A LEI GERAL DE PROTEÇÃO DE DADOS E SUAS REPERCUSSÕES NO E-COMMERCE DE EMPRESAS PRIVADAS

THE GENERAL LAW OF DATA PROTECTION AND ITS REPERCUSSIONS ON E-COMMERCE FOR PRIVATE COMPANIES

RESUMO: O presente estudo tem o objetivo de analisar os impactos que a Lei Geral de Proteção de Dados (Lei n° 13.709/2018) trouxe para a prática do comércio eletrônico. Tendo como base o constante avanço na área de tecnologia, bem como o aumento do consumo realizado por meio da internet, a Lei Geral de Proteção de Dados desempenhou papel fundamental na regulamentação das atividades de coleta, tratamento e armazenamento das informações que são colhidas por empresas privadas atuantes na modalidade online, com o propósito de garantir maior proteção aos usuários e aos negócios concretizados no espaço virtual. A metodologia empregada para a construção do trabalho foi a pesquisa descritiva, utilizando-se de levantamento bibliográfico a partir de legislações, artigos científicos, doutrinas, revistas e anais. Desse modo, conclui-se que a legislação de proteção de dados, ao impor que as empresas do *e-commerce* adotem princípios e procedimentos específicos no processamento de informações, salvaguarda as garantias fundamentais previstas na Constituição Federal de 1988, em especial no que concerne aos direitos à segurança, liberdade, personalidade e privacidade dos indivíduos.

PALAVRAS-CHAVES: Lei Geral de Proteção de Dados. *E-commerce*. Dados. Proteção. *Compliance*.

ABSTRACT: The present study seeks to analyze the impacts that the general law on data protection (Law No. 13,709/2018) brought to the practice of e-commerce. Based on the constant advancement in the area of technology, as the increase of consumption through the internet, the general law on data protection played a key role regulating the activities of collection, processing and storage of information that are collected by private companies operating in the online modality, with the purpose of ensuring greater protection for users and businesses done in the virtual space. The methodology used to construct this paper was descriptive research, using a bibliographic survey based on legislation, scientific articles, doctrine, journals and proceedings. Thus, we conclude that the data protection legislation, by imposing that e-commerce companies adopt specific principles and procedures when collecting information, safeguards the fundamental guarantees provided for the Federal Constitution of 1988, especially with regard to the rights to security, freedom, personality and privacy of individuals.

KEYWORDS: General Law of Data Protection. E-commerce. Data. Protection. Compliance.

1 INTRODUÇÃO

Observa-se na sociedade atual, diante dos inúmeros avanços realizados na área de tecnologia, que os dados pessoais de consumidores são constantemente disponibilizados na rede mundial de computadores, com o intuito de permitir que os usuários possam usufruir dos mais

variados tipos de serviços e produtos, oferecidos por empresas privadas a partir do *e-commerce*, tal como ocorre com a compra de peças de vestuário e insumos alimentícios, realizados por meio de aplicativos ou pela internet, o uso de bancos digitais, redes sociais, jogos eletrônicos, plataformas de *streaming* de vídeo e música, entre muitos outros bens e serviços que podem ser encontrados nas plataformas digitais.

Tendo como base essa constante troca de informações que ocorre atualmente por meio da internet, a Lei Geral de Proteção de Dados surge da necessidade de se regulamentar todas essas atividades de coleta, tratamento, armazenamento e descarte de informações que são realizadas por empresas privadas ou por órgãos públicos, seja por meio físico ou eletrônico, com o objetivo de preservar os direitos fundamentais da personalidade, privacidade e liberdade dos usuários.

Desse modo, serão analisados os impactos que a Lei Geral de Proteção de Dados causou às empresas que atuam no mercado digital, bem como as alterações necessárias para que essas instituições possam estar em consonância com a legislação de proteção de dados, e assim, evitar a aplicação das sanções provenientes do descumprimento dessa norma. Posto isso, o presente artigo expõe o seguinte problema a ser investigado: de que modo a Lei Geral de Proteção de Dados afeta o exercício das atividades que empreendem por meio do *e-commerce*?

O objetivo geral deste artigo, consiste em analisar os impactos e as alterações que a Lei Geral de Proteção de Dados acarretou na prática das empresas que operam no comércio eletrônico, ponderando as modificações internas que essas instituições precisam realizar, bem como apresentar as formas de *compliance* para que os estabelecimentos comerciais se adequem à legislação de proteção de dados.

A metodologia utilizada para a construção do presente trabalho, consiste em uma pesquisa descritiva, desenvolvida com base no levantamento bibliográfico, tendo sido executado mediante consultas em artigos científicos, anais, revistas, análise de legislações e posicionamentos doutrinários, com o propósito de identificar os efeitos jurídicos e sociais do problema apontado.

Inicialmente, será abordado no primeiro tópico a evolução histórica que levou a sociedade até o contexto atual, no qual os dados pessoais se tornaram uma mercadoria valiosa para a prática empresarial, bem como será demonstrado o desenvolvimento da legislação de

proteção de dados no ordenamento jurídico brasileiro. Neste tópico, será apresentado ainda os conceitos e princípios estabelecidos pela lei, bem como as hipóteses de exceção, na qual a coleta e o tratamento de informações não precisarão atender as exigências da Lei Geral de Proteção de Dados.

Posteriormente, o segundo tópico irá discorrer sobre o *e-commerce*, elucidando a respeito do seu surgimento, sua definição, seu papel na sociedade atual e as consequências práticas que a legislação de proteção de dados provocou na esfera do comércio eletrônico. Ademais, será analisada a prática do sequestro de dados diante do cenário do mercado virtual, e o tratamento diferenciado que deve ser destinado aos dados considerados sensíveis.

Por fim, o terceiro tópico tratará das principais modificações que as empresas que atuam no *e-commerce* necessitam realizar para se adequar e estar em *compliance* com a Lei Geral de Proteção de Dados, além de apresentar as penalidades previstas para os casos de inobservância da legislação de proteção de dados.

Em suma, demonstra-se a importância deste estudo diante da constante troca de dados que é realizada na sociedade atual, em especial no que diz respeito às informações que são coletadas de forma excessiva na internet, por meio do comércio eletrônico. Assim, a Lei Geral de Proteção de Dados desempenha um papel fundamental na regulamentação dessas atividades empresariais, que recolhem e processam informações, com o propósito de garantir total segurança aos usuários que precisam fornecer seus dados particulares para a concretização das transações comerciais.

2 CONTEXTO HISTÓRICO

A sociedade experimentou, no decorrer do desenvolvimento humano, diversas formas de organização, no qual em cada período ela possuía um elemento central responsável por conduzir a economia da época, bem como estruturar os marcos históricos.

De acordo com Bioni (2020), a primeira forma de sociedade compreendida foi a agrícola, em que a terra representava a maior fonte das riquezas, sendo o comércio fomentado principalmente através do escambo. Em seguida, tem-se a sociedade industrial, na qual as máquinas a vapor e a eletricidade protagonizaram o desenvolvimento econômico da época. Em

sequência, houve ainda a sociedade pós-industrial, que afastou a economia da produção manufatureira, sendo caracterizada pelo comércio e pela prestação de serviços.

Atualmente, está em vigor a sociedade da informação que teve seu início na década de 1970, devido aos significativos desenvolvimentos realizados na área de informática e telecomunicações. Segundo Oliveira (2019), essa comunidade está pautada pela constante transferência de dados, seja em ambiente físico ou virtual, o que impacta diretamente a prática econômico-empresarial.

Os contínuos avanços na área da tecnologia, são responsáveis pelo considerável aumento no processamento e armazenamento de dados, em especial na rede mundial de computadores. Assim, as informações, o perfil de consumo dos usuários e os dados pessoais, se tornaram produtos essenciais para fomentar a economia global, uma vez que essa nova matéria-prima permite a obtenção de um resultado satisfatório e eficaz na atuação governamental e empresarial, ante a facilidade de obtenção das informações disponibilizadas na internet. (FRAZÃO; TEPEDINO; OLIVA, 2020).

Dessa forma, com o protagonismo das informações na sociedade atual, viu-se a necessidade de efetivar uma proteção integral aos dados que são coletados e armazenados, seja por pessoas físicas, empresas privadas ou órgãos públicos, assegurando os direitos fundamentais previstos no artigo 5° da Constituição Federal de 1988, tais como a liberdade, a privacidade e a segurança.

Diante dessa necessidade, foi sancionada em 14 de agosto de 2018, a Lei n° 13.709, amplamente conhecida como a Lei Geral de Proteção de Dados (LGPD), encarregada de regulamentar toda e qualquer atividade que realize o tratamento e armazenamento de informações no território brasileiro.

É de se dizer, por outro lado, que a normatização voltada para a segurança dos dados pessoais no Brasil não teve seu início com a Lei n° 13.709/2018. Segundo Costa (2019), a legislação de proteção de dados veio para sanar um vazio normativo acerca deste tema, uma vez que existiam apenas leis setoriais que abordavam de forma superficial a proteção de dados, tais como a Lei do Cadastro Positivo, a Lei do Habeas Data, o Código de Defesa do Consumidor, entre outras.

Dentre as legislações que antecederam a LGPD, cabe destacar a Lei n° 12.527 de 2011 (Lei de Acesso à Informação) que visa regulamentar a coleta, o tratamento, o uso, e o descarte de dados, direcionada exclusivamente aos órgãos e entidades públicas, garantindo o acesso à informação nos moldes da Constituição de 1988. No entanto, tal norma não dispõe de planos expressamente direcionados à segurança de dados, constituindo apenas um embrião para o regulamento da proteção de dados pessoais. (PONTES; FIGUÊIREDO NETO, 2020).

De igual modo, importante mencionar a Lei n° 12.965 de 2014 (Marco Civil da Internet - MCI) que estabelece os princípios, deveres, direitos e garantias que regem o uso da internet e o fluxo de informações em território brasileiro, consolidando a proteção da privacidade e dos dados pessoais, que são considerados os pilares da MCI, além de garantir a liberdade de expressão, a preservação da estabilidade, segurança e funcionalidade da rede. Tratou também, de forma genérica os institutos da coleta, consentimento, tratamento e armazenamento de dados, contudo, limita-se a regulamentar apenas as informações disponibilizadas no ciberespaço. (SILVEIRA SOBRINHO, 2019).

Por sua vez, no âmbito internacional, os debates acerca da segurança direcionada aos dados pessoais teve início com a União Europeia (UE), que promulgou em 2016 a *General Data Protection Regulation* (GDPR), objetivando a proteção dos indivíduos no tratamento de informações realizadas por empresas e organizações, criando ainda, uma autoridade fiscalizadora incumbida de supervisionar a aplicação da norma. (COSTA, 2019).

A GDPR teve ainda, um papel fundamental no início da regulamentação de proteção de dados fora da União Europeia, uma vez que exigiu dos países aliados uma legislação equivalente, a fim de conservar as relações comerciais, dificultando assim, a realização de negócios com todos os países europeus. (PINHEIRO, 2020).

Portanto, observa-se que a Lei Geral de Proteção de Dados promove grandes repercussões no cenário brasileiro, no que se refere ao uso e tratamento de informações, afetando as mais diversas áreas de atuação, seja pública ou privada, sobretudo alterando o modo como as empresas manipulam os dados que estão sob seu domínio, tendo como objetivo principal garantir privacidade e proteção dos dados pessoais, e assim, resguardar os direitos e liberdades fundamentais dos usuários. (NUNES, 2019).

2.1 Conceitos concebidos pela legislação de proteção de dados

Tal como inicialmente mencionado, a Lei n° 13.709/2018 surgiu com o propósito de regulamentar todas as atividades que coletam, tratam e armazenam dados no Brasil. Nesse sentido, o referido dispositivo legal estabelece uma série de regras a serem atendidas pelas empresas que administram e utilizam quaisquer tipos de informações em seus processos, visando garantir maior segurança aos indivíduos que precisam disponibilizar seus dados pessoais. (FRAZÃO; TEPEDINO; OLIVA, 2020).

Com o intuito de auxiliar o regular cumprimento da legislação de proteção de dados, o artigo 5º da LGPD, trouxe determinados conceitos que possuem fundamental importância na compreensão e aplicação da norma, tendo por finalidade a harmonização de documentos, com enfoque especial às políticas, aos contratos e aos procedimentos. (PINHEIRO, 2020).

Assim, as terminologias estipuladas pela Lei Geral de Proteção de Dados, necessitam de estudo aprofundado a fim de corroborar com o entendimento da norma. Para tanto, serão conceituadas expressões como: a) dados pessoais; b) dados sensíveis; c) dados anonimizados; d) pseudonimização; e) banco de dados; f) transferência internacional de dados; e g) compartilhamento de dados.

Inicialmente, a LGPD faz uma distinção de conceitos, definindo como dados pessoais todas as informações relacionadas à pessoa natural, identificada ou aquela passível de identificação. Por sua vez, os dados pessoais sensíveis, são informações íntimas que possuem capacidade para ferir os direitos básicos dos indivíduos, tais como origem racial e étnica, posicionamento político, convicção religiosa, orientação sexual, entre outros que estão vinculados à uma pessoa natural, e, que podem gerar qualquer tipo de discriminação. (QUEIROZ, 2020).

Já os dados anonimizados, são informações pessoais que passaram por um processo técnico e específico, em que se torna impossível a identificação do titular, de modo que perde a possibilidade de associação aos indivíduos. Consoante a isto, o artigo 12º da LGPD dispõe que o dado anonimizado não configura como pessoal, portanto, não se aplica a presente legislação. (PONTES; FIGUÊIREDO NETO, 2020).

É de se destacar também, a informação contida no artigo 13°, § 4º da LGPD, que trata sobre a pseudonimização, que assim como a anonimização, é o tratamento direcionado a um determinado dado pessoal em que não há possibilidade de sua associação, direta ou indireta com o sujeito. Contudo, a diferença entre tais conceitos consiste no fato de que no processo de pseudonimização é possível a identificação do sujeito, através do uso de uma informação suplementar, que deverá ser mantida isoladamente, em ambiente seguro e controlado, sendo que, sobre os dados que passaram pelo processo de pseudonimização incide a aplicação da Lei Geral de Proteção de Dados.

Ademais, conceitua-se banco de dados, como o conjunto de dados estruturados, podendo estar estabelecido em apenas um único local ou distribuído em vários, independentemente de ser em meio físico ou eletrônico. (POHLMANN, 2019).

A transferência internacional de dados, consiste no deslocamento de informações pessoais realizadas entre países, ou para determinados organismos internacionais do qual o país integre, conforme dispõe o artigo 5°, inciso XV da LGPD, sendo de fundamental importância a sua previsão, tendo em vista a globalização da economia.

Por fim, o uso compartilhado de dados é estabelecido como todos os atos que proporcionam e viabilizam a distribuição de informações, tal como ocorre na transferência internacional, na relação entre informações, por intermédio da comunicação, ou pelo compartilhamento de bancos de dados por órgãos públicos ou empresas. (MACIEL, 2019).

2.1.1 Agentes de tratamento dos dados pessoais

A Lei Geral de Proteção de Dados estabelece ainda, figuras que estão essencialmente envolvidas no processamento de dados, como o titular, que é pessoa natural de quem os dados pessoais serão objeto de coleta e tratamento. Assim como, define os agentes responsáveis por processar essas informações, que são: o controlador, o operador e o encarregado.

O controlador é o agente encarregado de tutelar e recepcionar todos os dados fornecidos pelo titular, estabelecendo o primeiro contato com a informação coletada, além de tomar decisões acerca desse procedimento. Ademais, tal função pode ser ocupada tanto por

pessoa física quanto por pessoa jurídica de direito público ou privado, bem como por condomínios, sociedades de classe, entre outros. (QUEIROZ, 2020).

Por sua vez, o operador é o agente responsável por realizar qualquer tratamento de informações, agindo sob o comando do controlador, podendo ser um colaborador do estabelecimento comercial ou uma empresa terceirizada. Nas hipóteses de vazamento de informações, a LGPD prevê que tanto o controlador quanto o operador poderão ser responsabilizados, desde que não tenham cumprido com as medidas previstas na Lei Geral de Proteção de Dados. (PINHEIRO, 2020).

A norma prevê ainda, a necessidade de um encarregado pela proteção de dados pessoais dentro das empresas, que é equivalente a figura do *Data Protection Officer* (DPO) instituída pela GDPR, que será indicado pelo controlador e pelo operador, estando responsável por acompanhar as requisições e reclamações dos titulares, além de atuar como intermediador entre o controlador e o órgão regulamentador. (DONDA, 2020).

Segundo estabelece a LGPD, considera-se como tratamento de dados realizados pelos agentes, todas as operações executadas com dados pessoais, que dizem respeito a coleta, classificação, avaliação, utilização, controle, distribuição, comunicação, armazenamento, eliminação de informações, entre outros processos. (LESSA, 2020).

Além disso, o controlador será o responsável por elaborar o relatório de impacto, que poderá ser solicitado pela autoridade responsável, devendo conter a discriminação dos processos utilizados para o tratamento de dados pessoais, que podem ocasionar riscos às liberdades civis e aos direitos fundamentais, bem como deverá demonstrar quais medidas serão empregadas para mitigar tais ameaças e resguardar o titular. (LUPI; DASSAN; MEZZAROBA, 2019).

2.1.2 O consentimento do titular

O consentimento representa a base legal da autodeterminação e da livre manifestação individual, permitindo que terceiros manuseiem dados pessoais, mediante a autorização do titular ou de seu representante legal, para uma finalidade específica, devendo também esta vontade ser inequívoca e evidente para sua validade. (FRAZÃO; TEPEDINO; OLIVA, 2020).

Essa autorização será obtida no ato da coleta dos dados, devendo a empresa demonstrar de forma simples e objetiva a finalidade da concessão dessas informações. No caso de o consentimento ser manifestado por meio de instrumento contratual, será necessária a elaboração de uma cláusula distinta das outras, de modo que essa autorização não pode ser concedida de forma genérica, havendo necessidade de se detalhar a finalidade para a qual as informações foram recolhidas.

Dispensa-se a exigência do consentimento, mesmo para o uso de dados pessoais sensíveis, nas hipóteses previstas no artigo 11°, inciso II da LGPD, quais sejam: a) cumprimento de obrigação legal; b) tratamento compartilhado de dados necessários à execução de políticas públicas previstas em leis ou regulamentos; c) realização de estudos por órgão de pesquisa; d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo ou arbitral; e) proteção da vida ou da incolumidade física do titular ou de terceiro; f) tutela da saúde; ou g) garantia da prevenção à fraude e à segurança do titular.

Ademais, é possível a dispensa do consentimento, nos casos em que as informações tornaram-se expressamente públicas pelo próprio titular. Contudo, ainda deverão ser observados os princípios estabelecidos na Lei Geral de Proteção de Dados, segundo dispõe o artigo 7°, inciso X, § 4º da Lei n° 13.709/2018.

De acordo com Queiroz (2020), no que se refere ao consentimento para a coleta e o uso de dados de crianças e adolescentes, essa autorização terá que ser aprovada por pelo menos um dos pais ou pelo responsável legal, sendo que este consentimento deverá ser realizado com base no princípio do melhor interesse da criança e do adolescente.

A Lei Geral de Proteção de Dados estabelece ainda que, em algumas hipóteses, o consentimento poderá ser invalidado. Isso ocorre nos casos em que a finalidade apresentada no ato da coleta for disponibilizada de forma obscura, ou de modo que induza o titular ao erro, devendo ser demonstrado de forma clara e específica a razão pela qual tais informações estão sendo solicitadas. Ademais, haverá nulidade do consentimento quando a autorização for concedida mediante coação ou se essa requisição for realizada de modo contrário aos princípios da boa-fé exigidos pela LGPD. (QUEIROZ, 2020).

Além disso, existem outros institutos que estão ligados ao consentimento, tal como o bloqueio, que consiste na suspensão temporária de toda e qualquer operação de tratamento de

dados, impedindo o acesso a determinadas informações, decorrendo do requerimento realizado pelo titular, ou por aplicação de penalidade prevista na LGPD. Já a eliminação, constitui-se na exclusão de todo dado pessoal ou conjunto de informações que estejam armazenadas em bancos de dados, independente da forma utilizada para essa eliminação. (VILELA, 2021).

Desta forma, os conceitos concebidos pela Lei n° 13.709/2018 dizem respeito não apenas a uma área do conhecimento, posto que a Lei Geral de Proteção de Dados possui ampla abrangência, estando representados nestas terminologias diversos segmentos que apresentam grande relevância para a efetivação dessa lei. (POHLMANN, 2019).

2.2 Alterações na LGPD decorrentes da Lei n° 13.853/19

Sancionada em 08 de julho de 2019, a Lei n° 13.853 adveio da Medida Provisória n° 869/2018, com o propósito de alterar pontos significativos na legislação de proteção de dados, bem como modificar alguns artigos da lei que regulamenta o Marco Civil da Internet, desse modo, fornecendo maior completude a LGPD.

Dentre as modificações decorrentes do referido dispositivo legal, verifica-se a inclusão do parágrafo único no artigo 1° da Lei Geral de Proteção de Dados, na qual estabelece que a proteção destinada aos dados pessoais possui magnitude de caráter nacional, devendo ser observada por todos os entes da federação.

A norma proporciona ainda, a possibilidade de conciliação entre o titular e o controlador de forma direta, nas hipóteses em que ocorrerem vazamentos individuais de informações, assim como nas circunstâncias de acessos não autorizados. Nos casos em que não for possível a realização de acordo entre as partes, será aplicada ao controlador as penalidades previstas na LGPD.

Contudo, a alteração mais importante proporcionada pela Lei n° 13.853/2019, foi a criação da Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal que integra a Presidência da República, responsável por editar e fiscalizar a aplicação da Lei Geral de Proteção de Dados, possuindo caráter imprescindível para garantir a efetividade dessa legislação. (FRAZÃO; TEPEDINO; OLIVA, 2020).

A possibilidade de centralizar essa fiscalização em um único órgão, permite facilitar os avanços no implemento das novas exigências trazidas pela LGPD, tendo em vista que tal entidade foi planejada para assegurar a melhor forma de aproveitamento e cumprimento da norma, por intermédio de dispositivos complementares, pareceres técnicos e realização de inspeções, a serem executadas por uma equipe qualificada, diante da especificidade técnica do assunto, proporcionando maior estabilidade e segurança em sua aplicação. (PINHEIRO, 2020).

Dispõe ainda a Lei n° 13.853/2019, acerca da composição da ANPD, conforme consta no artigo 55-C da LGPD, que contará com um conselho diretor, encarregado de atuar como órgão máximo de direção, um conselho nacional de proteção de dados pessoais e da privacidade, composto por vinte e três representantes, sendo considerado serviço público relevante, possuindo também corregedoria, ouvidoria, um órgão para assessoramento jurídico próprio e unidades administrativas e especializadas essenciais para a aplicação da norma.

As principais funções que competem à Autoridade Nacional de Proteção de Dados, estão elencadas no artigo 55-J da Lei n° 13.709/2018, sendo as de fiscalizar e zelar pelo regular cumprimento da Lei Geral de Proteção de Dados; editar os dispositivos legais que versam acerca da proteção de dados; propiciar à população conhecimento sobre a legislação e as políticas públicas voltadas para a proteção de informações pessoais; aplicar as penalidades previstas na norma de acordo com o caso concreto, mediante instauração de processo administrativo; proporcionar a cooperação com órgãos internacionais que atuam na proteção de dados; desenvolver as diretrizes para a Política Nacional de Proteção de Dados e da Privacidade, entre outras atividades.

Ademais, acrescentou o § 5º no artigo 52 da LGPD, no qual dispõe que os valores oriundos da arrecadação de multas provenientes das sanções estabelecidas nesta lei, que deverão ser aplicadas pela ANPD, devem ser destinadas ao Fundo de Defesa dos Direitos Difusos, que possui sua previsão na Lei da Ação Civil Pública e na Lei n° 9.008/1995.

Destarte, compreende-se que a Lei n° 13.853/2019 gerou alterações fundamentais para o gerenciamento e a aplicação da Lei Geral de Proteção de Dados, abordando novos conceitos e trazendo novos institutos, como a Autoridade Nacional de Proteção de Dados, essenciais para integrar e regular a utilização da legislação de proteção de dados, garantindo também o

princípio da segurança jurídica que está implicitamente compreendido na LGPD e na Constituição Federal de 1988.

2.3 Princípios que regem a Lei Geral de Proteção de Dados

Os princípios são considerados os alicerces e a essência de uma norma jurídica, sendo utilizados também como uma das fontes para o estudo da ciência do direito, além de atuar como um modelo direcionador das leis, conforme preleciona Reale (2002, p. 299):

> [...] Princípios gerais de direito são enunciações normativas de valor genérico, que condicionam e orientam a compreensão do ordenamento jurídico, quer para a sua aplicação e integração, quer para a elaboração de novas normas. Cobrem, desse modo, tanto o campo da pesquisa pura do Direito quanto o de sua atualização prática.

Classifica-se a Lei Geral de Proteção de Dados como uma norma principiológica, uma vez que prevê em seu texto, inúmeros princípios a serem observados no tratamento dispensado às informações coletadas e processadas em território nacional. (PINHEIRO, 2020).

Assim, no artigo 6º da Lei n° 13.709/2018, é estabelecido que todas as atividades devem respeitar a boa fé e os princípios basilares do tratamento de dados, quais sejam: a) princípio da finalidade, b) princípio da adequação, c) princípio da necessidade, d) princípio do livre acesso, e) princípio da qualidade de dados, f) princípio da transparência, g) princípio da segurança, h) princípio da prevenção, i) princípio da não discriminação e j) princípio da responsabilização e prestação de contas.

Inicialmente, o artigo 6° da LGPD trata acerca do princípio da finalidade, no qual determina que no ato da coleta de dados, deverá ser informado de forma clara, explícita e justificada a intenção pela qual tais informações estão sendo solicitadas. Devendo ainda, tal finalidade possuir propósitos legítimos e específicos, estando vedada a coleta de dados para finalidades amplas e genéricas, não havendo possibilidade de tratamento posterior com objetivo incompatível ao informado no ato do colhimento.

Importante ressaltar o princípio da adequação, o qual visa estabelecer que as informações solicitadas e coletadas devem mostrar-se compatíveis com a atividade fim a que

se destina o tratamento, não sendo permitido o recolhimento de dados que não possuam o condão de auxiliar a finalidade determinada na coleta. (FINKELSTEIN, 2019).

Por sua vez, o princípio da necessidade dispõe que deverão ser coletados o mínimo de dados necessários à efetivação da finalidade pretendida, limitando a quantidade de informações a serem disponibilizadas, visando assim, evitar a coleta excessiva de dados desnecessários. (FRAZÃO; TEPEDINO; OLIVA, 2020).

A norma prevê também o princípio do livre acesso, que garante aos titulares que tiveram seus dados pessoais colhidos, a possibilidade de consultar, de forma fácil e não onerosa, todas as informações armazenadas pelas empresas, bem como a forma e o período de duração destinado ao processamento desses dados. O acesso e a confirmação de existência dessas informações, deverão ser solicitadas a critério do titular, mediante requisição, podendo a disponibilização dos dados ser realizada de forma simples e imediata, ou por intermédio de declaração completa, que informará a existência e origem da informação coletada, a utilização, o tratamento e a finalidade. (QUEIROZ, 2020).

Ademais, tem-se o princípio da qualidade de dados, que resguarda aos titulares o direito de que haja exatidão, clareza e relevância no tratamento de seus dados pessoais. Assim como, assegura a possibilidade de atualização das informações armazenadas, visando dar efetivo cumprimento à finalidade do processamento. (POHLMANN, 2019).

Em seu turno, o princípio da transparência garante aos titulares informações claras e precisas, permitindo fácil acesso no que diz respeito à realização do tratamento de dados, bem como dos respectivos agentes responsáveis por esse processamento, durante qualquer etapa, devendo ser observado o sigilo industrial e comercial. (SANTOS, Dhiulia, 2019).

Estabelece também o princípio da segurança, que determina a aplicação de medidas técnicas e administrativas, a fim de garantir efetiva proteção aos dados pessoais de ingressos não autorizados ou de situações ilícitas, assegurando a confidencialidade e inviolabilidade das informações coletadas e tratadas. (DONDA, 2020).

O princípio da prevenção, no que lhe concerne, prevê que sejam adotadas medidas que visem evitar a ocorrência de quaisquer danos oriundos do tratamento de dados, possibilitando um ambiente que minimize os prejuízos suportados pelo titular das informações processadas, através de medidas aptas de proteção contra incidentes.

Consta ainda, o princípio da não discriminação, o qual determina que o tratamento de dados, sob nenhuma hipótese, pode ser utilizado com finalidade discriminatória ilícita e abusiva, evitando que ocorra a exclusão de titulares de dados pessoais em razão de suas características particulares. (MACIEL, 2019).

Por fim, elenca-se o princípio da responsabilização e prestação de contas, em que os agentes responsáveis pelo tratamento de dados deverão comprovar todas as medidas necessárias para o efetivo cumprimento da legislação de proteção de dados, bem como demonstrar a eficácia das medidas que serão aplicadas.

Desse modo, observa-se que a Lei Geral de Proteção de Dados estabelece diversos princípios que devem ser observados por todos os órgãos e empresas que processam e armazenam dados no Brasil, impondo a realização de uma série de adaptações. Conforme aponta Natacha Santos (2019), torna-se necessária uma revisão e reestruturação de métodos e procedimentos internos, em todos os setores dos estabelecimentos comerciais, por meio de mapeamentos, relatórios de riscos, planos de ação e outros métodos, com a finalidade de adequar-se aos princípios e procedimentos previstos na LGPD.

2.4 Exceções de inaplicabilidade da legislação de proteção de dados

Conforme já elucidado, a Lei Geral de Proteção de Dados é responsável por regulamentar todas as operações que envolvem o tratamento de dados coletados em território nacional, bem como se aplica às empresas estrangeiras que disponibilizam seus bens e serviços no Brasil, independente desse tratamento ser realizado por pessoas naturais ou jurídicas, conforme estabelece o artigo 3° da LGPD.

Contudo, a Lei n° 13.709/2018 delimitou em seu artigo 4°, algumas hipóteses em que não será necessária a aplicação da legislação de proteção de dados no processamento de informações, tal como ocorre com os dados tratados por pessoa natural, desde que seja com finalidades exclusivamente particulares e não econômicas, como por exemplo os dados, fotos e correspondências de terceiros, entre outros, que decorram das relações cotidianas. (POHLMANN, 2019).

Além disso, dados coletados especificamente para fins jornalísticos ou destinados a atividades artísticas e acadêmicas, não há obrigatoriedade de observância da LGPD. Entretanto, no que se refere aos dados disponibilizados com propósitos acadêmicos, devem ser respeitados os requisitos para o tratamento dos dados pessoais e sensíveis, previstos respectivamente nos artigos 7° e 11° da Lei n° 13.709/2018. Segundo Pohlmann (2019), o intuito é evitar que ocorra a comercialização e o uso distinto da finalidade acadêmica direcionada a essas informações.

Ademais, é dispensável o cumprimento da LGPD para as situações que abarcam os interesses do Estado brasileiro, como é o caso do tratamento destinado a segurança pública, a defesa nacional, a segurança do estado ou as atividades de investigação e repressão de infrações penais, sendo que a essas hipóteses não há imposição do consentimento do titular para a utilização dos dados, devendo esse tratamento ser regido por lei específica e adequada a cada situação. (QUEIROZ, 2020).

De igual modo, o artigo 12° da Lei n° 13.709/2018, apresentou como exceção a aplicação da LGPD os dados anonimizados, que constitui toda informação que passou por um processo de anonimização, através de procedimento técnico e razoável em que não é possível realizar a identificação do titular, tal como já conceituado (item 2.1). Contudo, de acordo com Pinheiro (2020), é fundamental que ao realizar a anonimização de dados pessoais, a organização escolha um método em que não seja possível a sua reversão, a fim de evitar que ocorra eventual responsabilização.

Além disso, no tratamento de dados realizados no exterior, caso o país estrangeiro responsável pelo processamento das informações possua uma legislação voltada para a proteção de dados, o operador que estiver em território brasileiro, será eximido de providenciar o cumprimento da Lei Geral de Proteção de Dados, uma vez que o agente encarregado do processamento deverá encontrar-se de acordo com a norma de seu país. Porém, se o país estrangeiro não possuir uma lei equivalente à LGPD, esta precisará ser aplicada. (POHLMANN, 2019).

Portanto, observa-se que, embora a Lei Geral de Proteção de Dados normatize todo o processamento de dados realizados pelas empresas que atuam em território nacional ou que coletem dados no Brasil, ainda que estabelecidas em outro país, existe a previsão legal de algumas exceções em que é possível a dispensa de observância da LGPD.

3 AS CONSEQUÊNCIAS PRÁTICAS DA LEI GERAL DE PROTEÇÃO DE DADOS NO *E-COMMERCE* DE EMPRESAS PRIVADAS

A partir da criação da rede mundial de computadores, no final do século XX, bem como atrelado ao auxílio do alcance mundial proporcionado pela internet, constituiu-se uma nova forma de relação de consumo, que permitiu a expansão do comércio em todo o mundo. Desse modo, teve início o comércio eletrônico, também denominado de *e-commerce*, que pode ser compreendido como toda atividade de compra e venda, seja de produtos ou serviços, executada com recursos eletrônicos. (GARCEZ, 2020).

No que diz respeito ao *e-commerce*, ainda é possível a realização de negociação de bens materiais que possuem existência física, tal como livros, roupas, utensílios domésticos, entre outros, bem como de bens imateriais, como músicas, vídeos e programas de computador. Quanto à contratação de bens materiais, embora seja realizada por meio eletrônico, a entrega será efetuada fisicamente, em regra através de serviços postais. Por sua vez, na compra de bens imateriais, tanto a negociação quanto a entrega serão efetuadas pela via eletrônica, como ocorre com o *download* de *software*. (TEIXEIRA, 2018).

Segundo Bioni (2020), o comércio eletrônico praticado com o auxílio da internet tem proporcionado às empresas uma publicidade mais eficiente, posto que existem diversas ferramentas que possibilitam o rastreamento da navegação dos usuários, tal como os *cookies*, sendo que através deste registro de navegação é possível criar anúncios personalizados atrelados ao perfil do potencial consumidor. Assim, a publicidade realizada de forma *on-line* está associada ao material de leitura do cliente, aos *websites* visitados, bem como à informação de tudo que o indivíduo está interessado, viabilizando uma abordagem publicitária adequada à necessidade de cada pessoa.

Desse modo, compreende-se que os *cookies* são arquivos de texto que armazenam e identificam dados dos usuários que visitam determinados *websites*, sendo que a partir dele é possível armazenar informações como o nome, endereço de e-mail, páginas visitadas, entre muitas outras, que podem ser utilizados para fins de *marketing*. A coleta de tais informações se

enquadra na hipótese em que há necessidade de consentimento do titular para o tratamento desses dados, devendo ainda atender a uma finalidade definida. (DONDA, 2020).

Esse modelo de comércio realizado por meio eletrônico, apresenta grande predominância na sociedade atual, em especial por sua praticidade, uma vez que oferece maior variedade de produtos e serviços, além de possibilitar a realização de uma comparação mais eficaz nos preços das mercadorias. Contudo, as negociações empreendidas via *e-commerce* necessitam de uma cautela maior por parte das empresas e dos consumidores, posto que essa facilidade oferecida pelo comércio eletrônico, poderá também ser utilizada para a prática de violações aos direitos dos usuários. (SILVEIRA SOBRINHO, 2019).

Desse modo, verifica-se que a Lei Geral de Proteção de Dados impacta diretamente na atuação das empresas privadas que empreendem por meio do *e-commerce*, posto que a todo momento ocorre à disponibilização de dados pessoais, com o intuito de se usufruir os inúmeros serviços ofertados pelas instituições privadas estabelecidas na internet, sendo essa constante troca de dados uma característica inerente da era digital. (FRAZÃO; TEPEDINO; OLIVA, 2020).

Assim, a LGPD possui o objetivo proteger e garantir os direitos humanos fundamentais dos usuários, posto que diante da atual realidade da sociedade, verifica-se uma grande concentração de dados pessoais disponibilizados em serviços informáticos, havendo um risco muito maior de que ocorra o vazamento dessas informações armazenadas na internet, além de estarem suscetíveis a prática de crimes, tal como o sequestro de dados. (ALMEIDA, 2019).

De acordo com Willrich (2020), para que as empresas que atuam no *e-commerce* estejam em conformidade com a Lei Geral de Proteção de Dados, será necessário garantir a proteção dos usuários no tratamento das informações coletadas, observando ainda a forma de processamento destinada aos dados sensíveis, atendendo aos princípios trazidos pela LGPD, bem como realizando a adequação dos processos de governança corporativa e promovendo a adoção de programas de *compliance*. Desse modo, será possível evitar a aplicação das penalidades destinadas às instituições que violarem a Lei n° 13.709/2018, além de garantir o cumprimento da legislação de proteção de dados.

3.1 O sequestro de dados e o *e-commerce*

Constata-se, uma vez que o *e-commerce* ocorre exclusivamente em ambiente virtual, que ocorre diariamente a coleta de demasiadas informações, tal como nome, endereço, dados bancários e de cartões de crédito, entre muitas outras, para a execução de atividades que têm migrado para o meio eletrônico. Destaca-se entre essas práticas o mercado virtual, caracterizado pela compra e venda de produtos ou serviços através da internet, smartphones e aplicativos. Consequentemente, essa excessiva exposição dos usuários no ciberespaço, acaba por torná-los vulneráveis à prática de diversos crimes, em especial o roubo e o sequestro de dados, sendo as empresas privadas uma das principais vítimas. (MENDONÇA, 2020).

A prática do sequestro de dados, também conhecida como *ransomware*, tem sido um dos principais cibercrimes cometidos na atualidade, consistindo no ato de instalar no equipamento da vítima um tipo de código, responsável por criptografar todas as informações presentes no aparelho, impedindo o seu acesso. Verifica-se que, na maior parte dos casos, os criminosos pretendem solicitar dinheiro em troca do resgate dessas informações sequestradas, e, após o pagamento, encaminham à vítima uma chave que permite a remoção da criptografia, possibilitando que haja novamente o acesso aos dados. (MACÊDO, 2020).

Acerca do presente tema, explanam Silva e Teixeira (2019) que o sequestro de dados é resultado dos avanços tecnológicos, sendo potencializado pelo amplo uso da internet na sociedade atual. Asseveram ainda que, embora haja no Brasil algumas previsões legislativas que abordam de forma superficial essa prática, como a Lei n° 12.737/2012, popularmente conhecida como a Lei Carolina Dieckmann, a Lei Geral de Proteção de Dados e até o próprio Código Penal Brasileiro, não há nenhuma legislação nacional que prevê especificamente o combate e a prevenção a prática do *ransomware*.

3. 2 O tratamento de dados sensíveis no comércio eletrônico

De acordo com Mendonça (2020), a tecnologia tem sido cada vez mais presente no cotidiano da coletividade, no qual diversas esferas da vivência humana deslocaram-se para o

ambiente virtual. Contudo, tal modernização tem tornado os dispositivos e sistemas de informática consideravelmente mais vulneráveis, correndo o risco de expor os usuários e consumidores a práticas de crimes, vazamentos de informações particulares e discriminação, por meio dos dados pessoais sensíveis que são armazenados no ciberespaço.

Desse modo, uma vez que as empresas operantes no *e-commerce* se encontram principalmente na internet, sendo os produtos e serviços ofertados por meio de *websites*, essas organizações estão mais suscetíveis ao vazamento e roubo de informações. Assim, as empresas que atuam no mercado digital devem garantir aos clientes que as informações colhidas, em especial as sensíveis, serão tratadas e armazenadas de forma segura. (SARLET; RUARO, 2021).

Conforme disposto no artigo 5°, inciso II da Lei n° 13.709 de 2018, bem como definido alhures (item 2.1), os dados pessoais sensíveis são aqueles que se relacionam diretamente com as características da personalidade e opiniões pessoais dos indivíduos, necessitando de um sigilo maior que as demais informações no seu processamento, posto que se esses dados forem utilizados em desfavor do titular, poderá acarretar danos severos a sua pessoa, bem como a sua integridade, podendo ameaçar seus direitos e liberdades fundamentais. (QUEIROZ, 2020).

Segundo Mulholland (2018), a LGPD apresentou um conceito ampliado acerca dos dados considerados sensíveis, embora, sua definição e tratamento no ordenamento jurídico brasileiro já fosse conhecido a partir da promulgação da Lei n° 12.414 de 2011 (Lei do Cadastro Positivo), que prevê em seu artigo 3°, § 3º, inciso II, a proibição de anotação em bancos de dados de informações personalíssimas que não estejam ligadas a finalidade pretendida.

Assim, a Lei Geral de Proteção de Dados estipula em seu Capítulo II, Seção II, uma forma de tratamento diferenciado que deve ser direcionado aos dados apontados como sensíveis. Inicialmente, o artigo 11° da Lei n° 13.709/2018 prevê que o tratamento de dados sensíveis apenas poderá ser realizado mediante o consentimento do titular das informações pessoais ou de seu responsável legal, de modo específico e destacado, devendo possuir uma finalidade determinada. Existem ainda, algumas hipóteses em que é possível a dispensa desse consentimento para o tratamento de dados sensíveis, conforme os casos já mencionados (item 2.1.2), estabelecidos no artigo 11°, inciso II da LGPD.

Ademais, de acordo com o artigo 11°, § 3º da Lei n° 13.709/2018 poderá ser vedada a comunicação ou o uso compartilhado de dados sensíveis entre os agentes controladores, que visem a obtenção de proveito econômico a partir das informações coletadas.

Segundo o artigo 13° da Lei Geral de Proteção de Dados, é permitida a disponibilização de dados pessoais sensíveis aos órgãos de pesquisa para a elaboração de estudos na área da saúde pública, desde que essas informações sejam processadas exclusivamente dentro do próprio órgão e com única finalidade de estudo e pesquisa. Devendo ainda, ser realizada em ambiente seguro e controlado, garantindo, sempre que possível, a anonimização ou pseudonimização dos dados coletados.

De acordo com Queiroz (2020), os dados que se referem a crianças e adolescentes não foram tratados pela LGPD como sensíveis. Contudo, deve-se respeitar a sensibilidade de tais informações, sempre observando o princípio do melhor interesse da criança e do adolescente.

Deste modo, a Lei Geral de Proteção de Dados regulamentou que as empresas que recolhem informações pessoais de clientes, seja por meio físico ou digital, devem dispor de um tratamento diferenciado a ser aplicado aos dados sensíveis, devido a sua capacidade lesiva em caso de processamento inadequado dessas informações, tendo o propósito de evitar a ocorrência de tratamento discriminatório e de segregação dos titulares, em atenção ao princípio da não discriminação trazido pela LGPD. (MULHOLLAND, 2018).

4 PRINCIPAIS MODIFICAÇÕES

Verifica-se, que a Lei Geral de Proteção de Dados ocasionou grandes mudanças no ordenamento cultural das empresas, que precisaram começar a se preocupar com a política de dados, assegurando o uso e o tratamento adequado das informações coletadas, uma vez que a LGPD estabelece valores e padrões éticos, a fim de que haja segurança e responsabilidade por parte das organizações privadas no processamento de dados. (PONTES; FIGUÊIREDO NETO, 2020).

Conforme expõe Bioni (2020), embora a organização da sociedade atual esteja pautada na contínua transferência de dados, ela não está restrita às informações dispostas no meio

ambiente virtual, na internet, ou nos meios eletrônicos de comunicação e consumo, embora, estes apresentem-se como ferramentas de destaque nesse processo de uso e tratamento de dados.

No que tange ao comércio eletrônico, tendo em vista o constante avanço tecnológico, existe uma enorme necessidade de se regulamentar os processos de tratamento de dados, em face das diversas ferramentas de coleta de informação, como os *cookies*, que permitem o rastreamento da navegação dos usuários e assim relacionar os anúncios aos interesses particulares de cada indivíduo, proporcionando uma publicidade direcionada, que possui papel fundamental no fomento da economia atual. (BIONI, 2020).

Inicialmente, dentre as principais modificações que as empresas que atuam no mercado digital precisaram executar em seus processos internos, foi a realização de um mapeamento, com o objetivo de analisar toda a cadeia de dados que transitam dentro da organização, contendo todas as informações que estão sob o domínio da empresa, além de demonstrar a utilidade e a finalidade para o qual esses dados foram captados, permitindo assim a identificação dos riscos a que o estabelecimento está submetido. (JESUS, 2021).

Deverá ainda, na fase de mapeamento ser observado o ciclo de vida que os dados percorrem dentro das organizações empresariais. Segundo Pinheiro (2020), esse ciclo consiste na coleta, uso, compartilhamento, enriquecimento, armazenamento nacional ou internacional, havendo ou não a utilização de nuvem, eliminação e portabilidade.

Ademais, o relatório de impacto também auxilia nessa etapa de mapeamento dos dados, uma vez que constitui-se como o documento elaborado exclusivamente pelo controlador, que abrange as atividades de tratamento de dados pessoais que possam ocasionar qualquer tipo de prejuízo aos direitos fundamentais e as liberdades civis dos usuários, devendo também conter as medidas que possibilitem a mitigação desses riscos, conforme outrora mencionado (item 2.1.1). (MACIEL, 2019).

Posteriormente, será necessário definir a forma em que os dados coletados serão tratados por cada departamento da empresa, conforme suas necessidades específicas e de modo que esse processamento possa atenuar os riscos decorrentes da atividade comercial, assim, poderá ser realizada a correção dos problemas de segurança encontrados. Destarte, deverá ser providenciada a revisão dos termos de uso e políticas de privacidade da instituição, a fim de atender a legislação de proteção de dados (POHLMANN, 2019).

Segundo Almeida (2019), os termos de uso são os contratos realizados no meio digital, entre os usuários e os sites disponibilizados na internet, devendo constar no presente instrumento a previsão das condições em que o indivíduo está concordando em aderir, possuindo natureza de contrato de adesão, uma vez que não é possível a alteração do conteúdo contratual.

Em sequência, terá que se estabelecer um plano de recuperação para o caso de acidentes envolvendo os dados armazenados pelas empresas que atuam no mercado digital. De acordo com Donda (2020), esse planejamento tem por objetivo evitar que situações imprevistas afetem as operações das empresas, tal como ocorre em ataques de *hackers*, roubos e vazamentos de dados, que acabam por interromper o funcionamento do *e-commerce*.

Por fim, como uma das principais alterações decorrentes da legislação de proteção de dados, as empresas que atuam no meio eletrônico precisam gerenciar o término do tratamento das informações recolhidas, que se dará nos moldes do artigo 16° da Lei n° 13.709/2018, no qual dispõe que ao encerrar as atividades de processamento, os dados pessoais deverão ser excluídos, sendo resguardada a conservação das informações para o cumprimento de obrigação legal do controlador, estudos por órgãos de pesquisa, transferência a terceiros e o uso exclusivo do controlador, desde que os dados estejam anonimizados.

Além disso, considera-se terminado o tratamento nas hipóteses do artigo 15° da LGPD, quais sejam: a) a constatação de que a finalidade foi alcançada; b) o fim do período de processamento; c) por revogação do consentimento por parte do titular; e d) por determinação da ANPD em casos de violação a Lei Geral de Proteção de Dados.

Desse modo, conclui-se que a LGPD causou grandes repercussões na atuação empresarial, em especial nas organizações que exercem suas atividades em ambiente digital, como ocorre no *e-commerce*. Contudo, a aplicação dessas medidas é fundamental para que haja a garantia de um tratamento de dados seguro e transparente, assegurando os direitos fundamentais dos titulares. Além disso, uma vez que a instituição estiver em *compliance* com a Lei Geral de Proteção de Dados, poderá evitar a aplicação das sanções previstas para os casos de descumprimento dessa norma.

4.1 Penalidades provenientes do descumprimento da legislação de proteção de dados

Com relação às sanções previstas para os casos de inobservância da Lei Geral de Proteção de Dados, tais punições serão aplicadas somente após a instauração de procedimento administrativo, sempre proporcionando o exercício da ampla defesa, de modo gradativo, isolado ou cumulativo, observando as peculiaridades de cada caso, de acordo com o disposto no artigo 52, § 1º da LGPD.

Segundo Vilela (2021), existem duas formas de penalidades no tocante à proteção de dados previstas na Lei n° 13.709/2018, sendo elas a responsabilidade administrativa e a responsabilidade civil, na segunda hipótese será promovido o ressarcimento dos danos causados, por meio do poder judiciário.

Estabelece o artigo 52 da LGPD, as sanções administrativas que deverão ser aplicadas pela autoridade nacional aos agentes de tratamentos, em virtude das infrações cometidas contra as normas previstas na legislação de proteção de dados.

As penalidades administrativas previstas na LGPD são: a) advertências; b) multa simples; c) multa diária; d) publicização da infração; e) bloqueio dos dados pessoais a que se refere a violação, até a sua regularização; f) eliminação dos dados pessoais a que se refere o descumprimento; g) suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; h) suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; e i) proibição parcial ou total do exercício de atividades relacionadas ao tratamento de dados.

Existem ainda, alguns parâmetros e critérios definidos no § 1º, do artigo 52° da LGPD, para a execução de tais sanções, sendo eles: a gravidade e a natureza das infrações e dos direitos pessoais afetados; a boa-fé do infrator; a vantagem auferida ou pretendida pelo infringente; a condição econômica do transgressor; a reincidência; o grau do dano; a cooperação do violador; a demonstração de adoção de mecanismos e procedimentos internos capazes de minimizar os danos; a adoção de política de boas práticas e governança; a adoção de medidas corretivas; e a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

Ademais, a Lei Geral de Proteção de Dados garante aos titulares das informações a possibilidade de defesa de seus interesses através do poder judiciário, de forma individual ou coletiva, segundo dispõe o artigo 22° da LGPD. Para o direito, a responsabilidade civil é a obrigação de assumir as consequências jurídicas de um fato, promovendo a reparação dos danos causados, possuindo previsão no Código Civil Brasileiro. (GAGLIANO; PAMPLONA FILHO, 2019).

Destarte, o artigo 42 da LGPD, permite que o controlador ou o operador, em virtude de suas atribuições de tratamento de dados, repare o prejuízo material, moral, individual ou coletivo que causar ao titular pelo descumprimento da legislação de proteção de dados, respondendo de forma solidária, os agentes envolvidos no processamento que resultou no dano.

Contudo, poderá deixar de ocorrer a responsabilização nas hipóteses em que o agente efetivamente provar que não realizou o tratamento que incorreu em lesão ao indivíduo; quando, apesar de ter realizado o processamento dos dados pessoais, não descumpriu a LGPD; ou se comprovar que o dano decorreu por culpa exclusiva do titular ou de terceiros, segundo dispõe o art. 43 da Lei n° 13.709/2018.

O tratamento dos dados será considerado irregular, devendo ocorrer a responsabilização civil, nos moldes do artigo 44° da LGPD, quando deixar de cumprir a legislação de proteção de dados ou quando não houver o fornecimento da segurança que o titular pode esperar do estabelecimento.

Dessa maneira, as penalidades estabelecidas na Lei Geral de Proteção de Proteção de Dados possuem o intuito de submeter as empresas a estarem em *compliance* com a referida legislação e a realizarem a implementação das medidas nela prevista, posto que se a instituição estiver em conformidade com a LGPD, poderá evitar a aplicação de tais punições, bem como irá valorizar a sua reputação e garantir a confiança de seus consumidores, o que proporcionará maiores oportunidades no mercado, em especial no *e-commerce* que possui um alto fluxo de clientes e informações. (MACIEL, 2019).

4.2 *Compliance* na LGPD

O *compliance* pode ser definido como o conjunto de ações implementadas em ambientes corporativos, a fim de garantir a conformidade da atuação empresarial com as leis vigentes, de forma que venha a prevenir o eventual cometimento de infrações ou no caso de sua consumação, promover o retorno à regularidade junto a norma. (FRAZÃO, 2017).

Desse modo, compreende-se que o *compliance* na LGPD determina que as instituições privadas, incluindo o comércio eletrônico, operem em conformidade com a legislação de proteção de dados, atuando assim como um guia para direcionar a atividade empresarial, mitigando os riscos da organização e evitando a aplicação de penalidades pelo seu descumprimento. (SANTOS, Viviane, 2019).

Segundo expõe Willrich (2020), para que as empresas de *e-commerce* estejam em conformidade com a Lei Geral de Proteção de Dados, é fundamental que as organizações realizem a coleta e o tratamento de informações pessoais dos clientes de forma adequada com a norma, a fim de proteger seus usuários, bem como deverá atender aos princípios que regulamentam a LGPD, conforme já apresentado neste trabalho (item 2.3).

De acordo com Jesus (2021), a Lei Geral de Proteção de Dados determina a implantação de programas de *compliance*, atribuindo-lhes o nome de programas de governança em privacidade, estabelecidos nos artigos 50° e 51° da LGPD.

Assim, conforme prevê a legislação de proteção de dados, os controladores e operadores poderão criar normas de boas práticas e de governança, determinando as circunstâncias de sua organização; os procedimentos; o regime de funcionamento; as normas de segurança; as ações educativas; os padrões técnicos; as obrigações distintas para os envolvidos no tratamento; os mecanismos internos para mitigação e supervisão de riscos, além de outras questões pertinentes ao tratamento de dados pessoais.

Segundo o artigo 50°, § 2°, inciso I da Lei n° 13.709/2018, deverá ser implantado programa de governança em privacidade que pelo menos: a) demonstre o engajamento do controlador em adotar políticas internas que assegurem o cumprimento da LGPD; b) que possa ser aplicado a todos os dados que estejam sob seu controle; c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados; d) estabeleça

políticas, tendo por base processos de avaliação de impactos e risco a privacidade; e) possua o propósito de estabelecer relação de confiança com o titular; f) estabeleça e aplique em sua estrutura de governança mecanismos de supervisão internos e externos; g) detenha planos para resposta imediata a acidentes e sua remediação; ou h) atualizações contínuas baseadas em informações provenientes do monitoramento constante e de avaliações periódicas.

Ademais, registra-se que ao desenvolver um programa de *compliance* deverá ser observado as particularidades de cada empresa, inexistindo um método universal que seja aplicável a todas as especificidades das organizações. Dessa maneira, para que haja um *compliance* realmente eficaz, é fundamental que ocorra o reconhecimento dos principais riscos a que as empresas estão sujeitas ao realizarem o tratamento de dados, a fim de ser elaborado um plano de reparação de eventuais danos. (NUNES, 2019).

Contudo, segundo Frazão, Tepedino e Oliva (2020) existem alguns requisitos mínimos que devem ser adotados para que as instituições privadas estruturem seus programas de *compliance*, garantindo assim a sua efetividade. Por conseguinte, deverá ser realizada a avaliação contínua dos riscos e a atualização do programa, através dos relatórios de impactos elaborados pelo controlador, contendo os processos de tratamento que poderão ocasionar risco aos direitos fundamentais dos usuários, bem como abranger as medidas para mitigação desse dano.

Deverá ainda serem elaborados códigos de ética e conduta, estabelecendo os valores e princípios da organização, orientando as condutas que serão aceitas ou vedadas, instituindo ainda deveres de forma clara e objetiva. Terá que ser implantada também, uma organização com procedimentos internos compatíveis com a avaliação dos riscos, e a forma de suporte necessário para atender a esses danos. Ademais, o comprometimento e envolvimento da alta administração durante a execução é fundamental para o sucesso do *compliance*. (FRAZÃO; TEPEDINO; OLIVA, 2020).

Além disso, o setor de *compliance* dentro das empresas necessita de independência e autonomia, a fim de ser realizada a implantação das políticas, controles e procedimentos adequados, incluindo a tomada de decisões sem a necessidade de consultar as demais áreas. O treinamento periódico dos funcionários envolvidos no tratamento de dados, bem como a criação de uma cultura corporativa que propicie o respeito à ética e as leis, também contribuem para a

efetiva conformidade da instituição privada com a LGPD. (FRAZÃO; TEPEDINO; OLIVA, 2020).

Por fim, Frazão, Tepedino e Oliva (2020) estabelecem como requisitos mínimos para se atingir um processo de *compliance* eficaz, o monitoramento constante dos controles e processos, sendo que o resultado dessa monitoração será utilizada para a atualização do programa, quando necessário, sendo preciso também a instauração de um canal de comunicação de infrações, seguro e aberto, e a apuração e punição das atividades contrárias ao processo de *compliance* instituto pela empresa.

Portanto, tendo em vista que a atual economia está profundamente voltada para a coleta e o tratamento de dados, a partir da aprovação da LGPD as empresas do *e-commerce* precisaram passar por modificações em todo o seu processo de tratamento, arrecadação e utilização de informações pessoais, garantindo proteção não apenas ao titular, mas também a toda estrutura em que os dados estão envolvidos dentro do estabelecimento, devendo serem adotados métodos eficazes e condizentes com a realidade de cada organização, e sempre que possível de prevenção, para que as instituições estejam em *compliance* com a legislação de proteção de dados. (NUNES, 2019).

5 CONSIDERAÇÕES FINAIS

Com base no exposto, verifica-se que a Lei Geral de Proteção de Dados atua de modo essencial na normatização do comércio realizado por meio eletrônico, uma vez que impõe a todas as empresas que exercem atividades de coleta, armazenamento e tratamento de dados em território nacional, a necessidade de adequar-se aos procedimentos e princípios estabelecidos na LGPD, garantindo segurança e respeito a todos os indivíduos que precisam autorizar o uso de seus dados pessoais para terem acesso a determinados produtos e serviços.

Portanto, verifica-se que a Lei n° 13.709/2018 modificou profundamente o fluxo de tratamento de dados realizado dentro das empresas do *e-commerce*, conforme analisado no decorrer do presente artigo. Dessa forma, as instituições privadas que atuam no mercado digital precisam adotar medidas de identificação e prevenção de riscos, como o sequestro e o vazamentos de informações, bem como precisam efetuar a coleta do mínimo de dados

necessários para a concretização do negócio, além de ser necessária a obtenção do consentimento do usuário para o tratamento dos dados colhidos.

Contudo, o método mais eficaz para que essas empresas estejam em conformidade com a legislação de proteção de dados é executar a implantação de programas de *compliance*, que atuam de forma preventiva e possuem o objetivo de garantir a observância da LGPD. A instituição desses programas prevê a realização de uma avaliação constante dos riscos decorrentes da atividade comercial, o que permite o aprimoramento dos programas de segurança utilizados. Devendo ainda, serem elaborados códigos de ética e conduta responsáveis por nortear todo o tratamento de dados realizados pelos funcionários da instituição.

Por conseguinte, segundo Costa (2019) o impacto da legislação de proteção de dados será ainda maior para os pequenos empresários, posto que os custos para a implantação dos programas de *compliance*, bem como para a adequação dos processos internos, são bastante elevados, de modo que essas empresas menores não possuem recursos suficientes e enfrentaram maiores dificuldades para se adequarem a LGPD.

Desse modo, conclui-se que a Lei Geral de Proteção de Dados ocasionou significativas alterações nas relações cotidianas entre os usuários e as empresas atuantes no *e-commerce*, exigindo a efetivação da segurança dos dados pessoais recolhidos e tratados, uma vez que essa proteção está essencialmente ligada a tutela da dignidade da pessoa humana. Sendo crucial também, para assegurar os direitos fundamentais de liberdade e privacidade dos titulares, evitando a discriminação e a utilização ilícita das informações coletadas por empresas que operam no mercado eletrônico.

REFERÊNCIAS

ALMEIDA, Daniel Evangelista Vasconcelos. **Shadow profiles e a privacidade na internet: a coleta de dados pessoais de usuários e não usuários das redes sociais**. Porto Alegre: Editora Fi, 2019.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 2. ed. Rio de Janeiro: Forense, 2020.

BLUM, Renato Opice *et al*. **Proteção de dados: desafios e soluções na adequação à lei**. Rio de Janeiro: Forense, 2020.

BRASIL. **Constituição da República Federativa do Brasil**, de 5 de outubro de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 16/09/2021.

BRASIL. **Lei n° 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 27/09/2021.

BRASIL. **Lei n° 12.414, de 09 de junho de 2011. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 27/09/2021.

BRASIL. **Lei n° 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 06/05/2021.

BRASIL. **Lei n° 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 30/09/2021.

BRASIL. **Lei n° 12.965, de 23 de abril 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. Acesso em: 06/05/2021.

BRASIL. **Lei n° 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. Acesso em: 06/05/2021.

BRASIL. **Lei n° 13.853, de 8 de julho de 2019**. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art1. Acesso em: 06/05/2021.

COSTA, Leonardo Portugal da. **A construção da lei geral de proteção de dados e seus efeitos para o pequeno empresário e para o cidadão**. 23 f. Trabalho de Conclusão de Curso (Graduação em Sistemas de Informação)-Universidade Federal Fluminense, Niterói, 2019. Disponível em: https://app.uff.br/riuff/handle/1/13068?mode=full. Acesso em: 30/09/2021.

DONDA, Daniel. **Guia prático de implementação da LGPD: tudo que sua empresa precisa saber para estar em conformidade.** São Paulo: Labrador, 2020. Edição kindle.

FARIA. Luiz Antônio de. **Guia para trabalhos acadêmicos**. Aparecida de Goiânia: Editora Alfredo Nasser, 2017.

FINKELSTEIN, Cláudio; FINKELSTEIN, Maria Eugênia. **Privacidade e lei geral de proteção de dados pessoais**. Revista de Direito Brasileira, Florianópolis, vol. 23, ano 9, p. 284-301, 2019. Disponível em: https://indexlaw.org/index.php/rdb/article/view/5343. Acesso em: 03/09/2021.

FRAZÃO, Ana. **Programas de compliance e critérios de responsabilização de pessoas jurídicas por ilícitos administrativos.** In: ROSSETTI, Maristela Abla; PITTA, André Grunspun. (Coord.). Governança corporativa: avanços e retrocessos. São Paulo: Quartier Latin, 2017.

FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. (Coords.). **Lei geral de proteção de dados e suas repercussões no direito brasileiro**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

GAGLIANO, Pablo Stolze; PAMPLONA FILHO, Rodolfo. **Novo curso de direito civil**, v. 3: responsabilidade civil. 17. ed. São Paulo: Saraiva Educação, 2019.

GARCEZ, Pedro Rodrigues. **Direito digital no *e-commerce:* o consumidor brasileiro e a nova lei de proteção de dados.** 61 f. Trabalho de Conclusão de Curso (Graduação em Direito)-Universidade Evangélica de Goiás, Anápolis, 2020. Disponível em: http://repositorio.aee.edu.br/handle/aee/16827. Acesso em: 16/09/2021.

JESUS, Johnatan Douglas Andrade de. **A nova realidade do tratamento e da proteção de dados dos trabalhadores frente a LGPD e o *compliance* jurídico**. 50 f. Trabalho de Conclusão de Curso (Graduação em Direito)-Universidade de Sergipe, São Cristóvão, 2021. Disponível em: https://ri.ufs.br/handle/riufs/14531. Acesso em: 28/09/2021.

LAKATOS. Eva Maria; MARCONI, Marina de Andrade. **Fundamentos de metodologia científica**. 5. ed. São Paulo: Atlas, 2003.

LESSA, Alexandre Pereira. **Proteção de dados pessoais: um plano viável de adequação da governança de dados à LGPD em empresas de pequeno porte.** 37 f. Trabalho de Conclusão de Curso (Tecnólogo em Gestão da Tecnologia da Informação)-Universidade do Sul de Santa Catarina, Palhoça, 2020. Disponível em: https://repositorio.animaeducacao.com.br/handle/ANIMA/16204. Acesso em: 03/09/2021.

LUPI, André Lipp Pinto Bastos; DASSAN, Lucas Amaral; MEZZAROBA, Orides. **Lei geral de proteção de dados: impactos normativos no direito empresarial.** Revista Relações Internacionais do Mundo Atual, Curitiba, v. 2, n. 23, p. 272-288, 2019. Disponível em: http://revista.unicuritiba.edu.br/index.php/RIMA/article/view/3899/371372231. Acesso em: 01/05/2021.

MACÊDO, Luiz Fernando Belizário. **Cibercrimes: a internet como ferramenta na execução de crimes virtuais e o combate realizado pelo direito penal brasileiro**. 41 f. Trabalho de Conclusão de Curso (Graduação em Direito)-Faculdade Evangélica de Rubiataba, Rubiataba, 2020. Disponível em: http://45.4.96.19/handle/aee/17848. Acesso em: 29/09/2021.

MACIEL, Rafael Fernandes. **Manual prático sobre a lei geral de proteção de dados pessoais (Lei n° 13.709/18).** Goiânia: RM Digital Education, 2019.

MACHADO, Humberto César; PIETRAFESA, José Paulo. **Guia prático para trabalhos acadêmicos, monográficos e TCCs.** Aparecida de Goiânia: Editora Alfredo Nasser, 2014.

MENDONÇA, Júlia Fernandes de. **A responsabilidade civil e penal dos envolvidos em sequestros digitais em face da legislação brasileira de proteção de dados**. Revista do CEPEJ, Salvador, v. 22, p. 156-173, 2020. Disponível em: https://periodicos.ufba.br/index.php/CEPEJ/article/view/38329. Acesso em: 29/09/2021.

MULHOLLAND, Caitlin Sampaio. **Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18)**. Revista de Direitos e Garantias Fundamentais, Vitória, v. 19, n. 3, p. 159-180, 2018. Disponível em: https://doi.org/10.18759/rdgf.v19i3.1603. Acesso em: 26/09/2021.

NUNES, Gabriela Victória Miranda. **Governança e boas práticas na lei geral de proteção de dados pessoais: dos programas de *compliance***. 67 f. Trabalho de Conclusão de Curso (Graduação em Direito)-Universidade de Brasília, Brasília, 2019. Disponível em: https://bdm.unb.br/handle/10483/25080. Acesso em: 28/09/2021.

OLIVEIRA, Ana Paula de *et al*. **A lei geral de proteção de dados brasileira na prática empresarial.** Revista Jurídica da Escola Superior de Advocacia da OAB-PR. Curitiba, ano 4, n. 1, p. 172-200, 2019. Disponível em: http://revistajuridica.esa.oabpr.org.br/wp-content/uploads/2019/05/revista-esa-9.pdf. Acesso em: 10/05/2021.

PACHECO, Áurea Vaz. **Tutela da personalidade na lei geral de proteção de dados: os mecanismos legais de controle.** 26 f. Trabalho de Conclusão de Curso (Graduação em Direito)-Faculdade de Ciências Jurídicas e Sociais, Centro Universitário de Brasília, Brasília, 2019. Disponível em: https://repositorio.uniceub.br/jspui/handle/prefix/13795. Acesso em: 03/09/2021.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD).** 2. ed. São Paulo: Saraiva Educação, 2020.

POHLMANN, Sérgio Antônio. **LGPD ninja: entendendo e implementando a lei geral de proteção de dados nas empresas.** Rio de Janeiro: Fross, 2019. Edição kindle.

PONTES, Mayanne; FIGUÊIREDO NETO, Pedro Camilo de. (Orgs.). **Lei geral de proteção de dados: novos paradigmas do direito no Brasil.** Salvador: Mente Aberta, 2020. Edição kindle.

QUEIROZ, Isabel Cristina Arriel de. **Lei geral de proteção de dados: saiba como tudo vai funcionar.** São Paulo: Etheria, 2020. Edição kindle.

REALE, Miguel. **Lições Preliminares de Direito**. 27. ed. São Paulo: Saraiva, 2002.

SANTI, Leandro. **Lei nº 13.709/2018: análise à lei geral de proteção de dados pessoais (LGPD)**. 60 f. Trabalho de Conclusão de Curso (Graduação em Direito)-Universidade do Sul de Santa Catarina, Tubarão, 2020. Disponível em: https://repositorio.animaeducacao.com.br/handle/ANIMA/6086. Acesso em: 03/09/2021.

SANTOS, Dhiulia de Oliveira. **A validade do consentimento do usuário à luz da lei geral de proteção de dados pessoais (Lei n. 13.709/2018)**. 50 f. Trabalho de Conclusão de Curso (Graduação em Direito)-Faculdade de Ciências Jurídicas e Sociais, Centro Universitário de Brasília, Brasília, 2019. Disponível em: https://repositorio.uniceub.br/jspui/handle/prefix/13802. Acesso em: 03/09/2021.

SANTOS, Natacha Armstrong dos. **LGPD: lei geral de proteção de dados pessoais e seus reflexos empresariais.** Anais do EVINCI. UniBrasil, Curitiba, v.5, n.1, p. 142, 2019. Disponível em: https://portaldeperiodicos.unibrasil.com.br/index.php/anaisevinci/article/view/4852/3772. Acesso em: 08/05/2021.

SANTOS, Viviane Bezerra de Menezes. **Lei geral de proteção de dados: fundamentos e *compliance*.** 55 f. Trabalho de Conclusão de Curso (Graduação em Direito)-Universidade Federal do Ceará, Fortaleza, 2019. Disponível em: http://repositorio.ufc.br/handle/riufc/49370. Acesso em: 27/09/2021.

SARLET, Gabrielle Bezerra Sales; RUARO, Regina Linden. **A proteção de dados sensíveis no sistema normativo brasileiros sob o enfoque da lei geral de proteção de dados**. Revista de Direitos Fundamentais e Democracia. Curitiba, v. 26, n. 2, p. 81-106, 2021. Disponível em: https://revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/article/view/2172. Acesso em: 29/10/2021.

SILVA, Felipe Rangel da; TEIXEIRA, Rodrigo Giublin. **A sociedade da informação e seus desafios: a necessidade de efetivação de uma política pública de combate ao *ransomware* no Brasil.** RFD - Revista da Faculdade de Direito da UERJ, Rio de Janeiro, n. 36, p. 23-52, 2019. Disponível em: https://www.e-publicacoes.uerj.br/index.php/rfduerj/article/view/40697/32263. Acesso em: 30/09/2021.

SILVEIRA SOBRINHO, Nayara. **A proteção de dados pessoais no *e-commerce*: análise da aplicação da LGPD diante da vulnerabilidade do consumidor**. 52 f. Trabalho de Conclusão de Curso (Graduação em Direito)-Centro Universitário UNIFACIG, Manhuaçu, 2019. Disponível em: http://www.pensaracademico.facig.edu.br/index.php/repositoriotcc/article/view/1745. Acesso em: 17/09/2021.

TEIXEIRA, Tarcisio. **Direito empresarial sistematizado: doutrina, jurisprudência e prátic**a. 7. ed. São Paulo: Saraiva Educação, 2018.

VILELA, Gabriel. **LGPD: Um estudo sobre as principais responsabilidades e penalidades previstas na lei.** 49 f. Trabalho de Conclusão de Curso (Graduação em Engenharia de Computação)-Escola de Ciências Exatas e da Computação, Pontifícia Universidade Católica de Goiás, Goiânia, 2021. Disponível em: https://repositorio.pucgoias.edu.br/jspui/handle/123456789/1580. Acesso em: 03/09/2021.

WILLRICH, Adolfo Chávez. **Comércio eletrônico e a regulamentação da lei geral de proteção de dados pessoais.** 67 f. Trabalho de Conclusão de Curso (Graduação em Direito)-Universidade do Sul de Santa Catarina, Florianópolis, 2020. Disponível em: https://repositorio.animaeducacao.com.br/handle/ANIMA/7329. Acesso em: 01/10/2021.