

CENTRO UNIVERSITÁRIO BRASILEIRO – UNIBRA  
CURSO DE GRADUAÇÃO TECNÓLOGO EM  
REDES DE COMPUTADORES

FELIPE CARNEIRO DA SILVA BARROS

**VAZAMENTO DE DADOS PESSOAIS NA INTERNET:  
A POPULAÇÃO BRASILEIRA ESTÁ PROTEGIDA  
COM A LGPD.**

RECIFE/2021

FELIPE CARNEIRO DA SILVA BARROS

**VAZAMENTO DE DADOS PESSOAIS NA INTERNET:  
A POPULAÇÃO BRASILEIRA ESTÁ PROTEGIDA  
COM A LGPD.**

Trabalho conclusão de curso apresentado ao Centro  
Universitário Brasileiro – UNIBRA, como requisito parcial para  
obtenção do título de tecnólogo em Redes de Computadores.

Professor Orientador: Msc. Ameliara Freire Santos de Miranda

RECIFE/2021

Ficha catalográfica elaborada pela  
bibliotecária: Dayane Apolinário, CRB4- 2338/ O.

B277v Barros, Felipe Carneiro da Silva  
Vazamento de dados pessoais na internet: a população brasileira está protegida com a LGPD. / Felipe Carneiro da Silva Barros. - Recife: O Autor, 2021.  
24 p.  
Orientador(a): Ameliara Freire Santos de Miranda.  
Trabalho de Conclusão de Curso (Graduação) - Centro Universitário Brasileiro – UNIBRA. Tecnólogo em Redes de Computadores, 2021.  
Inclui Referências.  
1. Vazamento de dados. 2. Lei geral de proteção de dados. I. Centro Universitário Brasileiro - UNIBRA. II. Título.

CDU: 004

*Dedico esse trabalho aos meus parentes e Professores por todo apoio durante o curso.*

## **AGRADECIMENTOS**

Agradeço a Deus, pois toda a sabedoria é dada por ele. Eu sou grato aos meus familiares, principalmente a minha mãe por estarem me apoiando na torcida mostrando que eu sou capaz e aos amigos que me incentivaram a estudar.

A jornada deste trabalho não foi fácil, integrantes que inicialmente resolveram participar, mas nada contribuíram para o trabalho desistiram após verem o desafio a frente. O caminho certamente é difícil, mas todos somos capazes de ir além para conquistar nossos sonhos basta querer. Também quero agradecer aos professores por transmitirem o seu conhecimento e mostrarem que tenho potencial.

*“Os sonhos não determinam o lugar que  
você vai estar, mas produzem a força  
necessária para o tirar do lugar em que  
está.” (Augusto Cury)*

## SUMÁRIO

<b>1 INTRODUÇÃO</b> .....	<b>9</b>
<b>1.1 Considerações iniciais</b> .....	<b>9</b>
<b>1.2 Problemática</b> .....	<b>10</b>
<b>1.3 Justificativa</b> .....	<b>11</b>
<b>1.4 Objetivos</b> .....	<b>11</b>
1.4.1 <i>Objetivos Gerais</i> .....	11
1.4.2 <i>Objetivos Específicos</i> .....	12
<b>2 METODOLOGIA CIENTÍFICA</b> .....	<b>13</b>
<b>3 REFERENCIAL TEÓRICO</b> .....	<b>14</b>
<b>3.1 Segurança da informação</b> .....	<b>14</b>
3.1.1 <i>Princípios Fundamentais</i> .....	14
3.1.2 <i>Principais problemas de Segurança</i> .....	15
<b>3.2 Vazamento de dados</b> .....	<b>16</b>
<b>3.3 Lei geral de proteção de dados</b> .....	<b>17</b>
3.3.1 <i>Princípios referentes ao tratamento de dados</i> .....	18
3.3.2 <i>Dos direitos do Titular</i> .....	19
3.3.4 <i>Autoridade Nacional de Proteção de Dados</i> .....	20
3.3.5 <i>Das Sanções Administrativas</i> .....	21
<b>3.4 A necessidade da aplicação da LGPD</b> .....	<b>21</b>
<b>4 RESULTADO</b> .....	<b>23</b>
<b>4.1 A Lei geral de proteção de dados pessoais em empresas brasileiras: uma análise de múltiplos casos</b> .....	<b>23</b>
<b>4.2 LGPD (Lei geral de proteção de dados) e sua aplicabilidade no tratamento de dados no e-commerce</b> .....	<b>24</b>
<b>4.3 Lei geral de proteção de dados (LGPD): características e aplicações na biblioteconomia e ciência da informação</b> .....	<b>24</b>
<b>5 CONSIDERAÇÕES FINAIS</b> .....	<b>25</b>
<b>6 REFERÊNCIAS</b> .....	<b>27</b>

# **VAZAMENTO DE DADOS PESSOAIS NA INTERNET: A POPULAÇÃO BRASILEIRA ESTÁ PROTEGIDA COM A LGPD.**

Felipe Carneiro da Silva Barros  
Ameliara Freire Santos de Miranda

**Resumo:** Este estudo tem como objetivo analisar do que se trata vazamento de dados pessoais na internet e entender a importância da Lei Geral de Proteção de Dados, que entrou em vigor para proporcionar um maior controle sobre o tratamento dos dados, estabelecendo princípios e regras que devem ser observados por organizações. Tendo como justificativas recorrentes vazamentos de dados pessoais pela internet e, conseqüentemente, a exposição, venda ou utilização indevida desses dados, a necessidade por segurança digital é de fundamental importância. Foi realizada uma pesquisa exploratória com uma análise qualitativa por meio da pesquisa bibliográfica. O estudo demonstrou que é um desafio para as empresas se adequarem à lei e o desconhecimento sobre a legislação, por parte dos profissionais, deixa evidente a necessidade de mais esclarecimento, treinamento e mudança de comportamento, quando o assunto é segurança da informação nas organizações.

**Palavras-chave:** vazamento de dados, lei geral de proteção de dados



## **LISTA DE ABREVIATURAS E SIGLAS**

ANPD	Autoridade Nacional de Proteção de Dados
LGPD	Lei Geral de Proteção de Dados
MCI	Marco Civil da Internet
RGPD	Regulamento Geral de Proteção de Dados
SCIELO	Scientific Electronic Library Online

# 1 INTRODUÇÃO

## 1.1 Considerações iniciais

Diante da crescente utilização da internet, cada vez mais pessoas têm acessado o mundo virtual por meio de dispositivos tecnológicos. De acordo com Valente (2020), três em cada quatro brasileiros acessam a internet, o que equivale a 134 milhões de pessoas. Entre os dispositivos mais comuns para se conectar à internet estão os smartphones, computadores e TVs. Por meio desses equipamentos são acessados serviços como, por exemplo, o aplicativo de mensagens *Whatsapp*, portais de compras *online*, conteúdos via *streaming*, dentre outros.

Entretanto, usufruir desses serviços requer um compartilhamento de dados por parte do usuário que ao cadastrar suas informações como endereço de e-mail, telefone, número de documentos pessoais, dentre outros. Essas informações não somente são compartilhadas no mundo digital, mas podem ser compartilhadas no mundo físico, como por exemplo, um cadastro na academia para fazer uso de seus serviços ou a adesão de programas de fidelidade em farmácias (UNINCOR, 2021).

O tratamento de dados realizado pelas empresas para produção de informação representa um grande avanço para obtenção de seus objetivos, agregando valor a suas atividades econômicas. No entanto, o interesse voltado à produção de dados como ponto fundamental para estratégia de negócios traz uma preocupação em relação à proteção de dados pessoais. (BOTELHO, 2020).

A divulgação cada vez mais frequente de vazamento de dados vista em reportagens deixa evidente a necessidade de proteção de dados. Segundo a reportagem do G1 (2021), 223 milhões de dados brasileiros foram vazados, neles continham informações pessoais e até dados sobre veículos. De acordo com a reportagem de Loureiro (2020), milhares de conversas pessoais em vídeos feitos por usuários do aplicativo Zoom ficaram disponíveis na internet.

No Brasil os dados pessoais eram tratados pelo Marco Civil da Internet (Lei n. 12.965/2014), que continha direitos acerca da privacidade no uso da Internet. Mas, deixava lacunas para a forma com que os dados fornecidos pelos usuários poderiam ser utilizados pelas empresas (BRASIL, 2014).

Em 2018 foi publicada a Lei Geral de Proteção de Dados Pessoais (LGPD), nº 13.709/18, que busca preencher as lacunas acerca da privacidade das pessoas. A LGPD estabelece diversos direitos do titular dos dados pessoais, especialmente em seu artigo 18, os quais são: a informação, acesso, correção, portabilidade e eliminação (BRASIL, 2018).

Com a LGPD em vigor, a preocupação das empresas em proteger as informações de terceiros passou a ser um ativo valioso para o setor de segurança da informação de uma empresa. Visando a proteção de dados dos clientes uma empresa que antes não considerava a informação como um ativo deve se adequar à lei utilizando medidas de segurança para que nenhum dos princípios fundamentais como confidencialidade, disponibilidade e integridade dos dados fique vulnerável podendo ser expostos na internet (FERNANDES, 2013).

Tanto a União Europeia, que tem uma lei para proteção dos dados, a *General Data Protection Regulation 2016/679* (GDPR), como o Brasil, cuja lei é a Lei Geral de Proteção de Dados Pessoais (LGPD), visam aplicar multas severas às empresas que fazem mau uso dos dados de seus usuários. Sua atuação consiste em um sistema que promova segurança e privacidade a todos as pessoas no meio virtual.

## **1.2 Problemática**

O governo de diversos países têm observado o grande problema que o uso indiscriminado de dados por empresas pode trazer devido aos recorrentes vazamentos de dados pessoais pela internet. A exposição destes dados denotam que a necessidade por segurança digital é de extrema importância, e recentemente essa problemática está sendo discutida no Brasil.

A Lei geral de proteção de dados promete vários benefícios de segurança para a população, com esta lei em vigor, este trabalho dispõe-se a explorar como essa lei ajudará no papel da segurança na internet.

### 1.3 Justificativa

A insegurança no mundo digital devido às falhas de confidencialidade dos dados pessoais tratados pelas organizações no Brasil demonstram a necessidade de uma legislação específica para o tratamento de dados pessoais.

A lei do Marco Civil da Internet (MCI), sancionada em 2014, cumpre o papel de incumbir os devidos agentes a fiscalizar empresas e instituições para que estas garantam a privacidade e a proteção de dados pessoais do titular *online* durante o uso na internet. Entretanto, o MCI deixa lacunas referentes a como os dados pessoais do titular devem ser tratados pelas organizações.

Visando a proteção de dados pessoais, a transparência e a responsabilização pelo tratamento de dados, foi criada a Lei Geral de Proteção de Dados que abrange diretrizes para a proteção de dados nos ambientes *online* e *offline*.

Entre as diretrizes da LGPD estão os princípios para o tratamento de dados do titular por organizações, os direitos que o titular possui sobre os seus dados e os agentes responsáveis no tratamento de dados pessoais.

Em virtude do recente vigor da LGPD somado ao prazo estabelecido para que as empresas se adequassem a ela, uma parte dos titulares brasileiros não está a par dos direitos que possuem, no que diz respeito à coleta, ao armazenamento e tratamento de dados realizados pelas instituições.

### 1.4 Objetivos

#### 1.4.1 *Objetivos Gerais*

Este trabalho tem como objetivo geral analisar do que se trata vazamento de dados pessoais na internet e entender a importância da Lei Geral de Proteção de Dados que entrou em vigor, para proporcionar um maior controle sobre o tratamento dos dados, estabelecendo princípios e regras que devem ser observados por organizações.

#### 1.4.2 *Objetivos Específicos*

- Definir os princípios da segurança da informação;
- Analisar do que se trata os vazamentos de dados;
- Explicar os objetivos da LGPD;
- E avaliar a necessidade da aplicação desta Lei.

## 2 METODOLOGIA CIENTÍFICA

A pesquisa deste trabalho tem como finalidade a natureza básica que de acordo com Gerhardt (2009, p. 34), “objetiva gerar conhecimentos novos, úteis para o avanço da Ciência, sem aplicação prática”. Quanto ao objetivo foi realizado uma pesquisa exploratória, “este tipo de pesquisa tem como objetivo proporcionar maior familiaridade com o problema, com vistas a torná-lo mais explícito” (GERHARDT, 2009, p. 34). Já em relação a sua abordagem a pesquisa teve uma análise qualitativa. Na pesquisa qualitativa, o cientista é ao mesmo tempo o sujeito e o objeto de suas pesquisas. (GERHARDT, 2009 apud DESLAURIERS, 1991, p. 58).

Este trabalho teve como método a pesquisa bibliográfica. Segundo Gil (2009), a Pesquisa Bibliográfica, ou de fontes secundárias, abrange toda bibliografia pública em relação ao tema de estudo, desde livros, pesquisas, monografias, teses e dentre outros. Sua finalidade é colocar o pesquisador em contato direto com tudo o que foi escrito, dito ou formado sobre determinado assunto.

Para este trabalho foram utilizadas as bases de pesquisa Google Scholar (site: <https://scholar.google.com.br/?hl=pt>) e Scielo (site: <https://www.scielo.org>).

Ao realizar por meio da busca avançada foram aplicados os seguintes critérios para filtrar a pesquisa: período específico entre 2019 e 2021, o idioma somente em português. Para o Google Scholar foi desmarcado as citações.

### 3 REFERENCIAL TEÓRICO

Neste capítulo serão apresentados tópicos sobre segurança da informação, vazamento de dados, a sua relação com a lei geral de proteção de dados e a necessidade da aplicação LGPD.

#### 3.1 Segurança da informação

Hintzbergen et al. (2018), define informação como um dado que possui significado no contexto de quem o recebe, passa a ser tratado como dado após ser inserido ou armazenado em um computador. Sêmola (2003, p. 9 apud FERNANDES, 2013) define Segurança da Informação como “uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade”.

Na segurança da informação qualquer coisa que tenha valor para uma empresa, desde informação, a softwares, hardwares, as pessoas e dentre outros é definido como ativos (HINTZBERGEN et al, 2018). Estes ativos são vistos como essenciais para um departamento de segurança da informação de uma organização, pois as atividades desse setor envolvem a criação, implementação, controle e monitoramento de políticas que buscam proteger esses ativos (FERNANDES, 2013).

##### 3.1.1 *Princípios Fundamentais*

A segurança da informação aborda princípios fundamentais como confidencialidade, integridade e disponibilidade como um guia para tratar os dados, esses princípios visam a proteção contra ameaças e tentativas de violações aos dados (HINTZBERGEN et al, 2018).

A confidencialidade trata dados referentes a quem pode ter essa informação, permitindo que somente pessoas autorizadas possam ter acesso. A confidencialidade também assegura que seja aplicado um nível necessário para que se tenha um sigilo dos dados, o nível deve prevalecer enquanto os dados residirem em sistemas e

dispositivos na rede quando transmitidos e quando chegarem ao seu destino (HINTZBERGEN et al, 2018).

A integridade consiste na garantia que a informação permaneceu íntegra, o que significa dizer que ela não sofreu nenhuma espécie de modificação sem autorização do autor da mensagem (MORAES, 2010).

Já a disponibilidade está relacionada aos dados estarem sempre disponíveis quando necessário, havendo continuidade no serviço mesmo em caso de falhas, existindo capacidade para permitir que toda a equipe trabalhe no sistema. (HINTZBERGEN et al, 2018), essa disponibilidade deve ser garantida por meio de mecanismos de segurança para impedir que o sistema saia do “do ar” (MORAES, 2010 p.213).

Dessa forma, violações de segurança da informação podem levar a quebra da confidencialidade, violação da privacidade dos indivíduos e a perda ou indisponibilidade dos dados. Nesse contexto, a informação se torna um ativo valioso tanto para uma pessoa como para as organizações, devendo estar protegido de acessos não autorizados (FERNANDES, 2013).

### *3.1.2 Principais problemas de Segurança*

A violação de ativos na área de segurança da informação pode trazer impactos negativos para uma Organização. Estes impactos geram problemas que podem ocorrer por diversos fatores, podendo levar a perda e/ou violação dos dados. Exemplo disso se dá quando a segurança está passando por ameaças, riscos, vulnerabilidades, dentre outros (FERNANDES, 2013).

De acordo com Hintzbergen et al. (2018 p. 28), “Uma ameaça é um potencial causa de um incidente não desejado, o que pode resultar em prejuízo ao sistema ou à organização.” Este tipo de ataque pode ser feito por agentes externos (pessoas ou empresas fora da organização) ou internos (pessoas de dentro da organização) querendo tirar vantagem das vulnerabilidades apresentadas no sistema da empresa (FERNANDES, 2013).

Já as vulnerabilidades são falhas que um sistema possui, é caracterizada pela ausência ou uma fraqueza de uma proteção que pode ser explorada por falta de um



sistema atualizado ou o ambiente em que estão localizados os computadores. (FERNANDES, 2013; HINTZBERGEN et al, 2018).

E os riscos estão atrelados aos computadores de uma rede intranet estarem conectados à internet expondo a rede da organização, riscos esses que podem ser controlados por meio de políticas de segurança interna e o uso de antivírus atualizado. (FERNANDES, 2013).

Diante disso, é visto a importância do setor de segurança da informação nas empresas para controlar, implantar e monitorar políticas de segurança para evitar falhas de segurança ocorrendo vazamento de dados.

### **3.2 Vazamento de dados**

Um vazamento de dados consiste na exposição de informações sensíveis passando a ser tratado como um incidente de segurança. Segundo Hintzbergen et al. (2018), trata-se de um evento indesejado ou inesperado que tem a probabilidade de comprometer e ameaçar a segurança da informação.

Para Martins (2018), o vazamento de dados trata de invasão, acesso indevido e roubo ou sequestro de dados pessoais de usuários, seja uma loja na internet, seja um site fornecedor de software. Dessa forma, expondo os dados dos clientes. Esses vazamentos, ainda com o autor, são causados por pessoas mal intencionadas que têm um profundo conhecimento em informática com o objetivo de lucrar com a ação criminosa invadindo sistemas vulneráveis, explorando falhas e coletando os dados ilegalmente em troca de resgate em dinheiro ou criptomoedas (moedas digitais).

Casos como os citados na introdução mostram como as pessoas ficam expostas sem o seu consentimento, violando a privacidade de quem cadastra suas informações pessoais em sites, deixando o mundo virtual inseguro, sendo necessário regulamentações para proteção de dados por parte das empresas.

Entre os principais motivos que levam ao vazamento de dados por parte das empresas e instituições está a falta de segurança no uso de credenciais (login e senha para acessar o sistema) fracas pertencentes a funcionários que são usuários, contas obsoletas que ainda permanecem ativas e senhas de usuários que nunca expiram até que ocorra um incidente de segurança (BISSO et al, 2018).

No artigo sobre vazamento de dados do autor De Castro et al. (2020), foram elencados diversos casos de vazamentos. De acordo com o autor existem plataformas online como a *Have I Been Pwned*, o *Avast Hack Check* e o *Firefox Monitor*, onde o usuário pode realizar uma consulta para verificar se o seu endereço de email e dados pessoais foram vazados.

Em vista disso, a segurança dos dados passou a ser uma preocupação para as empresas nos dias atuais, esses dados que devem ser protegidos tanto no meio físico quanto no digital se tornaram informações importantes para a venda de produtos ou serviços por parte das empresas, pois, conforme as tecnologias melhoram o acesso aos produtos que antes eram vistos só em loja física passam a ser parte do comércio eletrônico. E conforme o negócio expande a necessidade de proteger as informações dos usuários também aumentam (BABY, 2018).

### **3.3 Lei geral de proteção de dados**

Influenciada pelo Regulamento Geral de Proteção de dados da União Europeia, (RGPD) a lei Geral de Proteção de Dados Pessoais de nº 13.709/18 (LGPD), se refere ao tratamento de dados pessoais de pessoas naturais com o objetivo de proteger os direitos de liberdade e privacidade. Tendo como os principais fundamentos o respeito a privacidade, a liberdade de expressão, inviolabilidade da intimidade, da honra e da imagem, entre outros constantes na constituição federal (BRASIL, 2018).

Na Europa o RGPD em vigor desde 25 de maio de 2018, se fundamentou no princípio do consentimento, onde as empresas por meio de um responsável pelo tratamento de dados devem se adequar ao regulamento respondendo por eventuais incidentes de segurança, em seu texto o regulamento diz que para ter o direito de tratar esses dados deve existir uma declaração autorizada pelo titular dos dados de forma escrita, eletrônica ou de forma oral. Ainda no regulamento é visto que alguns dados são considerados como sensíveis como opinião política ou convicção religiosa, origem racial ou étnica dentre outros, além de proibir a troca de informações entre organizações sem o consentimento do titular dos dados (União Europeia, 2016 apud PIURCOSKY et al, 2019).

No Brasil, sobre o contexto da confidencialidade, um dos princípios da segurança da informação, o Governo Brasileiro implementou a LGPD. Apresentando

um grande avanço quando falado na regulamentação de proteção de dados pessoais, a LGPD, passa um maior controle sobre o processamento dos dados pessoais aos titulares, cobrando diversas obrigações para os controladores (a quem competem as decisões sobre o tratamento dos dados) e operadores (aqueles que tratam os dados de acordo com o estipulado pelos controladores) (SILVEIRA, 2021).

São tidos como dados pessoais toda e qualquer informação que diga respeito a algo que permite identificar o titular ou a algo que remeta diretamente a este. Essas informações vão desde o nome dos pais do titular, que é um dado que permite identificá-lo, quanto a seu próprio nome, suas impressões digitais, biometria de voz e reconhecimento da íris até documentos cujas numerações são únicas e exclusivas daquela pessoa. Tratamento de dados, de acordo com o texto da Lei Geral de Proteção de Dados, é o termo que designa todos os processos pelos quais um dado pode vir a passar desde sua coleta até seu armazenamento. Esses dados podem passar por um processamento, podem ser alterados e podem até ser movimentados entre dois pontos por meio, também, de dispositivos eletrônicos (VELHO, 2020).

Possuir dados de uma pessoa natural é possível e permitido a pessoas físicas ou jurídica e a instituições públicas ou privadas desde que se adequem às regulamentações previstas pela LGPD, uma vez que, como lei, esta determina como é e como não é permitido operar com esses dados ao longo dos trâmites julgados necessários a quem os obteve para fins comerciais. A lei tem validade em todo território nacional, sendo assim, o uso indevido desses dados, seja por divulgação não autorizada ou quaisquer outras operações inapropriadas, acarreta em uma multa de R\$50 milhões, ou de 2% do faturamento anual da pessoa jurídica que o frigiou a lei (BISSO, 2020).

Em vista disso, a LGPD estabelece diretrizes importantes e obrigatórias para a coleta, processamento e armazenamento de dados pessoais. Se dedicando a proteção das pessoas naturais contra o tratamento ilegal de dados pessoais realizados por qualquer pessoa natural ou jurídica (Cots; Oliveira, 2018).

### *3.3.1 Princípios referentes ao tratamento de dados*

De acordo com Cots e Oliveira (2018), a LGPD define princípios que devem ser observados pelas organizações na execução de atividades relacionadas ao

tratamento de dados pessoais, dentre elas estão a finalidade, a adequação, a necessidade e a transparência.

No princípio da finalidade, o tratamento de dados deve possuir um propósito legítimo e específico informando ao titular o que será feito com os dados, apresentando o resultado que será alcançado com tal tratamento. O princípio da finalidade não é definido somente para determinar o objetivo final do tratamento, mas para prever o que dele se espera, impedindo o tratamento futuro fora da finalidade original. Como por exemplo, informar que a coleta dos dados servirá para faturar um produto ou serviço e que, a organização não vai utilizar os dados coletados do titular para campanhas de marketing sem o seu consentimento (Cots; Oliveira, 2018).

O princípio da adequação visa a preservação da finalidade informada ao titular ser compatível à do tratamento, abordando o procedimento realizado para chegar ao objetivo pretendido. Exemplo de violação do princípio de adequação é visto quando é informado que os dados serão excluídos, mas a organização continua com eles (Cots; Oliveira, 2018).

Em relação ao princípio da necessidade, só devem ser tratados dados imprescindíveis para finalidade pretendida, dispensando dados desnecessários, como por exemplo, solicitar a cor da pele titular para faturamento de produtos (Cots; Oliveira, 2018).

Já o princípio da transparência estabelece a garantia de informações claras, precisas, devendo estar acessíveis ao titular em relação ao tratamento de seus dados pessoais (Cots; Oliveira, 2018).

### *3.3.2 Dos direitos do Titular*

A LGPD assegura a toda pessoa natural, a titularidade de seus dados pessoais, concedendo o direito de obter a relação de seus dados que estão sendo tratados. Diante disso, o titular dos dados pessoais passa a ter o direito de obter da organização a relação dos seus dados armazenados, podendo solicitar correções em dados incompletos ou desatualizados, bloqueio ou eliminação de dados desnecessários ou tratados em desconformidade com a legislação vigente, portabilidade dos dados com a devida aprovação, e a revogação de consentimento (BRASIL, 2018).

### 3.3.3 *Agentes de tratamento de dados pessoais*

A LGPD define três agentes que serão responsáveis pela coleta e tratamento dos dados, o primeiro deles é o controlador, sendo pessoa física ou jurídica de empresa privada ou instituição pública, o controlador fica encarregado da tomada de decisões sobre o tratamento de dados. Enquanto que o operador é responsável pelo tratamento de dados em nome do controlador. Mencionado pela lei o terceiro agente, o encarregado dos dados, atuando como guardião de dados indicado pelo operador e o controlador para atuar no relacionamento entre o controlador, o titular dos dados e a Autoridade Nacional de Proteção de Dados (ANPD) (VELHO, 2020).

É previsto pela LGPD a obrigação do controlador e do operador em manter o registro das operações de tratamento que realizarem, uma vez que a atividade compete ao princípio da finalidade. O registro deve conter dados da atividade desenvolvida, assim como data, hora, identificação da pessoa natural que participou do processo, ferramentas como sistemas e softwares serão úteis (Cots; Oliveira, 2018).

É atribuído ao encarregado dos dados a função de aceitar as reclamações dos titulares e prestar os esclarecimentos com adoção de providências, ouvir autoridade nacional adotando providências, a orientar os funcionários a respeito de práticas a serem tomadas em relação a proteção de dados pessoais e por fim, executar atribuições determinadas pelo controlador ou estabelecidas em normas complementares (Cots; Oliveira, 2018).

### 3.3.4 *Autoridade Nacional de Proteção de Dados*

A lei nº 13.709 recém alterada pela lei nº 13.853, de 18 de julho de 2019, dispendo da proteção e criando a ANPD. “A ANPD é o órgão da administração pública federal responsável por zelar pela proteção de dados pessoais e por regulamentar, implementar e fiscalizar o cumprimento da LGPD no Brasil.” (ANPD, 2021). O papel da Autoridade Nacional de Proteção de dados é “assegurar a mais ampla e correta observância da LGPD no Brasil e, nessa medida, garantir a devida proteção aos direitos fundamentais de liberdade, privacidade e livre desenvolvimento da personalidade dos indivíduos.” (ANPD, 2021).

Dentre as atribuições da ANPD estão “elaborar diretrizes, fiscalizar e aplicar sanções, promover a população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança.” (ANPD, 2021).

### 3.3.5 *Das Sanções Administrativas*

As infrações cometidas pelos agentes de tratamento de dados às normas previstas na LGPD acarretam sanções administrativas aplicadas pela ANPD. Entre as sanções estão.

Há nove possíveis consequências para o não cumprimento das exigências previstas pela LGPD, dentre elas estão uma simples advertência junto a um prazo para que os erros sejam corrigidos; uma multa simples que não ultrapassa 2% do faturamento da PJ, não podendo exceder o valor de R\$ 50.000.000,00 por infração; multa diária, respeitando o limite total contido no inciso II da LGPD; ter a infração trazida ao conhecimento do público após ter sua ocorrência ter sido investigada e confirmada; ter os dados pessoais bloqueados até que a situação esteja regularizada; ter os dados deletados; ter o banco de dados suspenso parcialmente por um período máximo de um semestre, podendo ser prorrogado por mais um semestre até que a situação seja corrigida; ser absorvido do direito do exercício da atividade de tratamento de dados pessoais por no máximo um semestre, podendo ser prorrogado por mais um semestre e ser proibido parcial ou totalmente do exercício de atividades de tratamento de dados (BRASIL, 2018).

## **3.4 A necessidade da aplicação da LGPD**

Antes da LGPD existir, no Brasil a lei em vigor de nº 12.965 de junho de 2014, conhecida como a lei do Marco Civil da Internet foi a lei que inovou diversos aspectos da regulamentação de atividades das empresas operadoras de produtos ou serviços na internet. A lei teve três fundamentos para a maneira como as empresas prestadoras de serviços na internet deveriam tratar os clientes, a neutralidade da rede, a privacidade e a fiscalização.

A neutralidade da rede consiste em proibir ações abusivas praticadas por empresas na prestação de serviço de internet, por exemplo, limitar que os clientes

acessem alguns sites ou serviços. O objetivo da lei do Marco Civil foi proporcionar igualdade entre os consumidores de acordo com suas expectativas de velocidade dos dados. A privacidade trouxe garantia inviolabilidade e sigilo das comunicações dos usuários ao provedor de internet salvo exceção de ordem judicial, já a fiscalização era o dever de fiscalizar para que as empresas de serviço de internet não infringissem essa lei tendo como punição a indenização por danos materiais ou morais (TOMASEVICIUS FILHO, 2016).

Mas a lei do Marco Civil deixava lacunas em como os dados eram tratados pelas empresas deixando brechas para venda, compartilhamento de dados, ocorrendo incidentes de segurança como vazamentos de dados pessoais citados anteriormente na introdução. Motivando dessa forma, a elaboração e implementação da LGPD.

A necessidade dessa lei se dá por se tratar de uma legislação específica para o tratamento de dados pessoais no Brasil, o cumprimento dessa lei faz com que empresas privadas e instituições públicas tornem mais transparentes a forma da coleta, armazenamento e uso dos dados pessoais dos cidadãos brasileiros além de o titular dos dados possuir o poder do consentimento, podendo solicitar exclusão de informações, se achar necessário (SILVEIRA, 2021).

## **4 RESULTADO**

Foi realizada uma busca entre os anos de 2019 e 2021, utilizando como palavras-chave, Lei geral de proteção de dados e vazamento de dados pessoais.

Na busca realizada na base da Scielo não houveram resultados. Já no Google Scholar foram encontrados vários resultados, sendo aproximadamente 2.890. Foi feita uma leitura dos títulos e os respectivos resumos dos artigos encontrados comparando se tinham relação com o tema da pesquisa. A pesquisa restringiu as primeiras 4 páginas levando em consideração o tempo para elaboração do trabalho. Dessa forma, 10 foram selecionados para uma leitura do seu conteúdo. Visando atender os objetivos dessa investigação, 3 foram selecionados como relevantes e estão explicitados abaixo.

### **4.1 A Lei geral de proteção de dados pessoais em empresas brasileiras: uma análise de múltiplos casos**

PIURCOSKY et al. (2019) teve como objetivo descrever e compreender a realidade de organizações brasileiras quanto à adequação à LGPD. Fundamentando em sua pesquisa princípios da segurança da informação como a confidencialidade, integridade e a disponibilidade dos dados como práticas de segurança para mitigar ameaças. O autor em seus resultados obtidos através da técnica científica com o estudo de casos múltiplos, notou por meio de entrevistas que alguns dos entrevistados quando perguntados sobre a LGPD não souberam do que se tratava a lei, nem tão pouco em relação aos titulares dos dados. Ao saberem que devem excluir dados de funcionários após serem demitidos, os entrevistados responderam que deixavam o usuário inativo. Os autores destacam que o Brasil deu um passo importante para a proteção e privacidade dos dados pessoais, mas as organizações devem passar por mudanças na gestão em segurança da informação.



## **4.2 LGPD (Lei geral de proteção de dados) e sua aplicabilidade no tratamento de dados no e-commerce**

BROSTEL e NEVES (2021) buscaram explicar a LGPD trazendo a contextualização do comércio eletrônico como o principal captador das informações pessoais, apresentando os principais escândalos cometidos por parte das empresas em vazamento de dados de terceiros. Em suas considerações destacou-se que a legislação brasileira sancionou projetos de lei como o Marco Civil fornecendo princípios e garantias para o uso da internet no Brasil, mas que a necessidade da criação da LGPD é um importantíssimo avanço para a proteção de dados no Brasil.

## **4.3 Lei geral de proteção de dados (LGPD): características e aplicações na biblioteconomia e ciência da informação**

Já a última pesquisa vista na base do Google Scholar, Leite (2021) abordou a LGPD em sua origem, evolução características e aplicação em ambientes na biblioteconomia e ciência da computação. Como resultado foi considerado que a LGPD trouxe grandes impactos na adaptação das instituições em geral que tratam de dados pessoais, mas trouxe aspectos positivos para a sociedade e para os profissionais da informação.

Diante disso, ainda é um desafio para as empresas se adequarem a LGPD, mas é afirmado a necessidade dessa lei por se tratar de uma legislação específica para o tratamento de dados pessoais no Brasil, fazendo com que empresas e instituições tornem mais transparentes a forma da coleta, armazenamento e uso dos dados pessoais dos cidadãos brasileiros (SILVEIRA, 2021).

O conhecimento sobre a lei é fundamental para que as Organizações adotem políticas de segurança e passem a tratar como ativos os dados pessoais protegendo as informações para não perderem credibilidade e evitarem sanções da LGPD com incidentes de segurança.

## 5 CONSIDERAÇÕES FINAIS

O vazamento de dados é uma violação de segurança que expõe informações confidenciais e sensíveis afetando a privacidade das pessoas que acessam o mundo digital. A LGPD é uma regulamentação brasileira que entrou em vigor para fiscalizar e impor regras para como as empresas e instituições tratam os dados coletados, armazenados e manipulados com o objetivo de proteger as pessoas.

Para se adequar à lei quanto ao tratamento dos dados, as empresas devem rever suas políticas de segurança da informação adotando uma gestão para tratar aspectos fundamentais como a integridade e a confidencialidade tendo em vista mitigar os riscos e vulnerabilidades para não perder sua credibilidade e evitar sanções da LGPD.

Retomando a afirmação da pesquisa para guiar o estudo “A população está protegida com a LGPD.” Essa lei é vista como um benefício para a segurança e proteção da população brasileira na internet. Entretanto, ainda é um desafio para o setor de segurança da informação das empresas se adequar à lei. Conhecer sobre a lei é fundamental tanto para as empresas quanto para a população, evitando que ambas as partes sejam prejudicadas.

Nesse sentido, recomenda-se que as empresas além de adotarem proteções para o tratamento de dados, passem a realizar treinamento de funcionários transmitindo o conhecimento sobre a LGPD. Já a população brasileira cabe tomar precauções para quem está consentindo os seus dados. Tendo em vista os benefícios que a LGPD trouxe, o direito do titular dos dados alterar, atualizar seus dados se achar necessário, podendo até solicitar a exclusão revogando o seu consentimento.

Levando em consideração o tema dessa pesquisa, limitações foram encontradas devido a vigência da LGPD ser recente. Os preceitos da LGPD que tratam de sanções administrativas somente entraram em vigor em agosto de 2021, efetivando os poderes para fiscalização e cumprimento da legislação pela ANPD.

Com o objetivo de regulamentar e fiscalizar a Lei Geral de Proteção de Dados, a ANPD aplicará multas quando for o caso e torna-se responsável pela orientação às empresas sobre a aplicação da LGPD. Portanto, como sugestão para pesquisa futura,

é interessante realizar uma análise do atual comportamento das empresas depois da LGPD.

Tendo em vista os resultados obtidos neste trabalho, pode-se concluir que o Brasil deu um passo importante para a proteção e privacidade dos dados pessoais e a atuação da LGPD sobre o tratamento dos dados deixará o ambiente digital mais seguro para as pessoas.

## 6 REFERÊNCIAS

ANPD, Autoridade Nacional de Proteção de Dados. 2021 Disponível em: <https://www.gov.br/anpd/pt-br/acesso-a-informacao/perguntas-frequentes-2013-anpd#a1> Acesso em: 29 de out. de 2021.

BABY, Aiswarya; KRISHNAN, Hema. A literature survey on data leak detection and prevention methods. **International Journal of Advanced Research in Computer Science**, Udaipur, v. 8, n. 5, maio/jun., p. 2416-2418, 2017. Disponível em: <http://www.ijarcs.info/index.php/ijarcs/article/view/3925>. Acesso em: 25 out. 2021.

BISSO, Rodrigo *et al.* Vazamentos de Dados: Histórico, Impacto Socioeconômico e as Novas Leis de Proteção de Dados. **Revista Eletrônica Argentina-Brasil de Tecnologias da Informação e da Comunicação**, v. 3, n. 1, mar. 2020. Disponível em: <https://revistas.setrem.com.br/index.php/reabtic/article/view/378/174>. Acesso em: 20 set. 2021.

BOTELHO, Marcos César. A proteção de dados pessoais enquanto direito fundamental: considerações sobre a lei geral de proteção de dados pessoais. **Argumenta Journal Law**, Jacarezinho, PR, n. 32, p. 191-207, 2020. Disponível em: <http://seer.uenp.edu.br/index.php/argumenta/article/view/1840/pdf#>. Acesso em: 18 set. 2021.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm). Acesso em: 20 de set. de 2021.

BRASIL. Lei nº 12.965, de 23 de abr. de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2014/lei/l12965.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm). Acesso em: 20 de set. de 2021

BRASIL. Lei nº 13.709, de 14 de ago. de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm). Acesso em: 29 de out. de 2021

BROSTEL, Brendow e NEVES, David Pereira LGPD (Lei geral de proteção de dados) e sua aplicabilidade no tratamento dados no e-commerce **repositorio.animaeducacao.com.br** 2021. Disponível em: <https://repositorio.animaeducacao.com.br/handle/ANIMA/13902>. Acesso em: 29 de out. de 2021.

COTS, Márcio; OLIVEIRA, Ricardo. **Lei geral de proteção de dados pessoais: cimentada**. São Paulo: Revista dos Tribunais, 2018.

DE CASTRO, Ariel Góes *et al.* Os meus dados de fato vazaram? Uma análise de serviços que monitoram vazamentos de dados na Internet. **Revista Eletrônica Argentina-Brasil de Tecnologias da Informação e da Comunicação**, Rio Grande do Sul, v. 3, n. 1, mar. 2020. Disponível em: <https://revistas.setrem.com.br/index.php/reabtic/article/view/373/169>. Acesso em: 20 de set. de 2021.

FERNANDES, Nélia O. Campo. **Segurança da informação**. Cuiabá: UFMT: IF Rondônia, 2013. Disponível em: <https://docplayer.com.br/154795856-Seguranca-da-informacao-nelia-o-campo-fernandes.html>. Acesso em: 20 set. 2021.

GERHARDT, Tatiana Engel; SILVEIRA, Denise Tolfo (Org.). **Métodos de pesquisa**. Porto Alegre: Ed. UFRGS, 2009. (Série Educação a Distância). Disponível em: [www.ufrgs.br/cursopgdr/downloadsSerie/derad005.pdf](http://www.ufrgs.br/cursopgdr/downloadsSerie/derad005.pdf). Acesso em: 22 out. 2021.

GIL, A. C. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2009.

HINTZBERGEN, Jule et al. **Fundamentos de Segurança da Informação**: com base na ISO 27001 e na ISO 27002. 3 ed. Rio de Janeiro: Brasport 2018.

LOUREIRO, Rodrigo. Cometemos alguns erros, diz CEO da Zoom sobre vazamentos de conversas. **Exame**, 6 abr. 2020. Disponível em: <https://exame.com/tecnologia/cometemos-alguns-erros-diz-ceo-da-zoom-sobre-vazamento-de-conversas/>. Acesso em: 26 set. 2021.

LEITE, Vanessa Rodrigues Lei geral de proteção de dados (lgpd): características e aplicações na biblioteconomia e ciência da informação. **repositorio.ufrn.br** 2021. Disponível em: <https://repositorio.ufrn.br/handle/123456789/41518>. Acesso em: 29 de out. de 2021.

MARTINS, Ana Paula Pereira. **Vazamento e mercantilização de dados pessoais e a fragilidade da segurança digital do consumidor**: um estudo dos casos Netshoes e Uber. 2018. Disponível em: <https://www.academia.edu/download/62362494/BRASILCON20200313-80367-3bi0io.pdf>. Acesso em: 28 out. 2021.

MEGAVAZAMENTO de dados de 223 milhões de brasileiros: o que se sabe e o que falta saber. **G1**, 28 jan. 2021. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2021/01/28/vazamento-de-dados-de-223-milhoes-de-brasileiros-o-que-se-sabe-e-o-que-falta-saber.ghtml>. Acesso em: 26 set. 2021.

MORAES, Alexandre Fernandes de. **Redes de Computadores**: fundamentos. São Paulo: Érica, 2010.

PIURCOSKY, Fabrício Pelloso *et al.* A lei geral de proteção de dados pessoais em empresas brasileiras: uma análise de múltiplos casos. **Suma de negócios**, Bogotá, v. 10, n. 23, p. 89-99, jul./dic. 2019. Disponível em:

[https://blogs.konradlorenz.edu.co/files/rsn\\_1023\\_02\\_peloso-piurcosky.pdf](https://blogs.konradlorenz.edu.co/files/rsn_1023_02_peloso-piurcosky.pdf). Acesso em: 18 set. 2021.

SILVEIRA, Suzana Aparecida. **Segurança da informação e proteção de dados pessoais**: estudo de caso e proposta de governança para serviços de saúde. 2021. 211 f. Dissertação (Mestrado profissional em inovação tecnológica) – Departamento de Ciência e Tecnologia, Universidade de São Paulo, São Paulo, 2021. Disponível em: <https://repositorio.unifesp.br/bitstream/handle/11600/60909/Defesa%20MPIT%20SUZANA%20APARECIDA%20SILVEIRA%20VERSA%cc%83O%20FINAL%20UNIFESP%20CBM.pdf?sequence=1&isAllowed=y>. Acesso em: 20 set. 2021.

VALENTE, Jonas. Brasil tem 134 milhões de usuários de internet, aponta pesquisa. **Agência Brasil**, Brasília, 26 de maio de 2020. Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2020-05/brasil-tem-134-milhoes-de-usuarios-de-internet-aponta-pesquisa> Acesso em: 29 de out. de 2021

VELHO, Raphaela. Em vigor a partir de agosto, implementação da Lei Geral de Proteção de Dados ainda enfrenta desafios. **Ciência e Cultura**, São Paulo, v. 72, n. 2, abr./jun. 2020. Disponível em: [http://cienciaecultura.bvs.br/scielo.php?script=sci\\_arttext&pid=S0009-67252020000200004](http://cienciaecultura.bvs.br/scielo.php?script=sci_arttext&pid=S0009-67252020000200004). Acesso em: 20 out. 2021.

TOMASEVICIUS FILHO, Eduardo. Marco Civil da Internet: uma lei sem conteúdo normativo. **Estudos avançados**, São Paulo, v. 30, n. 86, p. 269-285, 2016. Disponível em: <https://www.revistas.usp.br/eav/article/view/115093>. Acesso em: 22 out. 2021.

UNINCOR, Universidade Vale do Rio Verde. O que é LGPD? Você sabia que a lei começa a valer a partir de 21 de agosto? **G1**, 28 maio de 2021. Disponível em: <https://g1.globo.com/mg/sul-de-minas/especial-publicitario/unincor/universidade-unincor/noticia/2021/05/28/o-que-e-lgpd-voce-sabia-que-a-lei-comeca-a-valer-a-partir-de-21-de-agosto.ghtml>. Acesso em: 18 nov. 2021