 de 2018), que entrará em vigor a partir de agosto de 2020.

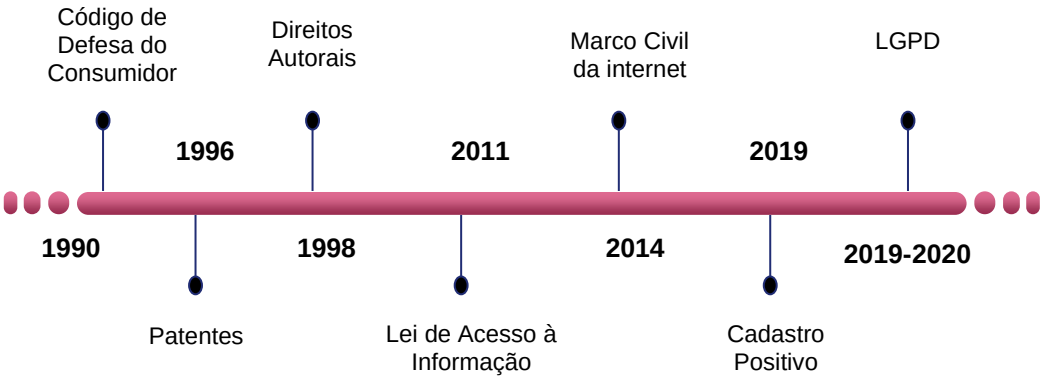
Com a sanção da LGPD em 2018, o país passou a contar com sua primeira LGPD Pessoais e tornou-se parte do grupo de mais de 120 países que dispõem de uma legislação sobre o assunto (RAMOS; GOMES, 2019).

Após anos de debates e construção legislativa nasceu uma norma bastante completa, comparável aos mais altos padrões internacionais. Nesse contexto, a criação da Autoridade Nacional de Proteção de Dados (ANPD) possui um papel indispensável, sendo o órgão regulador responsável pela criação de um ambiente de segurança jurídica, fiscalização e orientação para empresas e para os cidadãos. A existência de uma autoridade nacional forte, eficiente e independente segue ainda a tendência criada pela GDPR nos países europeus, visando que o órgão atenda aos interesses dos cidadãos, como observa Bezerra (2019, p. 56):

> Atualmente, há aproximadamente 120 países com leis vigentes de proteção de dados pessoais e até 2020 esse número deverá subir para cerca de 134. Destes 120 países, aproximadamente 80% editaram uma lei de proteção de dados pessoais e possuem uma autoridade nacional independente, enquanto somente 10% não contam com um órgão independente, por previsões legislativas expressas em obediência a diretivas ou orientações de outros órgãos do Poder Executivo. Nota-se que, embora os modelos de autoridades nacionais sejam os mais variados, estudos demonstram que a maioria dos países optou por um modelo em que o órgão de controle desfruta de um grau de independência bastante elevado.

Para melhor compreensão desse estudo, a Figura 2 apresenta em ordem cronológica de acordo com a data de aprovação o conjunto de leis brasileiras que tratam da proteção de dados.

Figura 2 - Leis brasileiras



Fonte: Elaborado pela autora, 2020

Ainda que não esteja em vigor, a LGPD já provocou mudanças que refletem na postura de grandes negócios como *Facebook* e *Google*.

2.1 Código de defesa do consumidor

O Código Brasileiro de Defesa do Consumidor (CDC) é um conjunto de normas que visa a proteção dos direitos do consumidor. Foi instituído pela lei nº. 8.078, de 11 de setembro de 1990, durante o mandato do presidente Fernando Collor. No entanto, o código teve a sua vigência protelada para a adaptação das partes envolvidas (BRASIL, 1990).

O CDC foi fruto de uma expressa determinação constitucional que buscou preencher uma lacuna legislativa existente no direito americano, em que as relações comerciais, tratadas de forma obsoleta por um código comercial do século XIX, não traziam nenhuma proteção ao consumidor. Assim, tornava-se necessária a elaboração de normas que acompanhassem o dinamismo de uma sociedade de massas que se formou no decorrer do século XX, conforme dispunha a Constituição Federal (1988), em seu artigo 5º, inciso XXXII:

"O Estado promoverá na forma da lei a defesa do consumidor."

Por outro lado, com a redemocratização do país, a partir da promulgação da Constituição Federal de 1988 houve um fortalecimento das entidades não-governamentais, aumentando o clamor popular pela regulamentação dos direitos sociais, o que levou à criação do Código de Defesa do Consumidor (BRASIL, 1990).

Uma das premissas essenciais para se estabelecer a chamada relação de consumo é o conceito legal de palavras como consumidor, fornecedor, serviço e produto. Elas estão estabelecidas nos artigos iniciais do CDC (Quadro 3):

Quadro 3 - Definições do código de defesa do consumidor

Consumidor	É toda pessoa física ou jurídica que adquire ou utiliza produto ou serviço como destinatário final. Equipara-se a consumidor a coletividade de pessoas, ainda que indetermináveis, que haja intervindo nas relações de consumo (art. 2º).
Fornecedor	É toda pessoa física ou jurídica, pública ou privada, nacional ou estrangeira, bem como os entes despersonalizados que desenvolvem atividades de produção, montagem, criação, construção, transformação, importação, exportação, distribuição ou comercialização de produtos ou prestação de serviços (art. 3º).
Produto	É qualquer bem, móvel ou imóvel, material ou imaterial (art. 3º, § 1º).
Serviço	É qualquer atividade fornecida no mercado de consumo mediante remuneração, inclusive as de natureza bancária, financeira, de crédito e securitária, salvo as decorrentes das relações de caráter trabalhista (art. 3º, § 2º).

Fonte: Elaborado pela autora com base em Brasil, 1990

2.2 Direito Industrial - Propriedade intelectual

O Direito industrial se divide em dois campos de estudos: patentes, que se refere aos direitos relacionados à inovação industrial; e direito autoral, que trata do mundo das ideias, criações artísticas e intelectuais.

2.2.1 Patente

A patente pode ser definida como registro formalizado por um documento expedido e certificado por um órgão público, o qual se confere e reconhece os direitos de propriedade e exclusividade que protege uma invenção ou criação industrializável de concorrentes.

Trata-se de um privilégio concedido pelo Estado aos inventores (pessoa física ou jurídica) detentores do direito de invenção de produtos e processos de fabricação, ou aperfeiçoamento de algum já existente.

No Brasil, o pedido de concessão de patente deve ser feito ao Instituto Nacional da Propriedade Industrial (INPI), autarquia federal vinculada ao Ministério do Desenvolvimento, Indústria e Comércio Exterior, que julgará sua validade com base nas disposições da Lei da Propriedade Industrial, nº. 9.279, de 14 de maio de 1996. Para fins de patente, a invenção precisa enquadrar-se em uma das seguintes naturezas e modalidades:

Privilégio de invenção: a invenção deve ser novidade e ter aplicação industrial;

Modelo de utilidade: nova forma ou disposição, envolvendo ato inventivo que resulte em melhoria funcional do objeto (BRASIL, 1996).

Podem ser patenteados:

A invenção que atenda aos requisitos de novidade, atividade inventiva e aplicação industrial;

O modelo de utilidade que seja objeto de uso prático, ou parte deste;

O modelo de utilidade que seja suscetível de aplicação industrial;

O modelo de utilidade que apresente nova forma ou disposição, envolvendo ato inventivo;

O modelo de utilidade que resulte em melhoria funcional no seu uso ou em sua fabricação (BRASIL, 1996).

As patentes são consideradas parte do conjunto de direitos de propriedade intelectual, e são importantes para garantir direitos de exclusividade e acirrar a competição entre as organizações (BRASIL, 1996).

2.2.2 Direito autorais

O Estado brasileiro garante a todo criador de uma obra intelectual direitos sobre a sua criação e sobre o uso da mesma. Esse direito é exclusivo do autor, de acordo com o artigo 5º da Constituição Federal (BRASIL, 1988). No Brasil, a Lei nº. 9.610, de 19 de fevereiro de 1998, consolida a legislação sobre os direitos autorais. A Lei de Direitos Autorais foi construída a partir de tratados e convenções internacionais, sendo a Convenção de Berna o mais notório entre estes.

O direito autoral ou direito de autor é um conjunto de prerrogativas conferidas por lei à pessoa física ou jurídica criadora da obra intelectual, para que ela possa usufruir de quaisquer benefícios morais e patrimoniais resultantes da exploração de suas criações. É derivado dos direitos individuais e situa-se como um elemento híbrido, especial e autônomo dentro do Direito Civil (BRASIL, 1998).

Para fins legais os direitos de autor se dividem em direitos morais e patrimoniais. Os direitos morais asseguram a autoria da criação ao autor da obra intelectual e são intransferíveis e irrenunciáveis. Já os direitos patrimoniais se referem principalmente à utilização econômica da obra intelectual, podendo ser transferidos e/ou cedidos a outras pessoas.

A transferência dos direitos patrimoniais se dá por meio de licenciamento e/ou cessão. Uma obra entra em domínio público quando os direitos patrimoniais expiram. Isso geralmente ocorre depois do tempo prescrito após o falecimento do autor (*post mortem auctoris*). O prazo mínimo é de 50 anos, previsto na Convenção de Berna. Nas legislações brasileira e europeia, o período é de 70 anos. Uma vez expirado o prazo, esse trabalho pode ser utilizado livremente, respeitando os direitos morais do autor. O direito de autor é uma modalidade da propriedade intelectual e um dos direitos humanos fundamentais na Declaração Universal dos Direitos Humanos.

2.3 Lei de acesso à informação

Apelidada de LAI, a Lei de Acesso à Informação (Lei nº. 12.527/2011) regulamenta o direito constitucional para o acesso às informações públicas (BRASIL, 2011). Essa normativa entrou em vigor a partir de 16 de maio de 2012 e criou mecanismos que possibilitam que qualquer pessoa, física ou jurídica, sem necessidade de apresentar motivo, solicite o recebimento de informações públicas dos órgãos e entidades (RAMOS; GOMES, 2019).

A LAI é válida no âmbito dos três Poderes da União, Estados, Distrito Federal e Municípios, inclusive nos Tribunais de Conta e Ministério Público. Entidades privadas sem fins lucrativos também são obrigadas a comunicar as informações referentes ao recebimento e à destinação dos recursos públicos por elas recebidos. No Governo Federal, a Lei de Acesso à Informação foi regulamentada pelo Decreto nº 7.724/2012 (BRASIL, 2011).

2.4 Marco civil da internet

A expansão da oferta de serviços e produtos digitais fomentou o debate acerca da regulamentação da internet. No Brasil, atualmente o acesso à internet é garantido pela Lei do Marco Civil da Internet, Lei 12.965/2014, que explicita em seu 7º artigo que o acesso à internet é essencial ao exercício da cidadania (BRASIL, 2014).

Já a LGPD aprofunda e regulamenta questões relativas aos direitos e deveres em relação aos dados pessoais nesse ambiente. Os impactos dessas normas são expressivos tanto no que se refere à tutela da privacidade quanto para atividades empresariais, uma vez que ambas as leis impõem diversas diretrizes exigindo adequação da sociedade de modo geral (PIURCOSKY *et al.*, 2019; RAMOS; GOMES, 2019).

Enquanto o Marco Civil da Internet legisla exclusivamente o âmbito das relações via internet, a LGPD aprofunda o tema e estende a proteção de dados do meio digital ao físico. Até então não havia nenhum tipo de controle sobre o cuidado empregado no tratamento dos dados cuja transação fosse efetuada fora dos meios digitais, ainda que existissem outras normativas em diferentes leis tais como o Código de Defesa do Consumidor, as leis do Cadastro Positivo, de Acesso à Informação e a

garantia fundamental à vida privada assegurada pelo artigo 5º da Constituição Federal Brasileira (RAMOS; GOMES, 2019).

Para Cavalcanti e Santos (2018) torna-se, portanto, obrigatório adotar, desde a concepção de serviços, produtos e modelos de negócio, a prática de se garantir direitos de proteção à privacidade e aos dados pessoais. São os chamados *privacy by design* e *by default*, nos quais o primeiro modelo permite uma adequação do formato e níveis de privacidade a ser cedida por determinado usuário, enquanto o segundo não se concebe tal possibilidade (PIURCOSKY *et al*., 2019).

Essa mudança de paradigma impacta de maneira relevante as atividades comerciais e industriais, principalmente considerando a “Quarta Revolução Industrial”, cujos traços marcantes incluem a velocidade, a amplitude, a profundidade e o impacto sistêmico. Esse fenômeno é explicado por conta do amadurecimento sobre a relevância da informação como ativo de valor financeiro e de mercado, principalmente os aspectos da ‘maleabilidade’ e ‘utilidade’ da informação, que influencia a tomada de decisão da organização (OLIVEIRA *et al*., 2019).

2.5 Cadastro positivo

O governo federal publicou, no dia 25 de julho de 2019, o decreto que regulamenta a nova Lei do Cadastro Positivo (Lei nº 12.414/2011 com as alterações trazidas pela LC nº 166/2019), em vigor desde 9 de julho de 2019.

A maioria dos artigos do decreto se refere à atuação dos bancos de dados e dos direitos dos consumidores e empresas cadastrados, especialmente no dia a dia da gestão do crédito dos consumidores das empresas.

A Lei do Cadastro Positivo (Lei nº 12.414, de 9 de junho de 2011) regulamenta o histórico de crédito dos consumidores e empresas. Os dados positivos considerados para o cálculo de nota ou *score* de crédito são os mesmos anteriormente considerados para as 12 milhões de pessoas que optaram pela adesão ao Cadastro Positivo antes de 9 de junho. É importante ressaltar que, com a nova lei, estima-se a inclusão de cerca de 137 milhões de pessoas físicas e jurídicas no Cadastro Positivo. Poderão constar no histórico de crédito dos consumidores e empresas:

Natureza da relação (creditícia, comercial, de serviço continuado ou outra);

Datas de concessão do crédito ou da assunção da obrigação de pagamento;

Valor do crédito concedido ou da obrigação de pagamento assumida;

Valores devidos nas datas de vencimento pretéritas, a vencer ou pagos, integral ou parcialmente; e

Datas de pagamentos realizados, a vencer ou pretéritas (BRASIL, 2019).

A Lei do Cadastro Positivo já estabelecia que poderiam ser consideradas informações de até 15 anos. Com o decreto, fica estabelecido que as fontes do Cadastro Positivo devem enviar informações aos gestores de bancos de dados de, pelo menos, 12 meses. Essa é uma informação bastante relevante para as áreas de crédito das empresas, pois assim que essas informações forem incorporadas ao Cadastro Positivo nos termos da nova lei, elas poderão ter acesso aos dados do hábito de pagamentos de cerca de 137 milhões de consumidores e empresas pelo menos desde julho de 2018.

Os cadastrados poderão, a qualquer momento, solicitar previamente que o seu Cadastro Positivo não seja aberto ou solicitar o cancelamento do seu Cadastro Positivo já aberto. Cabe aos *bureaus* de crédito oferecer essas possibilidades de forma facilitada pelos meios físico, telefônico ou eletrônico (BRASIL, 2019).

As empresas administradoras de bancos de dados, os *bureaus*, também precisam obedecer a uma série de critérios estabelecidos no decreto para operar com dados positivos. Elas devem demonstrar patrimônio líquido mínimo de R$ 100 milhões, dispor de certificação técnica emitida por uma empresa qualificada independente que ateste a segurança das informações constantes em seu banco de dados, e cumprir todos os requisitos de governança, transparência e de atendimento ao consumidor.

Segundo a Lei do Cadastro Positivo, as informações positivas somente podem ser acessadas por consulentes que mantenham ou pretendam manter relação comercial ou creditícia com o cadastrado, além de possibilitar o uso das informações apenas como insumo para o cálculo de nota ou pontuação de crédito. As informações de seu histórico de crédito serão disponibilizadas a consulentes de forma detalhada apenas se o consumidor (titular dos dados) autorizar (BRASIL, 2019).

Além disso, a Lei do Cadastro Positivo reitera o direito de acesso gratuito dos consumidores e empresas às suas próprias informações, o direito de impugnar informações eventualmente erradas, bem como estabelece a responsabilidade das partes pela segurança das informações, determinando, portanto, um tratamento de

dados pessoais proporcional, de acordo com finalidades específicas, norteado pela transparência e segurança dos titulares dos dados, em total compatibilidade com a LGPD.

3. PROTEÇÃO DE DADOS

3.1 *General data protection regulation* (GDPR)

A regulação de dados na União Europeia entrou em vigor em maio de 2018. Desde então, todas as empresas sob a GDPR estão ajustando seus termos de consentimento e uso.

O GDPR, ou *General Data Protection Regulation*, é um instrumento elaborado pela União Europeia para garantir a proteção dos indivíduos no que diz respeito ao processamento de dados pessoais e à sua livre movimentação. Refere-se à garantia de direitos relacionados à privacidade e à proteção de dados dos cidadãos europeus, mas não se limitando a esses, frente ao aumento da utilização de dados por novas tecnologias, que podem abusar ou fazer mal-uso desses dados.

Originado de duas diretivas (de 1995 e 2008), reunidas em um ato regulatório, o GDPR tem validade de lei em toda a União Europeia. É aplicável dentro ou fora dos limites da União Europeia, em empresas, governos com estabelecimento na Europa ou qualquer entidade que processe dados pessoais de indivíduos europeus ou ainda processe dados de indivíduos não europeus dentro dos limites da União Europeia. Apenas questões relativas à segurança pública não estão sob a regulação da GDPR.

É considerado dado pessoal qualquer dado, foto, ou gravação de voz que permita identificar o cidadão, mesmo que isolado de outros dados. Sendo assim, dados pessoais são quaisquer informações de uma pessoa natural, como nome, idade, e-mail, gênero, profissão, informações sobre saúde, em qualquer formato, físico ou digital. Bezerra (2019, p. 12) pontua que:

> Quanto à definição de dados pessoais, a GDPR adotou um conceito expansionista no qual, dado pessoal é qualquer tipo de informação que permita sua identificação, ainda que o vínculo não seja estabelecido de imediato, mas de maneira indireta. Esses dados se referem a circunstâncias pessoais ou materiais de um indivíduo identificado ou identificável.

Também são considerados dados pessoais informações que se referem ao indivíduo, como comportamentos ou características que possam influenciar o modo como uma pessoa é avaliada ou tratada, assim como dados que identifiquem uma

pessoa em um grupo, como nome, números de identificação, localização, e identificadores genéticos, médicos, culturais, econômicos ou sociais.

De acordo com GDPR, os dados podem ser sensíveis. Portanto, qualquer dado que revele as seguintes informações é considerado dado pessoal sensível:

- Raça ou origem étnica
- Orientação política
- Crença religiosa ou filosófica
- Filiação sindical ou a grupos
- Dados genéticos
- Dados biométricos que permitam identificar unicamente uma pessoa
- Dados de saúde
- Dados relativos à vida sexual do indivíduo
- Orientação sexual

Princípios da proteção aos dados

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.

Legalidade, justiça e transparência: o indivíduo deve poder saber quem controla e processa seus dados e com quais objetivos;

Limitação de propósito: os dados coletados não podem ser utilizados com propósitos incompatíveis ao propósito original;

Minimização dos dados: os dados coletados e processados devem ser os mínimos necessários ao propósito;

Acurácia: os dados devem ser mantidos corretamente. Dados desatualizados ou incorretos devem ser descartados ou corrigidos;

Limitação de armazenamento: os dados devem ser mantidos somente enquanto são necessários ao propósito.

Integridade e confidencialidade: deve-se garantir a segurança de acesso aos dados, com dispositivos como autenticação e criptografia (BIONI, 2019; BRASIL, 2019).

A GDPR dispõe de normativas para orientar as empresas a fim de que ofereçam produtos e serviços desenhados de forma a garantir privacidade e *compliance*, para que não somente os sistemas de tratamento dos dados como os bancos de dados em si sejam construídos considerando todos os princípios da GDPR. Portanto, medidas que visam a prevenção de exposição indevida de dados estão previstas por meio de boas práticas de anonimização e minimização dos dados, assim como aplicação de criptografia, com o objetivo de impedir a identificação do indivíduo de forma que não seja possível distingui-lo do grupo.

A lei recomenda que a empresa designe um *data protection officer*, ou DPO: um executivo de proteção de dados, cujas responsabilidades incluem o monitoramento, e a provisão de garantias e informações aos controladores e processadores de dados em relação às questões de proteção aos dados. Embora a responsabilidade sobre o que fazer com os dados não seja do DPO e sim dos controladores, o papel desempenhado pelo DPO orienta e garante o *compliance* da empresa às normas.

3.2 Lei geral de proteção de dados

A coleta de dados pessoais passou a ser objeto de discussão em diversos países, e a União Europeia é tida como pioneira e referência mundial, com a criação da legislação para a proteção de dados mais completa do mundo. A aplicabilidade da GDPR não se restringe a dados de pessoas naturais localizadas na União Europeia, mas também se refere a todo o fluxo de dados existente entre os países da União Europeia e os demais países com quem possui relações comerciais. Tornou-se um padrão normativo referencial para outras nações por tratar o tema de forma abrangente, com maturidade conceitual e amplitude legislativa (BEZERRA, 2019).

Além disso, a União Europeia, que já tinha um padrão legislativo de proteção relativamente avançado, adequou-se aos termos e procedimentos mais modernos e compatíveis às novas tecnologias de computação, automação e inteligência artificial. Nesse sentido, conceitos de coleta, processamento, transferência e vazamento de dados passaram a ser positivados na norma. O Brasil buscou inspiração em países vizinhos, mas a GDPR foi determinante para a criação da LGPD Pessoais (BIONI, 2019; BEZERRA, 2019; CAVALCANTI; SANTOS, 2018).

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, MEYER, SENDACZ E OPICE ADVOGADOS, 2018).

Com essa legislação todas as pessoas, física ou jurídica, 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.

Para melhor compreensão da LGPD é necessário ciência de conceitos que fundamentam a criação da lei, apresentados no Quadro 4.

Quadro 4 - 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.

Fonte: Elaborado pela autora com base em Brasil, 2018

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).

A LGPD não revoga e não impede a aplicação de normas relativas aos setores que também regulamentam a manipulação de dados pessoais. Dessa forma, qualquer organização que realize o tratamento de dados pessoais no Brasil ou que ofereça produtos e serviços para brasileiros deve estar atenta aos impactos da LGPD, para que suas atividades estejam em consonância com as regras.

A LGPD não se aplica ao tratamento de dados pessoais nos casos em que são coletados para fins particulares e não econômicos, jornalísticos, artísticos, acadêmicos; para fins exclusivos de segurança pública, de defesa nacional, de segurança do estado, investigação e repressão de infrações penais; e dados provenientes ou destinados a outros países, que apenas transitem pelo território.

Os princípios estabelecidos na LGPD impõem novas diretrizes e limitações sobre como os dados pessoais poderão ser tratados. São eles: finalidade; adequação; necessidade; livre acesso; qualidade dos dados; transparência; segurança; prevenção; não discriminação; e responsabilização e prestação de contas (RAMOS; GOMES, 2019).

Agentes de tratamento 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 (Quadro 5), independentemente do tamanho da base de dados existente.

Quadro 5 - 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.

Fonte: Elaborado pela autora com base em Brasil, 2018

O Marco Civil da Internet permite apenas o tratamento de dados pessoais mediante a obtenção de consentimento do titular dos dados. A LGPD, no entanto, estabelece dez hipóteses para o tratamento de dados, incluindo, além do consentimento, o interesse legítimo do controlador ou de terceiros, e a necessidade de cumprimento de contrato ou de obrigação legal ou regulatória.

Adiante a hipótese de consentimento, as hipóteses para o tratamento de dados pessoais sensíveis são mais restritas e não permitem o tratamento com base no

legítimo interesse e na proteção do crédito, por exemplo. A LGPD estabelece regras específicas para a obtenção do consentimento, que poderá ser anulado caso a autorização se mostre genérica demais ou que seja baseado em informações com conteúdo enganoso ou abusivo (BRANCO, 2020). Além disso, a lei pontua regras específicas no que se refere ao tratamento de dados pessoais de crianças e adolescentes. Do mesmo modo, o tratamento de dados pessoais considerados como “públicos” deve considerar a finalidade originária, a boa-fé e o interesse público que justificaram a disponibilização de tais dados.

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).

A LGPD estabelece hipóteses que justificam o tratamento de dados pessoais:

- Mediante o consentimento do titular dos dados pessoais;
- Para o cumprimento de obrigação legal ou regulatória pelo controlador dos dados;
- Pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos;
- Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
- Quando necessário para a execução de contrato ou de procedimentos contratuais preliminares;
- Para a proteção da vida ou da incolumidade física do titular ou de terceiros;
- Para o exercício regular de direito em processo judicial, administrativo ou arbitral;
- Para atendimento de interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecer direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais;
- Para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;

- Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente (BRASIL, 2018).

Consentimento

A LGPD estabelece que o consentimento é uma manifestação livre, informada e inequívoca que autoriza o tratamento de dados pessoais para uma finalidade determinada. Autorizações genéricas, isto é, autorizações que não têm como escopo uma finalidade específica, explícita e informada serão nulas.

O consentimento deverá ser fornecido por escrito em cláusula destacada ou por qualquer outra ação afirmativa que demonstre a vontade do titular dos dados. Não se admite em hipótese alguma o consentimento implícito.

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. 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 ao princípios estabelecidos na LGPD (BRANCO, 2020).

Interesse legítimo

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).

O interesse legítimo deverá ser verificado a partir da análise da situação concreta e com base nos princípios da LGPD, e poderá ser revisto pela ANPD.

A título de exemplo, a LGPD estabelece finalidades que podem vir a justificar o interesse legítimo do controlador ou de terceiros, a depender da situação concreta.

Apoio e promoção de atividades do controlador

A partir de situações concretas, que inclui, mas não se limita a proteção, em relação ao titular dos dados, do exercício regular dos direitos ou prestação de serviços que beneficiem o titular, desde que respeitadas suas legítimas expectativas (BRASIL, 2018).

No caso de tratamento de dados pessoais com fundamento no interesse legítimo do controlador, somente os dados estritamente necessários, considerando a finalidade pretendida, poderão ser utilizados.

Tratamento de dados pessoais sensíveis

Considerando a natureza de dados pessoais sensíveis, a LGPD se preocupou em diminuir as hipóteses para tratamento desses dados e impor um consentimento mais rigoroso. O consentimento para o tratamento de dados pessoais sensíveis deve ser fornecido de forma específica e destacada. 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).

Além disso, a LGPD não permite o tratamento de dados pessoais sensíveis para atender ao interesse legítimo do controlador ou de terceiros, ou proteção do crédito. 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).

Tratamento de dados pessoais de crianças e de adolescentes

O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse. O tratamento de dados pessoais de crianças deve ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal. Os controladores devem realizar todos os esforços razoáveis para verificar que o consentimento foi realmente fornecido pelo responsável pela criança (BRASIL, 2018).

A única hipótese em que a LGPD permite a coleta de dados pessoais sem o consentimento de pais ou responsável legal é no caso de a coleta ser necessária para

contatar os pais ou responsável legal. Neste caso, os dados pessoais coletados sem o consentimento podem ser utilizados somente uma vez e não podem ser armazenados em hipótese alguma, dado que sua única finalidade é a realização do referido contato.

Término do tratamento

O término do tratamento de dados pessoais ocorrerá quando:

- For verificado que a finalidade para a qual o consentimento foi obtido foi alcançada ou que os dados pessoais coletados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;
- Decorrer o fim do período de tratamento;
- Ocorrer uma manifestação do titular dos dados pessoais nesse sentido;
- Houver uma determinação legal. Nos casos de término de tratamento de dados pessoais, estes devem ser eliminados, salvo se de outra forma a sua guarda for autorizada pela LGPD, tal como o emprego de anonimização (BRASIL, 2018).

O titular dos dados tem direito ao acesso facilitado a informações sobre o tratamento de seus dados pessoais e a exigir correção de dados incompletos, inexatos ou desatualizados. Também poderá, mediante requisição expressa, solicitar a transferência de seus dados pessoais a outro fornecedor de serviço ou produto.

Quando o tratamento dos dados for baseado exclusivamente em decisões automatizadas, o titular dos dados tem o direito de solicitar a revisão de tal tratamento por pessoa natural. Quando verificado o descumprimento de disposições da LGPD, o titular dos dados poderá se opor ao tratamento de seus dados pessoais, se realizado com base em uma das hipóteses de dispensa de consentimento.

O titular dos dados também poderá revogar o consentimento dado anteriormente para o tratamento de seus dados pessoais. Do mesmo modo, é preciso adequar a estrutura operacional e técnica da sua organização para viabilizar e cumprir com todos os direitos que a lei garante ao titular dos dados; desenvolver mecanismos para permitir que os titulares de dados exerçam seus direitos, de forma facilitada e gratuita; e verificar se o conteúdo informativo proporcionado ao titular dos dados está com uma linguagem clara e adequada.

A LGPD impõe como seu principal objetivo a proteção dos direitos fundamentais de liberdade e de privacidade dos indivíduos. Para tanto, apresenta um rol de princípios e direitos especialmente voltados à garantia de informações claras ao titular dos dados e imposição de limitações ao seu tratamento (RAMOS; GOMES, 2019).

Além de ter o direito a informações claras acerca do tratamento de dados, o titular tem o direito a obter gratuitamente as seguintes providências, mediante requisição expressa ao controlador:

- Confirmação da existência de tratamento e acesso aos dados pessoais;
- Correção de dados incompletos, inexatos ou desatualizados;
- Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a legislação;
- Portabilidade dos dados a outro fornecedor de serviço ou produto;
- Eliminação dos dados pessoais tratados com o consentimento do titular, ressalvadas as hipóteses de guarda para cumprimento de obrigação legal ou regulatória;
- Informação a respeito do uso compartilhado de dados pessoais;
- Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
- Possibilidade de revogação do consentimento, por procedimento gratuito e facilitado (BRASIL, 2018).

Direito à informação

O titular dos dados tem direito a ter acesso facilitado a informações relacionadas ao tratamento de dados pessoais, incluindo, mas não se limitando a informações a respeito:

- Da finalidade específica do tratamento;
- Da forma e duração do tratamento;
- Da identificação e contato do controlador;
- Do uso compartilhado de dados e a respectiva finalidade;
- Da responsabilidade dos agentes de tratamento;
- De tratamento de dados pessoais como condição para o fornecimento de produto ou de serviço ou para o exercício de direito, caso aplicável.

- Dos demais direitos do titular, nos termos da LGPD. Tais informações deverão ser disponibilizadas de forma clara, adequada e ostensiva. No caso de tratamento de dados pessoais de crianças, as informações devem ser fornecidas de maneira simples, clara e acessível, considerando as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do público-alvo. As empresas poderão empregar recursos audiovisuais ou afins para passar as informações pertinentes. Dessa forma, além do fornecimento de informações aos pais ou ao responsável legal, que deverá consentir com o tratamento, será possível proporcionar um adequado entendimento à criança (BRASIL, 2018).

Confirmação e acesso aos dados pessoais

A qualquer momento, o titular dos dados pessoais tem o direito de obter confirmação da existência de tratamento e acesso aos seus dados pessoais. Isso poderá se dar de duas formas:

- Em formato simplificado, caso a confirmação ou o acesso seja providenciado imediatamente;
- Por meio de uma declaração clara e completa, com indicação da origem dos dados, inexistência de registro, critérios utilizados e finalidade do tratamento, conforme o caso, no prazo de quinze dias a contar da data do requerimento do titular dos dados (BRASIL, 2018).

As informações deverão ser fornecidas por meio eletrônico ou de forma impressa, de acordo com a solicitação do titular. Adicionalmente, quando o tratamento de dados tiver fundamento no consentimento ou em contrato, o titular poderá solicitar cópia eletrônica integral dos seus dados pessoais.

Correção, anonimização, pseudonimização, bloqueio ou eliminação de dados pessoais

O titular dos dados poderá requerer a correção de dados que considere incompletos, inexatos ou desatualizados, bem como solicitar a anonimização, bloqueio ou eliminação de dados pessoais considerados como desnecessários, excessivos ou tratados em desconformidade com a LGPD.

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.

Ademais, no caso de dados tratados com o consentimento, o titular poderá solicitar a eliminação de quaisquer dados coletados, ressalvadas as hipóteses de guarda permitidas pela LGPD, o que inclui a guarda de dados especialmente para cumprimento de obrigação legal pelo controlador ou para uso exclusivo do controlador, sendo que, neste último caso, os dados deverão ser anonimizados (BRASIL, 2018).

Caso a empresa tenha realizado uso compartilhado de dados cuja correção, anonimização, bloqueio ou eliminação fora requisitado pelo titular, a empresa deverá informar de maneira imediata tal providência aos demais agentes de tratamento de modo que repitam o procedimento.

Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratadas exclusivamente dentro do órgão e estritamente para a realização de estudos e pesquisas e mantidas em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas.

Para fins de atendimento dessa regra, pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

Portabilidade dos dados pessoais

A LGPD instituiu o direito de portabilidade, pelo qual o titular dos dados poderá, mediante requisição expressa, solicitar a transferência de seus dados pessoais a outro fornecedor de serviço ou produto.

Além disso, o titular dos dados também poderá requisitar a revisão, por pessoa natural, de decisões tomadas unicamente com base em tratamento automatizado, inclusive decisões destinadas à formação de perfis. O titular dos dados ainda poderá solicitar a disponibilização de informações claras e adequadas a respeito dos critérios

e dos procedimentos utilizados para formação da decisão automatizada (RAMOS; GOMES, 2019).

Caso não seja possível cumprir de imediato a providência requerida pelo titular dos dados, o controlador deverá enviar ao titular uma justificativa com as razões que impediram o cumprimento imediato do direito exercido ou uma comunicação para indicar que não é o agente de tratamento dos dados e, caso tenha conhecimento, apontar quem é o agente de fato (BRASIL, 2018).

Obrigações Previstas

Dentre as obrigações previstas na LGPD, o controlador deve:

- Provar que o consentimento foi obtido em conformidade com a LGPD;
- Manter registro das operações de tratamento de dados pessoais que realizar;
- Mediante solicitação da ANPD; elaborar relatório de impacto à proteção de dados;
- Informar o titular caso haja alguma alteração na finalidade para a coleta de dados;
- Responder solidariamente, em conjunto com o operador, se causar a terceiros danos por violação da LGPD (BRASIL, 2018);
- Adotar medidas técnicas que garantam o tratamento de dados de forma segura;
- Desenvolver processos internos e criar políticas que permitam realizar a criação e manutenção de registros das operações de tratamento de dados (BRASIL, 2018);
- Conservar os dados visando atender a finalidade pela qual foram coletados e para cumprir com obrigações legais e regulatórias. Nomear o encarregado pelo tratamento dos dados pessoais (BRASIL, 2018).

Do mesmo modo, cabe ao controlador tomar as decisões acerca do tratamento de dados pessoais, bem como zelar por sua conservação e atender aos requisitos e exigências formulados pelas autoridades.

Neste sentido, a LGPD impõe ao controlador as seguintes responsabilidades:

- Provar que o consentimento foi obtido em conformidade com a lei;
- Confirmar a existência ou providenciar o acesso a dados pessoais, mediante requisição do titular, em formato simplificado, imediatamente, ou por meio de uma declaração clara e completa, que indique a origem dos dados, a

inexistência de registro, os critérios utilizados e a finalidade do tratamento, fornecida no prazo de até 15 dias;

- Manter registro das operações de tratamento de dados pessoais que realize, podendo a autoridade nacional determinar que seja elaborado um relatório de impacto à proteção de dados (pessoais ou sensíveis) referente às suas operações (DONEDA, 2011).

Caso a autoridade faça essa requisição, o controlador não pode esquecer de inserir no relatório, no mínimo, as seguintes informações: descrição dos tipos de dados coletados; metodologia utilizada para a coleta de dados; metodologia utilizada para garantir a segurança das informações; análise do controlador com relação a essas medidas, salvaguardas e mecanismos de mitigação de riscos adotados (BRASIL, 2018).

O controlador também é responsável por indicar quem é o encarregado pelo tratamento dos dados pessoais, divulgando publicamente, de forma clara e objetiva, preferencialmente no seu sítio eletrônico, a identidade da pessoa e suas informações de contato (RAMOS; GOMES, 2019). Em linhas gerais, as atividades do encarregado consistem em:

- Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
- Receber comunicações da autoridade nacional e adotar providências;
- Orientar os funcionários e os contratados da organização a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;
- Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares emitidas pela ANPD (BRASIL, 2018).

Nas hipóteses em que o consentimento for exigido, o controlador deverá informar o titular caso haja alguma alteração na finalidade para a coleta de dados. Nesse momento, o titular poderá optar por renovar o consentimento ou revogá-lo.

Caso não haja consentimento do titular, o controlador somente poderá fundamentar o tratamento de dados pessoais se atestar finalidade legítima para tanto. Com relação a essa exigência, somente dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados, e deverão ser adotadas medidas que garantam sua transparência.

O controlador que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para tanto, exceto em caso de o titular dos dados tê-los tornado manifestamente públicos. O controlador responde solidariamente com o operador se, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à LGPD.

É facultado ao controlador formular regras de boas práticas e de governança que estipulem condições de organização, procedimentos, normas de segurança, padrões técnicos, obrigações específicas, mecanismos internos de supervisão e mitigação de riscos, bem como outros aspectos relacionados ao tratamento de dados pessoais, desde que respeitadas suas competências.

É permitida a conservação de dados pelo controlador quando encerrado o período de tratamento para que seja possível cumprir com as obrigações legais e regulatórias. O controlador também pode fazer uso exclusivo desses dados, desde que anonimizados, sendo seu acesso por terceiros expressamente vedado na lei.

A LGPD se aplica a qualquer operação de tratamento de dados, independentemente do país de sua sede ou do país onde estejam localizados os dados. A Lei determina expressamente as hipóteses em que é permitida a transferência internacional de dados, quais sejam:

- Para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto na lei;
- Quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos na Lei, através de cláusulas contratuais específicas para determinada transferência, cláusulas-padrão contratuais, normas corporativas globais ou selos, certificados e códigos de conduta regularmente emitidos;
- Quando a transferência for necessária para cooperação jurídica internacional entre órgãos públicos de inteligência, investigação e persecução, observados os instrumentos de direito internacional, ou quando for resultado de compromisso assumido em acordo de cooperação internacional;
- Quando autorizada a transferência pela ANPD;
- Quando a transferência for necessária para executar políticas públicas ou atribuições legais do serviço público;

- Quando o titular fornecer seu consentimento específico e em destaque para a transferência, tendo sido fornecida informação prévia e distinta de outras finalidades sobre o caráter internacional da operação;
- Quando necessário para cumprimento de obrigação legal ou regulatória pelo controlador;
- Para execução de contrato ou procedimentos relacionados ao contrato do qual seja parte o titular, desde que requerido pelo próprio titular;
- Para exercício regular de direitos em processo judicial, administrativo ou arbitral. Não obstante, o nível de proteção dos dados do país estrangeiro ou do organismo internacional será avaliado pela ANPD que observará, dentre outras hipóteses, a adoção de medidas de segurança, a natureza dos dados e as normas gerais vigentes no país de destino ou no organismo internacional.

Controlador e operador são os agentes de tratamento de dados pessoais, devendo manter registro das operações de tratamento que realizarem, especialmente quando baseadas em legítimo interesse (art. 37).

O operador deve realizar o tratamento de dados de acordo com as instruções fornecidas pelo controlador (art. 39).

O controlador deve indicar encarregado pelo tratamento de dados pessoais (art. 41), observando os seguintes aspectos:

- Deve ser pessoa natural que atue como canal de comunicação entre o controlador e a autoridade competente e os titulares;
- A identidade e as informações de contato do encarregado devem ser públicas, claras e objetivas, de preferência no site do controlador (art. 41, §1º); e o encarregado deverá receber reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências, receber comunicações das autoridades competentes, orientar funcionários e contratados do operador acerca das práticas a serem adotadas em relação à proteção de dados, entre outras atividades que venham a ser estabelecidas pelas autoridades competentes (art. 41, §2º) (BRASIL, 2018).

3.2.1 Encarregado de dados ou *data protection officer* (DPO)

Diante da universalidade de dados pessoais existentes no mundo virtual, e das novas consequências impactantes na sociedade, foi necessário a criação de legislações específicas sobre o tema. Nesse panorama, a LGPD, Lei n.º 13.709/2018, foi promulgada no Brasil. Com isso surgiram novos desafios, especialmente para quem manuseia dados pessoais, a exemplo das empresas privadas.

A LGPD insere a figura do encarregado de dados, que corresponde ao *data protection officer* (DPO) presente na GDPR. O encarregado de dados 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 a instituição pública ou privada (BRASIL, 2018).

A identidade do encarregado e a forma de comunicação deverão ser publicadas no site do controlador de maneira clara e objetiva, com a finalidade de facilitar requisições e comunicados dos titulares dos dados e da autoridade nacional. Inicialmente, as atividades do encarregado consistirão em receber reclamações e requisições dos titulares de dados, além de interagir com ANPD (BIONI, 2019).

Dentre suas funções estão orientar funcionários e prestadores de serviço acerca das boas práticas, e adotar providências necessárias de proteção de dados manipulados. É fundamental que o encarregado tenha conhecimento, e possa acompanhar e se envolver com todos os fluxos de processos realizados dentro da empresa controladora, bem como auxiliar diretamente no desenvolvimento de produtos e serviços, na elaboração de termos de consentimento, no processo de anonimização dos dados armazenados em bancos de dados, entre outros, de maneira que possa supervisionar todas as práticas de tratamento de dados, e certificar se estão em *compliance* com a LGPD (BRASIL, 2018).

Além disso, a autoridade de proteção de dados poderá através de normas complementares incluir novas atribuições ao encarregado, bem como definir sobre as hipóteses de dispensa da necessidade de sua indicação, conforme o tamanho e a natureza da empresa, e ou volume de tratamento de dados.

Em linhas gerais, o encarregado pela proteção de dados dentro das empresas controladoras deverá ser um profissional especializado em legislação de proteção de

dados, tecnologia da informação (especialmente criptografia), e gestão de processos; que desempenha um papel muito importante dentro das empresas a partir da vigência da LGPD, e está capacitado a agir em prol do cumprimento da lei.

Para a instituição do programa de integridade, além da observância dos princípios que protegem direitos fundamentais, é necessário ter boa governança corporativa, fazer a correta gestão dos riscos, possuir uma boa estrutura tecnológica de segurança da informação e capacitar adequadamente as equipes de funcionários.

A aplicação da LGPD no dia a dia do negócio envolverá a área de *compliance* das empresas. A lei detalha como, quando os dados pessoais devem ser tratados, e especialmente o porquê, pois determina dez princípios que justificam o tratamento de dados pessoais.

Salema (2020) define *compliance* como o termo utilizado para expressar o alinhamento do negócio com normas internas e externas, políticas e diretrizes para assegurar os padrões que o mercado exige. É o conjunto de atividades que assegura o cumprimento das regras trabalhistas, fiscal, contábil, financeira, ambiental, jurídica, previdenciária e ética.

Sendo o *compliance* um programa para garantir o cumprimento das normas, deverá absorver as normativas indicadas pela nova legislação. Entretanto no contexto dos pequenos negócios, a figura do DPO poderá representar o *compliance*, já que, assim como observado na GDPR, trata-se de um profissional com conhecimento em *compliance*, risco, governança, direito e tecnologia (SALEMA, 2020; BIONI, 2019; BRANCO, 2020).

3.2.2 Agência nacional de proteção de dados (ANPD)

No dia 29 de maio de 2019, o senado federal aprovou a medida provisória nº. 869/2018, que alterou a LGPD e criou a Autoridade Nacional de Proteção de Dados (ANPD) (BEZERRA, 2019).

O projeto de lei da câmara (PLC nº. 53/2018) previa a existência de uma autoridade para a proteção de dados, que seria um órgão da administração direta, vinculado ao Ministério da Justiça. No entanto, durante a tramitação no congresso, visando a adequação aos modelos internacionais, a natureza jurídica do órgão foi

modificada, transformando-o em uma autarquia da administração indireta, com todas as características de uma agência reguladora (BEZERRA, 2019).

Em razão dessa transformação, ao sancionar a lei nº 13.709/2018, o então presidente Michel Temer vetou a criação da autoridade nacional, alegando vício de inconstitucionalidade formal.

4. MÉTODO

Este capítulo aborda a metodologia adotada para realizar a pesquisa. No subcapítulo 4.1 é feita uma justificativa do método e das técnicas utilizadas, no subcapítulo 4.2 são apresentadas algumas definições operacionais, e no subcapítulo 4.3 são discutidos o universo populacional e amostral. No subcapítulo 4.4 são apresentadas as formas de obtenção dos dados, no item 4.5 demonstra-se a forma de tabulação, e no item 4.6, a operacionalização da pesquisa. Por fim, são apresentadas as limitações desta pesquisa no item 4.7.

4.1 Justificativa do método e das técnicas utilizadas

Esta pesquisa é qualitativa e quantitativa, isto é, de métodos mistos (ou, quali-quantitativa), do tipo exploratória, uma vez que esta dissertação tem o objetivo de explorar e descrever o objeto estudado. A abordagem escolhida é a fenomenológica, buscando-se por meio dela ferramentas que auxiliem na compreensão do objeto a ser estudado. Para complementar o estudo, foi também realizada uma pesquisa bibliográfica a fim de identificar o estado da arte sobre o tema na literatura.

O uso de métodos mistos é vantajoso pois permite uma visão ampla do objeto ou fenômeno estudado, já que o pesquisador pode extrair informações valiosas de ambas as abordagens (quantitativa e qualitativa). Nesse caso, o fenômeno estudado é recente e, portanto, quanto mais informações houver, mais rica será a descrição do estudo (CRESWELL, 2010).

Para tanto, a triangulação concomitante foi adotada para a coleta de dados. Segundo Creswell:

> Em uma abordagem de triangulação concomitante, o pesquisador coleta concomitantemente os dados quantitativos e os qualitativos e depois compara os dois bancos de dados para determinar se há convergência, diferenças ou alguma combinação (CRESWELL, 2010, p. 250).

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, 2017a, p. 64).

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.

Para o levantamento dos dados necessários para o desenvolvimento desta pesquisa, optou-se pela utilização do questionário, devido à vantagem dessa técnica relativa ao tempo, como mencionado a seguir:

> Evidentemente, esse tipo de instrumento de pesquisa oferece a vantagem da economia de custo, de tempo, bem como pode atingir um grande número de pessoas e proporcionar menor risco de interferência do pesquisador nas respostas dos pesquisados, mas suas desvantagens também são consideráveis: pequeno percentual de respostas (devolução do questionário preenchido), perguntas sem resposta, interferência de terceiros no preenchimento do questionário, falta de compreensão de alguma pergunta por parte do respondente (MARCONI, LAKATOS, 2017, p. 322).

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.

Gil (2017) define o questionário como a técnica de investigação na qual um conjunto de questões é submetido a pessoas com o propósito de obter informações. Diferente de Marconi e Lakatos, Gil ressalta como uma das principais desvantagens dos questionários a exclusão dos analfabetos, que poderia causar deformações nos resultados da investigação. Entretanto, essa consideração se torna irrelevante quando se considera o objeto e objetivo da pesquisa, dado a escolha do seu público alvo.

4.2 Definições operacionais da pesquisa

Abaixo são apresentadas algumas definições operacionais importantes para esta pesquisa.

Boas práticas: boa prática consiste em uma(s) técnica(s) identificada(s) e experimentada(s) como eficiente(s) e eficaz(es) em seu contexto de implantação, para a realização de determinada tarefa, atividade ou procedimento, ou ainda, em uma perspectiva mais ampla, para a realização de um conjunto destes, visando o alcance de um objetivo comum.

***Backup*:** em informática trata-se da cópia de segurança de dados de um dispositivo a outro para que possam ser restaurados em caso de perda dos dados originais.

Contratos jurídicos: o contrato é formado pela vontade das partes, deve ser composto por uma ou mais parte interessada, no qual se estabelecem as cláusulas que criam, extinguem ou modificam o direito.

Controlador: é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

Dados pessoais: o conceito de dado pessoal é bastante abrangente, sendo definido como a informação relacionada à pessoa identificada ou identificável. Isso quer dizer que um dado é considerado pessoal quando ele permite a identificação, direta ou indireta, da pessoa natural por trás dele, como por exemplo: nome, sobrenome, data de nascimento, documentos pessoais (como CPF, RG, CNH, carteira de trabalho, passaporte e título de eleitor), endereço residencial ou comercial, telefone, e-mail, *cookies* e endereço IP.

Dados pessoais sensíveis: dados pessoais que revelem a origem racial ou étnica; opiniões políticas e convicções religiosas ou filosóficas; filiação sindical; dados genéticos, ou dados biométricos tratados simplesmente para identificar um ser humano; dados relacionados à saúde; dados relativos à vida sexual ou orientação sexual da pessoa.

DPO: sigla para *data protection officer*. O DPO é o profissional encarregado de cuidar das questões referentes à proteção dos dados da organização e de seus clientes, de acordo com a GDPR.

Encarregado de dados: similar ao DPO, é o profissional responsável por tratar das questões de proteção de dados dos clientes, conforme descrito na LGPD.

Funcionário: é quem exerce e desempenha funções. É aquele com ocupação permanente e retribuída; empregado.

GDPR: significa *general data protection regulation* (regulamento geral de proteção de dados, em tradução livre), um novo conjunto de regras de privacidade.

Incidentes de dados pessoais: uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.

LGPD: é a sigla para Lei Geral de Proteção de Dados, Lei Federal n°. 13.709/2018, sancionada em agosto de 2018, que entrará em vigor em 2020. A LGPD estabelece regras sobre coleta, armazenamento, tratamento e compartilhamento de dados pessoais, impondo mais proteção e penalidades para o não cumprimento.

MPEs: micro e pequenas empresas.

Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

Término do tratamento: é o evento que determina o encerramento do tratamento e o descarte dos dados utilizados.

Titular: pessoa natural a quem se referem os dados pessoais.

Tratamento: toda operação realizada com dados pessoais, como a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

4.3 População e amostra

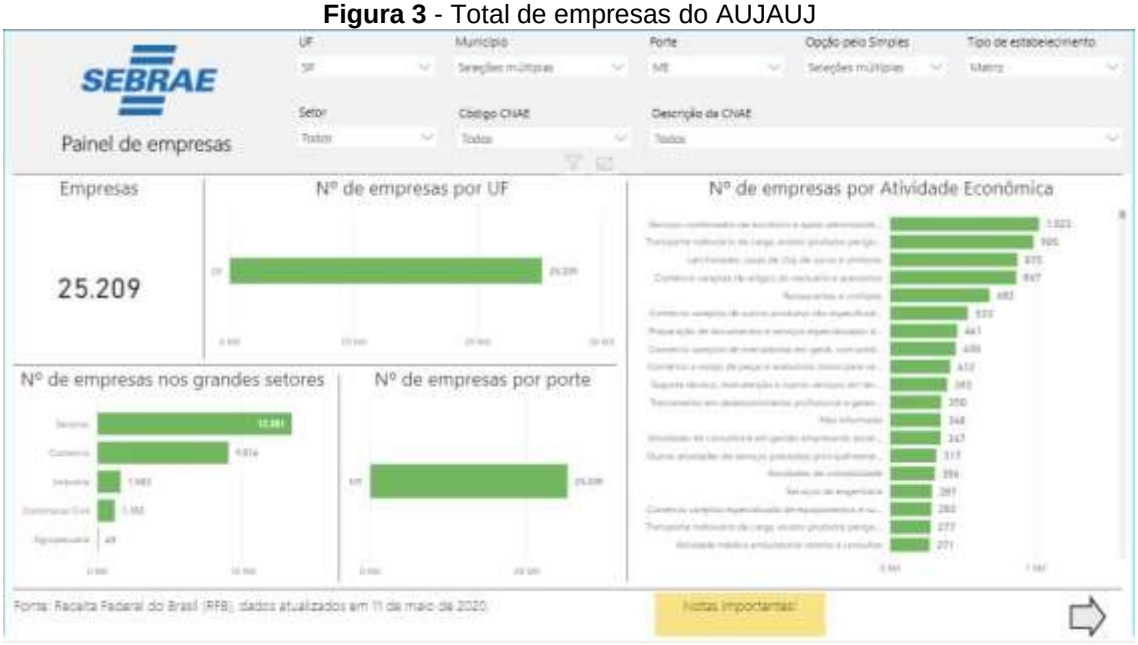
O universo populacional é composto de MPEs da Aglomeração Urbana de Jundiaí (AUJ), que, devido ao seu relacionamento com clientes, fazem uso de dados pessoais.

A lista das MPEs foi obtida em diversos órgãos da região estudada, como na Associação Comercial e Empresarial de Jundiaí (http://www.acejundiai.com.br/), no Sindicato do Comércio Varejista de Jundiaí e Região (http://www.sincomerciojundiai.com.br/), na Prefeitura de Jundiaí (http://www2.jundiai.sp.gov.br/), e nas Associações Comerciais de Jundiaí e de outros

municípios da região, especialmente os que constituem a AUJ: Jundiaí, Várzea Paulista, Campo Limpo Paulista, Jarinu, Louveira, Itupeva e Cabreúva.

No portal DataSebrae (2020), estão disponíveis informações das empresas brasileiras. Na Figura 3, é possível visualizar o *output* dos dados a partir do filtro de cidades que incluem o AUJ/AUJ. Estima-se que em 2020 estejam registradas um total de 25.209 MPEs.

Figura 3 - Total de empresas do AUJAUJ



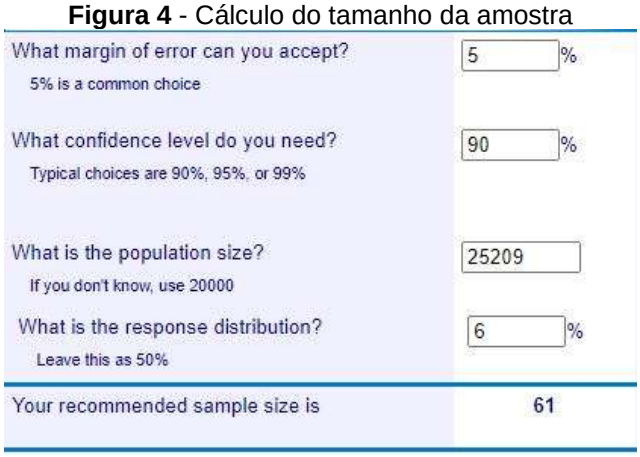
Fonte: DataSebrae, 2020

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.

Para realizar o cálculo, foi utilizado o *software Sample Size*. Na Figura 4, pode-se observar os dados imputados retirados do portal DataSebrae, em consonância com a Figura 3.

Figura 4 - Cálculo do tamanho da amostra



Fonte: Raosoft, 2004

Para selecionar os respondentes, foi constituída uma lista das MPEs na AUJ cujas atividades solicitem coleta de dados pessoais.

4.4 Obtenção dos dados

A coleta de dados foi realizada por meio de um questionário adaptado, com base em cinco diagnósticos/questionários utilizados por escritórios de direito digital e empresas que oferecem serviços e produtos para adequação da LGDP. O questionário foi construído com uma linguagem mais acessível, considerando os diferentes níveis de conhecimentos dos respondentes sobre o assunto, e visando também diminuir o enviesamento da pesquisa por falta de entendimento da questão.

O conteúdo original dos questionários está no Anexo A. Para fins da presente pesquisa, tal questionário foi modificado. Para realizar as alterações e adequações, foi feita uma consulta a três especialistas.

Os especialistas receberam o questionário integral exibido no Anexo A e foram solicitados a realizar a atividade descrita abaixo:

Prezado Senhor: Abaixo segue uma lista de questões que serão apresentadas aos responsáveis pelas pequenas e micro empresas com o intuito de fazer um diagnóstico em relação à LGPD que entrará em vigor em agosto do corrente ano.

Na coluna "Excluir?" ao lado, para cada linha exprima sua recomendação de excluir a questão usando:

<em branco> : permanecer

SIM = acredito que é necessária

NÃO = excluir

O resultado da consulta é visto na Tabela 1. Foram excluídas as questões nas quais os especialistas indicaram NÃO, e foram selecionadas para o pré-teste apenas as questões em que todos os especialistas marcaram SIM. Na Tabela 1, pode-se observar as respostas dos especialistas organizadas por colunas, indicando quais questões (linhas) faziam sentido para a construção do questionário.

Tabela 1 - Resultado da pesquisa com especialistas

1	Questões sobre LGPD de fontes diversas	opções de resposta A	opções de resposta B	Opções de resposta C	Especialista 1	Especialista 2	Especialista 3	Perguntas selecionadas
2								
3	A empresa possui atividades de marketing direcionado a pessoas físicas?*	Sim	Não		S	S	N	
4	A empresa possui certificações ISO ou similares?*	ISO	ITIL	PMI	S	S	S	S
5	A empresa possui contrato com empresas de DBM (Database Marketing) e CRM (Customer Relationship Management)?*	Sim	Não		S	S	S	S
6	A empresa possui contrato com plataforma de recrutamento ou headhunter?*	Sim	Não		S	S	S	S
7	A empresa possui documentação de processos internos?*	sim	não			S	S	
8	A empresa possui site que coleta cookies?*	Sim	Não		S	S	S	S
9	A empresa terceiriza sua folha de pagamentos?*	Sim	Não		S	S	S	S

Fonte: elaborado pela autora

Desta forma, o questionário foi construído a partir das questões selecionadas pelos especialistas. Após a aplicação do pré-teste, percebeu-se a necessidade de agrupar e reescrever algumas perguntas por conta da similaridade do conteúdo. Na Figura 5, é possível observar a estrutura lógica da ferramenta. O questionário foi organizado em três diferentes seções: seção 1, com informações gerais do respondente (questões de 1 a 10); seção 2, com perguntas relacionadas à proteção de dados (questões de 11 a 22); e, seção 3, com questões relacionadas à LGPD (questões de 23 a 32). O questionário completo encontra-se disponível no Apêndice.

Figura 5 - Estrutura lógica do questionário aplicado

Fonte: Elaborada pela autora, 2020

A partir da lista de empresas levantadas, foi criado um *mailing* para envio do questionário para todas as MPEs que, potencialmente, poderiam representar o público alvo pesquisado.

Para realizar o contato com os respondentes, foi elaborada uma mensagem padrão (Figura 6). Para essa etapa de distribuição do questionário foram utilizadas as seguintes ferramentas: correio eletrônico Gmail para distribuição, e o *software* YAMM (https://yet-another-mail-merge.com/) para acompanhamento dos e-mails enviados com o convite para a pesquisa.

Figura 6 - Modelo da mensagem de e-mail

Olá tudo bem?
Me chamo Talita Langen sou mestranda do programa em Administração de Empresas da UNIFACCAMP e gostaria da sua ajuda para responder a minha pesquisa. A pesquisa é anônima e são apenas 3 minutos para responder! Você pode acessar o questionário aqui

Você deve estar se perguntando, o que esta Lei tem a ver com o meu negócio? É muito importante que você conheça as exigências desta nova lei que tem por objetivo regulamentar a proteção dos dados pessoais de clientes e funcionários e isso pode impactar diretamente a sua empresa. A câmara revogou recentemente a decisão de postergar a aplicação da LGPD (LGPD LEI Nº 13.709, DE 14 DE AGOSTO DE 2018.) para 2021.
Espero que com isso possamos nos ajudar.

Você pode acessar o questionário aqui

Atenciosamente,
Talita S.C.Langen.
Bibliotecária e Mestranda em Administração.
Currículo lattes
Linkedin

Fonte: Elaborada pela autora, 2020

4.5 Tabulação dos dados

Os dados coletados pelo questionário foram tabulados usando uma coluna por respondente, como ilustra a Tabela 2. A tabulação exibida é parcial e destina-se a mostrar que para cada respondente há uma coluna com variáveis *dummy* mostrando a sua escolha. Variáveis *dummy* são variáveis binárias (0 ou 1) criadas para representar uma variável com duas ou mais categorias. Em caso de variável com três ou mais categorias, como ocorre em algumas questões da pesquisa desta dissertação, é necessário criar *n-1 dummies*.

Tabela 2 - Exemplo de tabulação dos dados coletados

Pergunta	**R1**	**R2**	**R8**	**R12**	**R14**	**R15**	**R16**	**R18**
Quantos funcionários a empresa possui?	1	4	1	4	1	2	2	2
Qual é a sua idade?	5	2	1	2	4	4	5	4
Qual o seu sexo?	1	2	1	2	2	1	1	2
Qual o seu grau de instrução?	4	4	1	4	3	3	2	1
Qual o seu cargo?	5	4	5	3	5	5	5	1
Qual o seu principal tipo de cliente?	2	2	2	3	2	1	1	1
Sua empresa coleta dados pessoais de quais públicos?	2	2	2	3	2	1	3	1
Qual o ramo de atuação do seu negócio?	3	3	3	3	1	3	2	2
A empresa é associada a algum tipo de organização, sindicato ou associação?	1	1	0	0	1	0	0	0
Quais os tipos de dados pessoais são tratados pela sua empresa?	2	1	1	5	1	4	1	1
A sua empresa utiliza serviços de *customer relationship management* (CRM), tais como disparadores de e-mail, sms, telemarketing, etc?	0	1	0	1	0	0	1	0
A empresa possui contrato com serviços de recrutamento e seleção ?	1	0	0	0	0	0	0	0
A sua empresa terceiriza sua folha de pagamentos?	0	0	0	0	0	1	1	0
A empresa possui site que coleta cookies?	1	2	0	1	2	0	0	0
A empresa possui certificações ISO ou similares?	0	0	0	2	0	0	0	2
A empresa possui políticas de segurança da informação documentadas (por ex: manuais, memorandos, termos, etc...)?	1	0	0	1	1	1	1	0
É permitido que os colaboradores utilizem dispositivos pessoais para realizar suas atividades de trabalho ou que levem dispositivos da empresa para locais externos?	0	1	0	1	0	1	0	0
Em algum momento são coletados dados biométricos (ex: reconhecimento facial, voz, digital, etc) de funcionários ou clientes?	0	0	0	0	0	1	0	0
Quais mecanismos de segurança da informação a empresa utiliza em seu ambiente?	11	3	32	63	1	3	3	1

Sua empresa realiza *backup* dos dados (cópia de segurança) ? Se sim, indique o modo como os *backups* são armazenados.	2	1	0	2	2	1	4	1

Fonte: Elaborada pela autora, 2020

Como mostra a Tabela 2, 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.

Essa tabulação possibilita a obtenção de dados para análise, como mostra a Tabela 3. Por exemplo, para o fator Dados Pessoais, o total de respostas afirmativas (“uns”) subiu de nove para 68.

Tabela 3 - Exemplo de disposição de dados para análise

Pergunta	**Fator**	**Zeros**	**Uns**	**Dois**	**Três**	**Quatros**	**Cincos**	**Total**
Quantos funcionários a empresa possui?		0	44	10	5	9	0	**68**
Qual é a sua idade?		0	5	21	21	13	8	**68**
Qual o seu sexo?		0	43	25	0	0	0	**68**
Qual o seu grau de instrução?		0	7	5	26	30	0	**68**
Qual o seu cargo?		0	4	2	5	7	50	**68**
Qual o seu principal tipo de cliente?		0	22	31	15	0	0	**68**
Sua empresa coleta dados pessoais de quais públicos?	Dados pessoais	0	9	29	30	0	0	**68**
Qual o ramo de atuação do seu negócio?		0	21	5	35	0	7	**68**
A empresa é associada a algum tipo de organização, sindicato ou associação?		41	27	0	0	0	0	**68**

Fonte: Elaborado pela autora, 2020

4.6 Operacionalização da pesquisa

A pesquisa foi operacionalizada da seguinte forma:

1. A lista de empresas contatadas foi constituída a partir de dados disponíveis *online* como da Receita Federal, entre outros. A delimitação se deu através da localização e porte das empresas, especialmente as que estão localizadas na AUJ: Jundiaí, Várzea Paulista, Campo Limpo Paulista, Jarinu, Louveira, Itupeva e Cabreúva.

2. Foram enviados e-mails com o questionário às empresas da lista, através das ferramentas Gmail e YAMM;

3. As respostam do questionário foram coletadas através ferramenta *survey monkey*.

4. Por meio dos mecanismos oferecidos na ferramenta *survey monkey*, foi possível excluir respostas que não pertenciam ao público pesquisado;

5. Os dados coletados foram transcritos para uma planilha, e verificou-se se os valores fornecidos eram consistentes com os dados tabulados. Em seguida, foram geradas duas planilhas: a primeira, com os dados fornecidos pelos 156 respondentes, e a segunda, com dados de 67 respondentes que se encaixavam no perfil delineado anteriormente.

6. Realizou-se a análise dos dados coletados e suas respectivas das conclusões.

4.7 Limitações da pesquisa

A presente pesquisa estudou as MPEs situadas na AUJ, localizada no Estado de São Paulo. Dada a situação epidemiológica imposta pelo COVID-19 no período de coleta de dados (maio a julho/2020), foi necessário realizar ajustes para consecução dos objetivos traçados anteriormente.

A proposta inicial era realizar a aplicação total ou parcial do questionário *in loco*, para poder realizar a observação e conversar com os respondentes, visando esclarecer eventuais dúvidas. Entretanto, por conta da pandemia do COVID-19, não foi possível, visto que as recomendações de isolamento social implicaram em restrições à sociedade.

A primeira coleta foi realizada utilizando o questionário da ABES (Associação Brasileira de Empresas de *Software*), tal qual disponível no site da ABES - Diagnóstico LGPD (ABES, 2019). Entretanto, o percentual de desistência foi elevado, pois foram obtidas apenas 14 respostas de um total de 700 e-mails enviados. Ao perceber a dificuldade na coleta de dados, foi necessário reestruturar esta etapa, criando um novo questionário e excluindo a possibilidade de aplicação presencial.

Parte-se da premissa de que as respostas dadas pelos participantes sejam verdadeiras.

5. ANÁLISE DOS RESULTADOS

Os resultados da pesquisa devem ser apresentados, segundo Vieira (2011), de forma sistemática, do geral para o particular, por meio de tabelas, quadros, gráficos e outros elementos de apresentação. Esse é o objetivo do presente capítulo. No subcapítulo 5.1 são apresentadas as respostas obtidas por meio do questionário aplicado, e no subcapítulo 5.2, os testes de hipóteses da pesquisa.

5.1 Respostas obtidas pelo questionário

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 (VIEIRA, 2011). 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.

A primeira seção do questionário permitiu explorar o perfil dos respondentes. 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.

Seção 1 do questionário

Como mencionado, 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, apresentada na Figura 7, 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.

Figura 7 - P1: Quantos funcionários a empresa possui?

OPÇÕES DE RESPOSTA	RESPOSTAS	
1 a 5 funcionários	41.03%	64
6 a 10 funcionários	8.33%	13
11 a 15 funcionários	3.85%	6
16 a 20 funcionários	8.97%	14
mais de 20 funcionários	37.82%	59
TOTAL		156

Fonte: Elaborada pela autora, 2020
Nota: Responderam: 77 Ignoraram: 0

Para o filtro 2, foi utilizado um conceito base da pesquisa, o uso de dados pessoais. Perguntou-se ao respondente de qual ou quais públicos a empresa coleta dados pessoais. Pode-se observar na Figura 8 que 19 empresas afirmaram não coletar nenhum dado pessoal, e 12 não sabem se coletam dados pessoais, o que indica 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.

Figura 8 - P8: Sua empresa coleta dados pessoais de quais públicos?

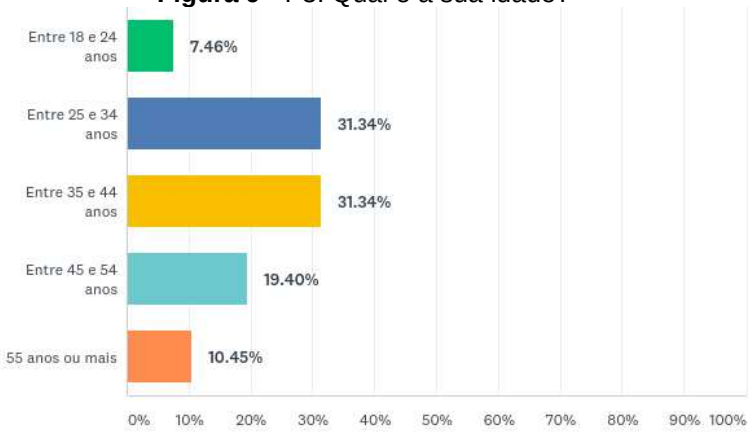
OPÇÕES DE RESPOSTA	RESPOSTAS	
Funcionários.	9.03%	14
Clientes.	29.68%	46
Ambos (funcionários e clientes)	41.29%	64
Nenhum	12.26%	19
Não sei.	7.74%	12
TOTAL		155

Fonte: Elaborada pela autora, 2020
Nota: Responderam: 76 Ignoraram: 1

Na questão 9, indicada na Figura 9, pode-se observar que entre os respondentes predominam indivíduos da geração Y. 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. Por essa razão, argumentam os autores, essas pessoas estão sempre em busca de novidades, são dotadas de criatividades e dinamismo, e não se limitam a conceitos pré-estabelecidos.

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 do paradigma da privacidade, essa geração vivenciou parte da privacidade analógica e digital.

Figura 9 - P3: Qual é a sua idade?



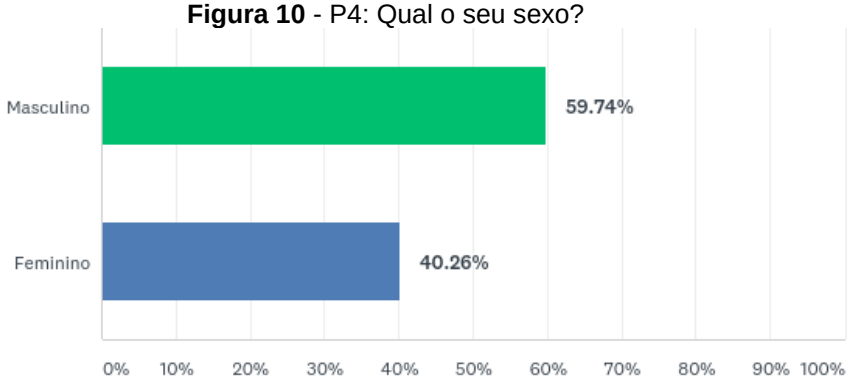
OPÇÕES DE RESPOSTA	RESPOSTAS	
Entre 18 e 24 anos (1)	6.49%	5
Entre 25 e 34 anos (2)	31.17%	24
Entre 35 e 44 anos (3)	29.87%	23
Entre 45 e 54 anos (4)	22.08%	17
55 anos ou mais (5)	10.39%	8
TOTAL		77

ESTATÍSTICAS BÁSICAS				
Mínimo	Máximo	Mediana	Média	Desvio padrão
1.00	5.00	3.00	2.99	1.10

Fonte: Elaborada pela autora, 2020
Nota: Responderam: 77 Ignoraram: 0

Os dados apresentados na Figura 10, derivados da pergunta 4, mostram que a maior parte da amostra é composta por respondentes do sexo masculino. Observa-se, ainda, uma diferença de quase 20% em relação ao gênero feminino.

Figura 10 - P4: Qual o seu sexo?



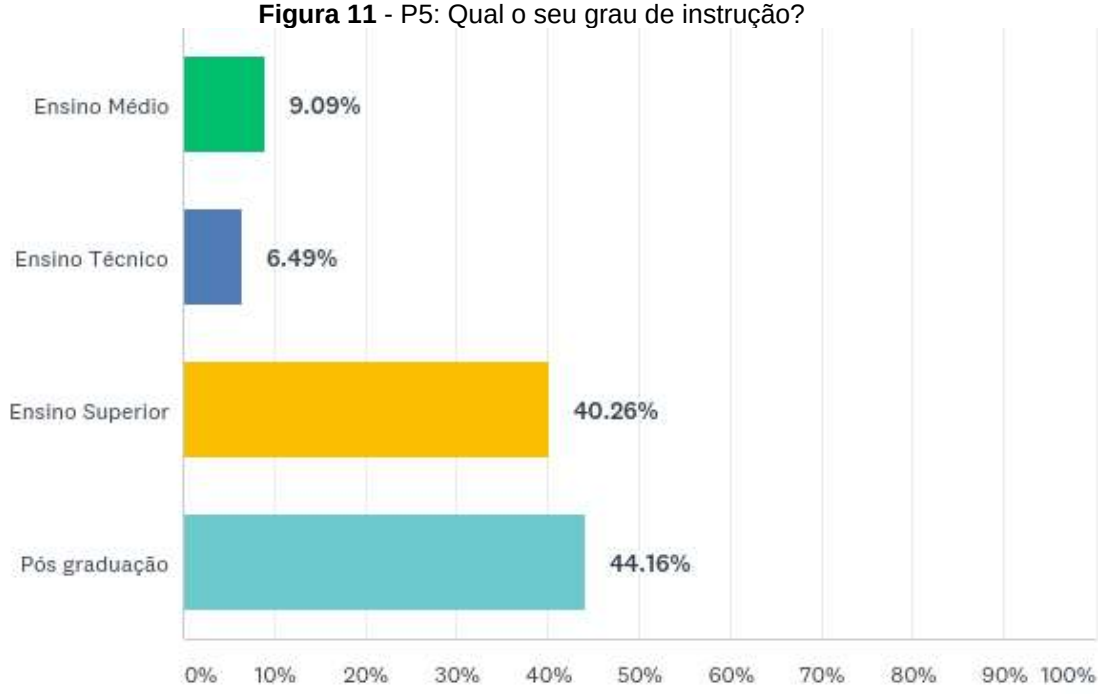
OPÇÕES DE RESPOSTA	RESPOSTAS	
Masculino (1)	59.74%	46
Feminino (2)	40.26%	31
TOTAL		77

ESTATÍSTICAS BÁSICAS				
Mínimo	Máximo	Mediana	Média	Desvio padrão
1.00	2.00	1.00	1.40	0.49

Fonte: Elaborada pela autora, 2020
Nota: Responderam: 77 Ignoraram: 0

Na Figura 11, constata-se 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%.

Figura 11 - P5: Qual o seu grau de instrução?



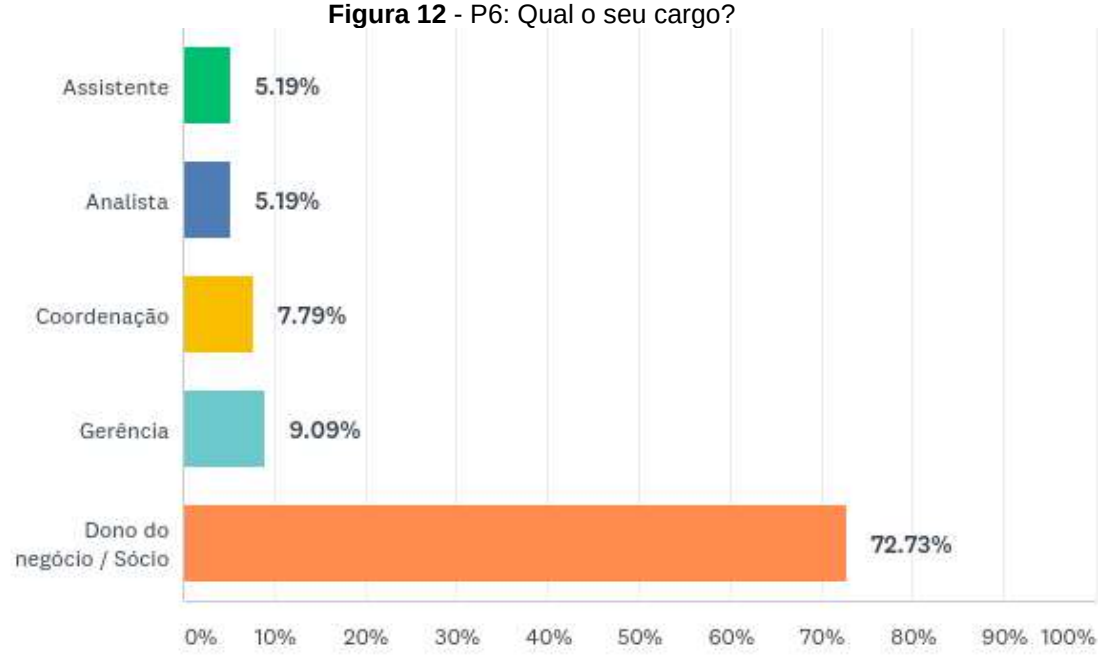
OPÇÕES DE RESPOSTA	RESPOSTAS	
Ensino Médio (1)	9.09%	7
Ensino Técnico (2)	6.49%	5
Ensino Superior (3)	40.26%	31
Pós graduação (4)	44.16%	34
TOTAL		77

ESTATÍSTICAS BÁSICAS				
Mínimo	Máximo	Mediana	Média	Desvio padrão
1.00	4.00	3.00	3.19	0.91

Fonte: Elaborada pela autora, 2020
Nota: Responderam: 77 Ignoraram: 0

A maioria dos respondentes é dona ou sócia das MPEs, como apresentado na Figura 12. Portanto, pode-se inferir que os principais processos dos negócios são conhecidos pelo respondente, o que aumenta a confiabilidade dos dados obtidos na pesquisa.

Figura 12 - P6: Qual o seu cargo?



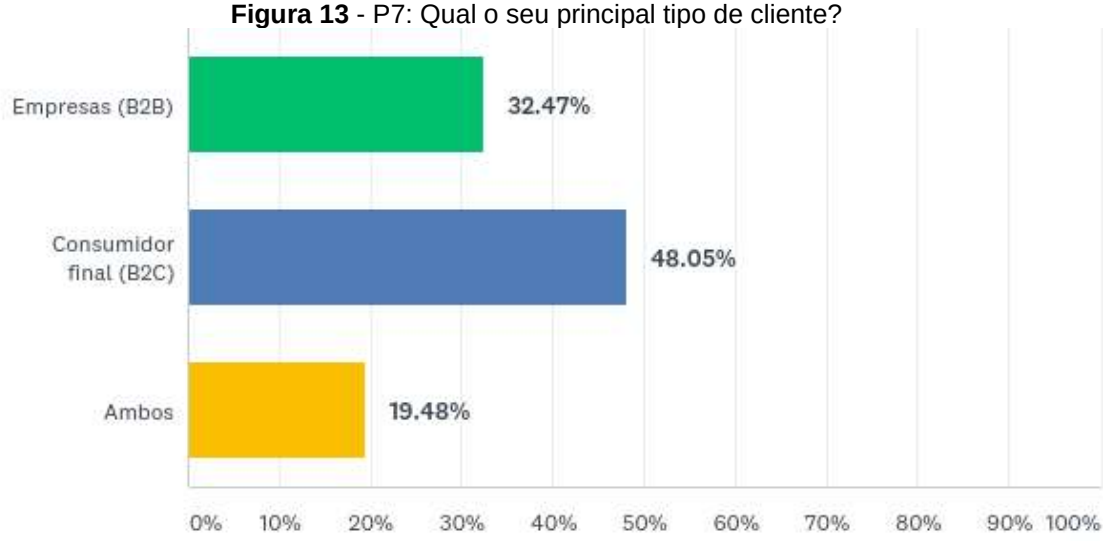
OPÇÕES DE RESPOSTA	RESPOSTAS	
Assistente (1)	5.19%	4
Analista (2)	5.19%	4
Coordenação (3)	7.79%	6
Gerência (4)	9.09%	7
Dono do negócio / Sócio (5)	72.73%	56
TOTAL		77

ESTATÍSTICAS BÁSICAS				
Mínimo	Máximo	Mediana	Média	Desvio padrão
1.00	5.00	5.00	4.39	1.15

Fonte: Elaborada pela autora, 2020
Nota: Responderam: 77 Ignoraram: 0

Na Figura 13, pode-se observar que o principal tipo de cliente dos respondentes é o consumidor final, ou seja, pessoas físicas. Isso indica uma tendência de a empresa procurar coletar dados pessoais, o que tende a diminuir no caso de B2B, em que os clientes são outras empresas.

Figura 13 - P7: Qual o seu principal tipo de cliente?



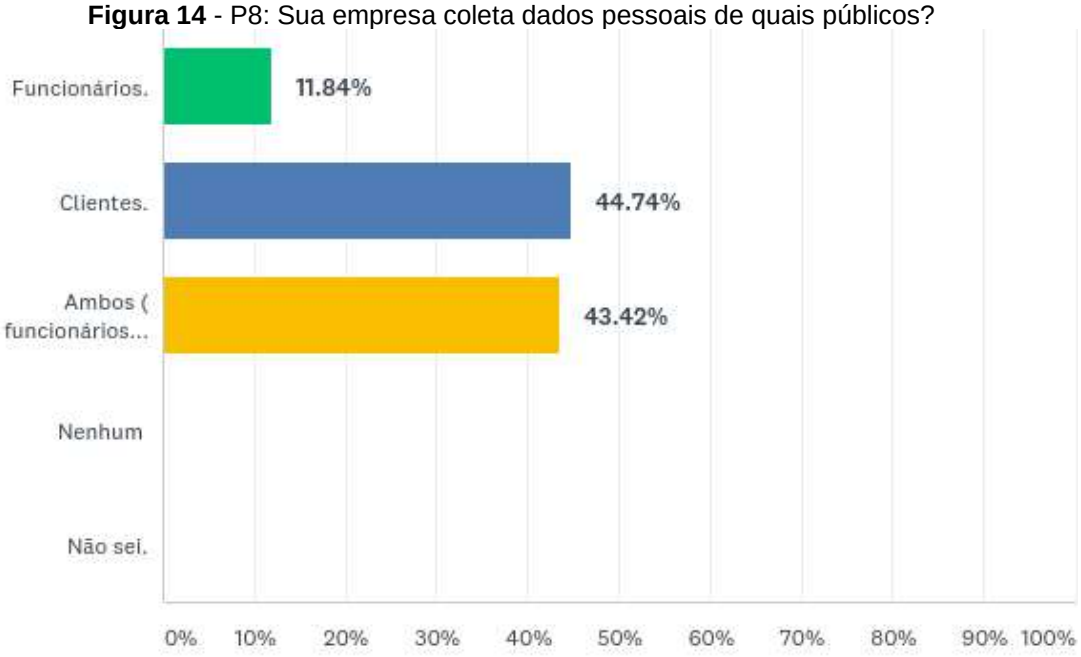
OPÇÕES DE RESPOSTA	RESPOSTAS	
Empresas (B2B) (1)	32.47%	25
Consumidor final (B2C) (2)	48.05%	37
Ambos (3)	19.48%	15
TOTAL		77

ESTATÍSTICAS BÁSICAS				
Mínimo	Máximo	Mediana	Média	Desvio padrão
1.00	3.00	2.00	1.87	0.71

Fonte: Elaborada pela autora, 2020
Nota: Responderam: 77 Ignoraram: 0

Os resultados apresentados na Figura 14 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 do seu público-alvo.

Figura 14 - P8: Sua empresa coleta dados pessoais de quais públicos?



OPÇÕES DE RESPOSTA	RESPOSTAS	
Funcionários. (1)	11.84%	9
Clientes. (2)	44.74%	34
Ambos (funcionários e clientes) (3)	43.42%	33
Nenhum (4)	0.00%	0
Não sei. (5)	0.00%	0
TOTAL		76

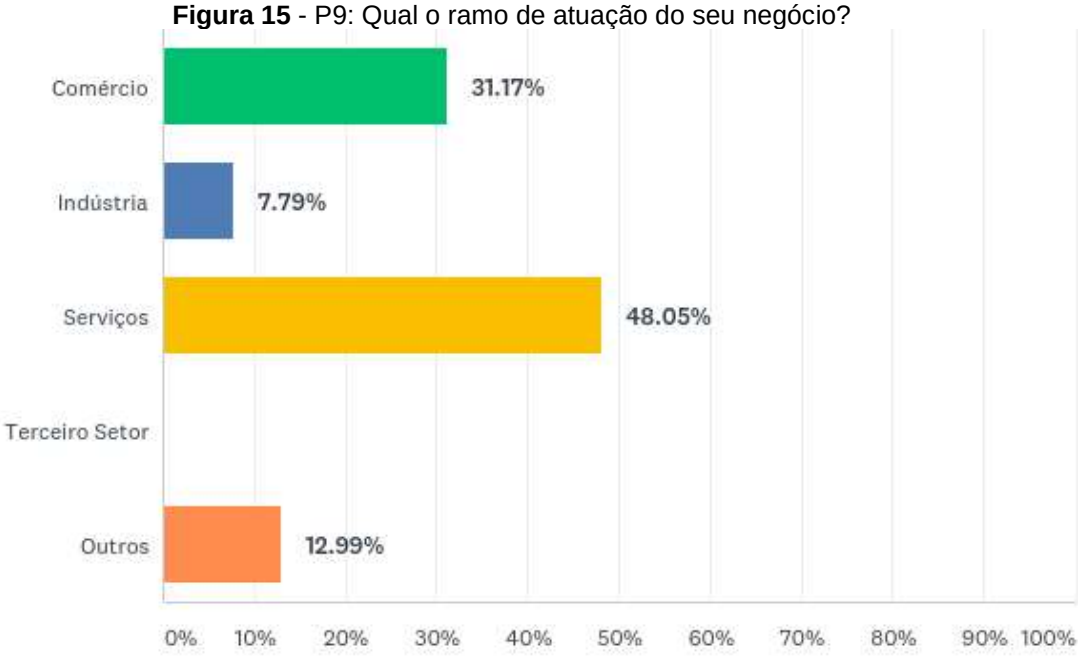
ESTATÍSTICAS BÁSICAS

Mínimo	Máximo	Mediana	Média	Desvio padrão
1.00	3.00	2.00	2.32	0.67

Fonte: Elaborada pela autora, 2020
Nota: Responderam: 76 Ignoraram: 1

A Figura 15 revela que 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.

Figura 15 - P9: Qual o ramo de atuação do seu negócio?



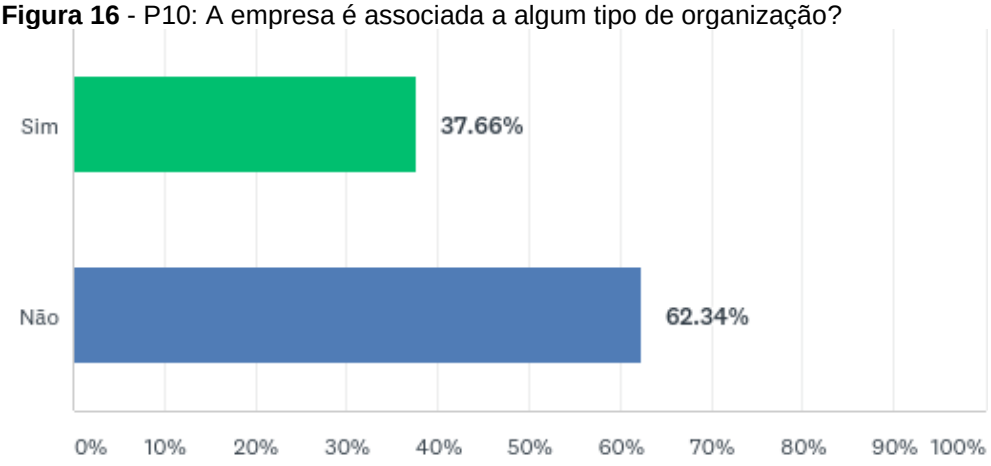
OPÇÕES DE RESPOSTA	RESPOSTAS	
Comércio (1)	31.17%	24
Indústria (2)	7.79%	6
Serviços (3)	48.05%	37
Terceiro Setor (4)	0.00%	0
Outros (5)	12.99%	10
TOTAL		77

ESTATÍSTICAS BÁSICAS				
Mínimo	Máximo	Mediana	Média	Desvio padrão
1.00	5.00	3.00	2.56	1.28

Fonte: Elaborada pela autora, 2020
Nota: Responderam: 77 Ignoraram: 0

As MPEs pesquisadas, em sua maioria, não estão fortemente ligadas a associações, como indicado na Figura 16. 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.

Figura 16 - P10: A empresa é associada a algum tipo de organização?



OPÇÕES DE RESPOSTA	RESPOSTAS	
Sim (1)	37.66%	29
Não (2)	62.34%	48
TOTAL		77

ESTATÍSTICAS BÁSICAS				
Mínimo	Máximo	Mediana	Média	Desvio padrão
1.00	2.00	2.00	1.62	0.48

Fonte: Elaborada pela autora, 2020
Nota: Responderam: 77 Ignoraram: 0

Com base nos dados apresentados na Seção 1, verifica-se que o perfil predominante do respondente é da geração Y, homens de 24 a 25 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 (B2C).

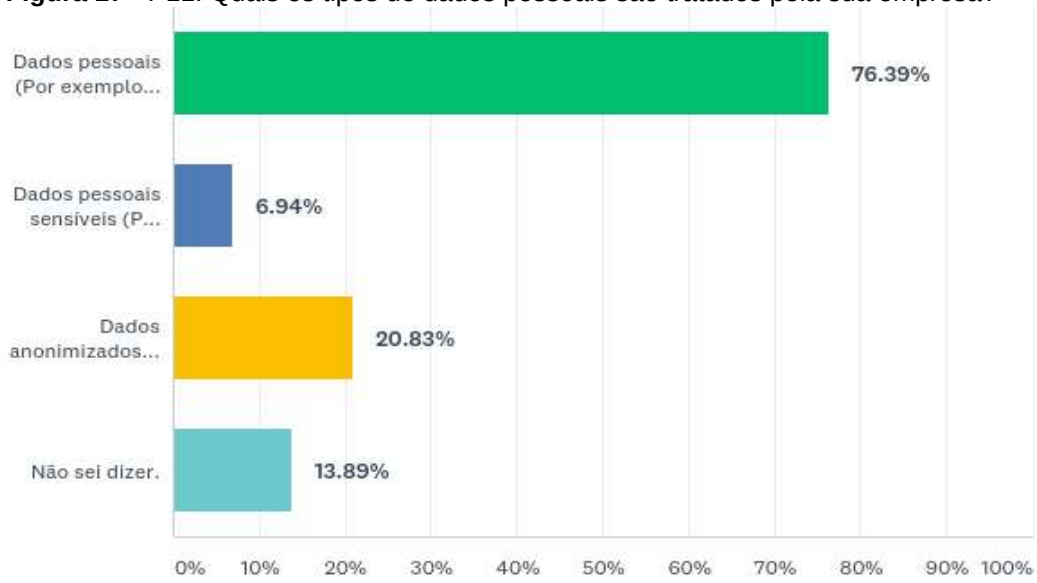
Seção 2 do questionário

A Seção 2 foi organizada para apresentar as perguntas de maneira randômica para os respondentes. Portanto, as perguntas a seguir não foram respondidas na mesma ordem. Buscou-se identificar quais os tipos de dados pessoais são mais comuns, como o tratamento de dados ocorre, e o modo como a proteção de dados aparece nesse contexto.

A Figura 17 mostra que houve desistência de cinco respondentes. Outros cinco respondentes afirmaram trabalhar com dados pessoais sensíveis, enquanto dez não souberam dizer com quais dados trabalham. Apenas quinze respondentes afirmaram

trabalhar com dados anonimizados, o que se leva a inferir que esses respondentes utilizam algum mecanismo de anonimização de dados.

Figura 17 - P11: Quais os tipos de dados pessoais são tratados pela sua empresa?



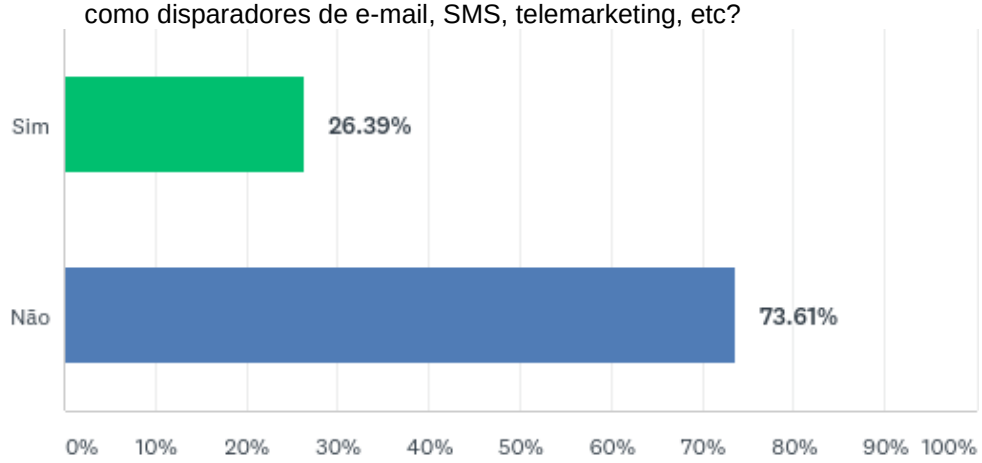
OPÇÕES DE RESPOSTA	RESPOSTAS	
Dados pessoais (Por exemplo: nome, RG, CPF, número de matrícula, entre outros que permitam a identificação da pessoa natural - Titular dos dados) (1)	76.39%	55
Dados pessoais sensíveis (Por exemplo: origem racial ou étnica, convicção religiosa, opinião política,filiação 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) (2)	6.94%	5
Dados anonimizados (dados que não permitem a identificação de uma pessoa, mas sim do grupo a qual pertence, como por exemplo perfil de cliente/publico-alvo) (3)	20.83%	15
Não sei dizer. (4)	13.89%	10
Total de respondentes: 72		

ESTATÍSTICAS BÁSICAS				
Mínimo	Máximo	Mediana	Média	Desvio padrão
1.00	4.00	1.00	1.76	1.11

Fonte: Elaborada pela autora, 2020
Nota: Responderam: 72 Ignoraram: 5

Na Figura 18, 53 respondentes afirmam não utilizar serviços de relacionamento com o consumidor. Isso pode indicar que os dados coletados dos clientes são subutilizados e, possivelmente, não são tratados de forma estruturada.

Figura 18 - P12: A sua empresa utiliza serviços de *customer relationship management* (CRM), tais como disparadores de e-mail, SMS, telemarketing, etc?



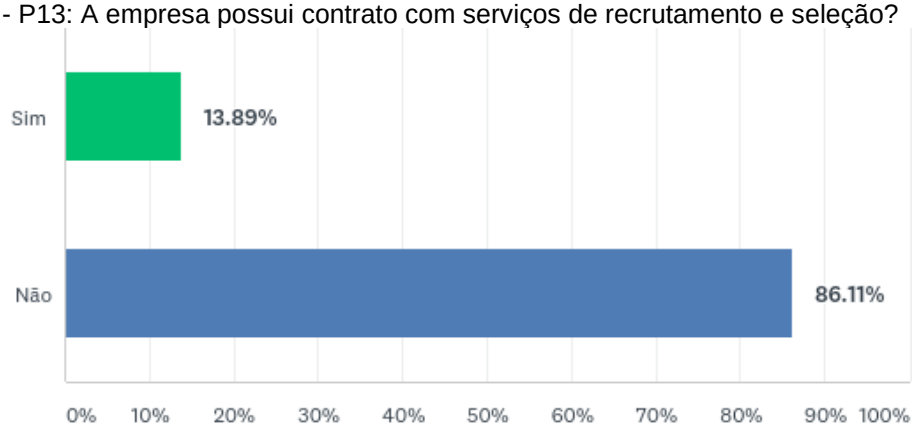
OPÇÕES DE RESPOSTA	RESPOSTAS	
Sim (1)	26.39%	19
Não (2)	73.61%	53
TOTAL		72

ESTATÍSTICAS BÁSICAS				
Mínimo	Máximo	Mediana	Média	Desvio padrão
1.00	2.00	2.00	1.74	0.44

Fonte: Elaborada pela autora, 2020
Nota: Responderam: 72 Ignoraram: 5

Na Figura 19, observa-se que apenas dez respondentes utilizam serviços externos de recrutamento e seleção. Considerando as limitações de pessoal típicas em MPEs, pode-se inferir que o processo de contratação ainda é pouco estruturado nas empresas pesquisadas.

Figura 19 - P13: A empresa possui contrato com serviços de recrutamento e seleção?



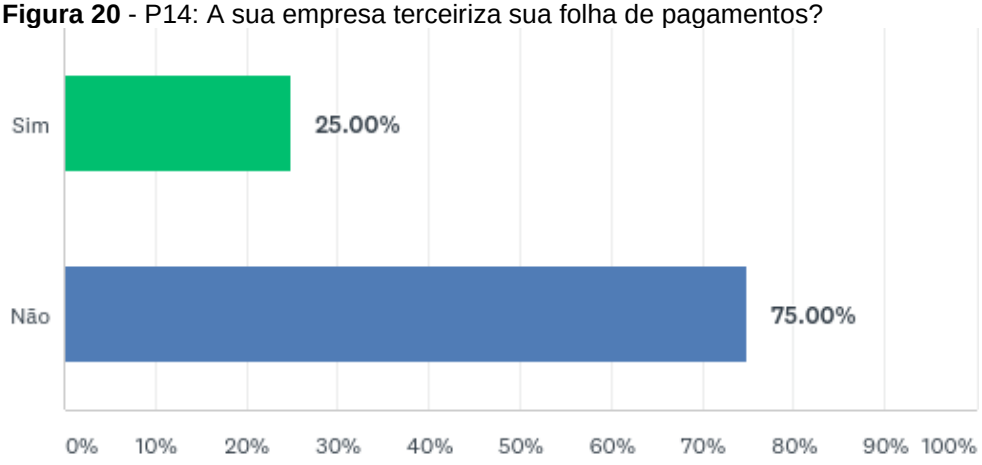
OPÇÕES DE RESPOSTA	RESPOSTAS	
Sim (1)	13.89%	10
Não (2)	86.11%	62
TOTAL		72

ESTATÍSTICAS BÁSICAS				
Mínimo	Máximo	Mediana	Média	Desvio padrão
1.00	2.00	2.00	1.86	0.35

Fonte: Elaborada pela autora, 2020
Nota: Responderam: 72 Ignoraram: 5

Na Figura 20, 18 respondentes (25% da amostra) afirmaram terceirizar a folha de pagamento. Portanto, nessas empresas pelo menos uma parte do serviço contábil/financeiro relacionado à gestão de pessoal é realizada externamente. Isso indica que há compartilhamento de dados pessoais sensíveis com terceiros.

Figura 20 - P14: A sua empresa terceiriza sua folha de pagamentos?



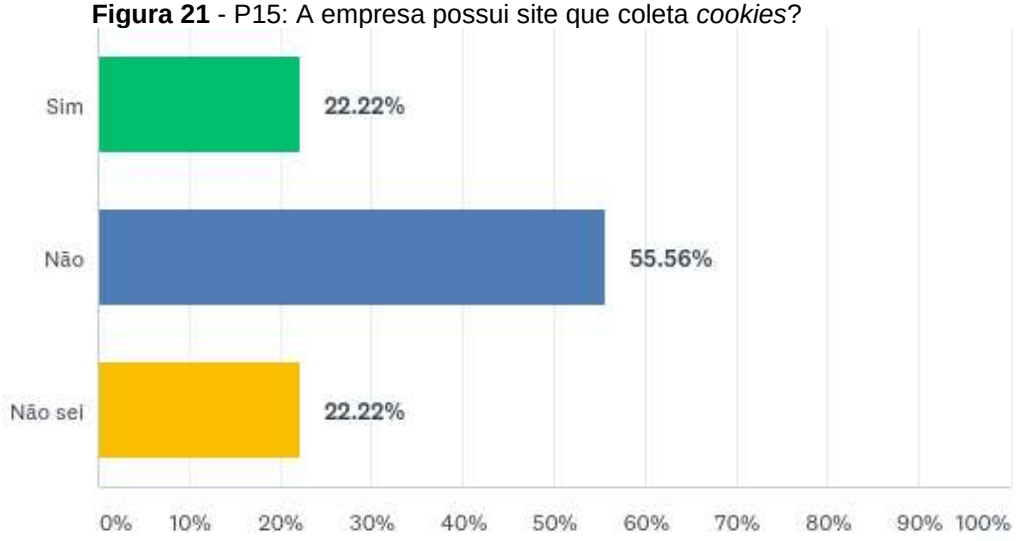
OPÇÕES DE RESPOSTA	RESPOSTAS	
Sim (1)	25.00%	18
Não (2)	75.00%	54
TOTAL		72

ESTATÍSTICAS BÁSICAS				
Mínimo	Máximo	Mediana	Média	Desvio padrão
1.00	2.00	2.00	1.75	0.43

Fonte: Elaborada pela autora, 2020
Nota: Responderam: 72 Ignoraram: 5

A Figura 21 mostra que 22,2% dos respondentes não sabem se o site coleta *cookies*, conforme visto na Figura 17.

Figura 21 - P15: A empresa possui site que coleta *cookies*?



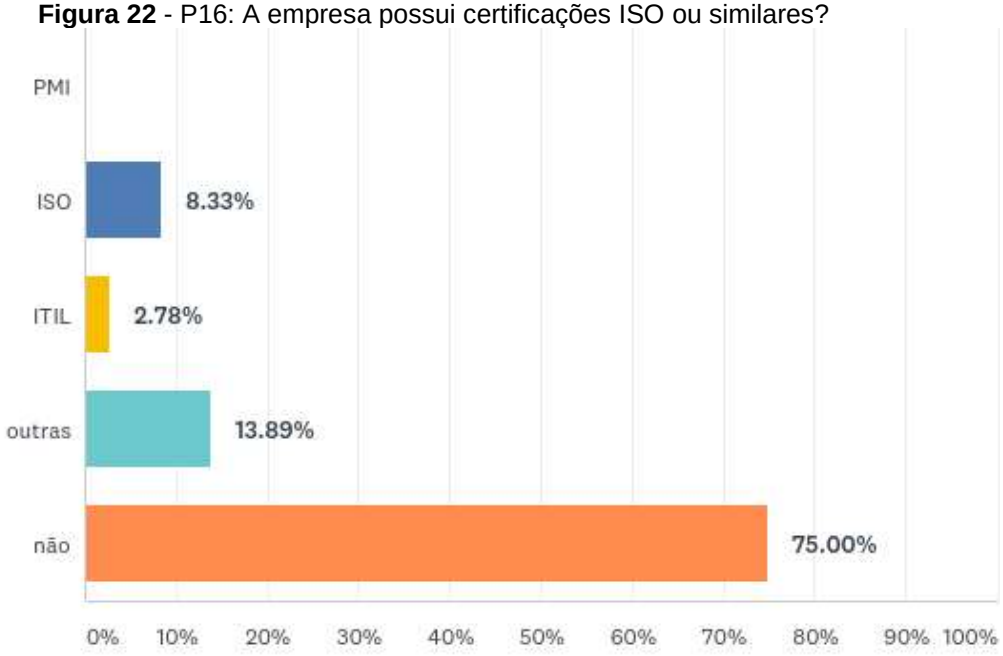
OPÇÕES DE RESPOSTA	RESPOSTAS	
Sim (1)	22.22%	16
Não (2)	55.56%	40
Não sei (3)	22.22%	16
TOTAL		72

ESTATÍSTICAS BÁSICAS				
Mínimo	Máximo	Mediana	Média	Desvio padrão
1.00	3.00	2.00	2.00	0.67

Fonte: Elaborada pela autora, 2020
Nota: Responderam: 72 Ignoraram: 5

Os dados apresentados na Figura 22 mostram que há baixa adesão de certificações, pois somente 25% das empresas pesquisadas possuem algum tipo de certificação. Negócios com certificações apresentam maior probabilidade de estar em *compliance* com regras, uma vez que a certificação exige o cumprimento de normas e processos.

Figura 22 - P16: A empresa possui certificações ISO ou similares?



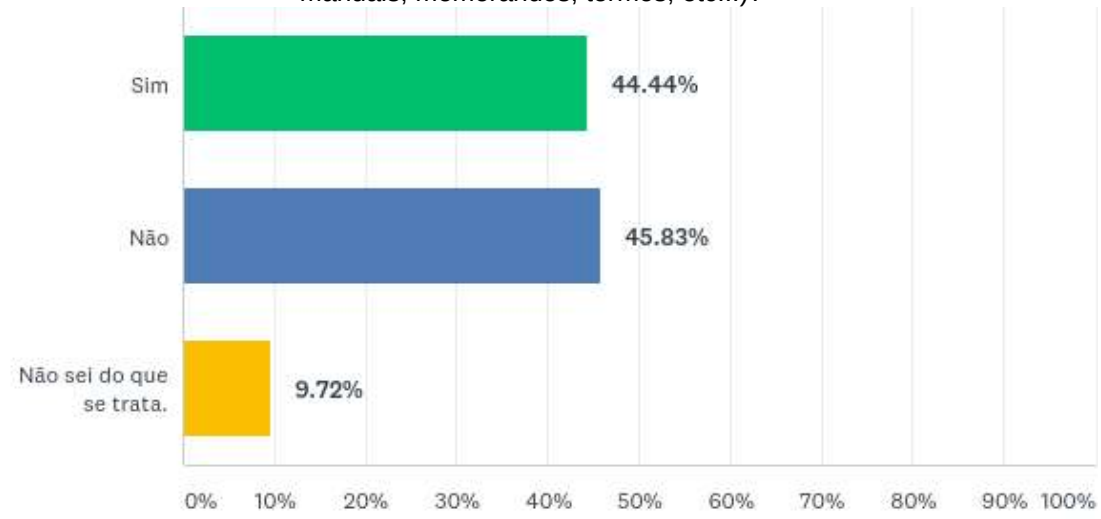
OPÇÕES DE RESPOSTA	RESPOSTAS	
PMI (1)	0.00%	0
ISO (2)	8.33%	6
ITIL (3)	2.78%	2
outras (4)	13.89%	10
não (5)	75.00%	54
TOTAL		72

ESTATÍSTICAS BÁSICAS				
Mínimo	Máximo	Mediana	Média	Desvio padrão
2.00	5.00	5.00	4.56	0.90

Fonte: Elaborada pela autora, 2020
Nota: Responderam: 72 Ignoraram: 5

A Figura 23 apresenta os dados referentes à documentação de políticas de segurança da informação. Com exceção dos 9,7% que não sabem a que se referem tais políticas, os demais respondentes se dividem em metade que possui e a outra metade que não possui uma política de segurança da informação documentada. O registro da política é uma etapa importante para a cultura organizacional da empresa que deseja estar em *compliance* com a LGPD. Além disso, o registro de informações do dia a dia da empresa é uma etapa importante para a gestão do conhecimento.

Figura 23 - P17: A empresa possui políticas de segurança da informação documentadas (por ex: manuais, memorandos, termos, etc...)?



OPÇÕES DE RESPOSTA	RESPOSTAS	
Sim (1)	44.44%	32
Não (2)	45.83%	33
Não sei do que se trata. (3)	9.72%	7
TOTAL		72

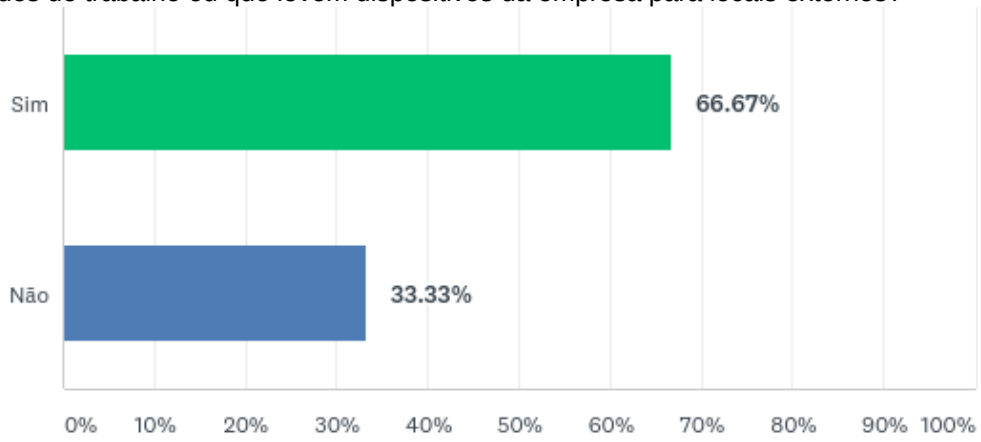
ESTATÍSTICAS BÁSICAS

Mínimo	Máximo	Mediana	Média	Desvio padrão
1.00	3.00	2.00	1.65	0.65

Fonte: Elaborada pela autora, 2020
Nota: Responderam: 72 Ignoraram: 5

Na Figura 24, é apresentado o conjunto de resultados relacionados ao uso de dispositivos pessoais no trabalho ou vice versa, isto é, o uso dispositivos de trabalho em locais externos. Em apenas 33,3% das empresas pesquisadas há uma divisão clara entre aquilo que é pessoal e o profissional. A maior parte das empresas parece confirmar uma característica da MPE de se misturar as vidas pessoal e profissional, sem uma divisão clara entre elas.

Figura 24 - P18: É permitido que os colaboradores utilizem dispositivos pessoais para realizar suas atividades de trabalho ou que levem dispositivos da empresa para locais externos?



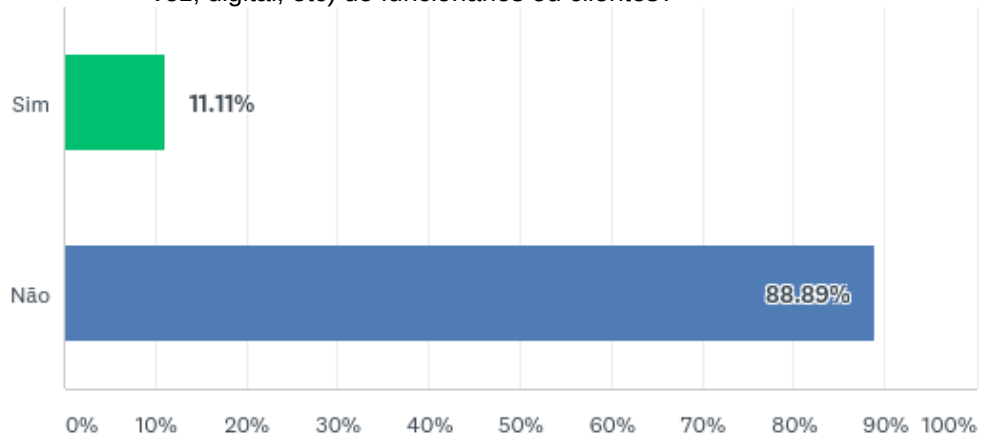
OPÇÕES DE RESPOSTA	RESPOSTAS	
Sim (1)	66.67%	48
Não (2)	33.33%	24
TOTAL		72

ESTATÍSTICAS BÁSICAS				
Mínimo	Máximo	Mediana	Média	Desvio padrão
1.00	2.00	1.00	1.33	0.47

Fonte: Elaborada pela autora, 2020
Nota: Responderam: 72 Ignoraram: 5

Apenas oito respondentes afirmaram coletar dados biométricos (Figura 25). Isso parece indicar que poucas empresas têm recursos de proteção avançados e, também, que na maioria das empresas não há controle digital da jornada de trabalho dos funcionários.

Figura 25 - P19: Em algum momento são coletados dados biométricos (ex: reconhecimento facial, voz, digital, etc) de funcionários ou clientes?



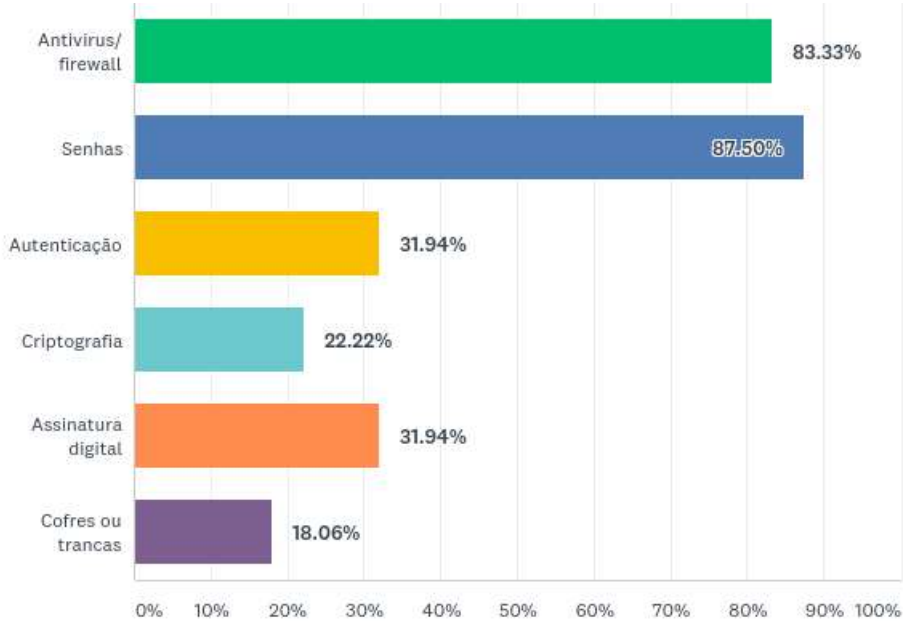
OPÇÕES DE RESPOSTA	RESPOSTAS	
Sim (1)	11.11%	8
Não (2)	88.89%	64
TOTAL		72

ESTATÍSTICAS BÁSICAS				
Mínimo	Máximo	Mediana	Média	Desvio padrão
1.00	2.00	2.00	1.89	0.31

Fonte: Elaborada pela autora, 2020
Nota: Responderam: 72 Ignoraram: 5

Quanto à segurança da informação, um dos itens de maior relevância no que se refere à proteção de dados, as MPEs pesquisadas, em sua maioria, utilizam métodos mistos, como apresentado na Figura 26. A grande maioria das empresas adota apenas dois mecanismos básicos de segurança: antivírus/*firewall* e senha. Portanto, no que se refere à segurança da informação do negócio, as MPEs utilizam recursos genéricos, com pouca ou nenhuma personalização no quesito segurança.

Figura 26 - P20: Quais mecanismos de segurança da informação a empresa utiliza em seu ambiente?



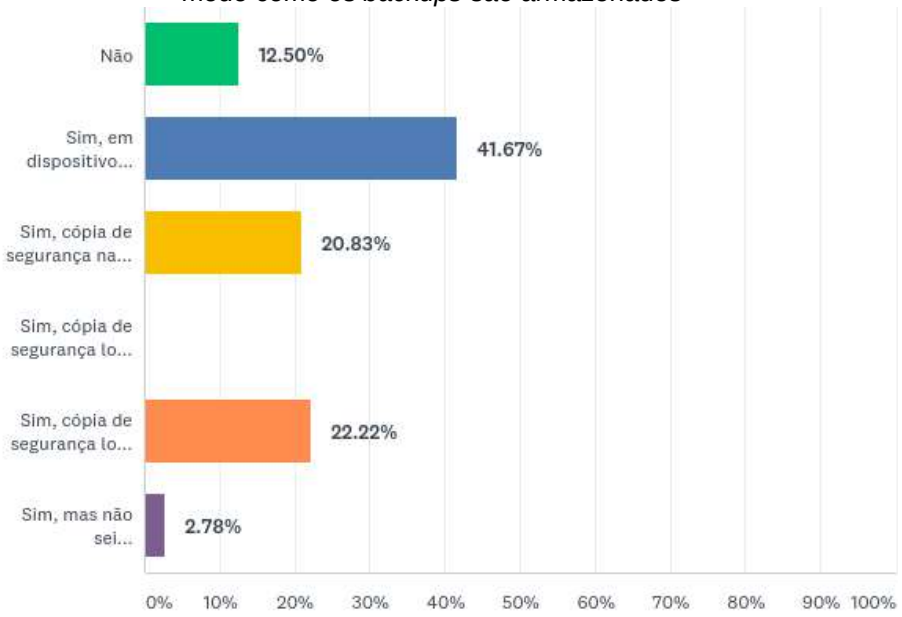
OPÇÕES DE RESPOSTA	RESPOSTAS	
Antivirus/ firewall (1)	83.33%	60
Senhas (2)	87.50%	63
Autenticação (3)	31.94%	23
Criptografia (4)	22.22%	16
Assinatura digital (5)	31.94%	23
Cofres ou trancas (6)	18.06%	13
Total de respondentes: 72		

ESTATÍSTICAS BÁSICAS				
Mínimo	Máximo	Mediana	Média	Desvio padrão
1.00	6.00	2.00	2.59	1.58

Fonte: Elaborada pela autora, 2020
Nota: Responderam: 72 Ignoraram: 5

Cerca de 42% dos respondentes preferem realizar o *backup* apenas em dispositivos externos, como HD e *pen drive*. A Figura 27 indica também que apenas 22,2% dos respondentes optam por sistema duplo de cópia de segurança.

Figura 27 - P21: Sua empresa realiza *backup* dos dados (cópia de segurança)? Se sim, indique o modo como os *backups* são armazenados



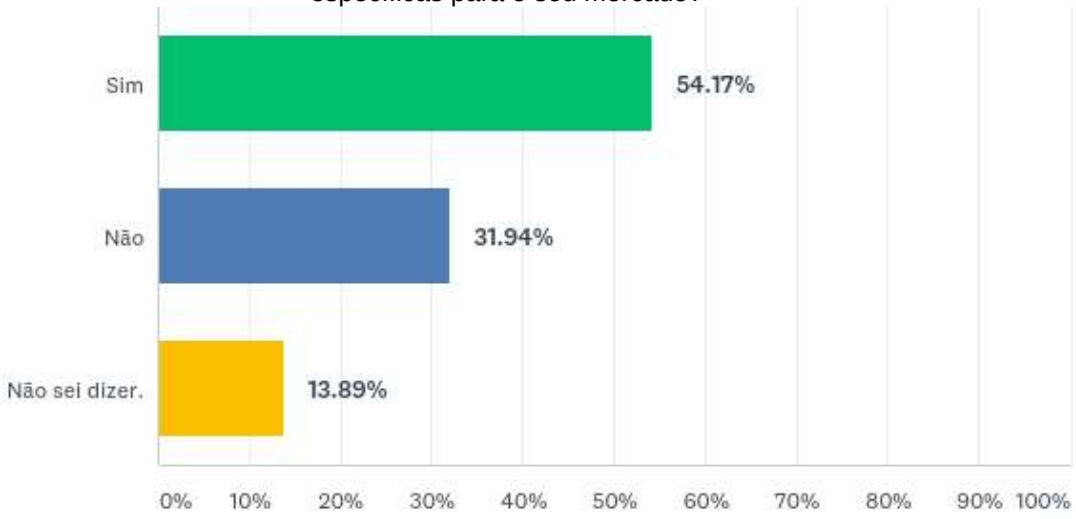
OPÇÕES DE RESPOSTA	RESPOSTAS	
Não (1)	12.50%	9
Sim, em dispositivo externo (HD externo, pen drive, fita magnética etc...) (2)	41.67%	30
Sim, cópia de segurança na nuvem (in cloud) (3)	20.83%	15
Sim, cópia de segurança local (on premise) (4)	0.00%	0
Sim, cópia de segurança local e na nuvem (in cloud e on premise) (5)	22.22%	16
Sim, mas não sei especificar. (6)	2.78%	2
TOTAL		72

ESTATÍSTICAS BÁSICAS				
Mínimo	Máximo	Mediana	Média	Desvio padrão
1.00	6.00	2.00	2.86	1.43

Fonte: Elaborada pela autora, 2020
Nota: Responderam: 72 Ignoraram: 5

Os resultados apresentados na Figura 28, por sua vez, revelam que 54,2% das empresas pesquisadas atuam em ramos com normas específicas. Isso não exclui a possibilidade de desconhecimento por parte dos respondentes de eventuais regulamentações aplicáveis ao seu negócio. O atendimento a essas regulamentações contribui para criar uma cultura de observância a normas e padrões, o que vem ao encontro das necessidades relacionadas à segurança da informação.

Figura 28 - P22: Sua empresa atua em um setor ou ramo com normas e regulamentações específicas para o seu mercado?



OPÇÕES DE RESPOSTA	RESPOSTAS	
Sim (1)	54.17%	39
Não (2)	31.94%	23
Não sei dizer. (3)	13.89%	10
TOTAL		72

ESTATÍSTICAS BÁSICAS				
Mínimo	Máximo	Mediana	Média	Desvio padrão
1.00	3.00	1.00	1.60	0.72

Fonte: Elaborada pela autora, 2020
Nota: Responderam: 72 Ignoraram: 5

Os resultados apresentados na Seção 2 do questionário revelam, entre outros resultados, 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, se parece mais um desconhecimento da criticidade das informações sob seu poder, haja visto o compartilhamento 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 tão comuns a todos os respondentes.

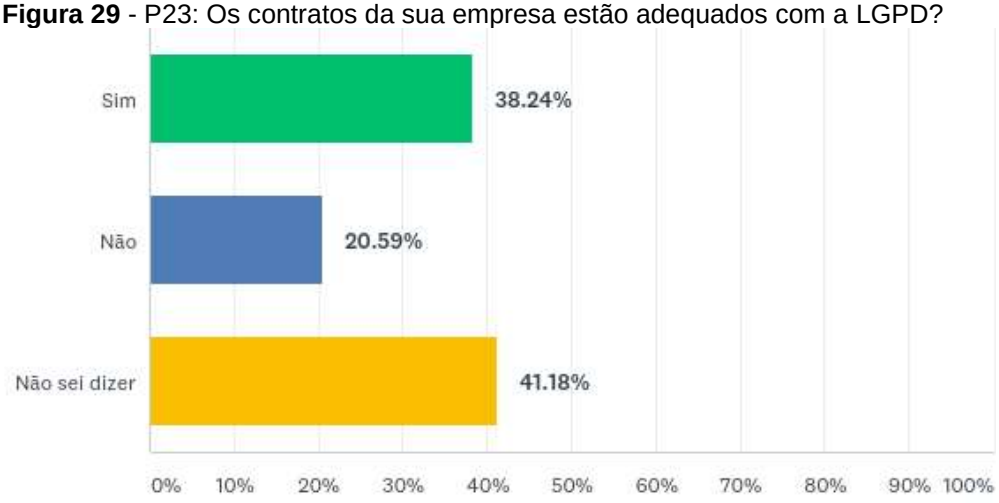
Seção 3 do questionário

O objetivo desta seção é investigar o grau de conformidade da MPEs à LGPD. As questões foram apresentadas de forma randômica.

A Figura 29 mostra um aumento de cinco para nove no número de respondentes que abandonaram o preenchimento do questionário. Isso pode indicar a dificuldade do participante em responder questões de cunho mais específico.

Como apresentado na figura mencionada, 41,2% dos respondentes não sabem dizer se os contratos de suas empresas estão de acordo com a LGPD, indicando a falta de conhecimento sobre a lei. Somadas às empresas que afirmaram que os seus contratos não estão adequados à LGPD (20,6%), os resultados sugerem que apenas os 38,2% que responderam afirmativamente à questão 23 possuem contratos condizentes com as boas práticas de proteção de dados.

Figura 29 - P23: Os contratos da sua empresa estão adequados com a LGPD?



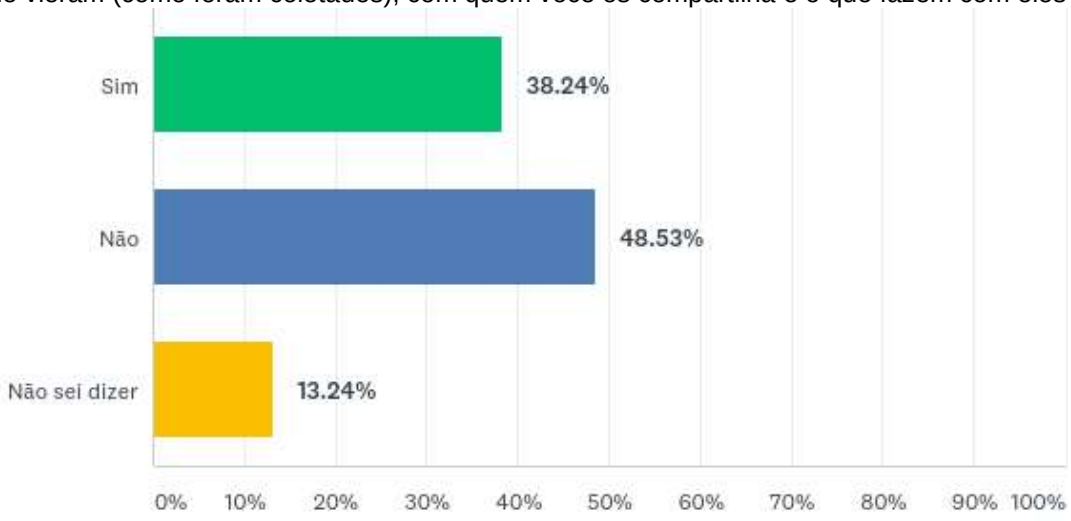
OPÇÕES DE RESPOSTA	RESPOSTAS	
Sim (1)	38.24%	26
Não (2)	20.59%	14
Não sei dizer (3)	41.18%	28
TOTAL		68

ESTATÍSTICAS BÁSICAS				
Mínimo	Máximo	Mediana	Média	Desvio padrão
1.00	3.00	2.00	2.03	0.89

Fonte: Elaborada pela autora, 2020
Nota: Responderam: 68 Ignoraram: 9

Observa-se na Figura 30 o mesmo percentual anterior de respondentes (38,2%) que gerencia os dados pessoais. Essas 26 empresas informaram ter procedimentos para armazenar, coletar, compartilhar e utilizar os dados pessoais.

Figura 30 - P24: 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?



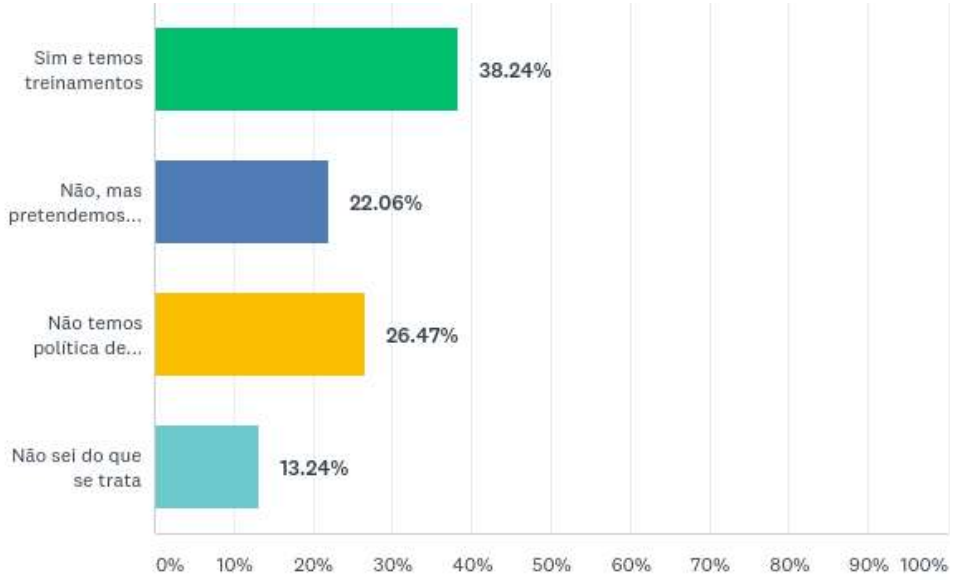
OPÇÕES DE RESPOSTA	RESPOSTAS	
Sim (1)	38.24%	26
Não (2)	48.53%	33
Não sei dizer (3)	13.24%	9
TOTAL		68

ESTATÍSTICAS BÁSICAS				
Mínimo	Máximo	Mediana	Média	Desvio padrão
1.00	3.00	2.00	1.75	0.67

Fonte: Elaborada pela autora, 2020
Nota: Responderam: 68 Ignoraram: 9

As 26 empresas citadas nos parágrafos anteriores, as quais representam 38,2% da amostra pesquisada, informaram que os seus funcionários têm ciência da política de proteção de dados. A convergência de respostas nessas três questões (apresentadas nas Figuras 29, 30 e 31) sugere haver uma atenção efetiva com a segurança de informação nessas empresas.

Figura 31 - P25: Os funcionários da sua empresa estão cientes da política de proteção de dados adotada?



OPÇÕES DE RESPOSTA	RESPOSTAS	
Sim e temos treinamentos (1)	38.24%	26
Não, mas pretendemos realizar treinamentos (2)	22.06%	15
Não temos política de proteção de dados (3)	26.47%	18
Não sei do que se trata (4)	13.24%	9
TOTAL		68

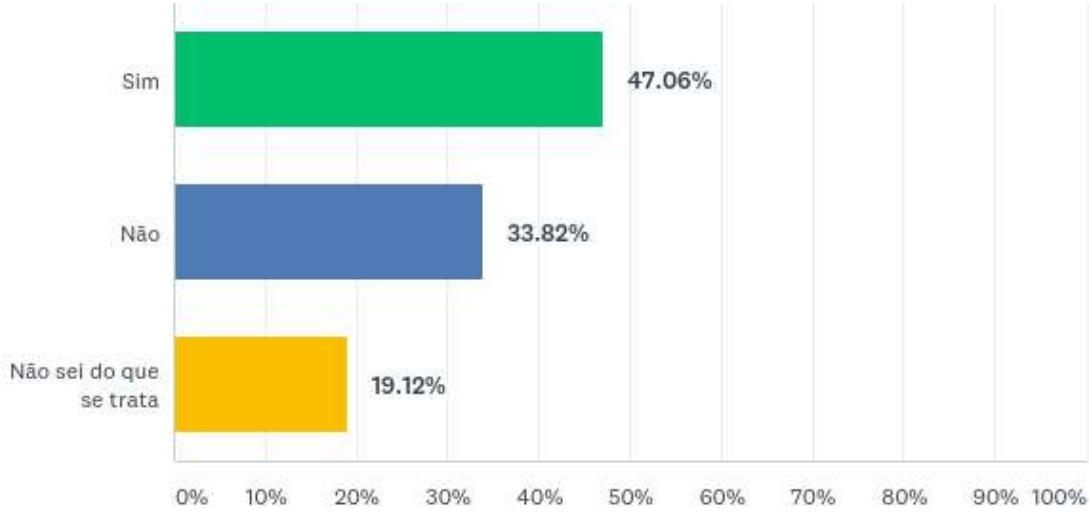
ESTATÍSTICAS BÁSICAS				
Mínimo	Máximo	Mediana	Média	Desvio padrão
1.00	4.00	2.00	2.15	1.07

Fonte: Elaborada pela autora, 2020
Nota: Responderam: 68 Ignoraram: 9

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%), como revelado pela Figura 33. 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.

Figura 32 - P26: Sua empresa entende quando um relatório de impacto à proteção de dados é necessário?

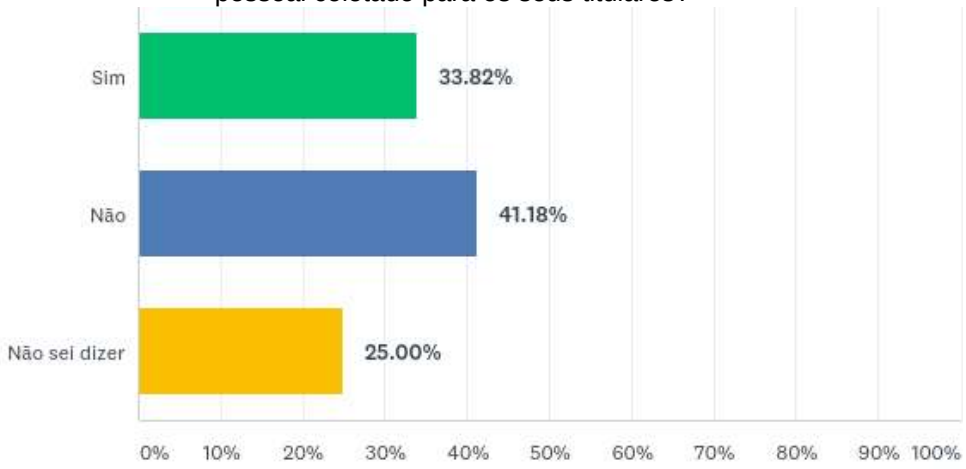


OPÇÕES DE RESPOSTA	RESPOSTAS	
Sim (1)	47.06%	32
Não (2)	33.82%	23
Não sei do que se trata (3)	19.12%	13
TOTAL		68

ESTATÍSTICAS BÁSICAS				
Mínimo	Máximo	Mediana	Média	Desvio padrão
1.00	3.00	2.00	1.72	0.76

Fonte: Elaborada pela autora, 2020
Nota: Responderam: 68 Ignoraram: 9

Figura 33 - P27: Sua empresa fornece informações sobre as finalidades do tratamento de cada dado pessoal coletado para os seus titulares?



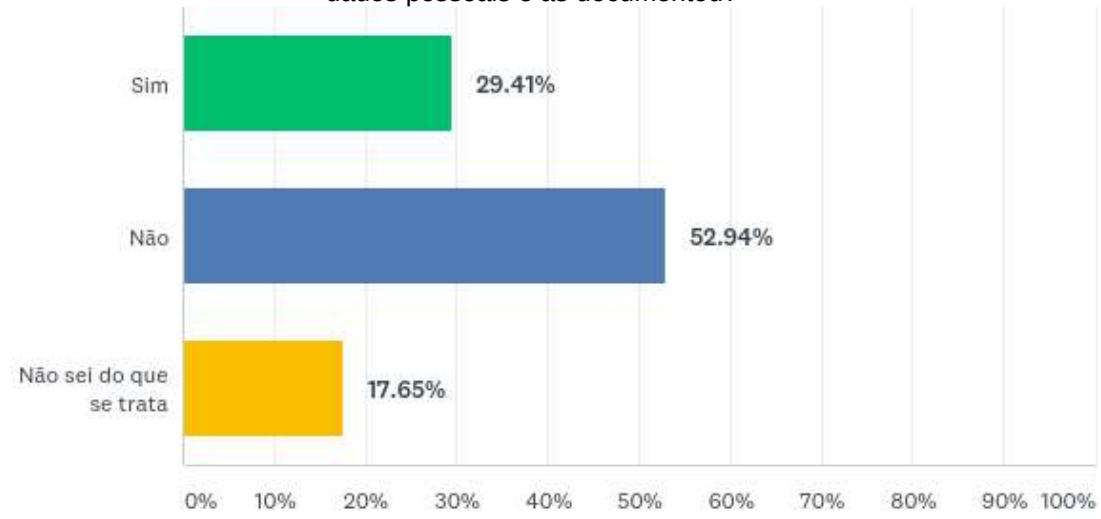
OPÇÕES DE RESPOSTA	RESPOSTAS	
Sim (1)	33.82%	23
Não (2)	41.18%	28
Não sei dizer (3)	25.00%	17
TOTAL		68

ESTATÍSTICAS BÁSICAS				
Mínimo	Máximo	Mediana	Média	Desvio padrão
1.00	3.00	2.00	1.91	0.76

Fonte: Elaborada pela autora, 2020
Nota: Responderam: 68 Ignoraram: 9

Os resultados apresentados na Figura 34 mostram que apenas 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.

Figura 34 - P28: Sua empresa identificou suas bases legais para processamento e tratamento de dados pessoais e as documentou?



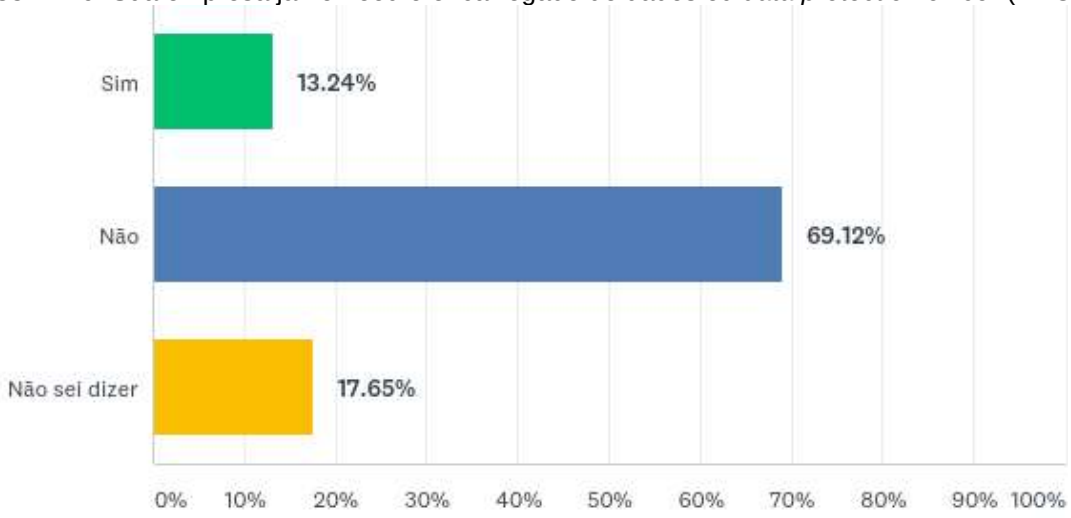
OPÇÕES DE RESPOSTA	RESPOSTAS	
Sim (1)	29.41%	20
Não (2)	52.94%	36
Não sei do que se trata (3)	17.65%	12
TOTAL		68

ESTATÍSTICAS BÁSICAS				
Mínimo	Máximo	Mediana	Média	Desvio padrão
1.00	3.00	2.00	1.88	0.68

Fonte: Elaborada pela autora, 2020
Nota: Responderam: 68 Ignoraram: 9

Apenas nove empresas da amostra possuem um DPO (encarregado de dados), conforme apresentado na Figura 35. 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.

Figura 35 - P29: Sua empresa já nomeou o encarregado de dados ou *data protection officer* (DPO)?



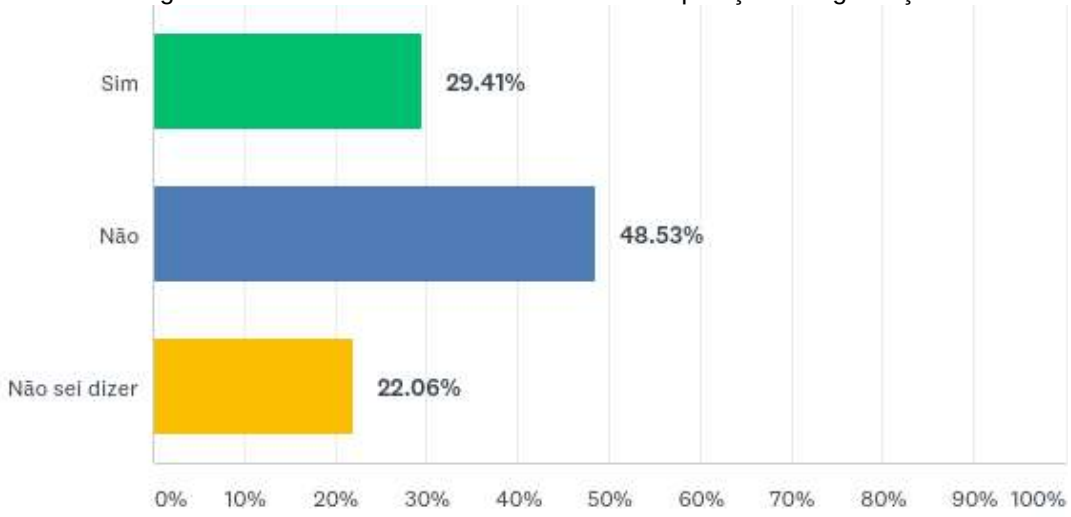
OPÇÕES DE RESPOSTA	RESPOSTAS	
Sim (1)	13.24%	9
Não (2)	69.12%	47
Não sei dizer (3)	17.65%	12
TOTAL		68

ESTATÍSTICAS BÁSICAS				
Mínimo	Máximo	Mediana	Média	Desvio padrão
1.00	3.00	2.00	2.04	0.55

Fonte: Elaborada pela autora, 2020
Nota: Responderam: 68 Ignoraram: 9

Os dados apresentados na Figura 36 referem-se ao monitoramento que a empresa faz de sua própria conformidade com as políticas de proteção de dado, 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 em relação à Figura 27, indicando que as políticas de segurança dos respondentes não estão atualizadas conforme previsto na LGPD.

Figura 36 - P30: 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?



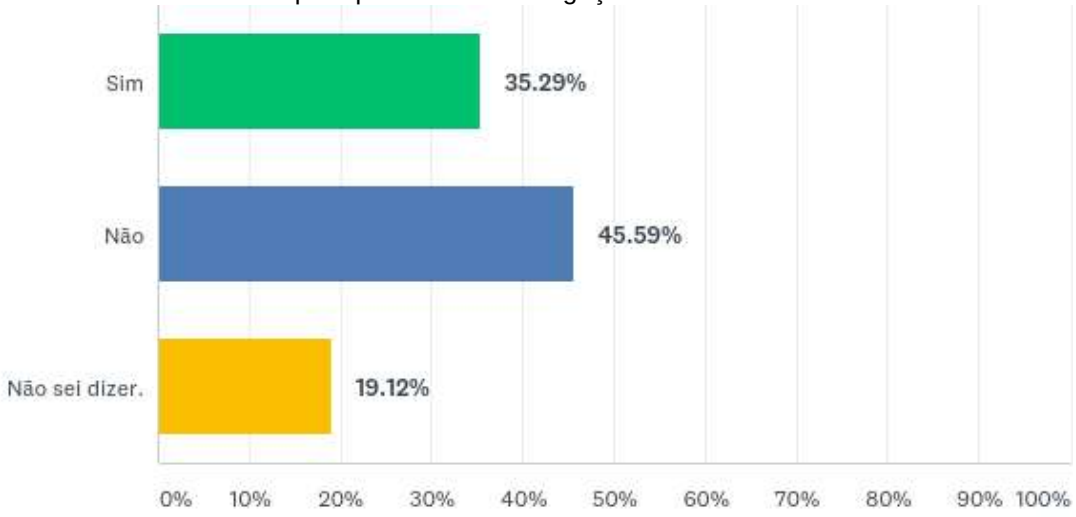
OPÇÕES DE RESPOSTA	RESPOSTAS	
Sim (1)	29.41%	20
Não (2)	48.53%	33
Não sei dizer (3)	22.06%	15
TOTAL		68

ESTATÍSTICAS BÁSICAS				
Mínimo	Máximo	Mediana	Média	Desvio padrão
1.00	3.00	2.00	1.93	0.71

Fonte: Elaborada pela autora, 2020
Nota: Responderam: 68 Ignoraram: 9

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 na Figura 37 mostram que apenas 35,3% das empresas responderam afirmativamente a essa questão.

Figura 37 - P31: Sua empresa possui sistemas para registrar e gerenciar os consentimentos dados, assim como para possibilitar a revogação de consentimento?



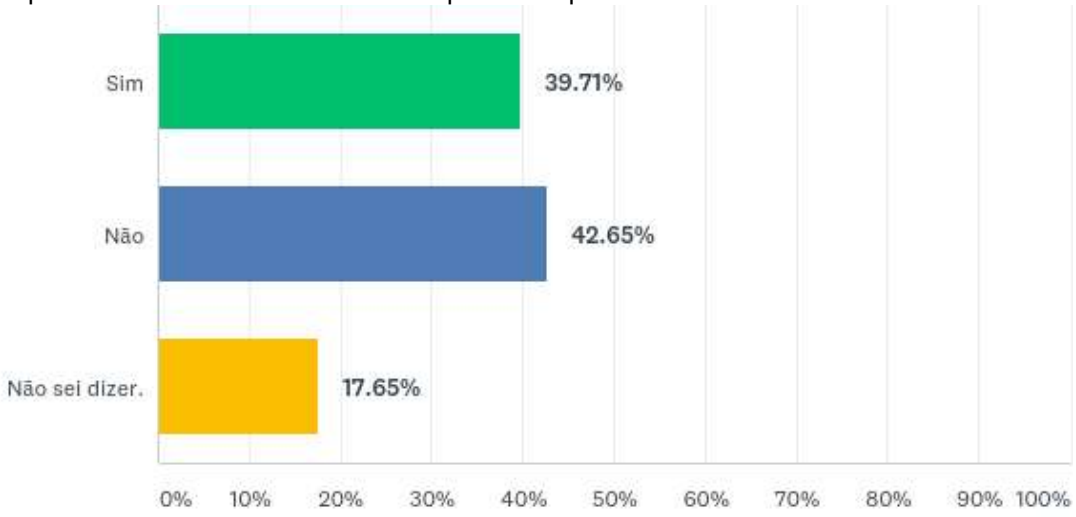
OPÇÕES DE RESPOSTA	RESPOSTAS	
Sim (1)	35.29%	24
Não (2)	45.59%	31
Não sei dizer. (3)	19.12%	13
TOTAL		68

ESTATÍSTICAS BÁSICAS				
Mínimo	Máximo	Mediana	Média	Desvio padrão
1.00	3.00	2.00	1.84	0.72

Fonte: Elaborada pela autora, 2020
Nota: Responderam: 68 Ignoraram: 9

Os resultados apresentados na Figura 38, em comparação aqueles apresentados na Figura 37, 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.

Figura 38 - P32: 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?



OPÇÕES DE RESPOSTA	RESPOSTAS	
Sim (1)	39.71%	27
Não (2)	42.65%	29
Não sei dizer. (3)	17.65%	12
TOTAL		68

ESTATÍSTICAS BÁSICAS				
Mínimo	Máximo	Mediana	Média	Desvio padrão
1.00	3.00	2.00	1.78	0.72

Fonte: Elaborada pela autora, 2020
Nota: Responderam: 68 Ignoraram: 9

Nesta seção do questionário, os dados analisados apontaram a existência de preocupações a respeito da proteção de dados pessoais, mas com pouca ou nenhuma ação ou processo formalizado para tratar essa questão. Conforme observado nas seções anteriores, o perfil predominante dos respondentes é o de pessoas com acesso e familiaridade à tecnologia, mas com conhecimentos apenas 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.

5.2 Testes das hipóteses da pesquisa

Neste item, buscou-se considerar as hipóteses mais relevantes levantadas na seção 1.5 desta dissertação. Para tanto, após aplicação do teste da mediana, foram selecionadas por conveniência as hipóteses Ha, Hb, Hc, Hd e Hp.

A seguir, serão feitas algumas considerações a respeito dos resultados obtidos.

Hipótese Ha

A hipótese Ha está assim formulada: 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.

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 4.

Tabela 4 - 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 ex: manuais, memorandos, termos, etc...)?	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	35	33	51,47	48,53

eficácia dos controles de manipulação e segurança de dados?				
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 porcentuais
Fonte: Elaborada pela autora, 2020

A Tabela 5 mostra as estatísticas descritivas das variáveis que serviram para testar a hipótese Ha para as 13 questões relacionadas na Tabela 4. Em termos percentuais, a mediana das conformidades representou 57,35% e as não conformidades, 42,65%.

Tabela 5 - Estatísticas descritivas das variáveis da hipótese Ha

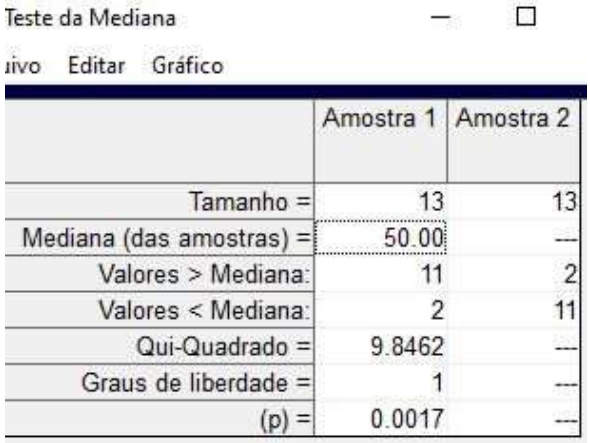
Descriptive Statistics: Conf; NãoC; Conf%; NãoC%

	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

Fonte: Elaborada pela autora, 2020

Para testar se a proporção de não conformidades de todos os respondentes é significativamente maior do que as conformidades, utilizou-se o teste não paramétrico da mediana, como apresentado na Figura 39. O resultado do teste mostra que a diferença é significativa ao nível de significância de 0,01.

Figura 39 - Teste da mediana para a hipótese Ha



Fonte: Elaborada pela autora, 2020

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).

Hipótese Hb

A hipótese Hb está assim formulada: aplicando-se o questionário diagnóstico, o nível de conformidade dos respondentes, considerando a mediana das respostas, não é superior a 20%.

Como observado na Tabela 4, a mediana das conformidades representou 57,35% e as não conformidades 42,65%. Com base nesses resultados, a hipótese Hb é rejeitada, isto é: o nível de conformidade dos respondentes é superior a 20%.

Hipótese Hc

A hipótese Hc está assim formulada: ao nível de significância de 0,05, a proporção de não conformidades, considerando-se o fator Tratamento de Dados Pessoais, é significativamente maior do que as conformidades.

Na Tabela 6 são apresentadas as questões utilizadas para calcular a hipótese Hc, indicando uma mediana de 54% de conformidade e 46% de não conformidade, considerando o fator tratamento de dados pessoais.

Tabela 6 - Conformidade e não conformidade - hipótese Hc

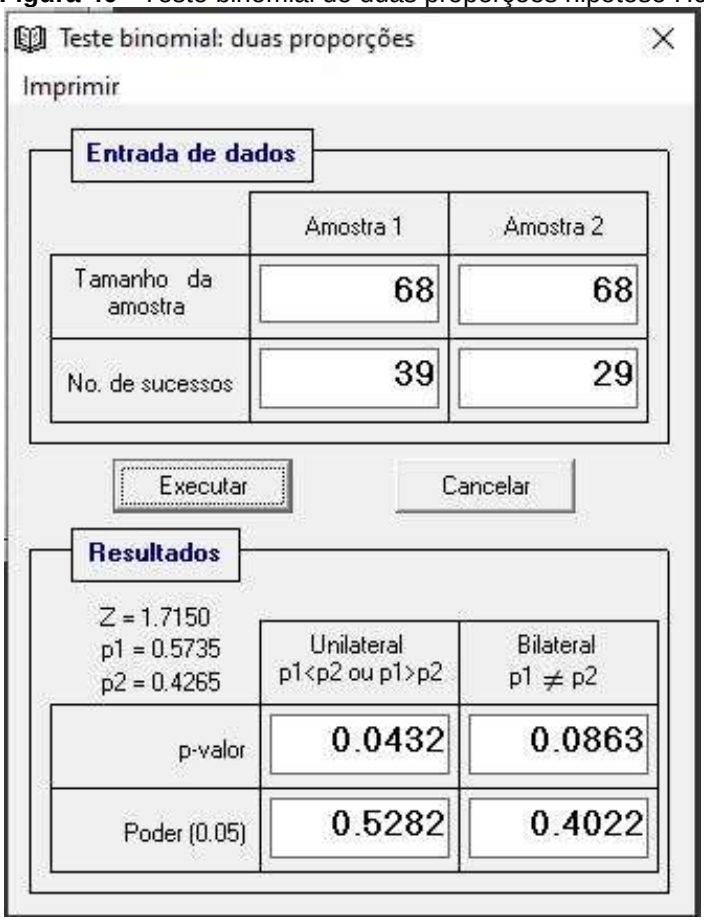
Questões	Conf	NãoC	Conf%	NãoC%
17. A empresa possui políticas de segurança da informação documentadas (por ex: manuais, memorandos, termos, etc...)?	37	31	54,41	45,59
19. Em algum momento são coletados dados biométricos (ex: reconhecimento facial, voz, digital, etc) de funcionários ou clientes?	8	60	11,76	88,24
20. Quais mecanismos de segurança da informação a empresa utiliza em seu ambiente?	68	0	100,00	-
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
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

28. Sua empresa identificou suas bases legais para processamento e tratamento de dados pessoais e as documentou?	32	36	47,06	52,94
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	37	31	54,41	45,59

Legenda: Conf = resposta em conformidade com a LGPD; NãoC = resposta não conforme a LGPD.% indicam valores porcentuais
Fonte: Elaborada pela autora, 2020

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, como mostra a Figura 40. O resultado do teste mostra que não é encontrada significância entras 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.

Figura 40 - Teste binomial de duas proporções hipótese Hc



Fonte: Elaborada pela autora, 2020

Hipótese Hd

A hipótese Hd está assim formulada: 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.

A Tabela 7 mostra as questões que serviram para testar a hipótese Hd. Em termos percentuais, a mediana das conformidades representou 56% e as não conformidades, 43%.

Tabela 7 - Conformidade e não conformidade - hipótese Hd

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 ex: manuais, memorandos, termos, etc...)?	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

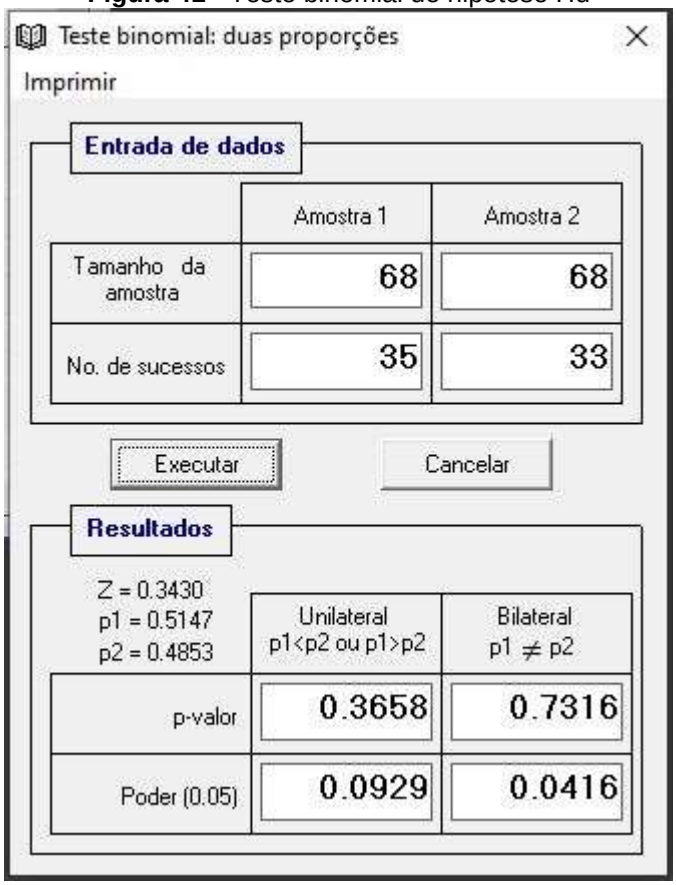
Legenda: Conf = resposta em conformidade com a LGPD; NãoC = resposta não conforme a LGPD. % indicam valores porcentuais

Fonte: Elaborada pela autora, 2020

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 binomial de proporção, como mostra a Figura 41.

O resultado do teste mostra que a diferença é significativa ao nível de 0,3, confirmando a hipótese Hd.

Figura 41 - Teste binomial de hipótese Hd



Fonte: Elaborada pela autora, 2020

Hipótese Hp

A hipótese Hp está assim formulada: 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 8 mostra as questões que serviram para testar a hipótese Hp. Em termos percentuais a mediana das conformidades representou 87%; e as não conformidades de 34%.

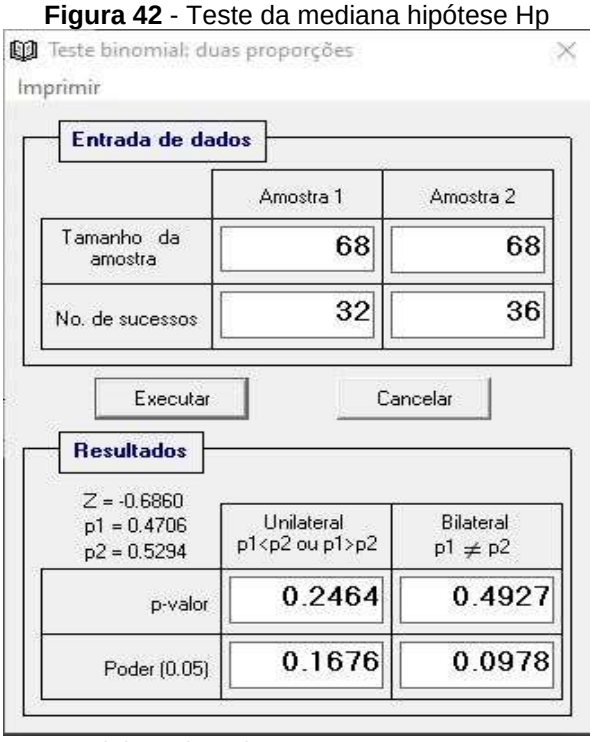
Tabela 8 - Conformidade e não conformidade - hipótese Hp

Questões	Conf	NãoC	Conf%	NãoC%
17. A empresa possui políticas de segurança da informação documentadas (por ex: manuais, memorandos, termos, etc...)?	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 porcentuais
Fonte: Elaborada pela autora, 2020

Na Figura 42 pode ser observado o teste binomial de duas proporções, sendo que, com um p-valor (unilateral) de 0,05, não foi encontrada significância na análise comparativa.

Figura 42 - Teste da mediana hipótese Hp



Fonte: Elaborada pela autora, 2020

Testes de hipóteses considerados

Após a aplicação do teste de mediana em todas as hipóteses, optou-se por analisar as hipóteses consideradas mais relevantes para a dissertação, pois compreendeu-se que as hipóteses Ha, Hb, Hc, Hd e Hp melhor contribuiam com os objetivos propostos por esta pesquisa.

Das cinco hipóteses testadas, somente a hipótese Hd 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 Hb 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.

6. CONSIDERAÇÕES FINAIS

A necessidade de regulamentações em atividades econômicas em torno dos dados pessoais é crescente no mundo globalizado. No Brasil, a proteção de dados tem sido debatida atualmente nas esferas pública e privada. Nesse sentido, o Brasil, ao avançar na discussão, coloca empresas brasileiras em um patamar competitivo frente às exigências internacionais, mas também desafiador para as empresas que necessitam se adequar às novas “regras do jogo”.

Para atender ao objetivo específico de se elaborar uma revisão teórica sobre gestão de dados em organizações, bem como sua proteção e leis relacionadas, esta dissertação apresentou estudos de diversos autores sobre a gestão de dados em MPEs. Além disso, foram identificadas as leis brasileiras que subsidiam as normativas para a regulação da proteção de dados físicos e digitais, apresentadas nos capítulos 1, 2 e 3. Dentro desse conjunto de regulamentos, ressalta-se a importância da LGPD, inspirada no Regulamento Europeu de Proteção de dados (GDPR), que traz definições importantes para a regulação do tratamento de dados, tais como dados pessoais, dados pessoais sensíveis, princípios e hipóteses de tratamento desses dados.

A revisão bibliográfica permitiu a fundamentação teórica para a construção de um questionário diagnóstico, a fim de verificar se as MPEs estão se preparando para cumprir os requisitos da LGPD, especialmente no que se refere à proteção de dados. Nos capítulos 4 e 5 foram apresentados, respectivamente, os métodos escolhidos para a pesquisa de campo e a análise dos dados obtidos.

Por meio da aplicação de um questionário em MPEs do AUJ-SP, foi possível coletar dados para, em concordância com o objetivo específico “c”, verificar o nível de não conformidades relacionadas aos fatores Tratamento de Dados Pessoais e Término de Tratamento de Dados Pessoais, e testar as hipóteses Hc e Hd.

Para realizar a análise quantitativa dos dados foram aplicados testes não-paramétricos, teste da mediana, para calcular o grau de conformidade das MPEs, segundo as hipóteses dispostas no subcapítulo 1.5. Para análise qualitativa dos dados foram realizadas inferências que permitiram relacionar a literatura da proteção de dados aos dados coletado das MPEs.

Para atender o objetivo específico de propor caminhos possíveis conforme com o grau de conformidade identificado nas MPEs, a partir da discussão das hipóteses Ha, Hb, Hc, Hd e Hp, foi possível indicar meios para melhorar a conformidade das MPEs à LGPD.

De modo geral, a literatura indica várias soluções para a implementação de uma governança de dados eficiente. Mas, na realidade observada nas MPEs brasileiras, verifica-se problemas tais como falta de mão-de-obra especializada, e restrições de recursos financeiros e tecnológicos. Nesse sentido, faz-se necessário buscar soluções que sejam passíveis de implementação em MPEs de diferentes setores. Essas soluções precisam ser de baixo custo, sem desconsiderar as exigências previstas em lei.

Uma solução inclui a adoção do modelo de Ciclo de Vida dos Dados para mapear os processos do negócio relacionando com as fases de tratamento dos dados dispostas na LGPD. Isso porque essa lei não obriga o uso de uma tecnologia específica mas, sim, que haja transparência nos processos adotados. Portanto, a adoção das normas ABNT e ISO de proteção de dados, bem como o modelo de Ciclo de Vida dos Dados são recomendações para a construção da governança de dados em *compliance* com a lei.

Tendo em vista a importância dos dados pessoais, esta pesquisa buscou também conhecer o nível de conformidade das MPEs pesquisadas em relação aos requisitos da LGPD.

Com base nos resultados encontrados, é possível afirmar que as MPEs pesquisadas estão preocupadas com a proteção dos dados pessoais. No entanto, o preparo delas ainda é incipiente. Isso provavelmente se deve ao fato de que a compreensão dos princípios e hipóteses previstos na LGPD é ampla, exigindo um conjunto de conhecimentos específicos para mapear o fluxo dos dados dentro do negócio.

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.

Além disso, pode-se observar que 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 a 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.

Um outro ponto encontrado afirma que 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 disseminadores de ações em respeito às normas e leis aplicáveis.

Apesar de os dados indicarem a adoção de algum tipo de solução tecnológica a respeito da segurança dos dados, foi possível identificar 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.

Diferente de outras legislações, a LGPD possibilita que os clientes se tornem uma peça fundamental na cobrança de conformidade das empresas. Sendo assim, a MPE é passível de ser fiscalizada não apenas por órgãos governamentais, mas por todos os cidadãos.

Conforme apresentado no subitem 4.7, a postergação da data de início do vigor da lei por conta da pandemia do COVID-19 não diminuiu a discussão acerca da proteção de dados. Pelo contrário, a exposição indevida de dados sensíveis da saúde

dos cidadãos contaminados mostrou que a privacidade e a proteção dos dados de cidadãos, empresas e governos são assuntos de interesse público.

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.

Recomenda-se, portanto, que em estudos futuros sejam feitas pesquisas sobre os vários 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

ABES. **ABES anuncia ferramenta sobre a LGPD e parceria para redução do lixo eletrônico durante conferência**. 2019. Disponível em: http://www.abessoftware.com.br/noticias/abes-anuncia-ferramenta-sobre-a-lgpd-e-parceria-para-reducao-do-lixo-eletronico-durante-conferencia. Acesso em: 27 mar. 2020.

ALEXANDRE ATHENIENSE ADVOGADOS. **Pré diagnóstico para adequação à LGPD**: lei geral de proteção de dados. 2019. Disponível em: https://www.alexandreatheniense.com.br/lgpd-pre-diagnostico-az/wp-content/uploads/2019/10/Formulario-Pr%C3%A9-diagn%C3%B3stico-Alexandre-Atheniense-Advogados-adequa%C3%A7%C3%A3o-%C3%A0-LGPD-Formul%C3%A1rios-Google.pdf. Acesso em: 05 mai. 2020.

BEZERRA, Maria Ruth Borges. Autoridade nacional de proteção de dados pessoais: a importância do modelo institucional independente para a efetividade da lei. **Caderno Virtual**, v. 2, n. 44, p.1-95, 2019.

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Editora Forense, 2019.

BOFF, Salete Oro; FORTES, Vinícius Borges; FREITAS, Cinthia Obla-den de Almendra. **Proteção de dados e privacidade: do direito às novas tecnologias na sociedade da informação**. Rio de Janeiro: Lumen Juris, 2018.

BRANCO, Sérgio. As hipóteses de aplicação da LGPD e as definições legais. *In*: MULHOLLAN, Caitlin (org). **A LGPD e o novo marco normativo no Brasil**. São Paulo: Editora Arquipélago, 2020.

BRASIL**. Constituição da República Federativa do Brasil de 1988**. Brasília, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 09 abr. 2019.

BRASIL. **Lei nº. 8.078, de 11 de setembro de 1990**. Código de Defesa do Consumidor. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/Leis/L8078.htm. Acesso em: 09 abr. 2019.

BRASIL. **Lei nº. 9.279, de 14 de maio de 1996**. Regula direitos e obrigações relativos à propriedade industrial. Brasília, 1996. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9279.htm#:~:text=LEI%20N%C2%BA%209.279%2C%20DE%2014,obriga%C3%A7%C3%B5es%20relativos%20%C3%A0%20propriedade%20industrial.&text=Art.&text=6%C2%BA%20Ao%20autor%20de%20invenn%C3%A7%C3%A3o,nas%20condi%C3%A7%C3%B5es%20estabelecidas%20nesta%20Lei. Acesso em: 09 abr. 2019.

BRASIL. **Lei nº. 9.610, de 19 de fevereiro de 1998**. Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências. Brasília, 1998. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9610.htm. Acesso em: 09 abr. 2019.

BRASIL. **Lei nº. 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5o, no inciso II do § 3o do art. 37 e no § 2o do art. 216 da Constituição Federal; altera a Lei no 8.112, de 11 de dezembro de 1990; revoga a Lei no 11.111, de 5 de maio de 2005, e dispositivos da Lei no 8.159, de 8 de janeiro de 1991; e dá outras providências. Brasília, 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12527.htm#art1. Acesso em: 09 abr. 2019.

BRASIL. **Lei nº. 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 09 abr. 2019.

BRASIL. **Lei nº. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 09 abr. 2019.

BRASIL. **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, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D9936.htm. Acesso em: 21 ago. 2020.

CAVALCANTI, Natália Peppi; SANTOS, Luiza Mendonça da Silva Belo. A lei geral de proteção de dados do brasil na era do big data. *In*: Tecnologia Jurídica & Direito Digital - II Congresso Internacional de Direito, Governo e Tecnologia, 2., 2018, Belo Horizonte. **Anais** [...]. Belo Horizonte: Fórum, 2018, v.1, p. 351-366.

CHOO, Chun Wei. **A organização do conhecimento**: como as organizações usam a informação para criar significado, construir conhecimento e tomar decisões. São Paulo: Ed. SENAC São Paulo, 2003.

CRESWELL, John W. **Projeto de pesquisa**: métodos qualitativo, quantitativo e misto. 3. ed. Porto Alegre: Artmed, 2010.

DATASEBRAE. **Painel de empresas**. 2020. Disponível em: https://datasebrae.com.br/totaldeempresas/. Acesso em: 21 ago. 2020.

DERBLI, Ludimila Santos. O transplante jurídico do regulamento geral de proteção de dados da União Europeia (“GDPR”) para o direito brasileiro. E-legis, n. 30, p. 181-193, 2019.

DE SORDI, José Osvaldo. **Administração da informação**: fundamentos e práticas para uma nova gestão do conhecimento. 2. ed. São Paulo: Saraiva, 2015.

DE SORDI, José Osvaldo. **Desenvolvimento de projeto de pesquisa**. São Paulo: Saraiva, 2017a.

DE SORDI, José Osvaldo. **Gestão por processos**: uma abordagem da moderna administração. São Paulo: Saraiva, 2017b.

DIAGNÓSTICO LGPD. **Ferramenta de diagnóstico LGPD**. 2019. Disponível em: https://diagnosticolgpd.abes.org.br/. Acesso em: 05 mai. 2020.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, v. 12, n. 2, p. 91-108, 2011.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. 6.ed. São Paulo: Atlas, 2017.

LEI GERAL DE PROTEÇÃO DE DADOS. **Guia de boas práticas para implementação na administração pública federal**. 2020. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-lgpd.pdf. Acesso em: 20 ago. 2020.

LIMA, Jeane Firmo; SILVA, Glessia. Desafios para inovar na micro e pequena empresa. **Revista da Micro e Pequena Empresa**, v. 13, n. 2, p. 85-97, 2019.

MACHADO, H. P. V. CONFIGURAÇÃO DE ESTUDOS SOBRE GESTÃO DO CONHECIMENTO EM PEQUENAS EMPRESAS NO BRASIL. **Perspectivas Em Gestão & Conhecimento**, Ano 8 v.3, 209-227, 2018.

MACHADO, MEYER, SENDACZ E OPICE ADVOGADOS. **Lei 13.709/18**: lei de proteção de dados pessoais. 2018. Disponível em: https://www.machadomeyer.com.br/images/publicacoes/PDFs/Lei_Protecao_de_Dados_ebook_18.pdf. Acesso em: 12 mai. 2020.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Fundamentos de metodologia científica**. 8. ed. São Paulo: Atlas, 2017.

MEDEIROS, Lílian O. *et al*. Avaliação da maturidade em gestão de dados das empresas de Uberlândia e região. **e-Rac**, v. 3, n. 1, p.1-17, 2013.

MENEZES, Cassio Roberto Conceição de; OLAVE, Maria Elena Leon. Práticas de gestão do conhecimento em micro e pequenas empresas de Sergipe. **Gestão & Regionalidade**, v. 32, n. 94, p. 4-19, 2016.

MINISTÉRIO PÚBLICO FEDERAL. **Levantamento sobre a lei geral de proteção de dados (LGPD) no MPF**. 2019. Disponível em: https://pesquisa.mpf.mp.br/index.php/213612?lang=pt-BR. Acesso em: 05 mai. 2020.

MOLINA, Leticia Gorri; SANTOS, Juliana Cardoso dos. Gestão da informação e a 4a Revolução Industrial. **AtoZ**: novas práticas em informação e conhecimento, v. 8, n. 2, p. 39-48, 2020.

MORAES, Alexandre F. **Segurança em redes**: fundamentos. São Paulo: Érica, 2010.

MOSIMANN, HORN & ADVOGADOS ASSOCIADOS. **Avalie a conformidade do seu negócio com a lei geral de proteção de dados (LGPD)**. 2019. Disponível em: https://content.ostec.com.br/diagnostico_lgpd_mh/?utm_source=Mosimann%2C+Horn&utm_campaign=7d35e19a97-EMAIL_CAMPAIGN_2019_04_17_10_14&utm_medium=email&utm_term=0_b0af218eee-7d35e19a97-324751765. Acesso em: 05 mai. 2020.

OLIVEIRA, Ana Paula de *et al*. A LGPD brasileira na prática empresarial. **Revista Jurídica da Escola Superior de Advocacia da OAB-PR**, ano 4, n.1, p. 172-200, 2019.

OLIVEIRA, Thallita Pâmela Pinho de; SARAIVA, Piedley Macedo. A influência do marketing digital no perfil de consumo da geração y. **Id on Line Revista Multidisciplinar e de Psicologia**, v. 13, n. 44, p. 589-600, 2019.

PIURCOSKY, Fabricio Pelloso *et al*. A LGPD pessoais em empresas brasileiras: uma análise de múltiplos casos. **Suma de negócios**, v. 10, n. 23, p.89-99, 2019.

RAHUL, Kumar; BANYAL, Rohitash Kumar. Data life cycle management in big data analytics. **Procedia Computer Science**, v. 173, p. 364-371, 2020.

RAMOS, Lara Castro Padilha; GOMES, Ana Virgínia Moreira. Lei geral de proteção de dados pessoais e seus reflexos nas relações de trabalho. **Scientia Iuris**, v. 23, n. 2, p. 127-146, 2019.

RAOSOFT. **Sample size calculator**. 2004. Disponível em: http://www.raosoft.com/samplesize.html. Acesso em: 21 ago. 2020.

SALEMA, Rodolfo Fernandes de Souza. Aspectos legais do compliance como ferramenta de gestão empresarial estratégica. **Revista Jurídica da Escola Superior de Advocacia da OAB-PR**, ano 5, n.1, p. 177-210, 2020.

SANT'ANA, Ricardo César Gonçalves. Ciclo de vida dos dados: uma perspectiva a partir da ciência da informação. **Informação & Informação**, v. 21, n. 2, p. 116-142, 2016.

SEBRAE. **Pequenos negócios em números**. 2019. Disponível em: https://m.sebrae.com.br/sites/PortalSebrae/ufs/sp/sebraeaz/pequenos-negocios-em-numeros,12e8794363447510VgnVCM1000004c00210aRCRD. Acesso em: 20 ago. 2020.

SILVEIRA, Marco Antonio (org.), Becaro, Taiane Cristiane**. Competitividade com qualidade de vida**: O capital humano como fator de produção. CTI, Campinas – SP, 2014.

VIEIRA, Sonia. **Estatística básica**. Rio de Janeiro: Ed. Cengage, 2011.

APÊNDICE

QUESTIONÁRIO APLICADO

LGPD: Diagnóstico do grau de conformidade de micro e pequenas empresas
Convite para pesquisa
Olá, seja bem-vindo! Este questionário faz parte da minha pesquisa para conclusão do Mestrado em Administração de Empresas da Unifaccamp. Os dados aqui coletados são anônimos e serão utilizados exclusivamente para fins de pesquisa acadêmica. Em caso de dúvidas, por favor entre em contato através do e-mail talitabiblio32@gmail.com Obrigada! Talita Langen
1. Quantos funcionários a empresa possui?
1 a 5 funcionários
6 a 10 funcionários
11 a 15 funcionários
16 a 20 funcionários
mais de 20 funcionários
2. Indique a Cidade e Estado da sua empresa:
3. Qual é a sua idade?
Entre 18 e 24 anos
Entre 25 e 34 anos
Entre 35 e 44 anos
Entre 45 e 54 anos
55 anos ou mais
4. Qual o seu sexo?
Masculino
Feminino
5. Qual o seu grau de instrução?
Ensino Médio
Ensino Técnico
Ensino Superior
Pós graduação
6. Qual o seu cargo?
Assistente
Analista

Coordenação
Gerência
Dono do negócio / Sócio
7. Qual o seu principal tipo de cliente?
Empresas (B2B)
Consumidor final (B2C)
Ambos
8. Sua empresa coleta dados pessoais de quais públicos?
Funcionários.
Clientes.
Ambos (funcionários e clientes)
Nenhum
Não sei.
9. Qual o ramo de atuação do seu negócio?
Comércio
Indústria
Serviços
Terceiro Setor
Outros
10. A empresa é associada a algum tipo de organização, sindicato ou associação?
Sim
Não
11. Quais os tipos de dados pessoais são tratados pela sua empresa?
Dados pessoais (Por exemplo: nome, RG, CPF, número de matrícula, entre outros que permitam a identificação da pessoa natural - Titular dos dados)
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
Dados anonimizados (dados que não permitem a identificação de uma pessoa, mas sim do grupo à qual pertence, como por exemplo perfil de cliente/público-alvo)
Não sei dizer
12. A sua empresa utiliza serviços de *customer relationship management* (CRM), tais como disparadores de e-mail, SMS, telemarketing, etc?
Sim
Não
13. A empresa possui contrato com serviços de recrutamento e seleção?
Sim
Não
14. A sua empresa terceiriza sua folha de pagamentos? *

Sim
Não
15. A empresa possui site que coleta cookies?
Sim
Não
Não sei
16. A empresa possui certificações ISO ou similares?
PMI
ISO
ITIL
outras
não
17. A empresa possui políticas de segurança da informação documentadas (por ex: manuais, memorandos, termos, etc...)?
Sim
Não
Não sei do que se trata.
18. É permitido que os colaboradores utilizem dispositivos pessoais para realizar suas atividades de trabalho ou que levem dispositivos da empresa para locais externos?
Sim
Não
19. Em algum momento são coletados dados biométricos (ex: reconhecimento facial, voz, digital, etc) de funcionários ou clientes?
Sim
Não
20. Quais mecanismos de segurança da informação a empresa utiliza em seu ambiente?
Antivírus/ firewall
Senhas
Autenticação
Criptografia
Assinatura digital
Cofres ou trancas
21. Sua empresa realiza *backup* dos dados (cópia de segurança)? Se sim, indique o modo como os backups são armazenados.
Não
Sim, em dispositivo externo (HD externo, pen drive, fita, magnética etc...)
Sim, cópia de segurança na nuvem (*in cloud*)
Sim, cópia de segurança local (*on premise*)

Sim, cópia de segurança local e na nuvem (*in cloud* e *on premise*)
Sim, mas não sei especificar
22. Sua empresa atua em um setor ou ramo com normas e regulamentações específicas para o seu mercado?
Sim
Não
Não sei dizer.
23. Os contratos da sua empresa estão adequados com a LGPD?
Sim
Não
Não sei dizer
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?
Sim
Não
Não sei dizer
25. Os funcionários da sua empresa estão cientes da política de proteção de dados adotada?
Sim e temos treinamentos
Não, mas pretendemos realizar treinamentos
Não temos política de proteção de dados
Não sei do que se trata
26. Sua empresa entende quando um relatório de impacto à proteção de dados é necessário?
Sim
Não
Não sei do que se trata
27. Sua empresa fornece informações sobre as finalidades do tratamento de cada dado pessoal coletado para os seus titulares?
Sim
Não
Não sei dizer
28. Sua empresa identificou suas bases legais para processamento e tratamento de dados pessoais e as
documentou?
Sim
Não
Não sei do que se trata
29. Sua empresa já nomeou o encarregado de dados ou *data protection officer* (DPO)?

Sim
Não
Não sei dizer
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?
Sim
Não
Não sei dizer
31. Sua empresa possui sistemas para registrar e gerenciar os consentimentos dados, assim como para possibilitar a revogação de consentimento?
Sim
Não
Não sei dizer.
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?
Sim
Não
Não sei dizer

Fonte: Elaborado pela autora, 2020

ANEXO A

QUESTIONÁRIO DIAGNÓSTICO

As questões de 1 a 6 foram adaptadas, as demais estão transcritas conforme disponível no site da Associação Brasileira de Empresas de *Software* (ABES).

Pergunta N	Diagnóstico LGPD - ABES
1	1. A empresa é associada da ABES?
	Sim
	Não
2	2. Qual o porte da sua empresa?
	Microempresa (faturamento até R$ 360k)
	Pequena empresa (faturamento R$ 360k até R$ 4,8 MM)
	Médio Porte (faturamento R$ 4,8 MM até R$ 300 MM)
	Grande Porte (faturamento maior que R$ 300 MM)
3	3. Quantos funcionários sua empresa possui?
	até 19 empregados
	de 20 a 99 empregados
	100 a 499 empregados
	mais de 500 empregados
4	4. Qual o seu principal tipo de cliente?
	Empresas
	Consumidor Final
5	5. Qual a unidade federativa da sede da sua empresa?
6	6. Qual o setor da sua empresa?
	Informações Gerais
7	7. A empresa realiza o tratamento de dados pessoais?
	Sim
	Não
8	8. A empresa realiza o tratamento de dados pessoais sensíveis?
	Sim
	Não
9	9. A empresa realiza o tratamento de dados pessoais de crianças e adolescentes?

	Sim
	Não
10	10. O tratamento de dados pessoais é realizado com base na boa-fé e os princípios da LGPD (i.e., finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas)?
	Sim
	Não
11	11. O tratamento de dados pessoais realizado pela empresa inclui automatização de qualquer tomada de decisão (RPA), criação de perfis com base nos dados pessoais transferidos (profiling) ou utilização analítica (analytics)?
	Sim
	Não
	Tratamento de Dados Pessoais
12	12. O tratamento de dados pessoais realizado pela empresa é fundamentado nas bases legais estipuladas na LGPD?
	Sim
	Não
13	13. O tratamento de dados pessoais de acesso público é baseado na finalidade, boa-fé e o interesse público que justificaram sua disponibilização?
	Sim
	Não
14	14. O consentimento para tratamento de dados pessoais é obtido por escrito ou por outro meio que demonstre a manifestação de vontade do titular de dados?
	Sim
	Não
15	15. Ao obter o consentimento do titular de dados pessoais a empresa deixa de forma clara, precisa e objetiva as finalidades para as quais os dados serão tratados?
	Sim
	Não
16	16. A empresa garante ao titular de dados pessoais o direito de retirar o consentimento para tratamento de dados a qualquer momento (opt-out)?
	Sim
	Não
17	17. O acesso a dados pessoais está restrito somente a funcionários autorizados?
	Sim
	Não
18	8. A empresa possui um Portal de Privacidade para os titulares de dados pessoais nos quais as informações sobre o tratamento de seus dados são disponibilizadas de forma clara, adequada e ostensiva?
	Sim
	Não
19	19. Caso haja alteração na finalidade do tratamento de dado pessoal, a empresa possui um procedimento para informar os titulares dos dados pessoais acerca dessa mudança?

	Sim
	Não
20	20. A empresa realiza o tratamento de dados pessoais sensíveis de acordo com as bases legais específicas previstas na LGPD?
	Sim
	Não
21	21. Os dados pessoais sensíveis tratados pela empresa são compartilhados com terceiros?
	Sim
	Não
22	22. A empresa obtém o consentimento específico e destacado de um dos pais ou responsável legal para tratar dados pessoais de crianças?
	Sim
	Não
23	23. A empresa condiciona a participação de crianças em jogos, aplicações de internet ou outras atividades ao fornecimento de dados pessoais?
	Sim
	Não
	Término do Tratamento de Dados Pessoais
24	24. A empresa possui uma política periódica para eliminação de dados pessoais?
	Sim
	Não
25	25. Os dados pessoais são tratados por período indeterminado?
	Sim
	Não
26	26. A empresa possui um procedimento para eliminação de dados pessoais?
	Sim
	Não
27	27. A empresa possui um procedimento para atender solicitações para eliminar dados pessoais de seus sistemas, se necessário?
	Sim
	Não
28	28. A empresa anonimiza os dados pessoais que permanecem em seus sistemas após o término do tratamento?
	Sim
	Não
	Direitos dos Titulares
29	29. A empresa possui um procedimento para atender às solicitações de acesso aos dados pessoais realizadas por titulares?
	Sim

	Não
30	30. A empresa possui registros de todos os dados pessoais por ela tratados e seus respectivos titulares?
	Sim
	Não
31	31. A empresa possui procedimento para disponibilização e acesso dos dados pessoais de seus titulares caso venham a ser solicitados em até 15 dias após o requerimento?
	Sim
	Não
32	32. Os dados pessoais tratados são acessados por terceiros?
	Sim
	Não
33	33. A empresa possui a capacidade de indicar para os titulares de dados pessoais em quais processos existe tomada de decisão gerada pelo tratamento automatizado de dados pessoais?
	Sim
	Não
	Transferência Internacional de Dados
34	34. A empresa realiza transferência internacional de dados pessoais?
	Sim
	Não
35	35. A empresa realiza transferência internacional de dados pessoais de acordo com as bases legais da LGPD?
	Sim
	Não
	N/A
36	36. Os países para os quais a empresa realiza transferência internacional de dados possuem grau de proteção de dados adequado?
	Sim
	Não
	N/A
	Deveres do Controlador e do Operador
37	37. A empresa possui Record of Processing Activities (Registro das Operações de Tratamento de Dados Pessoais), conforme exigido pelo art. 30 da GDPR e 37 da LGPD?
	Sim
	Não
38	38. Em caso de atividades de tratamento de dados pessoais que resultem em um alto risco para os titulares de dados, você realiza um Relatório de Impacto à Proteção de Dados Pessoais (Data Protection Impact Assessment - DPIA)?
	Sim
	Não
39	39. A empresa nomeou um Encarregado (*data protection officer* - DPO)?

	Sim
	Não
40	40. A empresa limita o tratamento de dados pessoais ao tratamento necessário para os fins específicos que justificam a sua coleta?
	Sim
	Não
	Boas Práticas
41	41. A empresa possui políticas, procedimentos, e medidas protetivas (e.g., controles de acesso, criptografia, modificação de dados, mascaramento de dados) que asseguram a segurança e garantia de conformidade com os regulamentos/leis de privacidade?
	Sim
	Não
42	42. A empresa possui uma política/procedimento de back-up em relação aos dados pessoais?
	Sim
	Não
43	43. A empresa contratou algum serviço de assessoria para implementação da LGPD?
	Sim
	Não
44	44. A empresa possui estratégia e roadmap de implementação para estar em conformidade com as novas regulamentações?
	Sim
	Não
45	45. A empresa possui um programa de governança em privacidade?
	Sim
	Não
46	46. Os dados pessoais são armazenados em um local e ambiente seguros?
	Sim
	Não
47	47. Existe um processo para atualizar políticas, procedimentos, diretrizes de gerenciamento de riscos, procedimentos de violação, etc. para refletir as atualizações / mudanças das expectativas regulatórias ou mudanças internas no programa de privacidade?
	Sim
	Não
48	48. A empresa conduz avaliações de vulnerabilidade e testes de penetração em seus sistemas de tratamento de dados pessoais?
	Sim
	Não
49	49. A empresa é certificada em algum padrão ou framework de segurança?
	Sim
	Não

	Funcionários
50	50. A empresa promove treinamentos obrigatórios para os funcionários, conscientizando-os sobre a importância e sobre suas responsabilidades em relação à privacidade e proteção de dados pessoais?
	Sim
	Não
51	51. Existe um processo formal para revisar e atualizar o treinamento periodicamente?
	Sim
	Não
52	52. A empresa oferece orientação aos funcionários de terceiros a respeito das práticas a serem tomadas em relação à proteção de dados pessoais?
	Sim
	Não
53	53. A empresa exige que seus funcionários e prestadores de serviços assinem acordos de confidencialidade e segurança de dados?
	Sim
	Não
54	54. A empresa instrui seus funcionários e contratados a limitar o armazenamento de dados pessoais do cliente em dispositivos de armazenamento móvel ao mínimo exigido para fins comerciais?
	Sim
	Não
55	55. A empresa possui uma política de revisão regular das permissões de acesso aos dados pessoais que garanta o acesso somente aos funcionários e contratados que precisam ter acesso, bem como um procedimento para prevenir prontamente funcionários e contratados desligados de acesso a dados pessoais?
	Sim
	Não
	Incidentes de Dados Pessoais
56	56. A empresa possui um processo apropriado para notificar os titulares de dados pessoais sobre uma violação de dados, quando aplicável?
	Sim
	Não
57	57. A empresa é capaz de detectar rapidamente incidentes de segurança (e.g., incluindo acesso não autorizado, destruição, perda, alteração e violações de dados)?
	Sim
	Não
58	58. A empresa possui um procedimento para agir, prontamente, em caso de incidentes de segurança, incluindo notificação aos titulares de dados pessoais afetados?
	Sim
	Não
59	59. A empresa pode fornecer uma lista de todas as notificações de privacidade de dados que possui?
	Sim

	Não
60	60. Sua empresa já passou por algum incidente de violações de segurança da informação nos últimos dois (2) anos?
	Sim
	Não
61	61. Sua empresa está atualmente sujeita a quaisquer ações de execução, investigações ou litígios relacionados à privacidade ou à segurança da informação?
	Sim
	Não
	Jurídico
62	62. Os contratos com terceiros da empresa possuem cláusulas compatíveis com os termos e condições das leis de proteção de dados, em vigor?
	Sim
	Não
63	63. Os contratos de trabalho da empresa possuem cláusulas compatíveis com os termos e condições das leis de proteção de dados, em vigor?
	Sim
	Não
64	64. A empresa possui cláusulas contratuais de privacidade e proteção de dados em seus contratos em casos de transferência internacional de dados pessoais?
	Sim
	Não
65	65. A empresa possui uma metodologia de auditoria prévia de privacidade e proteção de dados para fins de negociação com terceiros?
	Sim
	Não
66	66. A empresa possui políticas de privacidade (interna e externa) e boas práticas com relação a proteção de dados pessoais alinhadas com as regras da LGPD?
	Sim
	Não
67	67. A empresa possui algum tipo de metodologia para fins de acompanhamento das alterações jurídicas, legais e de jurisprudência relacionadas à LGPD e proteção de dados pessoais no Brasil?
	Sim
	Não

Fonte: Diagnóstico LGPD, 2019

ANEXO B

QUESTÕES PARA SUBSIDIAR O QUESTIONÁRIO DIAGNÓSTICO

Questões sobre LGPD de fontes diversas
Quantos funcionários a empresa possui?*
Qual o produto ou serviço desenvolvido pela empresa?*
Qual tipo de negócio é realizado?*
A empresa possui certificações ISO ou similares?*
Existe setor ou comitê para implementação da LGPD?*
Os fluxos de dados da empresa estão mapeados e formalizados?*
A empresa possui documentação de processos internos?*
Possui políticas de segurança da informação documentadas?*
Possui manuais de conduta do usuário de tecnologia?*
Possui documentos que auxiliem os profissionais na realização de suas atividades?*
Sua empresa mantém negócios com outros países? Se sim, quais?*
A empresa utiliza câmeras de vigilância?*
Em algum momento são coletados dados biométricos de funcionários ou clientes?*
A hospedagem dos arquivos e banco de dados da empresa estão em qual país?*
Selecione o cenário tecnológico da estrutura de servidores.*
Quantidade de servidores físicos:*
Quantidade de servidores virtuais:*
Selecione o modo como backups são armazenados.*
Quais mecanismos de segurança da informação a empresa utiliza em seu ambiente?*
Quantidade de estações de trabalho:*
É permitido que os colaboradores utilizem dispositivos pessoais para realizar suas atividades de trabalho?*
É permitido que os colaboradores levem dispositivos da empresa para locais externos?*
Quantos departamentos existem dentro da empresa? Exemplo: RH, Financeiro, Marketing, Comercial, etc.*
São oferecidos benefícios que se estendem a dependentes ou parentes do empregado? (Cônjuge, filhos, etc)*
A empresa terceiriza sua folha de pagamentos?*
A empresa possui contrato com plataforma de recrutamento ou headhunter?*
A empresa possui atividades de marketing direcionado a pessoas físicas?*

A empresa possui contrato com empresas de DBM (*database marketing*) e CRM (*customer relationship management*)?*
A empresa utiliza disparadores de e-mail, sms, etc?*
A empresa possui site que coleta cookies?*
Qual é o seu nome? *
Qual o seu cargo ? *
Qual é o nome da sua empresa ou grupo econômico? *
Ramos de atividade
Ramos de atividade
A sua empresa presta serviços ou vende produtos para pessoas físicas localizadas na União Europeia, Japão ou Canadá ?
A sua empresa vende produtos ou serviços para outros países ? Quais ?
De quem são os dados pessoais tratados pela empresa? *
Quantos departamentos da sua empresa tratam dados pessoais de clientes, funcionários e terceiros? *
Aproximadamente quantos processos internos da empresa envolvem o tratamento de dados pessoais? * Exemplo : RH - Tem um processo onde ocorre o tratamento de dados pessoais na admissão de novo empregado
Quantos softwares internos ou de terceiros controlam bases de dados pessoais?
Os dados pessoais tratados pela empresa ou terceiros estão armazenados fora do país ?
Os dados pessoais tratados pela empresa ou terceiros estão armazenados fora do país ?
Há formalização de consentimento dos titulares de dados pessoais * (clientes, funcionários etc.) para a realização dos tratamentos desses
Quais tipos de dados pessoais são tratados pela sua empresa? *
Os dados pessoais tratados pela empresa são compartilhados com * outras empresas localizadas no estrangeiro ?
A sua empresa possui política de segurança da informação ou * governança de proteção de dados pessoais?
Informe o grau de dependência de tecnologia em sua operação*
Informe o nível de maturidade em Gestão de Riscos da sua empresa
Informe aqui o grau de exposição a fraudes e cibercrime do setor onde sua empresa atua*
Sua empresa atua num setor com normas e regulamentações específicas para o seu mercado? *
Sua empresa já realizou o mapeamento de dados? *
Sua empresa documentou quais dados pessoais vocês possuem, de onde vieram, com quem você os compartilha e o que fazem com eles?
Sua empresa identificou suas bases legais para processamento e as documentou? *
Sua empresa está ciente de como funciona o consentimento para tratamento de dados pessoais, segundo nova LGPD?
Sua empresa possui sistemas para registrar e gerenciar os consentimentos dados, assim como para possibilitar a revogação de consentimento? *
Sua empresa faz o armazenamento seguro dos dados pessoais que trata? *

Sua empresa forneceu informações sobre as finalidades do tratamento de cada dado pessoal para os titulares? *
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? *
Sua empresa possui Politicas de privacidade adequadas às LGPD?
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? *
Seus funcionários estão cientes da política de proteção de dados da empresa? *
Os contratos da sua empresa estão adequados com a LGPD? *
Sua empresa entende quando um relatório de impacto à proteção de dados é necessário? *
Sua empresa já nomeou o Encarregado (DPO)? *

Fonte: Alexandre Atheniense Advogados, 2019; Ministério Público Federal, 2019; Mosimann, Horn & Advogados Associados, 2019