



**Lei Geral de Proteção de Dados em empresas de pequeno porte: uma
discussão sobre o contexto do Marketing**

DOI: 10.31994/rvs.v15i1.984

Elisângela de Oliveira Briganon¹

Barbara Regina Lopes Costa²

Richard Medeiros de Araújo³

**General Data Protection Law in small businesses: a discussion on the
Marketing context**

RESUMO

A Lei Geral de Proteção de Dados (LGPD) é uma legislação brasileira para proteger a privacidade e a segurança dos dados das pessoas físicas. Ela estabelece direitos dos titulares, como acesso e exclusão das informações, e impõe obrigações a agentes de tratamento, como às empresas, de adotar medidas de segurança. O descumprimento pode resultar em multas e penalidades. O Marco Civil da Internet é outra lei brasileira que aborda a neutralidade da rede, liberdade de expressão e privacidade, exigindo que os provedores protejam os dados dos usuários. Por sua

¹ Tecnóloga em Gestão de Serviços pela fatec Indaiatuba. Representante de Desenvolvimento de Negócios (SDR).E-mailebriganon@gmail.com e ORCID orcid: 0009-0000-6632-4022

² Graduação em Comunicação Social / Publicidade e Propaganda pela Universidade Santa Cecília (1998), Graduação em Administração pela Faculdade Santa Bárbara (2016), Mestrado em Administração pela Universidade Municipal de São Caetano do Sul (2005) e Doutorado em Administração - Universidad de la Empresa (2016). e-mail : babhy@terra.com.br e ORCID: <https://orcid.org/0000-0002-5756-3256>

³ Doutor em Administração pelo PPGA/UFRN. E-mail: richardmaraujo@uol.com.br e ORCID: <https://orcid.org/0000-0002-6718-8912>

vez, a visibilidade de dados e a segurança são essenciais nas redes sociais, exigindo transparência no tratamento das informações e medidas de proteção contra ameaças. Sendo assim, o objetivo desta pesquisa é analisar o cumprimento da LGPD por empresas de pequeno porte, especialmente no que se refere à segurança dos dados e o uso de dados de clientes (pessoa natural), para fins de marketing nas redes sociais. Para tal foi realizada uma pesquisa exploratória quantitativa, abordando aspectos como o conhecimento da lei pelos empreendedores e as práticas de uso de dados e de marketing nas redes sociais. Os dados foram coletados por meio de questionários e analisados com auxílio da visualização de gráficos. A amostra é composta por gestores e empreendedores da cidade de Indaiatuba. Os resultados revelam que apenas 17% das empresas informam, em cláusula contratual, o termo de usar dados do cliente para divulgação, 40% das empresas fazem *backup* dos dados dos clientes e que as empresas de pequeno porte estão diante de mais um desafio para o cumprimento da LGPD.

PALAVRAS-CHAVES: LGPD. MARCO CIVIL DA INTERNET. REDES SOCIAIS. DADOS DOS CLIENTES. EPP - EMPRESA DE PEQUENO PORTE.

ABSTRACT

The General Data Protection Law (LGPD) is Brazilian legislation to protect the privacy and security of data of individuals. It establishes rights of holders, such as access and deletion of information, and imposes obligations on processing agents, such as companies, to adopt security measures. Non-compliance can result in fines and penalties. The Marco Civil da Internet is another Brazilian law that addresses network neutrality, freedom of expression and privacy, requiring providers to protect user data. In turn, data visibility and security are essential in social networks, requiring transparency in the processing of information and protection measures

against threats. Therefore, the objective of this research is to analyze compliance with the LGPD by small companies, especially with regard to data security and the use of customer data (individuals) for marketing purposes on social networks. To this end, quantitative exploratory research was carried out, addressing aspects such as entrepreneurs' knowledge of the law and data use and marketing practices on social networks. Data were collected through questionnaires and analyzed using graphs. The sample is made up of managers and entrepreneurs from the city of Indaiatuba. The results reveal that only 17% of companies inform, in a contract clause, the term of using customer data for disclosure, 40% of companies back up customer data and that small companies are facing yet another challenge to compliance with the LGPD.

KEYWORDS: LGPD. BRAZILIAN INTERNET CIVIL RIGHTS FRAMEWORK. SOCIAL MEDIA. CUSTOMER DATA. SMALL BUSINESS.

INTRODUÇÃO

Com a maior usabilidade tecnológica social, a vulnerabilidade dos dados, em específico nas atividades executadas na internet, ficou mais evidente, sejam dados de algum cadastramento realizado em sites, no momento de compras, de participação em pesquisas, com o uso de imagens em redes sociais ou até mesmo de transações bancárias realizadas por aplicativos.

A preocupação acerca do princípio da inviolabilidade à segurança estabelecidos nos artigos 5º e 144º da Constituição Federal, demanda de legislações apropriadas a circulação de dados, como a Lei nº 12.965/2014, chamada de Marco Civil da Internet, onde estabeleceu a proteção da rede com os princípios fundamentais a privacidade, neutralidade e a liberdade de expressão.

A Lei Geral de Proteção de Dados (LGPD), Lei nº13.709/2018, preconiza a proteção dos direitos de privacidade e de livre liberdade de personalidade do cidadão, orientando como devem ser tratados os dados pessoais da pessoa natural

no meio digital e físico. Dados são responsáveis por todo tráfico de informação relacionado ao meio digital ou meio físico, sendo assim o principal objetivo da lei, em âmbito empresarial, é o tratamento de dados em atividade que utiliza dados pessoais.

Deste modo, o cuidado com os dados dos clientes dentro das organizações se tornou mais uma demanda para a área de gestão, e o objetivo deste estudo é entender como as empresas de pequeno porte estão lidando com a LGPD, quando se trata da divulgação nas redes sociais. Há compreensão da LGPD e ação para resguardar os dados dos clientes? De que maneira as EPP - Empresas de Pequeno Porte cuidam dos dados de seus clientes em suas divulgações nas redes sociais?

Como delineamento da pesquisa, adotou-se o levantamento de dados relacionados às EPP - Empresas de Pequeno Porte da cidade de Indaiatuba, que atuam como prestadoras de serviços e utilizam a rede social *Instagram* para divulgação dos seus serviços, produtos e/ou prospecção de novos clientes.

Esse estudo tem como hipótese que a maioria dos empreendedores de pequeno porte não tem compreensão sobre a LGPD e, conseqüentemente, não tomam as medidas necessárias para resguardar os dados dos clientes em suas divulgações nas redes sociais. As empresas de pequeno porte que possuem menos recursos financeiros e técnicos, têm menos capacidade para se adequar à LGPD e, portanto, apresentam maior vulnerabilidade à violação de dados dos clientes.

Para desenvolver o estudo sobre a Lei Geral de Proteção de Dados e sua aplicação em empresas de pequeno porte na cidade de Indaiatuba, foi implementada uma metodologia exploratória, uma vez que se trata de um tema relativamente recente. O estudo será apresentado em três etapas. A primeira etapa consistirá na realização de pesquisa bibliográfica através de artigos científicos, *sites* e periódicos a fim de compreender a LGPD, que representa um compromisso de respeito das empresas com seus clientes; a importância do Marco Civil da Internet, que apresenta garantias, direitos e deveres para o uso da Internet no Brasil; e visibilidade *versus* segurança de dados, que trata do dilema enfrentado pelas redes

sociais em relação à privacidade e segurança dos dados de seus usuários. A segunda etapa deste estudo consiste na realização da pesquisa de campo, conforme a metodologia delineada, a fim de obter dados das empresas de pequeno porte localizadas na cidade de Indaiatuba. Um levantamento de dados utilizando o *Google Forms*, com perguntas previamente orientadas, direcionadas à proposta do estudo. A última etapa a ser apresentada será a análise dos dados coletados para responder as perguntas problemas norteadoras do estudo.

1 FUNDAMENTAÇÃO TEÓRICO EMPÍRICA

1. 1 A Lei Geral de Proteção de Dados – LGPD, um compromisso de respeito das empresas com seus clientes

A Lei 13.709/2018 - Lei Geral de Proteção de Dados (LGPD) é uma lei brasileira que entrou em vigor em setembro de 2020, estabelecendo regras para a coleta, uso, armazenamento e compartilhamento de dados pessoais por empresas e organizações. A ideia da LGPD surgiu a partir de uma preocupação crescente com a privacidade e segurança dos dados pessoais, tomando de base iniciativas semelhantes em outros países, como o GDPR (*General Data Protection Regulation*) da União Europeia (Brasil, 2018).

A LGPD define dados pessoais como “informação relacionada a pessoa natural identificada ou identificável”, sendo tais dados, sobrenome, RG, CPF, e-mail e outros. O artigo 5º, inciso II, disciplina sobre os dados sensíveis que são aqueles que se referem às características íntimas da pessoa, como dados de saúde, etnia, orientação sexual, religião, entre outros, quando relacionado a pessoa natural (Brasil, 2018).

Vale ressaltar que a LGPD permite, em seu artigo 11, inciso II, b, o uso de dados sensíveis sem o consentimento do titular dos dados, quando for indispensável

para o tratamento compartilhado dos dados pela administração pública para a execução de políticas públicas previstas em leis ou regulamentos, além de outras hipóteses que se referem, em grande parte, a interesses públicos (Costa; Oliveira, 2019).

A LGPD apresenta os direitos dos titulares dos dados, como o direito de acesso, retificação e exclusão de informações, e aborda a necessidade das empresas se adequarem à LGPD, incluindo a adoção de medidas de segurança para proteção dos dados, destaca penalidade para as empresas que não cumprem as normas protegidas pela lei, que incluem multas que podem chegar a 2% do faturamento da empresa, limitado a R\$ 50 milhões por infração, além de demais penalidades, como a suspensão do tratamento de dados (Brasil, 2018).

Guimarães (2020) aborda os principais pontos da LGPD, como os princípios de finalidade, adequação, necessidade, livre acesso e transparência, bem como as sanções previstas para as empresas que não cumprirem as normas estabelecidas, ressalta a importância das empresas se adequarem à LGPD, a fim de evitar possíveis danos à sua imagem e reputação perante os seus clientes.

A LGPD foi criada para regulamentar o tratamento de dados pessoais por pessoas físicas e jurídicas públicas e privadas, garantindo o direito à privacidade e à proteção dos dados pessoais dos cidadãos brasileiros. Aplica-se a todas as empresas que implementam tratamento de dados pessoais, independentemente do tamanho ou do setor em que operam. Além disso, a LGPD apresenta algumas mudanças, como o consentimento explícito para o tratamento de dados, a possibilidade de solicitar a exclusão de dados pessoais e o direito de acesso às informações armazenadas pelas empresas (IPEA, 2021). Segundo Cunha (2018) a LGPD é aplicável a todas as atividades que implicam no tratamento de informações independentemente de serem pessoas físicas ou jurídicas, em qualquer parte do mundo, incluindo tanto o território brasileiro quanto os países onde se encontram esses dados. A figura 1 apresenta os 10 princípios para o tratamento dos dados de acordo com o art. 6º da Lei.

Figura 1-Princípios de tratamentos de dados



Fonte: Cunha, 2018.

Zito (2021) observa que a LGPD não se aplica em determinadas situações, como quando os dados pessoais são tratados para fins jornalísticos ou artísticos, quando o tratamento é realizado por pessoas naturais sem propósito econômico, e quando os dados são usados para fins de segurança pública, defesa nacional, segurança do estado e atividades de investigação e repressão de infrações penais, descritos no art. 4º da lei. A Autoridade Nacional de Proteção de Dados (ANPD) é o órgão responsável pela fiscalização do tratamento de dados pessoais de pessoas naturais.

De acordo com Mafra (2023), a LGPD na proteção da privacidade no Brasil, pode ser vista como desafios e oportunidades, pois embora seja um importante marco regulatório na proteção de dados pessoais, passou a depender da existência de controle de fiscalização e sanção passiva. Haja vista a importância da conscientização dos indivíduos sobre a proteção de seus dados pessoais, assim como o papel das empresas na adoção de medidas de segurança e privacidade, que pode demandar a implementação de programas de *compliance*, conhecido como conjunto de atividades para cumprir regulamentos internos, normas e leis relevantes, visando garantir conformidade e minimizar riscos envolvendo políticas, treinamentos,

auditorias e sistemas de gestão de riscos. Necessitando de investimentos em tecnologia e capacitação dos profissionais envolvidos na proteção de dados, o que evidenciam alguns dos desafios enfrentados na aplicação da LGPD, como a falta de recursos dos órgãos reguladores responsáveis para a fiscalização da lei e a necessidade de desenvolvimento tecnológico que garantam a privacidade dos dados pessoais sem comprometer a inovação tecnológica, por outro lado pode ser visto como uma oportunidade para a inovação no segmento tecnológico. A LGPD surgiu com uma necessidade para complementar lacunas deixadas no Marco Civil da Internet (Mafra, 2023).

1.2 O marco civil da internet: garantias, direitos e deveres para o uso da Internet no Brasil

A Lei nº 12.965/2014, conhecida como Marco Civil da Internet, foi criada para estabelecer princípios, garantias, direitos e deveres para o uso da internet no Brasil. A lei foi sancionada em abril de 2014 e entrou em vigor em junho do mesmo ano (Brasil, 2014). O Marco Civil da Internet dispõe sobre a neutralidade da rede, a privacidade e a liberdade de expressão em seu artigo 3º. Além disso, também estabelece sobre a responsabilidade dos provedores de internet a respeito do conteúdo gerado pelos usuários. A Lei é considerada um marco importante na regulamentação do uso da internet no Brasil (TJDFT, 2017).

Queiroz (2017) diz que a criação do Marco Civil da Internet teve como objetivo garantir a liberdade, a privacidade e a segurança dos usuários da internet no Brasil, ao mesmo tempo em que estabelece princípios e diretrizes para a proteção dos direitos humanos fundamentais. Destaca-se que o Marco Civil da Internet é influenciado por normas internacionais de proteção dos direitos humanos, como a Declaração Universal dos Direitos Humanos e o Pacto Internacional sobre Direitos Civis e Políticos.

Ainda para Queiroz (2017) a questão da neutralidade da rede, que é um dos princípios apresentados no Marco Civil da Internet, é vista como um elemento

fundamental para garantir que a internet continue a ser um espaço de expressão livre e de inovação, sem demonstrar o tratamento diferenciado de conteúdo.

Segundo CGI (2014), o Marco Civil da Internet é uma legislação pioneira no mundo e serve de exemplo para outros países que buscam regulamentar a internet de forma democrática e participativa, com vista a garantir a proteção dos direitos dos cidadãos na era digital e promover a inovação e o desenvolvimento tecnológico responsável e sustentável.

De fato, o Marco Civil da Internet foi uma legislação importante que estabeleceu princípios para a governança da internet no Brasil, como a neutralidade da rede e a liberdade de expressão. No entanto, a Lei não abordou especificamente a proteção de dados pessoais na internet. Com a entrada em vigor da LGPD em 2020, a proteção dos dados pessoais se tornou mais completa e detalhada, aplicando-se não apenas aos dados coletados *online*, mas também *offline*. Essa nova legislação coloca o Brasil em sintonia com outras nações que já possuem leis de proteção de dados pessoais, como a União Europeia (Celidonio; Neves; Doná, 2020).

O Portal Fiocruz [2023] aborda três princípios fundamentais do Marco Civil da Internet, sendo eles, a neutralidade da rede, princípio que garante que todos os *sites* e serviços tenham igualdade de velocidade e acesso, sem cobranças diferenciadas dos provedores de internet. Portanto assegura a livre escolha do usuário na navegação *online*; a liberdade de expressão, que garante a igualdade de direitos na disseminação de informações e opiniões. Provedores de acesso e serviços não podem ser responsabilizados pelo conteúdo publicado pelos usuários, e só pode ser removido com autorização do autor ou ordem judicial. Esse princípio busca preservar a livre manifestação do pensamento e evitar a censura indevida; e a privacidade, que estabelece que provedores e *sites* não podem utilizar dados dos usuários para fins comerciais e devem armazenar esses dados por no mínimo seis meses. Além disso, empresas estrangeiras devem obedecer às leis brasileiras de

segurança da informação, mesmo que seus *datacenters* estejam localizados fora do país.

Gomes (2019) explica que a empresa que coleta dados pessoais de seus clientes através de um *site* ou aplicativo deve assegurar que a coleta seja feita de forma clara e transparente, informando aos usuários quais dados serão coletados, para que serão utilizados e como serão protegidos, bem como garantir que o usuário tenha a opção de consentir ou não, com a coleta e o tratamento desses dados. Em se tratando de uma rede social que coleta dados pessoais de seus usuários para fins publicitários, a empresa deve possibilitar que os usuários tenham acesso às informações coletadas e possibilidade de corrigir ou excluir esses dados, caso desejem, e da mesma forma garantir que o usuário tenha a opção de não receber publicidade personalizada, se assim desejar.

1.3 Visibilidade *versus* Segurança de Dados: dilema nas redes sociais

Segundo Endo (2022), é importante adotar uma abordagem estratégica no gerenciamento da visibilidade de dados. Não apenas para garantir a segurança dos dados, mas também para viabilizar o acesso e a compreensão das informações relacionadas à infraestrutura de Tecnologia da Informação (TI) e ao fluxo de dados. Essencialmente, esse conhecimento profundo torna a segurança vital, permitindo a proteção de sistemas contra ameaças que podem comprometer a segurança organizacional.

A visibilidade de dados permite identificar atividades suspeitas e responder rapidamente a incidentes de segurança. A falta de visibilidade pode levar a vulnerabilidades e falhas de segurança, no entanto, se faz fundamental investir em soluções que garantam a visibilidade completa dos dados para fortalecer as estratégias de segurança (Endo, 2022).

A visibilidade de dados refere-se à transparência no tratamento das informações pessoais, de modo que as pessoas devam ser informadas sobre a coleta, o armazenamento e o uso de seus dados. Essa transparência permite que os

titulares dos dados exercitem seus direitos e tenham controle sobre o uso de suas informações. Portanto, é fundamental que as empresas adotem políticas de privacidade claras e transparentes, que informem aos usuários sobre o armazenamento e processamento de dados pessoais. Essas medidas contribuem para a construção de um ambiente digital mais seguro e confiável, que respeite os direitos e a privacidade dos usuários (Franke, 2022).

De acordo com OCI (2023) a segurança de dados refere-se às práticas e tecnologias utilizadas para proteger as informações de uma organização contra ameaças internas e externas. Sendo essencial para garantir a privacidade dos dados dos clientes e cumprir as regulamentações governamentais, dentre elas a LGPD. Para alcançar a segurança de dados, são adotadas medidas como criptografia, autenticação de usuários, *backup* e recuperação de dados. Essas práticas visam preservar a integridade, confidencialidade e disponibilidade dos dados, minimizando os riscos de violação e protegendo a reputação da organização.

A proteção dos dados pessoais é um tema multidisciplinar, que envolve tanto questões jurídicas quanto técnicas, sendo necessário um esforço conjunto para garantir a segurança e privacidade dos dados pessoais dos usuários da internet. A visibilidade dos dados pessoais na internet deve ser acompanhada de medidas efetivas de proteção, bem como que os usuários da internet sejam mais conscientes sobre os riscos envolvidos na divulgação de informações pessoais na rede (Santos, 2021).

A LGPD estabelece que as empresas de redes sociais sejam responsáveis pelo conteúdo publicado em suas plataformas. Sendo assim, destaca os desafios que a regulação das redes sociais enfrenta, como a dificuldade de identificar o conteúdo ilegal e a ameaça à liberdade de expressão. São também discutidos os possíveis efeitos psicológicos e as reações das empresas de tecnologia à regulação proposta. Embora seja necessário encontrar soluções para o dilema das redes sociais, o controle deve ser cuidadosamente considerado para equilibrar a liberdade

de expressão com a proteção dos usuários contra conteúdo prejudicial (Barroso, 2022).

As redes sociais se consagraram como ferramenta fundamental para os negócios, permitindo que as empresas se conectem com seus clientes de forma mais eficiente e eficaz. Para as empresas que desejam alcançar o sucesso nos negócios se faz necessário estar em alguma rede social (Oliveira, 2023), embora ainda se discuta como as empresas podem medir o sucesso de sua estratégia de mídia social, analisando indicadores como envolvimento do usuário, alcance e conversão de vendas.

Uma das principais vulnerabilidades nas redes sociais é a falta de controle sobre a privacidade dos dados pessoais. Muitos usuários não se dão conta de que as informações que são armazenadas nas redes sociais podem ser acessadas por terceiros, incluindo anunciantes, empresas de marketing e até mesmo criminosos. Outro ponto que deve ser levado em consideração é que muitos usuários não sabem como proteger suas informações pessoais nas redes sociais e acabam se tornando vítimas de golpes e fraudes *online*. É importante que os usuários tomem medidas para proteger suas informações pessoais, como definir corretamente as opções de privacidade em suas contas e evitar compartilhamento de informações pessoais (Carvalho; Cappelli; Oliveira, 2020).

De acordo com Costa e Oliveira (2019), os dados pessoais que podem ser considerados para a LGPD nas redes sociais são informações de identificação pessoal, como nome completo, data de nascimento, endereço e número de identidade; informações de contato, como endereço de e-mail, número de telefone e endereço residencial; dados financeiros, como número de cartão de crédito, histórico de transações bancárias e informações de conta bancária; informações de localização, como histórico de localização em dispositivos móveis e endereços IP; informações de atividades, como histórico de pesquisa, interesses, compras e bem-estar nas redes sociais; informações de saúde, como histórico médico e tratamentos; informações de emprego, como currículo, histórico de trabalho e

informações de pagamento; e informações pessoais sensíveis, como orientação sexual, afiliação religiosa, política e informações genéticas.

Souza e Mozetic (2022) mencionam que inúmeras pessoas guardam informações pessoais em redes sociais sem ter consciência dos riscos de privacidade envolvidos. Um exemplo citado pelos autores é o compartilhamento de fotos do usuário e/ou informações de localização em tempo real, que empresas podem utilizar os dados pessoais compartilhados nas redes sociais para criar perfis de consumo e direcionar anúncios personalizados ou que podem invadir a privacidade dos usuários.

2 METODOLOGIA DA PESQUISA

O objetivo desta pesquisa consiste em realizar uma análise exploratória acerca do tratamento de dados realizados ou não pelas EPP - Empresas de Pequeno Porte com base na LGPD, em especial no que se refere à proteção e garantia de segurança dos dados de seus clientes (pessoa natural), armazenados no sistema empresarial. Também investigar a forma como essas empresas utilizam as redes sociais, em particular o *Instagram*, para promover seus produtos ou serviços, quanto ao uso de dados de seus clientes (pessoa natural) para fins de gestão de marketing.

Conforme preconiza Gil (2019) esse tipo de pesquisa é adequado para situações em que se tem poucas informações sobre o tema, justificando a necessidade de uma análise mais aprofundada. Sendo um tema relativamente recente, pois ambas as leis basilares deste estudo foram expedidas em 2014, Marco Civil da Internet, e 2018, LGPD.

Segundo o site Empresaqui (2023), a cidade de Indaiatuba, localizada na região metropolitana de Campinas, interior de São Paulo, possui 38.507 empresas em atividade. Desse montante, destacam-se 29.733 microempresas, 18.699 MEIs, 2.995 pequenas empresas e 5.779 empresas de porte médio e grande. A

proximidade da cidade ao aeroporto de Viracopos favorece a logística de escoamento da produção, o que faz da região um polo atraente para a instalação de empresas.

O Sebrae (2013) explica que a definição da EPP se dá por um dos dois fatores: quantidade de funcionário, sendo que comércios e serviços variam de 10 a 49 funcionários e na indústria de 20 a 99 funcionários ou por faturamento anual acima de R\$ 360 mil e menor de R\$ 4,8 milhões (DAU, 2022), assim o critério da amostra para esta pesquisa foi determinada com base na quantidade de funcionários.

O questionário foi formatado no *Google forms*, enviado aos gestores das empresas e empresários por e-mail e pela rede social WhatsApp, tais contatos (e-mail ou WhatsApp) foram obtidos por meio de levantamento feito no site da prefeitura de Indaiatuba, junto a secretária de governo, através do catálogo das indústrias de Indaiatuba, em buscas realizadas pelo *Google* e por *network* dos pesquisadores com empresários e gestores de Indaiatuba, no período de 25 de outubro à 13 de novembro de 2023, caracterizando-se documental, por conveniência e acessibilidade. Assim apresenta variáveis de acordo os segmentos empresariais podendo ser comércio, serviço ou indústria.

Foram elaboradas 14 questões com alternativas fechadas de respostas, as questões foram distribuídas para responder cada elemento de análise. Conforme definido pelo SEBRAE (2013) a quantidade de funcionários foi fator para classificar se uma empresa se enquadra como EPP. Outro fator relevante para o critério de delimitação da pesquisa foi se a empresa está presente na rede social. O instrumento de coleta de dados buscou verificar o conhecimento da LGPD, em relação a coleta, retenção, processamento, compartilhamento e eliminação dos dados aplicado na empresa, se a empresa faz marketing dos seus serviços ou produtos nas redes sociais e usa imagem ou outro dado de seus clientes para divulgação ou para outros tipos de uso. Isso permitiu observar, se há compreensão da LGPD e ação para resguardar os dados dos clientes, bem como as empresas de

pequeno porte cuidam dos dados de seus clientes em divulgações nas redes sociais.

Os dados coletados foram separados de acordo com cada categoria, organizados em planilha no Excel, analisados e utilizados na elaboração de gráficos, a partir da estatística descritiva. Embora a abordagem deste estudo tenha foco nas EPP da cidade de Indaiatuba que estão presentes na rede social Instagram, é importante esclarecer que, por razões operacionais, esta pesquisa trata de uma amostra com características não probabilística, o que inviabiliza a generalização dos resultados para descrever, em sua totalidade, as EPP de Indaiatuba.

3 ANÁLISE E DISCUSSÃO DOS DADOS

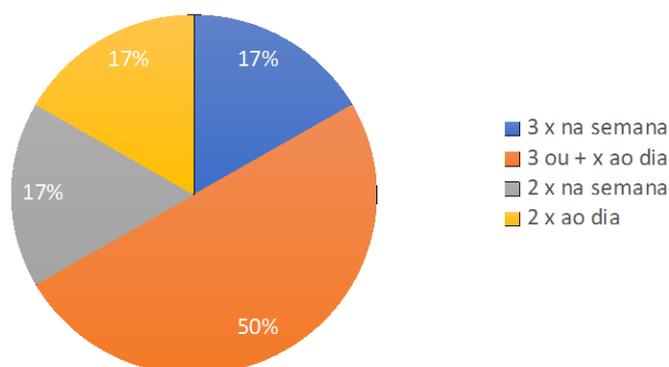
Das 20 empresas respondentes do questionário apenas 14 empresas, que representam 70% da amostra, enquadraram-se na categoria MEIs (Microempreendedores Individuais) tendo entre 1 e 9 funcionários. As outras 6 empresas, que representam 30%, enquadraram-se na categoria de EPP - Empresas de Pequeno Porte, tendo entre 10 e 49 funcionários, de acordo com a definição do SEBRAE (2023). Para esta pesquisa, a análise foi focada nas empresas definidas como EPP.

Quando perguntado qual o ramo de atuação da empresa, pode ser identificado que elas estão divididas em 50% por comércios, 45% de prestadoras de serviços e 05% como indústria.

Todas as 6 EPP, 100% das empresas analisadas, estão presentes nas redes sociais para divulgar seus produtos e/ou serviços e fazem uso do Instagram. Segundo Oliveira (2023) estar presentes nas redes sociais é importante, para criar estratégias e alcançar maior envolvimento com os clientes, a fim de convertê-los em taxas de vendas.

Em se tratando de frequência das postagens nas redes sociais o gráfico 01 deixa claro o quanto essas empresas de pequeno porte utilizam o Instagram para promover o marketing dos serviços e/ou produtos. A constância de publicações das empresas no Instagram é de 50% três vezes ou mais ao dia, 17% duas vezes ao dia, 17% duas vezes na semana e 16% três vezes na semana.

Gráfico 1 - Frequência de postagem no Instagram



Fonte: Elaboração própria com base na tabulação dos dados obtidos pelo questionário.

Quanto ao Marco Civil da Internet, sobre direitos e deveres, segundo Gomes (2019), a empresa deve garantir que os clientes possam escolher receber ou não publicidades personalizadas. Dentre as empresas respondentes da pesquisa, 33,33% não disponibilizam a opção aos clientes de receber ou não publicidade personalizada, as outras 4 empresas respondentes, 66,67%, disponibilizam a opção ao cliente de receber ou não a publicidade personalizada.

Quando perguntado sobre e-mail marketing foi identificado que 50% oferecem a opção de receber ou não o e-mail marketing e as outras 3 empresas, 50%, não oferecem a opção ao cliente de não receber e-mail marketing. Analisando os dados apurados, verifica-se que 3 EPP respondentes, 50% da amostra, não se enquadram no que se refere a garantia e privacidade, infringindo o que preconiza o Marco Civil da Internet, que estabelece a não utilização de dados dos usuários para fins comerciais sem autorização.

A transparência é um dos princípios da LGPD, o usuário deve ser informado de maneira clara e acessível sobre os riscos e direitos dos seus dados (Cunha, 2018). 50% das empresas respondentes assinalaram que sempre informam aos clientes à possibilidade de fazer divulgação do atendimento realizado nas redes sociais e 17% às vezes comunicam e 33% nunca fazem a comunicação da possibilidade de usar o atendimento ou prestação de serviços e/ou venda de produtos para divulgação em redes sociais. No entanto, conforme apresentado por Cunha (2018), a LGPD estabelece a necessidade de manter e utilizar apenas os dados essenciais dos clientes, apagando-os quando deixarem de ser relevantes, e tratando da adequada disponibilização das informações sobre a coleta e uso de dados para o usuário de forma honesta, para que possa cumprir com a legislação.

Conforme descreve a lei a autorização da divulgação no Instagram ou em qualquer mídia social deve ser feita por escrito ou em cláusula de contrato. Entre as empresas respondentes da pesquisa, somente 17% informam em cláusula de contrato o termo de usar dados do cliente para divulgação, 33% declararam informar verbalmente e pessoalmente, 17% comunicam por WhatsApp e 33% não comunicam. Os dados levantados e analisados revelam que a maioria as empresas de pequeno porte de Indaiatuba que fizeram parte da pesquisa, não tem este cuidado.

Quando perguntado quais dados dos clientes são utilizados pela empresa nas postagens em redes sociais, identificou-se que 57% fazem marcação no Instagram, 14% fazem uso de imagens, vídeos, compartilhamento de pesquisa respondida, reposta comentários (referente a experiência do atendimento) e 29% não utilizam dados das pessoas naturais para publicação no Instagram.

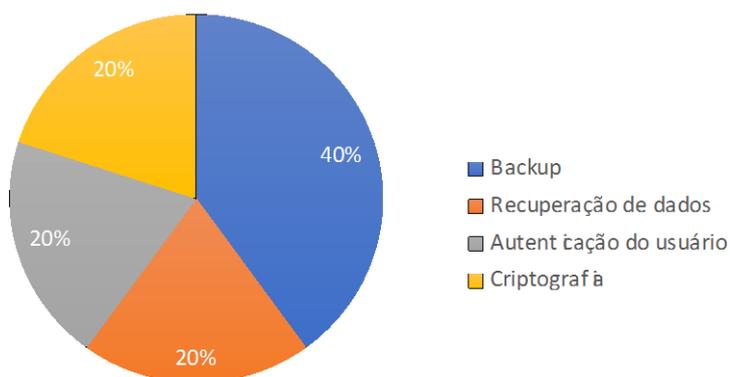
Ao verificar quais dados dos clientes a empresa cadastra em banco de dados, teve como objetivo abordar a principal finalidade da LGPD, que é cuidar da legitimidade e clareza do porquê a informação se faz necessária para a coleta, podendo verificar quais dados são comuns e quais os dados sensíveis, 13% das empresas respondentes armazenar dados sensíveis (Sexo e Filiação) de seus

clientes, 87% cadastram dados comuns (CPF/RG, Endereço, Sobrenome, E-mail, Filiação, Rede Social).

Para entender se as EPP de Indaiatuba, respondentes da pesquisa, armazenam os dados das pessoas naturais de acordo com o tempo determinado pelo Marco Civil da Internet que no quesito privacidade especifica pôr no mínimo 6 meses (Portal Fiocruz, [2023]), apurou-se que 67% armazenam os dados por mais de 6 meses e 33% não sabem dizer por quanto tempo os dados são armazenados pelas empresas de pequeno porte.

Conforme apresentado por OCI (2023) se faz necessário algumas medidas de segurança com os dados dos clientes cadastrados no sistema da empresa, apresentado no gráfico 2, 40% dos respondentes da pesquisa declaram que fazem *backup*, 20% fazem recuperação de dados, 20% fazem autenticação do usuário e 20% fazem criptografia, deve-se levar em consideração que cada empresa que participou da pesquisa faz uso somente de um dos meios de segurança.

Gráfico 2-Medidas de segurança



Fonte: Elaboração própria com base na tabulação dos dados obtidos pelo questionário.

Ao final foi perguntado se a empresa tem conhecimento da LGPD, constatando que 100% das empresas de pequeno porte respondentes de Indaiatuba declaram ter conhecimento da LGPD.

CONSIDERAÇÕES FINAIS

O presente estudo teve como objetivo entender como as EPP - Empresas de Pequeno Porte estão lidando com a LGPD quando se trata da divulgação nas redes sociais. Para tal, foi preciso compreender o que preconiza a LGPD e Marco Civil da Internet, bem como desvelar questões sobre a visibilidade e segurança de dados dos usuários das redes sociais.

Como resultado constatou-se que as empresas participantes deste estudo declaram conhecer as novas regras de proteção de dados pessoais, no entanto, há pontos que precisam ser melhorados. Apenas 17% das empresas informam em cláusula de contrato o termo de usar dados do cliente para divulgação. Não mais de 67% têm ciência que armazenam os dados por mais de 6 meses, conforme determinado pelo Marco Civil da Internet. Outro ponto importante a destacar é que somente 40% das empresas fazem *backup* dos dados dos clientes. Isso representa um risco, pois os dados podem ser perdidos ou roubados caso ocorra algum problema com o sistema da empresa.

Com base na pesquisa realizada, pode-se concluir que as EPP de Indaiatuba declaram ter conhecimento da LGPD, mas ainda há um desconhecimento quanto às suas aplicações práticas, especialmente no que diz respeito ao uso de redes sociais para divulgação de serviços e/ou produtos e para promover ações de marketing.

A partir dos resultados obtidos verificou-se que a hipótese de partida é suportada parcialmente, pois os empreendedores de pequeno porte da cidade de Indaiatuba, participantes deste estudo, não têm compreensão plena sobre a importância da LGPD e, conseqüentemente, não tomam as medidas necessárias para resguardar os dados dos clientes em suas divulgações nas redes sociais.

No entanto, o estudo não conseguiu trazer à luz o motivo segundo o qual as EPP – empresas de pequeno porte não adotam as medidas necessárias para resguardar os dados dos clientes em suas divulgações nas redes sociais. Sendo



assim, sugere-se que futuras pesquisas apurem se recursos financeiros e/ou técnicos são os limitadores para que as EPP possuam capacidade para se adequar à LGPD e, portanto, apresentem menor vulnerabilidade à violação de dados dos clientes.

REFERÊNCIAS

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**. 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/ato2015-2018/2018/lei/L13709.htm. Acesso em: 26 mar. 2023.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial da União**. 24 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/ato2011-2014/2014/lei/l12965.htm. Acesso em: 28 mar. 2023.

BARROSO, Fernanda. Artigo: Uma lei para o dilema das redes: **Veja**. 2020. Disponível em: <https://veja.abril.com.br/tecnologia/artigo-uma-lei-para-o-dilema-das-redes/>. Acesso em: 02 abr. 2023.

CARVALHO, Luiz Paulo; CAPPELLI, Claudia; OLIVEIRA, Jonice. **Pesquisas em Análise de Redes Sociais e LGPD, análises e recomendações**. Porto Alegre, 2020. Disponível em: <https://sol.sbc.org.br/index.php/brasnam/article/view/11164>. Acesso em: 02 abr. 2023.

COSTA, Ramon Silva; OLIVEIRA, Samuel Rodrigues de. Os direitos da personalidade frente à sociedade de vigilância: privacidade, proteção de dados pessoais e consentimento nas redes sociais. **Revista brasileira de direito civil em perspectiva**, v. 5, n. 2, p. 22-41, 2019.

CGI. Lei do Marco Civil da Internet no Brasil. 23 abril 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial da União**. Disponível em: <https://www.cgi.br/lei-do-marco-civil-da-internet-no-brasil/>. Acesso em: 29 mar. 2023.



CELIDONIO, Tiago; NEVES, Paulo Sergio; DONÁ, Claudio Melim. Metodologia para mapeamento dos requisitos listados na LGPD (Lei Geral de Proteção de Dados do Brasil número 13.709/18) e sua adequação perante a lei em uma instituição financeira - Um estudo de caso. **Brazilian Journals** São José dos Pinhais; Paraná, v. 2, n. 4, p.1-23, out. 2020. DOI: 10.34140/bjbv2n4-012. Disponível em: <https://ojs.brazilianjournals.com.br/ojs/index.php/BJB/article/view/18382/14839>. Acesso em: 28 mar. 2023.

CUNHA, Caio. LGPD: entenda o que muda com a Lei Geral de Proteção de Dados. **Blog.wsiconsultoria**. 19 out. 2018. Disponível em: <https://blog.wsiconsultoria.com/lgdp-entenda-o-que-muda-com-a-lei>. Acesso em 20 abr. 2023.

DAU, Gabriel. Entenda Todos Os Tipos De Porte De Empresa E Suas Definições. 8 Jul 2022. **Rede jornal contábil**. Disponível em: <https://www.jornalcontabil.com.br/entenda-todos-os-tipos-de-porte-de-empresa-e-suas-definicoes/>. Acesso em: 15 mai. 2023.

EMPRESAQUI. **Listas de empresas em Indaiatuba, SP: abertas recentemente, maiores empresas, por segmento (CNAE), indústrias, com dívidas, quantidade de habitantes e mais!** [online]. Publicado em 08 abril 2023. Disponível em: <https://www.empresaquei.com.br/listas-de-empresas/SP/INDAIATUBA>. Acesso em: 02 mai. 2023.

ENDO, Jun. **Visibilidade de dados é vital para estratégias de segurança**. 23 mar. 2022. Disponível em: <https://itforum.com.br/posts/brandspaces/visibilidade-de-dados-e-vital-para-estrategias-de-seguranca/>. Acesso em: 29 mar. 2023.

FIOCRUZ. Fundação Oswaldo Cruz. **Princípios fundamentais do Marco Civil da Internet**. [2023]. Disponível em: <https://portal.fiocruz.br/documento/principios-fundamentais-do-marco-civil-da-internet>. Acesso em: 20 abr. 2023.

FRANKE, Ana Laura Fonseca. *et.al.* FELICIDADE COMPRADA: UMA ANÁLISE DOS REFLEXOS DA LGPD NA COMERCIALIZAÇÃO DA FELICIDADE DENTRO DAS REDES SOCIAIS. **Revista de Direito FAE – RDF**, Curitiba, v. 3 n. 1, Jun. 2021.

GIL A. C. **Como elaborar Projetos de pesquisa**. 6 ed. São Paulo. Atlas, 2019.



GOMES, Heloisa dos Santos. LEI GERAL DE PROTEÇÃO DE DADOS (LGPD): UMA ANÁLISE DOS IMPACTOS DA LEI NA CULTURA E TRATAMENTO DE DADOS NO BRASIL. Florianópolis 2019. **Repositório Universitário da Ânima (RUNA)**. Disponível em: <https://repositorio.animaeducacao.com.br/handle/ANIMA/11112>. Acesso em: 27 mar. 2023.

GOV.BR. **GUIA DE BOAS PRÁTICAS LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)**. 2020. Disponível em https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf Acesso em :28 mar. 2023.

GUIMARÃES, Leonardo. LGPD: o que é a Lei Geral de Proteção de Dados Pessoais e como funciona? **CNN Brasil Business**. São Paulo 27 ago. 2020. Disponível em: <https://www.cnnbrasil.com.br/economia/lgpd-o-que-e-e-para-que-serve-a-nova-lei-de-protecao-de-dados>. Acesso em: 28 mar. 2023.

IPEA. **O que é a LGPD**. 2021. Disponível em: <https://www.ipea.gov.br/protecaodedados/O-que-e-a-LGPD>. Acesso em: 28 mar. 2023.

MAFRA, Ediléia. Proteção da Privacidade no Brasil: Desafios, Oportunidades e Avaliação da efetividade da LGPD. 06 abr. 2023. **Jus.com.br**. Disponível em: <https://jus.com.br/artigos/103414/protecao-da-privacidade-no-brasil-desafios-oportunidades-e-avaliacao-da-efetividade-da-lgpd>. Acesso em: 30 mar. 2023.

OLIVEIRA, Eder. Redes sociais viram ferramenta fundamental para os negócios. 03 abr. 2023. **Terra**. Disponível em: <https://www.terra.com.br/noticias/redes-sociais-viram-ferramenta-fundamental-para-os-negocios,eaed67753dee13260054d1228853c3cbz3q31bsq.html>. Acesso em: 05 abr. 2023.

OCI. **O que é Segurança de Dados?** [2023]. Disponível em: <https://www.oracle.com/br/security/database-security/what-is-data-security/>. Acesso em: 29 mar. 2023.

PREFEITURA DE INDAIATIBA. **Secretarias e Órgãos**. S.d. Disponível em: <https://www.indaiatuba.sp.gov.br/governo/assuntos-industriais/catalogo-das-industrias/>. Acesso em 12 ago. 2023.



QUEIROZ; Tayrine. Marco Civil da Internet: um estudo da sua criação sob a influência dos direitos humanos e fundamentais, a neutralidade da rede e o interesse público versus privado. 2017. **Jusbrasil**. Disponível em: <https://tayrine.jusbrasil.com.br/artigos/303303808/marco-civil-da-internet-um-estudo-da-sua-criacao-sob-a-influencia-dos-direitos-humanos-e-fundamentais-a-neutralidade-da-rede-e-o-interesse-publico-versus-privado>. Acesso em: 29 mar. 2023.

SANTOS, Chistiane Oliveira dos. Lei geral de proteção de dados pessoais (LGPD), Lei nº 13.709/2018: direito à privacidade aplicada às redes sociais. **Puc Goiás**. 05 jun 2021. Disponível em: <https://repositorio.pucgoias.edu.br/jspui/handle/123456789/1576>. Acesso em: 01 abr. 2023.

SEBRAE. **MPE_conceito_empregados. Definição de porte de estabelecimentos segundo o número de empregados**. 2013. Disponível em: https://sebrae.com.br/Sebrae/Portal%20Sebrae/UFs/SP/Pesquisas/MPE_conceito_e_mpregados.pdf. Acesso em: 22 out. 2023.

SOUZA, Giordana Carloto de; MOZETIC, Vinícius Almada. O fenômeno sharenting: intromissões ilegítimas de direitos à privacidade das crianças nas redes sociais. **Seminário de Iniciação Científica e Seminário Integrado de Ensino, Pesquisa e Extensão**, 10 nov. 2022. Disponível em: <https://periodicos.unoesc.edu.br/siepe/article/view/31469>. Acesso em: 27 mar. 2023. TJDF - Tribunal de Justiça do Distrito Federal e dos Territórios. **Marco Civil da Internet**. 2017. Disponível em: <https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/direito-facil/edicao-semanal/marco-civil-da-internet>. Acesso em: 29 mar. 2023.

ZITO, Fernando Augusto. **Quando a LGPD não se aplica?** 15 jun. 2021. Disponível em: <https://www.zmr.adv.br/2021/07/15/quando-a-lgpd-nao-se-aplica/>. Acesso em: 30 abr. 2023.

Recebido em 31/01/2024

Publicado em 02/08/2024