LEI GERAL DE PROTEÇÃO DE DADOS E A QUESTÃO DA CONFORMIDADE DE MICRO, PEQUENAS E MÉDIAS EMPRESAS

Matheus de Azevedo Michalski[1]

Daniela Pellin[2]

RESUMO

A Lei Geral de Proteção de Dados irá atingir empresas brasileiras de todos os tamanhos e começou a vigorar em setembro de 2020, no entanto, no meio empresarial há dificuldades no processo de conformidade com a nova regulação. Nesse sentido, o problema que este estudo visa responder consiste na seguinte pergunta de pesquisa: As conformidades exigidas pela LGPD podem ser implementadas de forma diferenciada em micro, pequenas e médias empresas de acordo com o tratamento constitucional distinguido? Para isso, o objetivo geral da pesquisa é propor um *framework* para a implementação da conformidade da Lei Geral de Proteção de Dados às micro, pequenas e médias empresas. Para responder ao problema de pesquisa e atender ao objetivo geral proposto, a metodologia utilizada é a *Design Science Research*, que através das suas sete etapas, viabiliza o desenvolvimento de artefato, na forma de um fluxograma de trabalho para que micro, pequenas e médias empresas consigam implementar tais conformidades. Para validar o artefato, será construído cenário para verificação da conformidade. Como conclusão, o estudo foi capaz de confirmar a hipótese de que é possível oferecer às micro, pequenas e médias empresas um fluxo de trabalho compatível com as suas condições econômicas e que as coloquem em conformidade com a Lei Geral de Proteção de Dados, tendo em vista o seu tratamento constitucional diferenciado estabelecido no artigo 170, da Constituição Federal, representando, com isso, impactos de sustentabilidade econômica e competitividade.

PALAVRAS-CHAVE: Lei Geral de Proteção de Dados; Gestão de Dados Pessoais; ME/EPP; Constituição Federal; Conformidade.

ABSTRACT

The General Data Protection Law (LGPD) has been impacted Brazilian companies of all sizes and took effect since September 2020. However, in the business environment, there are challemges in achieving compliance with the new regulation. In this context, the problem that tis study aims to adress is the following research question: can the compliance requirements of the LGPD be implemented differently in Micro, Small, and medium-sized enterprises based on distinguished constitutional treatment? To achieve this, the general objective of the research is to propose a framework for implementation LGPD compliance in Micro, Small, and Medium-sized enterprises. In order to adress the research problem and achieve the proposed general

[1] Administrador de Empresas com ênfase em Gestão para Inovação e Liderança pela UNISINOS. Empresário. Email: matheus.michalskii@gmail.com

[2] Professora Pesquisadora do Programa do Mestrado Profissional em Direito da Empresa e dos Negócios da UNISINOS. Pós-Doutora em Direito Privado pela UFRGS/RS. Doutora em Direito Público pela UNISINOS/UNIVERSITÀ DEGLI STUDI DI PADOVA (Itália). Mestre em Direito da Sociedade da Informação. Especialista em Direito Empresarial e Governança de TI. Advogada e Empresária. E-mail: dpellin@unisinos.br

objective, the methodology used is Design Sciense Research, which, through its seven steps, facilitates the development of an artifact in the form a workflow diagram. This diagram is intended to help micro, small and medium-sized enterprises implement the required compliances. To validate the artifact, a scenario is going to be constructed to verify the compliance. The study was able to confirm the hypothesis that it is possible to provide micro, small, and medium-sized enterprises with a workflow compatible with their economic conditions, bringing them into compliance with the General Data Protection Law. This takes into account their constitutionally differentiated treatment established in Article 170 of the Federal Constitution, representing economic sustainability and competitiveness impacts.

KEYWORDS: General Data Protection Law; Personal Data Management; Micro, Small and Medium-sized enterprises; Federal Constitution; Compliance.

1 INTRODUÇÃO

A Organização para a Cooperação e Desenvolvimento Econômico (OCDE) aponta que o processamento e utilização de dados pessoais é um ativo para as empresas, capaz de gerar benefícios econômicos e sociais. No entanto, existem desafios em relação a proteção e ao escopo das regulações de proteção da privacidade (OCDE, 2013).

Essa discussão não é nova. Em 1890, o artigo *The Right to Privacy* já afirmava que "recentes inovações e métodos de negócio chamam atenção para o próximo passo que deve ser dado para a proteção da pessoa e segurança do indivíduo[3]" (WARREN, BRANDEIS, 1890, p.195, tradução nossa). Isso sinaliza que, mesmo há 130 anos, novos negócios e inovações já indicavam problemas na sua relação com a privacidade individual. Nos dias de hoje, o único aspecto que mudou daqueles tempos parece ser a forma como isso acontece.

Com o avanço das tecnologias nos últimos anos, a questão de Privacidade de Dados adquiriu ainda maior relevância no Brasil, principalmente devido a transformação dos dados em um ativo econômico para algumas empresas (SILVEIRA *et al.*, 2016). Doneda e Mendes (2018) argumentam que a privacidade de dados se transformou em um tema ímpar para a segurança de um indivíduo, tendo em vista que o contexto atual é de um mundo hiperconectado, em que as informações circulam de forma simples e veloz. Nesse sentido, os autores comentam da necessidade de regulações para garantir a privacidade nesse novo cenário, tanto na esfera física quanto na digital, com objetivos bastante específicos.

Embora a Constituição Federal de 1988, no artigo 5º, tenha instituído a privacidade como um direito fundamental inviolável, o Brasil adotou legislação específica sobre o tema Privacidade de Dados envolvendo todas as organizações com atividades econômicas e os

[3] Recent innovations and business methods call attention to next step which must be taken for the protection of the person and for the securing to the individual.

cidadãos consumidores no trânsito informacional de dados pessoais. Trata-se da Lei 13.709 de 2018, conhecida como Lei Geral de Proteção de Dados (LGPD). Conforme o novo cronograma, a Lei Geral de Proteção de Dados entrou em vigor em setembro de 2020. Belli *et al.* (2018) definem a LGPD como uma versão brasileira do Regulamento Europeu de Proteção de Dados (GDPR) e da Convenção 108 do Conselho da Europa. Zanatta (2019) corrobora com essa visão, adicionando que a GDPR provocou uma espécie de efeito guinada em diversos outros países sobre a necessidade de legislações específicas sobre privacidade de dados, definindo essas legislações como "Códigos de Defesa do Consumidor" do Século XXI.

A grande questão é que a adaptação para a nova regulação pode gerar custos elevados para as empresas. De acordo com Koski e Valmari (2020), as empresas europeias contrataram, em conjunto, cerca de 500 mil *Data Protection Officers*, especialistas em proteção de dados, representando um custo adicional coletivo de 40 bilhões de Euros para as organizações. Os autores ainda argumentam que a GDPR, em alguns modelos de negócios, afetou a expectativa de retornos por parte de investidores, dificultando o financiamento dessas empresas junto a investidores.

Esta perspectiva pode refletir sobre o caso brasileiro de uma forma ainda mais intensa, tendo em vista que Rapôso *et al.* (2019) adicionam outro desafio no caso das empresas brasileiras: a insegurança jurídica[4], afirmando que a aplicação prática da LGPD nas empresas brasileiras está sendo desorganizada e confusa. Nesse sentido, embora haja crescente literatura acadêmica sobre o tema da Lei Geral de Proteção de Dados, há lacuna na questão de sua aplicabilidade nas rotinas do contexto empresarial brasileiro, principalmente nos casos específicos de pequenas e médias empresas, que terão de entrar a conformidade com a nova legislação.

Com este contexto, o problema que esta pesquisa visa responder é: As conformidades exigidas pela LGPD podem ser implementadas de forma diferenciada em micro, pequenas e médias empresas de acordo com o tratamento constitucional distinguido?

Sendo assim, o objetivo geral deste estudo é propor um *framework* de implementação da conformidade da LGPD às micro, pequenas e médias empresas. Para isso, os objetivos específicos desta pesquisa são:

I. Analisar os impactos regulatórios sobre a Proteção de Dados Pessoais em

[4] O termo "insegurança jurídica" está sendo aplicado na pesquisa no sentido da ausência de parâmetros quanto ao alcance jurídico e aos impactos econômicos imprevisíveis na estruturação interna e na operação externa da proteção dos dados pessoais, transformando o processo de adaptação inseguro para as empresas.

relação aos tópicos que afetam as rotinas operacionais diárias das empresas;

II. Construir um fluxograma de trabalho e de baixo custo que contenha práticas de gestão adequadas às Micro, Pequenas e Médias Empresas para que possam se conformar com a LGPD na medida de suas peculiaridades socioeconômicas;

III. Avaliar o fluxograma de trabalho em um cenário de cadastro de clientes em uma empresa do setor de serviços.

Para responder ao problema de pesquisa e alcançar o objetivo proposto, será utilizada a metodologia de *Design Science Research*, que utiliza a pesquisa com o objetivo final da concepção de um artefato, modelo, constructo ou método (DRESCH *et al.*, 2015). Após a conclusão deste estudo, empreendedores, gestores e executivos poderão utilizar os resultados encontrados neste artigo para modificar processos e adequar as empresas em que atuam à nova legislação de proteção de dados.

Além desta introdução ao tema, o artigo se dividirá em quatro outras seções. Na Seção 2, será apresentado o referencial teórico que dá suporte ao estudo. Na Seção 3, serão expostas a metodologia de pesquisa que dará suporte a construção do artefato. Por último, nas Seções 4 e 5, serão discutidos os resultados da pesquisa e feitas considerações finais, confirmando ou não a hipótese de que é possível oferecer às micro, pequenas e médias empresas um fluxo de trabalho compatível com suas condições econômicas e que as coloquem em conformidade com a LGPD na medida do seu tratamento constitucional diferenciado estabelecido no artigo 170 da Constituição Federal, representando, com isso, impactos de sustentabilidade econômica e competitividade.

2 O CONTEXTO ESTRUTURAL E FUNCIONAL DA LGPD

2.1. Lei Geral de Proteção de Dados

O direito à vida privada é entendido como fundamental e inviolável pela Constituição Federal de 1988 (BRASIL, 1988). Nesse sentido, a Lei 13.709/2018, conhecida como Lei Geral de Proteção de Dados, foi fundamentada para assegurar a privacidade, a liberdade de expressão e a preservação da honra, não deixando de lado, também, os aspectos mercadológicos relacionados às empresas, através da proteção da livre iniciativa e da livre concorrência, além da garantia ao desenvolvimento tecnológico e a inovação (BRASIL, 2018). Do ponto de vista estrutural, Doneda e Mendes (2018) analisam que a LGPD é composta por

cinco pilares:

> i)unidade e generalidade da aplicação da Lei; ii) legitimação para o tratamento de dados (hipóteses autorizativas); iii) princípios e direitos do titular; iv) obrigações dos agentes de tratamento de dados; v) responsabilização dos agentes. (DONEDA E MENDES, 2018, p. 471)

O pilar de unicidade e generalidade da aplicação da lei está expresso no artigo 3º da LGPD: todas as pessoas físicas e jurídicas, de direito público ou privado, registradas, no Brasil ou no exterior, mas que comercializem produtos ou serviços para indivíduos dentro do Brasil, bem como aquelas que coletam dados no Brasil estão sujeitas a aplicação dos termos da LGPD (BRASIL, 2018). Esse fato torna a LGPD uma legislação de extrema relevância, visto que conforme o Serviço Brasileiro de Apoio às Micro e Pequenas Empresas (SEBRAE), atualmente, existem mais de 19 milhões de empresas registradas no Brasil (SEBRAE, 2020).

Com relação aos princípios e direitos do titular, presentes do artigo 18 ao artigo 22 da LGPD, Doneda e Mendes (2018) destacam a questão da obrigação de dar ao usuário cidadão consumidor o direito de exercer o consentimento, de ser informado de forma transparente acerca do tratamento de seus dados e, sobretudo, ser informado acerca da finalidade que será dada ao ceder seus dados, fatores que, em conjunto, devem deixar claro para o cliente ou usuário o fator que motivou a coleta e o tratamento dos dados. Na questão de legitimação para o tratamento de dados, o entendimento sobre a definição específica do conceito de dados pessoais é importante. Assim, para a LGPD, dado pessoal consiste em "informação relacionada a pessoa natural identificada ou identificável" (BRASIL, 2018). Também é relevante a definição de dado pessoal sensível, isto é, o dado pessoal que contenha informações sobre algumas esferas específicas da vida íntima e privada de uma pessoa, como:

> Dado pessoal sobre 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 (BRASIL, 2018, art. 5º).

Ainda na questão de dados individuais, a LGPD também aborda o conceito de dado anonimizado, cuja definição comporta "dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento" (BRASIL, 2018). Ao observar o ponto de vista prático em relação à LGPD, Quiroga (2018) argumenta que se os dados pessoais fossem tratados de maneira individual carregariam problemas menores do que nos casos em que é realizado o seu tratamento em conjunto, situação essa que apresenta riscos reais à violação da privacidade e intimidade da

pessoa. A Lei Geral de Proteção de Dados define Tratamento de Dados da seguinte maneira:

> Toda operação realizada com dados pessoais, como as que se referem 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 (BRASIL, 2018, art. 5º).

Especificamente no tema de tratamento de dados, a LGPD indica que nos casos em que houver tratamento de dados pessoais, é obrigatório o consentimento desta atividade por parte do titular das informações, exceto nas situações de cumprimento de obrigação legal ou regulatória, realização de estudos por órgãos de pesquisa, exercício regular de direitos, proteção da vida do titular, prevenção à fraudes e tutela da saúde em procedimentos realizados por profissionais da saúde, serviços da saúde ou autoridade sanitária (BRASIL, 2018). A questão legal acerca do tratamento de dados pode parecer algo distante do cotidiano quando observada do ponto de vista legal, mas é algo rotineiro para as empresas, que podem utilizar as informações que possuem sobre os seus clientes para definir estratégias de marketing, distribuição e suporte (SILVEIRA *et al.*, 2016).

Do ponto de vista da responsabilização dos agentes, Parentoni (2019) aponta que todo sistema de proteção de dados pessoais precisa ter como premissa uma instituição reguladora, acumulando a questão de privacidade de dados junto as suas outras atribuições. Assim, um dos principais termos da Lei Geral de Proteção de Dados é a criação da Autoridade Geral de Proteção de Dados, caracterizada como órgão público subordinado à Presidência da República, cuja responsabilidade é fiscalizar o cumprimento dos termos da LGPD, impondo sanções às empresas que, não tenham processos de tratamento de dados ou os tenham em desconformidade ou em conformidade insuficiente e, consequentemente, não atendam aos critérios previstos na lei, de tal forma que retirem o direito de informar o usuário cidadão consumidor sobre os direitos e deveres em relação a garantia da privacidade dos seus dados pessoais (BRASIL, 2018).

Segundo Quiroga (2018), as instituições públicas e privadas, no curso das suas rotinas operacionais diárias, acabam criando bancos de dados com informações de cidadãos, clientes e fornecedores, dependendo da atividade. Nakamura *et al.* (2019) também argumentam que as empresas, em pelo menos um de seus processos operacionais, manejam dados pessoais de terceiros. Mendes (2018) adiciona que as últimas gerações são as sociedades que mais geraram dados pessoais em toda a história. Em razão disso, Nakamura *et al.* (2019) concluem que é necessário que as empresas que pretendem utilizar esses bancos de dados para fins

econômicos tenham processos bastante definidos, como forma de minimizar os riscos gerados pelo tratamento de dados pessoais, o que cria um potencial problema na questão da conformidade com a nova regulação brasileira referente a proteção de dados.

2.2 Gestão de Dados Pessoais em Empresas

A LGPD surge no momento em que a Organização para Cooperação e Desenvolvimento Econômico (OCDE) aponta que o tratamento de dados, embora reconhecidamente benéfico para os campos econômico e social, traz desafios tanto para a privacidade dos indivíduos quanto para a gestão de riscos das empresas, principalmente nos casos de vazamentos de dados de clientes ou usuários (OCDE, 2013). Assim, a Lei Geral de Proteção de Dados pode ser entendida como um novo paradigma socioeconômico sobre gestão e tratamento de dados pessoais em empresas e instituições públicas. No entanto, para Rapôso *et al.* (2019), no caso brasileiro, as empresas estão tendo sérias dificuldades para entrar em conformidade com a nova legislação, visto que a discussão acerca da aplicabilidade deste tema ainda é muito vaga.

Essa visão é complementada por uma pesquisa realizada pela Serasa *Experian* (2019) com 508 empresas de 18 setores, cujos resultados apontam que 85% das empresas brasileiras ainda não estão prontas para atender aos direitos e deveres estabelecidos na Lei Geral de Proteção de Dados, sendo que 72% da amostra de empresas com mais de 100 funcionários pretende contratar algum tipo de profissional especializado ou consultoria para auxiliar no processo de conformidade a LGPD. Outro levantamento realizado pela empresa de consultoria ICTS Protiviti (2020) deixa claro que as micro e pequenas empresas, com faturamento anual de até R$ 4.8 milhões, estão atrás em relação às grandes empresas na questão de adaptação à LGPD. Por isso, fica evidente a necessidade de metodologias e *frameworks* para ajudar a resolver este problema.

Na questão do processo de gestão e tratamento de dados pessoais, Nakamura *et al.* (2019) cita os *frameworks* da família NBR ISO/IEC 27.000 como o modelo mais utilizado pelas empresas para garantir a segurança dessa rotina operacional, na qual as informações circulam a todo o momento. Lopes e Guarda (2019) adicionam que a norma ISO 27.001 é o principal *framework* internacional em relação a gestão de segurança de informações que, hoje, em dia, é tema relevante para as empresas atingirem os seus objetivos estratégicos. No fim de 2019, houve extensão da NBR ISO/IEC 27.001:2013 através da NBR ISO/IEC 27.701:2019,

com o objetivo de incluir novas diretrizes acerca do tratamento de dados, em virtude da implementação da Lei Geral de Proteção de Dados no Brasil (ABNT, 2019).

Segundo a NBR ISO/IEC 27.701 (2019), o número de situações em que as empresas tratam dados pessoais em cooperação com outras vêm aumentando nos últimos anos, fato que corrobora à necessidade de as organizações terem Sistemas de Gestão de Segurança da Informação (SGSI). Piurcosky *et al.* (2019) argumentam que as empresas devem adotar os SGSI para mitigar riscos relacionados a violações na privacidade de dados dos seus usuários e clientes, evitando sanções legais, que podem gerar impactos negativos na performance financeira dos seus negócios. A política de SGSI pode "ser vista como um guia de procedimentos para proteger os dados que a organização tem em seu poder e a forma de sua utilização" (PIURCOSKY *et al.*, 2019, p. 91).

Nesse sentido, Cavoukian (2020) discute o conceito de *Privacy by Design* e o define como uma mudança de paradigma no entendimento da proteção de dados dentro do contexto empresarial, principalmente em empresas dependentes do mercado digital, conceituando-o como uma estrutura para implementar o cuidado com a privacidade dos clientes e usuários dentro do funcionamento das operações, processos, produtos e serviços das organizações. Cavoukian (2020) também cita que as empresas podem utilizar isso como um elemento para o ganho de confiança com os seus clientes e com o mercado, o que representa benefícios no longo prazo. Doneda e Mendes (2018) relacionam a LGPD com o conceito de *Privacy by Design*, como princípio da prevenção, que está exposto no artigo 6º da LGPD, através do qual as empresas podem se antecipar às demandas necessárias para adequação dos seus produtos, serviços e processos à legislação vigente. Para Cavoukian (2020), o conceito de *Privacy by Design* é composto por 7 princípios fundamentais:

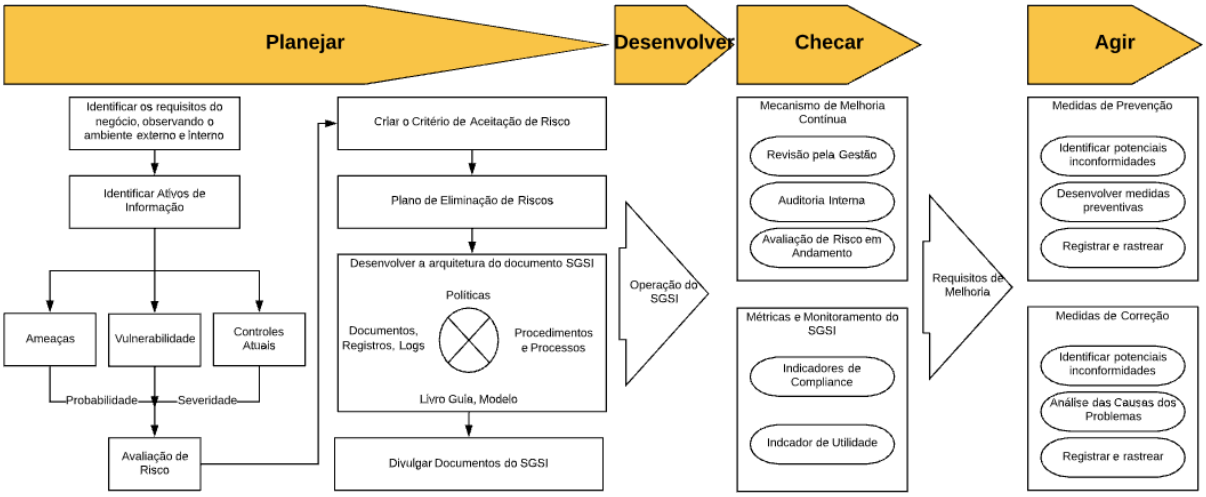
> 1) proactive not reactive, which focuses on prevention; 2) privacy as the default setting; 3) privacy embedded into design; 4) full functionality (not zero-sum!); 5) end-to-end security; 6) visibility and transparency; and 7) respect for user privacy[5] (CAVOUKIAN, 2020, p. 79).

Conforme Lopes e Guarda (2019), a adequação à ISO 27.001 é baseada em três pilares: pessoas, processos e tecnologia, e tem como objetivo ajudar a empresa a aumentar a eficiência de processos, proteger dados pessoais e a reputação da companhia, além de buscar auxiliar a

[5] 1. proativa, não reativa, que foca na prevenção; 2. privacidade como configuração padrão; 3. privacidade inclusa no design; 4. total funcionalidade (não soma zero); 5. segurança ponta- a-ponta; 6. visibilidade e transparência 7. respeito pela privacidade do usuário (tradução livre)

empresa a entrar em conformidade com as regulações locais de proteção de dados. Para Sun *et al.* (2020), as empresas podem criar os seus SGSI, entrando em conformidade com a norma ISO 27.001, através de processos que seguem um ciclo com quatro fases: planejar, fazer, checar e agir, que focam respectivamente em requisitos e arquitetura dos processos, utilização de medidas de avaliação de riscos adequadas, monitoramento das operações e melhoria contínua dos processos, como pode ser observado na figura abaixo.

Figura I - Implementação do SGSI em empresas



Fonte: Adaptado de Sun et al. (2019)

No entanto, embora os *frameworks* da família NBR ISO/IEC 27.000 sejam um modelo amplamente utilizado no contexto empresarial, Nakamura *et al.* (2019) alertam que ao serem utilizados de forma isolada, estes modelos não fazem com que as empresas entrem em total conformidade com os requisitos da LGPD. Além disso, a argumentação de Piurcosky *et al.* (2019) criam um contraste de perspectiva entre o *framework* e a LGPD, pois enquanto as normas da família NBR ISO/IEC 27.000 buscam criar procedimentos para minimizar riscos para as empresas, a LGPD busca "proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da pessoa natural" (BRASIL, 2018). Isso provoca a necessidade de as empresas utilizarem outros instrumentos para entrarem em conformidade de maneira integral à Lei Geral de Proteção de Dados, tópico que será o centro das próximas seções deste artigo.

3 MATERIAL(IS) E MÉTODOS

A metodologia é a estrutura normativa do procedimento científico, que tem como objetivo apresentar a forma que o pesquisador chegou aos resultados do estudo, possibilitando que outras pessoas que sigam o mesmo método alcancem uma descoberta similar (MATIAS-PEREIRA, 2016). Com relação a natureza de pesquisa, este estudo se enquadra em uma pesquisa exploratória, que se mostra o mais adequado para o problema de pesquisa proposto, pois de acordo com Gil (2008), a natureza exploratória é o melhor método para temas de pesquisa ainda pouco explorados. Ainda, Matias-Pereira (2016) sugere que seja utilizada a pesquisa aplicada, que tem como objetivo gerar produtos e processos que possam ser utilizados de maneira imediata.

Quanto aos procedimentos, essa pesquisa será conduzida através da metodologia *Design Science Research*, que de acordo com Dresch *et al.* (2015), tem o objetivo de possibilitar a projeção e construção de artefatos, constructos, modelos e *frameworks*, além de expandir a base de conhecimento já existente. Com relação ao conceito de artefato, corresponde à "organização dos componentes do ambiente interno para atingir objetivos em um determinado ambiente externo" (DRESCH *et al.*, 2015, p.57). Hevner *et al.* (2004) argumentam que os artefatos oriundos de pesquisas realizadas através de *Design Science* possuem a finalidade de auxiliar na resolução de problemas enfrentados pelas empresas.

Com relação ao método de pesquisa, Hevner *et al.* (2004) propuseram um padrão para a atividade de pesquisa em trabalhos que utilizam *Design Science Research*, indicando que essa metodologia possui 7 diretrizes principais: relevância do problema, rigor de pesquisa, *design* como processo de pesquisa, *design* como artefato, avaliação do artefato, contribuições da pesquisa e comunicação da pesquisa. Dresch *et al.* (2015) ainda acrescentam que essas etapas costumam passar pelas abordagens científicas abdutiva, dedutiva e indutiva, visto que a proposta de apresentar um artefato ou solução como produto de pesquisa não poderia ser atingida com os mesmos métodos de pesquisa utilizados nas ciências tradicionais. Conforme Hevner *et al.* (2004), cada uma das 7 etapas de pesquisa possui papel relevante para a criação de artefatos que possam ser implementados nas empresas.

Assim, segundo Hevner *et al.* (2004), em *Design Science Research*, a descrição de cada uma das diretrizes de pesquisa é a seguinte: relevância do problema consiste na relação entre o problema enfrentado pelas empresas e as oportunidades de solução, baseadas em diminuição de custo ou aumento de receita. Rigor de pesquisa é tratado como o uso efetivo de bases teóricas e métodos sistematizados para a criação do artefato. *Design* como processo de pesquisa é a utilização do design com o objetivo de buscar soluções válidas para um problema.

Design como artefato é a concepção do modelo, constructo ou *framework* para resolver de maneira efetiva um problema relevante nas rotinas empresariais. Avaliação do artefato é o processo utilizado para testar o que foi concebido, sendo que o *feedback* serve para melhorar o artefato. Contribuições da pesquisa são os avanços que o estudo e o artefato trouxeram para o campo de conhecimento e para o campo de negócios. Por último, comunicação da pesquisa corresponde a difusão do artefato desenvolvido no estudo dentro do mundo empresarial. Utilizando as diretrizes de Hevner *et al* (2004), as etapas de pesquisa e a maneira como elas serão inseridas neste estudo foram sistematizadas em uma tabela.

Tabela I – Aplicação da *Design Science Research* na pesquisa

Diretriz	Aplicação da diretriz nessa pesquisa
Relevância do Problema	A Lei Geral de Proteção de Dados entra em vigor no mês de agosto de 2021 e cerca de 85% das empresas ainda não estão adaptadas (SERASA EXPERIAN, 2019). Ainda, Rapôso *et al.* (2019) argumentam que a regulamentação ainda está distante do cotidiano das empresas, que não possuem domínio acerca dos procedimentos para conformidade.
Rigor de Pesquisa	Através da Design Science Research, será criado um artefato, conforme apontado por Hevnet *et al.* (2004). O artefato terá como base os cinco eixos da Lei Geral de Proteção de Dados propostos por Doneda e Mendes (2018) e será modelado através do método de *Business Process Modeling Notation* (BPMN).
Design como processo de pesquisa	Hevner *et al.* (2004) argumenta que o artefato construído deve ter como base os problemas que ele pretende solucionar, que no caso deste artigo consistem na adaptação de pequenas e médias empresas a Lei Geral de Proteção de Dados. Desta forma, o artefato será desenvolvido através da análise dos requerimentos da Lei Geral de Proteção de Dados, observando os cinco pilares da LGPD apontados por Doneda e Mendes (2018), os quais já foram abordados na fundamentação teórica. Assim, serão mapeados quais Artigos da LGPD de acordo com a sua relação com o universo empresarial, tendo em vista que muitos pontos da Lei estão relacionados ao Poder Público, que não é objeto de estudo deste artigo.
Design como artefato	A forma do artefato será um fluxograma de trabalho, que torne simples e prática a adaptação de empresas às exigências da Lei Geral de Proteção de Dados.
Avaliação do artefato	A avaliação do artefato será feita através da criação de um cenário de utilização para o modelo proposto. Para Dresch *et al.* (2015), esse método de avaliação do artefato se enquadra no formato descritivo, pois a construção de cenários permite que a utilidade do modelo seja comprovada.

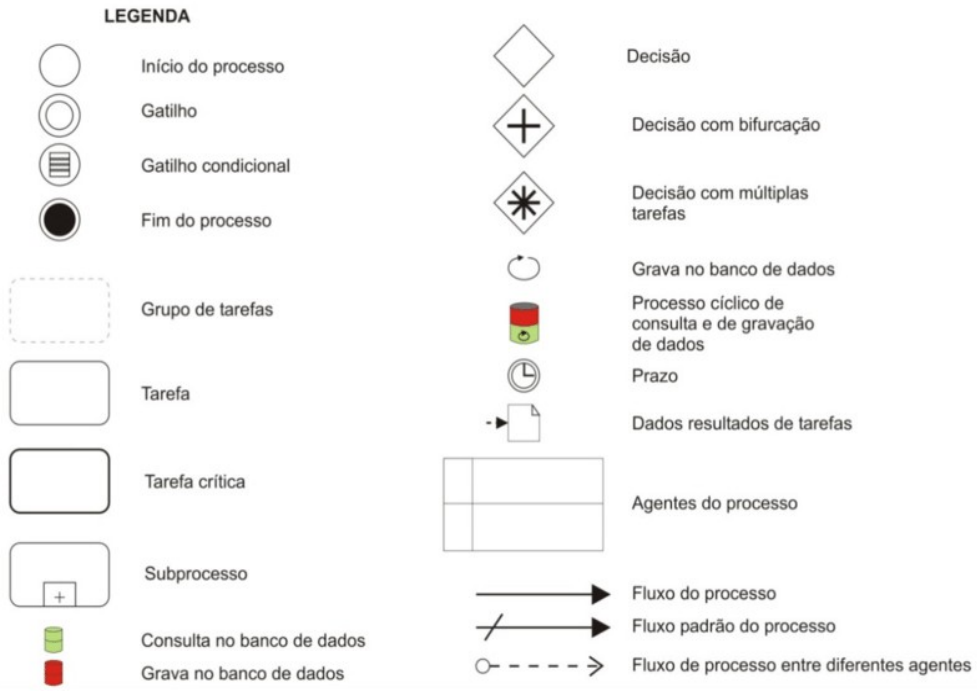
Contribuições da pesquisa	A principal contribuição desta pesquisa é um fluxograma de trabalho voltado para as empresas entrarem em conformidade com a Lei Geral de Proteção de Dados.
Comunicação da pesquisa	Os principais *stakeholders* da pesquisa são gestores e proprietários de micro, pequenas e médias empresas brasileiras.

Fonte: elaborado pelo autor.

Em razão de a Lei Geral de Proteção de Dados se tratar de uma legislação aplicável tanto para instituições privadas quanto para instituições públicas, para a criação do artefato, serão considerados apenas os Artigos da LGPD que sejam válidos para organizações privadas, nos moldes dos cinco eixos da LGPD apontados por Doneda e Mendes (2018). Ainda, nos estudos que utilizem Design Science Research, a avaliação do artefato produzido pelo estudo é essencial (DRESCH *et al.*, 2015). Neste sentido, os fluxogramas de trabalho deste estudo serão avaliados utilizando a criação de cenários, por meio do formato descritivo. Assim, o modelo proposto neste estudo será inserido dentro da situação do cadastro de uma empresa de serviços que realize operações de tratamento de dados com finalidade econômica, com o objetivo de validar a utilização do artefato em um ambiente empresarial.

Por se tratar de um fluxograma de trabalho, sua criação será feita utilizando as técnicas do *Business Process Modeling Notation* (BPMN), que conforme Maranhão e Macieira (2008), consiste em uma metodologia que une Gestão e Tecnologia da Informação, propondo uma série de regras e normas utilizadas para padronizar a modelagem de processos de trabalho, sendo por isso a mais adequada para ilustrar o artefato que este trabalho busca desenvolver. A modelagem de processos através do BPMN possui ilustrações próprias, descritas na figura.

Figura II – Legendas do *Busines Process Modeling Notation* (BPMN)



Fonte: França (2016)

Na próxima seção deste estudo, as diretrizes apresentadas na tabela I serão utilizadas como base para atingir o objetivo geral da pesquisa, através da concepção de um artefato para que micro, pequenas e médias empresas consigam entrar em conformidade com a Lei Geral de Proteção de Dados.

4 *DESIGN* DO ARTEFATO

Nas pesquisas com o método *Design Science Research*, desenvolve-se um artefato ou constructo com o objetivo de resolver um problema relevante nas organizações. Nesse sentido, especificamente nessa pesquisa, o artefato que será desenvolvido no seu decorrer, terá a forma de um fluxograma de trabalho, tendo como base as principais exigências estabelecidas nos termos da Lei Geral de Proteção de Dados.

4.1 A Lei Geral de Proteção de Dados e as Empresas

Com o objetivo de facilitar o entendimento acerca das exigências da LGPD, assim como já foi colocado em uma seção anterior, a qual tratava do contexto estrutural e funcional da Lei Geral de Proteção de Dados, é importante observar o trabalho de Doneda e Mendes (2018), que dividiram a LGPD em cinco pilares: unidade e generalidade de aplicação,

requisitos para o tratamento de dados, princípios e direitos do titular dos dados, deveres dos agentes que realizam o tratamento de dados, bem como a sua responsabilização em caso de eventuais desvios em relação à legislação, os quais já foram detalhados em profundidade na fundamentação teórica deste artigo. Assim, é possível observar com maior clareza as categorias dos objetivos da legislação, o que por sua vez também pode auxiliar as empresas a visualizarem o que é preciso ser feito para adaptação correta a nova legislação.

Utilizando como base os cinco pilares conceituados por Doneda e Mendes (2018) para analisar a Lei Geral de Proteção de Dados, foram encontrados 21 artigos que dispõem sobre medidas efetivas que devem ser implementadas pelas empresas, tendo como base a relação entre o tema principal do artigo e os processos empresariais. Esta etapa é relevante na medida que existem uma série de outros artigos na Lei Geral de Proteção de Dados que estão relacionados ao Poder Público e Órgãos Governamentais, que não constituem parte do problema de pesquisa e nem do objetivo geral deste artigo. Os artigos encontrados estão detalhados na tabela abaixo, bem como o tema principal ao qual cada um deles se refere.

Tabela II – Artigos da LGPD que exigem adaptação por parte das empresas

Pilar	Artigo da LGPD	Tema Principal do Artigo
Unidade e Generalidade de Aplicação	Artigo 3º	Operação de Tratamento
Unidade e Generalidade de Aplicação	Artigo 4º	Exceções de Aplicação
Unidade e Generalidade de Aplicação	Artigo 6º	Princípios do Tratamento
Requisitos para o Tratamento de Dados	Artigo 7º	Hipóteses do Tratamento
Requisitos para o Tratamento de Dados	Artigo 8º	Consentimento
Requisitos para o Tratamento de Dados	Artigo 9º	Informações para o Titular
Requisitos para o Tratamento de Dados	Artigo 11º	Tratamento de Dados Sensíveis
Requisitos para o Tratamento de Dados	Artigo 14º	Tratamento de Dados de Crianças e Adolescentes
Requisitos para o Tratamento de Dados	Artigo 15º	Término do Tratamento de Dados
Requisitos para o Tratamento de Dados	Artigo 16º	Eliminação de Dados Pessoais
Princípios e Direitos do Titular	Artigo 18º	Direitos do Titular para o Controlador
Princípios e Direitos do Titular	Artigo 19º	Requisição de Dados Pessoais pelo Titular
Princípios e Direitos do Titular	Artigo 21º	Prejuízo ao Titular

Obrigações dos Agentes de Tratamento	Artigo 37º	Figura Controlador e Operador
Obrigações dos Agentes de Tratamento	Artigo 39º	Instruções para o Operador
Obrigações dos Agentes de Tratamento	Artigo 41º	Encarregado por Dados Pessoais
Obrigações dos Agentes de Tratamento	Artigo 46º	Medidas de Segurança
Obrigações dos Agentes de Tratamento	Artigo 48º	Comunicação sobre Falhas
Obrigações dos Agentes de Tratamento	Artigo 50º	Boas Práticas e Governança
Responsabilização dos Agentes	Artigo 52º	Sanções Administrativas
Responsabilização dos Agentes	Artigo 54º	Tamanho das Sanções

Fonte: elaborado pelo autor.

Todos os artigos inseridos na tabela acima serão utilizados como base para a construção de fluxogramas de trabalho que contenham práticas de gestão adequadas às Micro, Pequenas e Médias Empresas, para que possam se conformar com a LGPD na medida de suas peculiaridades socioeconômicas. Com o intuito de tornar mais simples a visualização das exigências da Lei Geral de Proteção de Dados em Empresas, a próxima seção também será organizada conforme os cinco eixos da Lei Geral de Proteção de Dados, conceituados por Doneda e Mendes (2018).

4.2 Um Modelo para Empresas se adaptarem a Lei Geral de Proteção de Dados

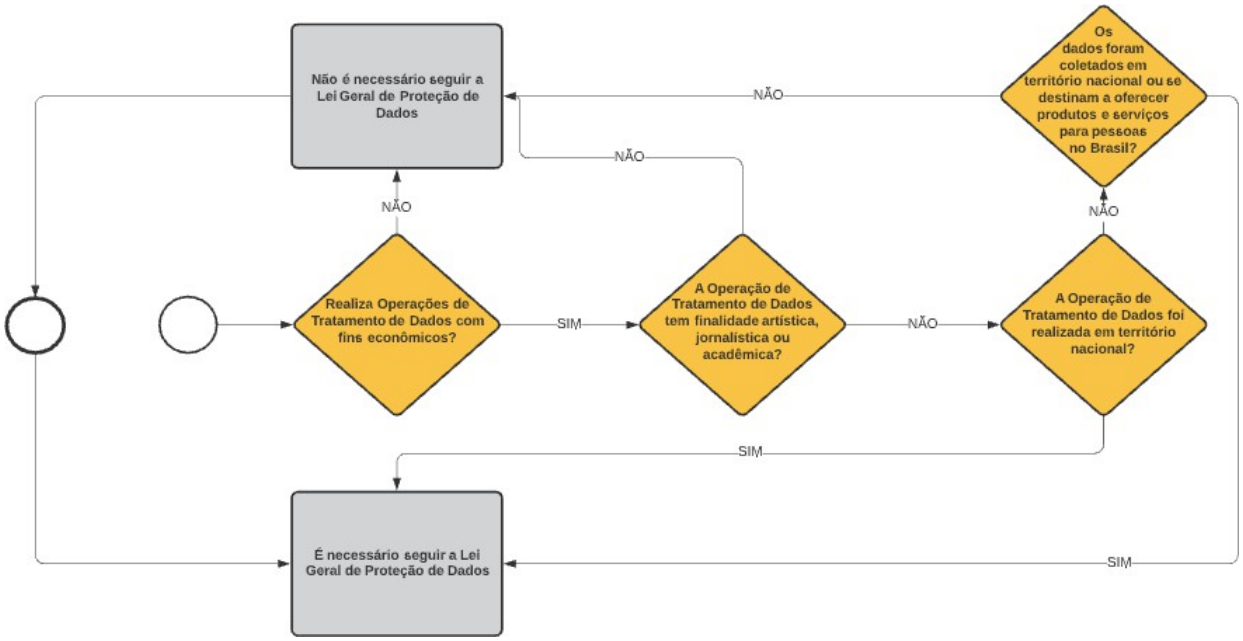
Não são todas as empresas que estão sujeitas à aplicação da Lei Geral de Proteção de Dados, sendo que o requisito base é a operação de tratamento de dados, cujas características já foram definidas em seções anteriores deste trabalho. O artigo 3º da LGPD é bastante claro em relação ao requisito do tratamento de dados, dispondo que os termos da Lei apenas se aplicam a empresas que realizem ou tenham realizado operações de tratamento de dados dentro território nacional, ou operações de tratamento de dados com dados coletados no território nacional, ou ainda operações de tratamento de dados cujo objetivo seja fornecer produtos e serviços para indivíduos localizados no território nacional (BRASIL, 2018).

Também é importante notar a necessidade da finalidade econômica como propósito para a coleta, tratamento e armazenamento dos dados. Com relação ao tratamento de dados, conforme o artigo 4º da LGPD, nos casos de operações de tratamento realizadas por pessoas físicas sem finalidade econômica, ou por empresas quando o tratamento de dados tiver por objetivo fins jornalísticos, artísticos ou acadêmicos, a Lei Geral de Proteção de Dados não se

aplica (BRASIL, 2018). A LGPD também cria diretrizes de boa fé com relação ao tratamento de dados, as quais estão contidas no artigo 6º e consistem nos princípios de finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas (BRASIL, 2018).

Tendo como base os artigos mencionados nos parágrafos anteriores, encontra-se abaixo a figura de um fluxograma cujo objetivo é ilustrar quais são as pessoas jurídicas que devem seguir a Lei Geral de Proteção de Dados, através de figuras de decisão relacionadas as características das operações de tratamento de dados realizadas.

Figura III – Aplicação da Lei Geral de Proteção de Dados



Fonte: elaborado pelo autor.

Através do fluxograma acima, as pequenas e médias empresas podem entender se é necessário adaptar as suas operações em razão da Lei Geral de Proteção de Dados, tendo como base, na realização ou não, de operações de tratamento de dados com finalidade econômica. Após delimitar a abrangência da Lei Geral de Proteção de Dados, isto é, indicar quais são as pessoas jurídicas que devem seguir esta legislação, é necessário observar quais são os princípios e diretrizes que devem nortear todas as operações de tratamento de dados que tenham algum tipo de finalidade econômica.

As operações de tratamento de dados, dependendo do conteúdo e propósito de utilização dos dados, podem criar riscos tanto para empresas quanto para os titulares destas informações (NAKAMURA *et al.*, 2019). Devido a isso, a Lei Geral de Proteção de Dados

impõe uma série de requisitos para as pessoas naturais e jurídicas que realizem a atividade de tratamento de dados com fins econômicos.

Conforme o artigo 7º da Lei Geral de Proteção de Dados, existe uma série de hipóteses que justificam a realização do tratamento de dados: quando existe o consentimento do titular, quando existe a necessidade do cumprimento de exigências regulatórias, legais ou contratuais pela empresa (controlador), quando existe a concepção de estudos realizados por órgãos de pesquisa, quando existe ameaça a vida do titular ou terceiro relacionado, quando existe a necessidade da tutela da saúde, quando existe a necessidade de proteção de crédito ou em qualquer outra situação que atenda interesses do controlador que não violem direitos fundamentais do titular (BRASIL, 2018).

Outro ponto já mencionado anteriormente é que o ato de consentimento é um ponto chave dentro da legislação de proteção de dados. O artigo 8º da Lei Geral de Proteção de Dados reforça a necessidade do titular expressar o seu consentimento com relação a utilização dos seus dados pelo controlador, incluindo para quais razões estes dados serão utilizados, sendo que isso deve ser feito de maneira escrita ou de outra forma que deixe clara a manifestação do titular (BRASIL, 2018). Além disso, também relacionado a transparência, nos casos em que o consentimento é requerido, o artigo 9º da Lei Geral de Proteção de Dados estabelece que o titular deve ter acesso a informações como finalidade e duração do tratamento, identificação do controlador, responsabilidade dos agentes de tratamento e direitos do titular, citando explicitamente o conteúdo do artigo 18º da LGPD (BRASIL, 2018).

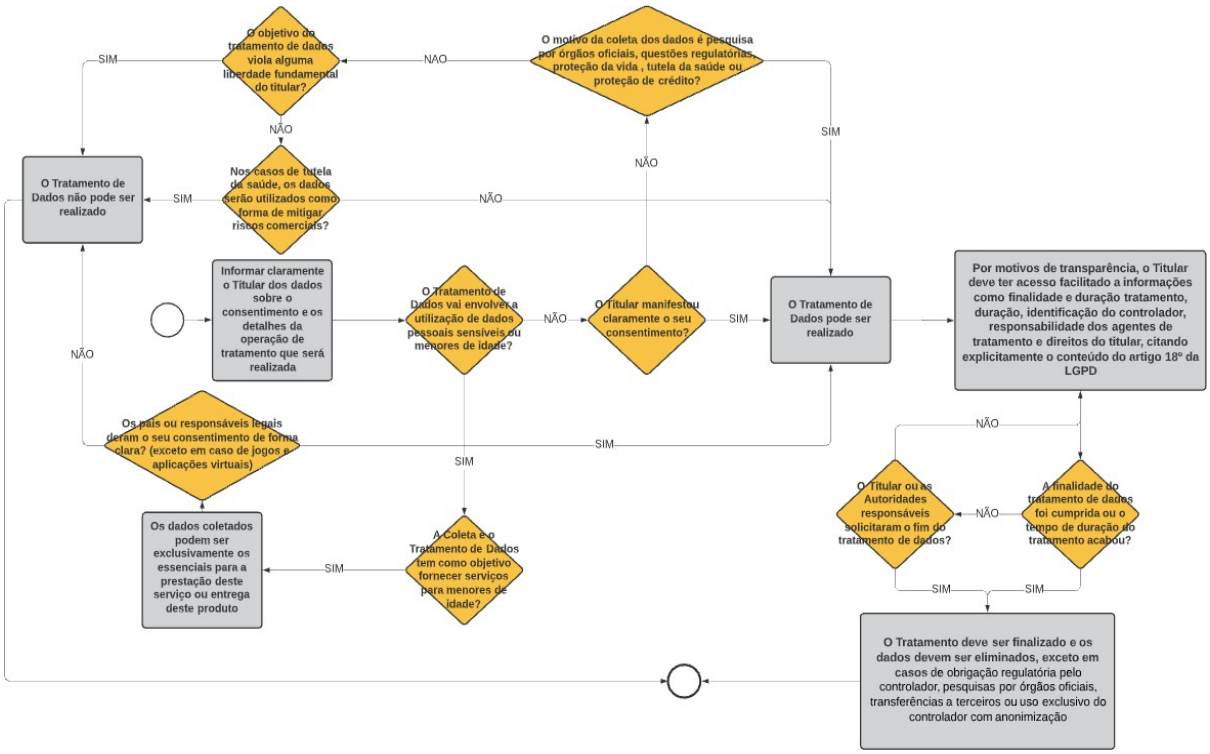
Ainda com relação aos requisitos para o tratamento de dados, também é necessário abordar as requisições nos casos de tratamento de dados pessoais sensíveis, bem como de dados pessoais de crianças e adolescentes. Conforme o artigo 11º da Lei Geral de Proteção de Dados, nos casos de empresas, o tratamento de dados pessoais sensíveis só é permitido nos casos em que o controlador seja obrigado a fazê-lo por razões legais, contratuais, processuais ou regulatórias, além dos casos de tutela da saúde, quando aplicável em casos de serviços médicos, embora, seja vedada, aos planos de saúde privados, a utilização destes dados como forma de mitigação de riscos comerciais (BRASIL, 2018).

Nos casos em que ocorra o tratamento de dados de crianças e adolescentes, o artigo 14º da Lei Geral de Proteção de Dados condiciona que, pelo menos um dos pais ou responsáveis legais, precisa dar o seu consentimento acerca do processo de tratamento de dados, que só não é exigido nos casos em que os dados sejam utilizados uma única vez pela empresa para contato com o responsável ou para a proteção da criança (BRASIL, 2018). Ainda, nos casos de jogos,

aplicações online e afins, o consentimento do responsável não é exigido, sendo que os dados coletados devem ser exclusivamente os essenciais para o fornecimento destes serviços (BRASIL, 2018).

O processo de tratamento de dados possui algumas hipóteses que ocasionam o seu término, bem como a eliminação dos dados coletados e tratados. Essas hipóteses estão condicionadas nos artigos 15 e 16 da Lei Geral de Proteção de Dados e consistem em situações como o fim do período de tratamento, o alcance da finalidade de tratamento, a comunicação pelo titular ou a determinação pelas autoridades, ocorrendo então a eliminação dos dados, exceto nos casos em que exista a necessidade de obrigação regulatória pelo controlador, pesquisas por órgãos oficiais, transferências a terceiros ou uso exclusivo do controlador com anonimização (BRASIL, 2018).

Figura IV – O Processo de Tratamento de Dados



Fonte: elaborado pelo autor

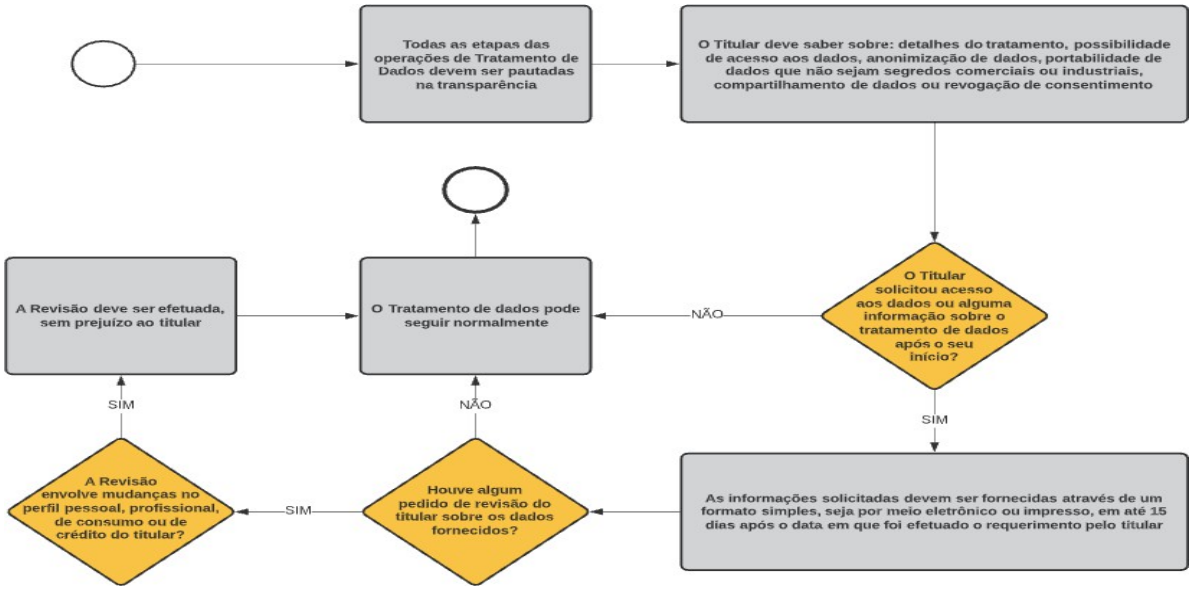
Na qualidade do fato gerador da necessidade de adaptação com a Lei Geral de Proteção de Dados, é importante que pequenas e médias empresas compreendam as particularidades e as regras envolvidas nas operações de tratamento de dados, principalmente no caso de empresas que, devido às características da operação do negócio, acabem coletando dados pessoais sensíveis junto ao fornecimento de seus produtos e serviço aos consumidores. É importante

que as empresas utilizem essas normas na própria concepção dos seus produtos e serviços, incorporando o conceito de *Privacy by Design*, metodologia focada no triângulo pessoas, processos e tecnologia, que é cada vez mais discutida e aplicada por algumas das maiores empresas do mundo, como GE, Intel e IBM (CAVOUKIAN, 2020). Através deste conceito, as empresas podem utilizar as diretrizes e restrições oriundas das legislações de proteção de dados para pensar no próprio negócio, especificamente em seus produtos e processos, colocando o usuário no centro e utilizando a transparência como elemento fundamental para a geração de confiança na companhia.

Um dos principais pilares da Lei Geral de Proteção de Dados é a transparência como forma de garantir as liberdades individuais e intimidade dos cidadãos, possibilitando a legitimação de direitos pelo titular dos dados. O artigo 18 da Lei Geral de Proteção de Dados elenca uma série de direitos do titular dos dados junto ao controlador, como a confirmação e detalhes do tratamento, acesso aos dados, correção de dados, anonimização de dados, portabilidade de dados que não constituam segredos comerciais ou industriais, eliminação de dados, informações sobre compartilhamento de dados ou revogação de consentimento (BRASIL, 2018). Ainda, de acordo com o artigo 19 da Lei Geral de Proteção de Dados, as informações referentes aos direitos do titular elencados no artigo 18 devem ser fornecidas através de um formato simples, seja por meio eletrônico ou impresso, em até 15 dias após a data em que foi efetuado o requerimento pelo titular (BRASIL, 2018).

Nos casos de tratamento automatizado de dados, o artigo 20 impõe que o titular tem direito a solicitar uma revisão em situações que afetem o seu interesse, nos casos em que decisões automatizadas tenham sido “destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade” (BRASIL, 2018). Por último, o artigo 21 delimita que em todas as situações quando houver o exercício de direitos através do pedido de revisão pelo titular, os dados pessoais referentes ao pedido não podem ser utilizados em prejuízo ao titular (BRASIL, 2018).

Figura V – Princípios e Direitos do Titular



Fonte: elaborado pelo autor

O fluxograma acima se dedica a ilustrar os principais direitos do titular com relação aos seus dados, incluindo o que as empresas devem fazer nos casos de solicitação de informações e pedidos de revisão dos dados por parte do titular. Além disso, o fluxograma também desperta a necessidade de as empresas tornarem transparentes os detalhes sobre as suas operações de tratamento de dados, o que pode ser feito através da criação e divulgação de um documento de políticas de privacidade para o qual o titular tenha que dar o seu consentimento antes da comercialização do produto ou serviço.

Um documento nesse formato é essencial, na medida em que ao mesmo tempo informa o titular sobre o que a empresa faz com os seus dados e mitiga riscos para as micro, pequenas e médias empresas, tendo em vista que divulga os detalhes sobre a utilização dos dados coletados, informações sobre os procedimentos realizados e também sobre os métodos utilizados para garantir a segurança das informações dos clientes ou usuários. Além disso, ainda que as políticas de privacidade sejam reconhecidas há bastante tempo por serem necessárias para empresas com negócios *on-line*, agora também é imprescindível que empresas sem negócios digitais definam e divulguem as suas políticas de privacidade, como forma de obter o consentimento dos clientes acerca dos seus procedimentos de coleta, manuseio e tratamento de dados pessoais.

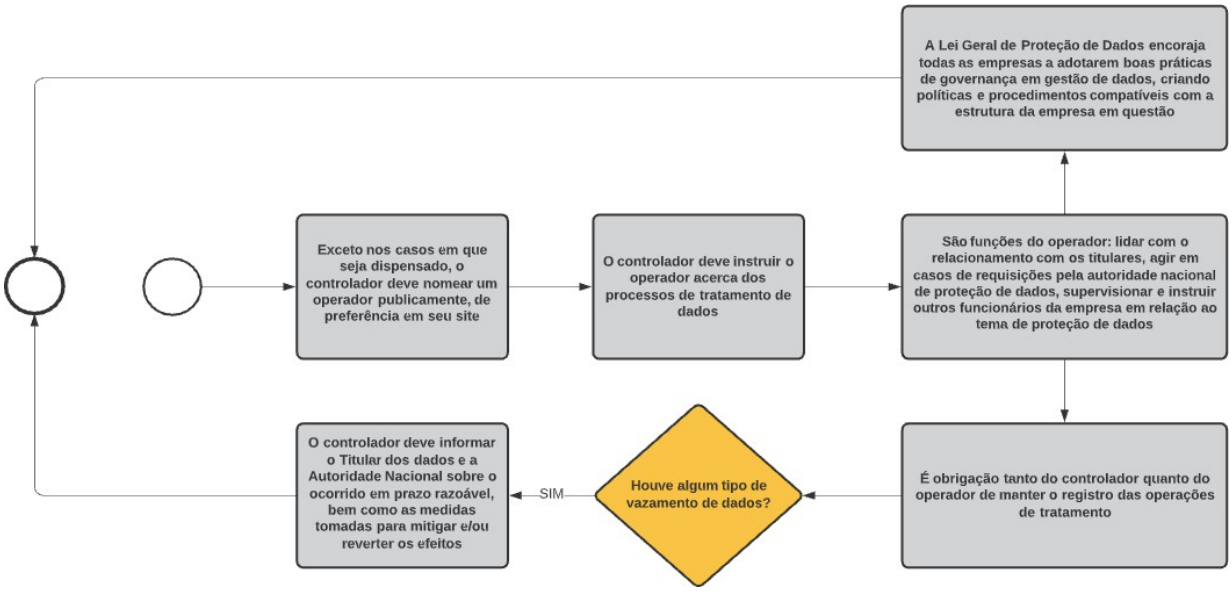
A Lei Geral de Proteção de Dados é bastante clara com relação à delimitação das Obrigações dos Agentes de Tratamento, focadas especificamente em processos gerenciais que

devem ser tomados pelas empresas para garantir a segurança e transparência das operações de tratamento de dados. O artigo 37 da Lei Geral de Proteção de Dados impõe que tanto o controlador quanto o operador "devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse" (BRASIL, 2018). Ainda, toda a operação de tratamento de dados realizada pelo operador deverá ser baseada inteiramente nas instruções do controlador, as quais devem estar dentro das normas (BRASIL, 2018).

Além disso, o Controlador, nos casos em que não seja dispensado pela Autoridade Nacional de Proteção de Dados, também deve nomear publicamente um encarregado pelo tratamento de dados pessoais cujas principais funções residem em lidar com o relacionamento com os titulares, agir em casos de requisições pela Autoridade Nacional De Proteção De Dados, supervisionar e instruir outros funcionários da empresa em relação ao tema de proteção de dados (BRASIL, 2018). Em casos de possíveis vazamentos, o controlador é responsável por comunicar tanto a Autoridade Nacional quanto ao titular dos dados acerca do ocorrido, em detalhes, após um prazo razoável, bem como as medidas tomadas para mitigar ou reverter as consequências do vazamento (BRASIL, 2018).

Em todos os casos, a Lei Geral de Proteção de Dados também incentiva que as empresas adotem boas práticas de governança sobre a questão da privacidade de dados e sua relação com a gestão das organizações. O artigo 50 da Lei Geral de Proteção de Dados incentiva, embora não obrigue as empresas a criarem uma política geral que contenha regras claras e procedimentos compatíveis com a estrutura da organização para as operações de tratamento de dados, medidas de segurança, ações de conscientização, processos internos em casos de vazamentos, processos para mitigação e contenção de riscos, entre outros, como forma de estabelecer uma relação com os principais *stakeholders* da empresa pautada na transparência (BRASIL, 2018).

Figura VI – Obrigações dos Agentes de Tratamento

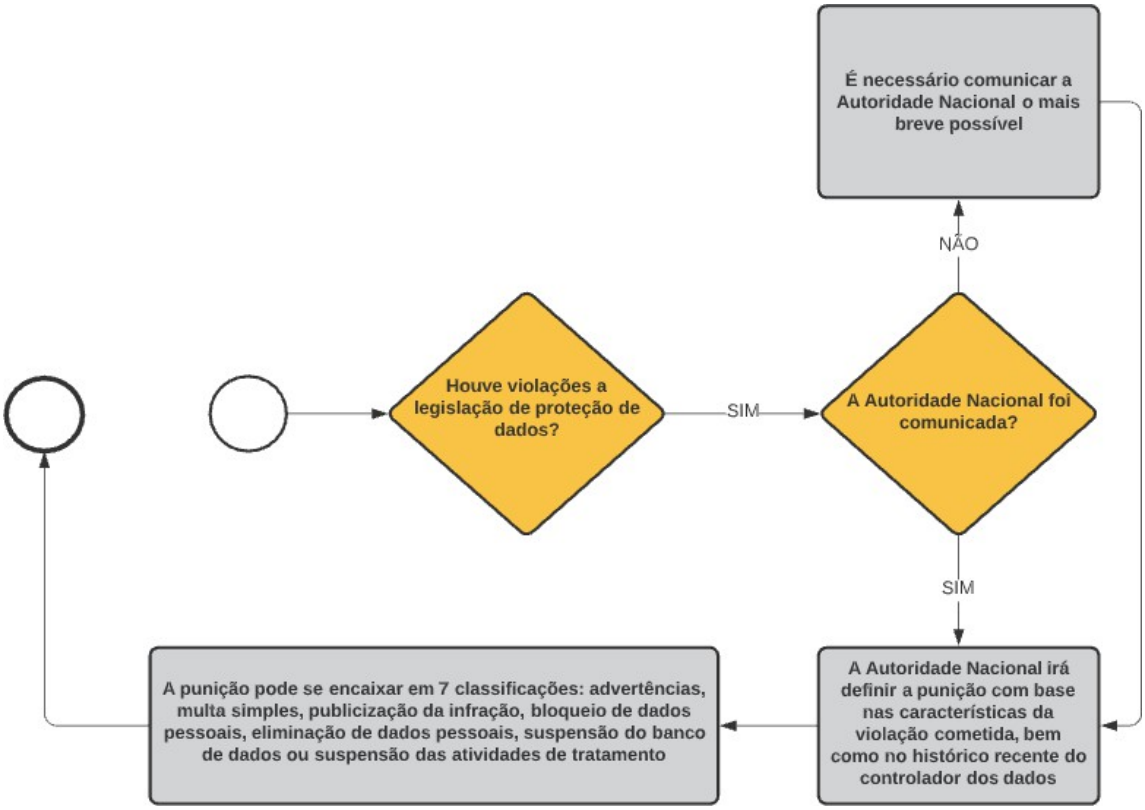


Fonte: elaborado pelo autor

A Figura VI, abordou as determinações da Lei Geral de Proteção de Dados sobre as responsabilidades dos Agentes de Tratamento, mais especificamente o controlador e o operador dos dados. No entanto, devido ao tamanho reduzido de muitas pequenas e médias empresas, muitas vezes o operador dos dados acabará sendo um dos próprios sócios da empresa, que além de ser responsável por diversas atividades operacionais, também terá de lidar com as demandas referentes à segurança e privacidade dos dados dos clientes.

A Lei Geral de Proteção de Dados criou sanções relacionadas a eventuais violações da legislação que forem cometidas pelos controladores dos dados. O artigo 54 da Lei Geral de Proteção de Dados impõe que as sanções aplicadas pela autoridade nacional devam ser diretamente proporcionais a gravidade da violação cometida, bem como dos seus efeitos para os titulares dos dados (BRASIL, 2018). Essa regulamentação está relacionada com o que está disposto no artigo 52 da Lei, que classifica as possíveis sanções em 7 grupos: advertências, multa simples, publicização da infração, bloqueio de dados pessoais, eliminação de dados pessoais, suspensão do banco de dados, suspensão das atividades de tratamento, tudo isso dependendo das características da violação cometida, bem como no histórico recente do controlador dos dados (BRASIL, 2018).

Figura VII – Responsabilização dos Agentes de Tratamento



Fonte: elaborado pelo autor

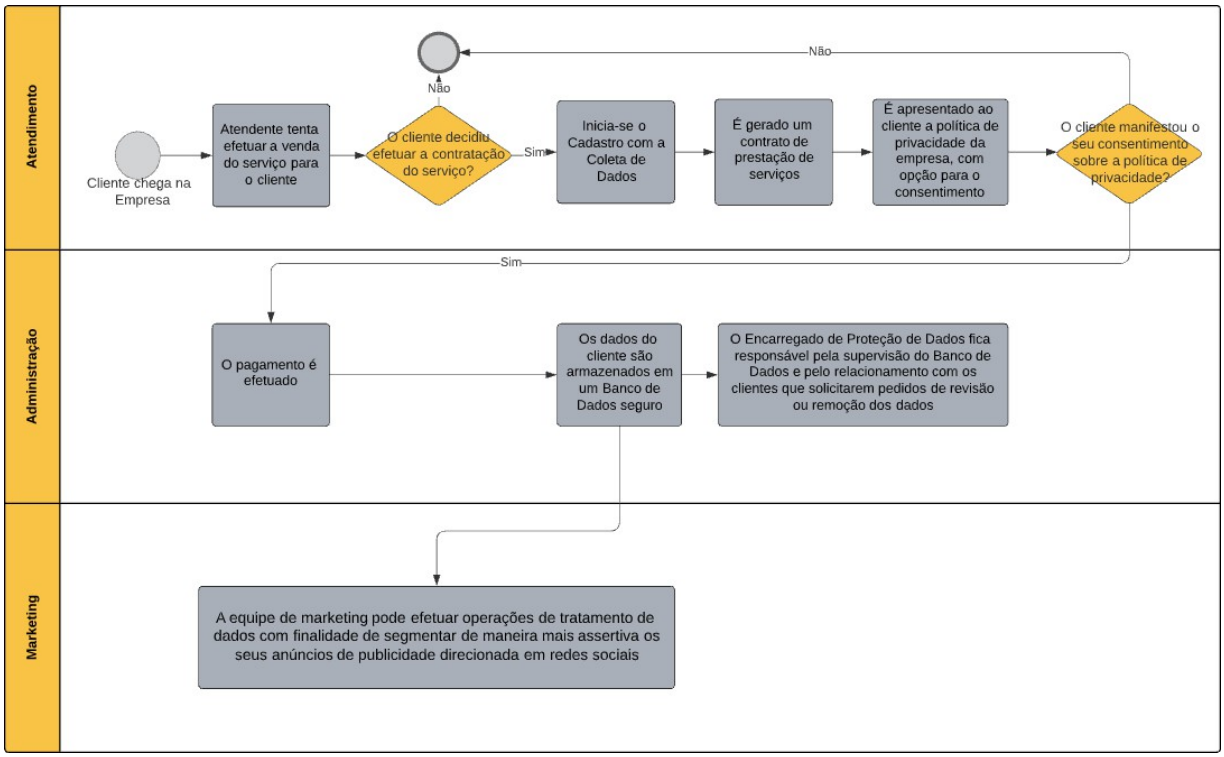
O fluxograma acima não consiste em processos regulares que devem ser implantados dentro das empresas, mas sim em algo não recorrente, que deve ocorrer apenas nos casos em que houve algum tipo de vazamento. Nessas situações, é importante que as pequenas e médias empresas estejam atentas em informar a Autoridade Nacional no menor prazo possível, caso contrário, podem ser aplicadas 7 tipos de sanções diferentes, que foram citadas no início da seção, as quais trazem um risco adicional ao negócio.

4.3 Avaliação do Artefato

Todo artefato produzido através de uma pesquisa de *Design Science Research* precisa ser avaliado para verificar a sua adaptação dentro da realidade do contexto empresarial, com base no problema para o qual ele pretenda fornecer uma solução. Assim, o artefato deste estudo será avaliado através da construção de um cenário baseado no processo de cadastro dos clientes em uma empresa do setor de serviços que utilize operações de tratamento de dados com finalidade econômica, como, por exemplo, a veiculação de anúncios em redes sociais utilizando dados de clientes para segmentar de maneira mais assertiva o seu público-alvo. A situação de cadastro criada será baseada na coleta de dados presencial junto a clientes, pessoas

físicas, maiores idade, na qual serão fornecidos os dados: Nome Completo, Sexo, Número de Telefone, Endereço Eletrônico, RG, CPF, Endereço de Moradia, Data de Nascimento e Atividade Econômica. Neste cenário, a coleta de dados e a conclusão do cadastro ocorrem antes do início da prestação do serviço que está sendo contratado. O processo de coleta de dados e requisição do consentimento, já com a utilização do modelo proposto, será ilustrado no fluxograma abaixo.

Figura VIII – Cenário de Cadastro em uma Empresa do setor de Serviços



Fonte: elaborado pelo autor.

Através das etapas do fluxograma, é possível observar que muitas das exigências da Lei Geral de Proteção de Dados podem ser cumpridas por meio de um documento completo de políticas de privacidade, que torne transparente os processos realizados pela empresa com os dados do cliente, tanto por razões legais quanto por razões de boas práticas de governança, que são essenciais para qualquer negócio atingir sucesso econômico no longo prazo, principalmente nos casos de pequenas e médias empresas. Nesse sentido, uma política de privacidade deve detalhar todos os procedimentos realizados pela empresa na questão da privacidade de dados, em suas diferentes estruturas, incluindo o modelo das operações de tratamento de dados, procedimentos de segurança para garantir a integridade dos dados e coibir vazamentos, ações de conscientização e processos internos para mitigar riscos de

vazamentos ou coibir as suas consequências caso elas aconteçam.

Além disso, é importante que as empresas reforcem a questão da obtenção de consentimento junto aos clientes sobre a política de privacidade da empresa e sobre as operações de tratamento de dados que serão realizadas, caso contrário, elas não podem acontecer de maneira legal, o que cria possibilidades para a aplicação de sanções, que acabam significando novos riscos para o negócio, os quais poderiam ter sido facilmente evitados. Assim, com processos e políticas claras, as pequenas e médias empresas podem transformar a obrigação de adaptar suas rotinas empresariais a uma nova legislação com oportunidade de reforçar o seu nível de governança e estrutura corporativa.

CONSIDERAÇÕES FINAIS

A Lei Geral de Proteção de Dados entrou em vigor em setembro de 2020 e mudou o paradigma das questões de transparência e segurança no assunto de proteção de dados em rede, adequando a legislação brasileira ao padrão europeu, reconhecido por ser um dos mais completos do mundo. Toda essa nova base legal acabou por exigir adaptações dos processos empresariais em todos os tipos de empresas, no Brasil. No entanto, com as dificuldades de gestão de micro, pequenas e médias empresas brasileiras, este estudo buscou desenvolver um modelo de fácil implementação para que essas organizações, tendo em vista o seu tratamento constitucional diferenciado, conseguissem facilmente se adaptarem a nova legislação, sem ser necessário alocar grandes quantias de recursos financeiros em consultorias para o processo de adaptação.

Nesse sentido, o objetivo geral deste trabalho consistia em propor um *framework* de implementação da conformidade da LGPD às micro, pequenas e médias empresas. Para tanto foi realizada uma pesquisa no formato de *Design Science Research*, na qual o pesquisador cria um artefato que funciona como a solução de um problema enfrentado dentro do cotidiano empresarial. Este artefato foi construído através de sete etapas propostas por Hevner *et al.* (2004), que incluem relevância do problema, rigor de pesquisa, *design* como processo de pesquisa, *design* como artefato, avaliação do artefato, contribuições da pesquisa e comunicação da pesquisa. O artefato foi dividido em cinco fluxogramas de trabalho no formato *Business Process Modeling Notation* (BPMN), tendo como base os cinco eixos fundamentais da Lei Geral de Proteção de Dados, propostos por Doneda e Mendes (2018): unidade e generalidade de aplicação, requisitos para o tratamento de dados, princípios e

direitos do titular dos dados, deveres dos agentes que realizam o tratamento de dados, sendo que em cada um destes pilares houve uma análise prévia da própria Lei Geral de Proteção de Dados, que serviu como base para a criação dos processos contidos nos fluxogramas.

Este trabalho buscou construir modelos de processos gerenciais que podem ser replicados e utilizados em praticamente qualquer empresa, através da união de campos do direito com campos da gestão, representando uma contribuição direta e prática para a eficiência e profissionalização de micro, pequenas e médias empresas, auxiliando também na diminuição de riscos legais. Após a realização do estudo, foi confirmada a hipótese de que é possível oferecer para micro, pequenas e médias empresas um fluxo de trabalho que as coloquem em conformidade com a Lei Geral de Proteção de Dados e que seja compatível com a estrutura corporativa e condições econômicas, tendo em vista o seu tratamento constitucional diferenciado, estabelecido no Artigo 170, da Constituição Federal.

As limitações desta pesquisa incluem o fato de não ter sido possível trazer o ponto de vista das empresas e gestores sobre a implementação da Lei Geral de Proteção de Dados, tendo em vista que a legislação entrou parcialmente em vigor pouco tempo antes da conclusão do estudo e muitas empresas ainda não fizeram as modificações necessárias para a conformidade. Nesse sentido, existe espaço para avanços nas bases teóricas relacionadas a Lei Geral de Proteção de Dados, assim, sugere-se que estudos futuros busquem avaliar os impactos desta legislação diretamente em empresas específicas, através de estudos de caso aprofundados.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO/IEC 27001**:2013. Rio de Janeiro, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO/IEC 27701**:2019. Rio de Janeiro, 2019.

BELLI, Luca *et al.* Governança e regulações da Internet na América Latina: análise sobre infraestrutura, privacidade, cibersegurança e evoluções tecnológicas em homenagem aos dez anos da South School on Internet Governance. **FGV Direito Rio**, 2018. Disponível em <https://bibliotecadigital.fgv.br/dspace/handle/10438/27164> Acesso em 05 de maio de 2020.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Senado Federal, 1988. Disponível em < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm> Acesso em 10 de maio de 2020.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados.** Brasília, DF, 2018 Disponível em < http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm> Acesso em 10 de maio de 2020.

CAVOUKIAN, Ann. Understanding How to Implement Privacy by Design, One Step at a Time. IEEE Consumer Electronics Magazine, v. 9, n. 2, p. 78-82, 2020.

DONEDA, Danilo; MENDES, Laura. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor**, São Paulo, v. 120, 2018, p. 469-483.

DRESCH, Aline; LACERDA, Daniel Pacheco; ANTUNES, Junico. **Design science research**: método de pesquisa para avanço da ciência e tecnologia. Porto Alegre: Bookman, 2015.

FRANÇA, Ana Judite Galbiatti Limongi. Melhoria contínua aplicada a edificações de tipologia padronizada: a gestão do conhecimento no contexto do portfólio de ativos de uma organização. 2016. Tese de Doutorado. Universidade de São Paulo.

GIL, Antonio Carlos. **Métodos e Técnicas de Pesquisa Social**. 6. ed. Editora Atlas, 2008.

HEVNER, Alan *et al*. Design science research in information systems. **MIS quarterly**, v. 28, n. 1, 2004, p. 75-105. Disponível em <https://www.jstor.org/stable/25148625> Acesso em 29 de maio de 2020

ICTS PROTIVITI. Resultados da Avaliação de Adequação à LGPD. 2020. Disponível em <https://www.protiviti.com/sites/default/files/brazil/solutionsindustries/infografico_-_resultados_da_avaliacao_de_adequacao_a_lgpd_-_marco_2020.pdf> Acesso em 15 de julho de 2020

LACHAUD, Eric. **ISO/IEC 27701**: Threats and opportunities for GDPR certification. SSRN, 2020. Disponível em < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3521250> Acesso em 14 de maio de 2020.

LOPES, Isabel Maria; GUARDA, Teresa; OLIVEIRA, Pedro. How ISO 27001 can help achieve GDPR compliance. *In*: **2019 14th Iberian Conference on Information Systems and Technologies (CISTI)**. IEEE, 2019. p. 1-6. Disponível em < https://ieeexplore.ieee.org/abstract/document/8760937/?casa_token=7BbljJDFXTwAAAAA:AnIpWaz9cWPnwAMDk5SELfV0msuVMAsmVUeTHknxroks9fExNVJPH2xIhP

7KIqHF1aELK6tTAtNS> Acesso em 15 de maio de 2020.

MATIAS-PEREIRA, José. **Manual de metodologia da pesquisa científica**. 4. ed., rev. e atual. São Paulo: Atlas, 2016.

MARANHÃO, Mauriti; MACIEIRA, Maria Elisa Bastos. O processo nosso de cada dia: modelagem de processos de trabalho. Rio de Janeiro: Qualitymark, 2008.

NAKAMURA, Emilio Tissato; FILHO, José Reynaldo Formigoni; IDE, Marcos Cesar. **Metodologia de Avaliação de Riscos e Medidas de Segurança na Proteção de Dados Pessoais**. *In*: XIX Simpósio Brasileiro de Segurança da Informação e Sistemas Computacionais, São Paulo, 2019.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO (OCDE). The OECD privacy framework. 2013. Disponível em < https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf> Acesso em 15 de junho de 2020

PARENTONI, Leonardo. Autoridade Nacional de Proteção de Dados brasileira: uma visão otimista. **Revista do Advogado**, v. 144, 2019, p, 209-219.

RAPÔSO, Cláudio Filipe Lima *et al*. LGPD: Lei Geral de Proteção de Dados Pessoais em Tecnologia da Informação: revisão Sistemática. **RACE-Revista da Administração**, v. 4, 2019, p. 58-67.

SERASA EXPERIAN. 85% das empresas declaram que ainda não estão prontas para atender às exigências da Lei de Proteção de Dados Pessoais, mostra pesquisa da Serasa Experian. 2019. Disponível em < https://www.serasaexperian.com.br/sala- de-imprensa/85-das-empresas-declaram-que-ainda-nao-estao-prontas-para-atender- as-exigencias-da-lei-de-protecao-de-dados-pessoais-mostra-pesquisa-da-serasa- experian> Acesso em 15 de julho de 2020

SERVIÇO BRASILEIRO DE APOIO ÀS MICRO E PEQUENAS EMPRESAS (SEBRAE). **Painel de Empresas 2020**. Disponível em: <https://datasebrae.com.br/totaldeempresas/> Acesso em 12 de maio de 2020.

SILVEIRA, Sergio Amadeu; AVELINO, Rodolfo; SOUZA, Joyce. A privacidade e o mercado de dados pessoais | Privacy and the market of personal data. **Liinc em Revista**, v. 12, n. 2, 2016. Disponível em <http://revista.ibict.br/liinc/article/view/3719> Acesso em 11 de maio de 2020.

SUN, Zhe *et al*. **Research on the Effectiveness Analysis of Information Security Controls**. In: 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC). IEEE, 2020. p. 894-897. Disponível em < https://ieeexplore.ieee.org/abstract/document/9084809/> Acesso em 13 de maio de 2020.

WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. **Harvard Law Review**, 1890, p. 193-220. Disponível em<https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf> Acesso em 12 de maio de 2020.

ZANATTA, Rafael. A tutela coletiva na proteção de dados pessoais. **Revista do Advogado**, v. 144, 2019, p. 201-208.