PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
PRÓ-REITORIA DE GRADUAÇÃO
ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO
CURSO DE DIREITO
NÚCLEO DE PRÁTICA JURÍDICA
COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO

A LEI GERAL DE PROTEÇÃO DE DADOS NO E-COMMERCE

ORIENTANDO: VINÍCIUS FERNANDES ARAÚJO

ORIENTADOR (A): PROFA. DRA. MARIA CRISTINA VIDOTTE B. TÁRREGA

GOIÂNIA-GO
2023

VINÍCIUS FERNANDES ARAÚJO

A LEI GERAL DE PROTEÇÃO DE DADOS NO E-COMMERCE

Artigo Científico apresentado à disciplina Trabalho de Curso II, da Escola de Direito, Negócios e Comunicação da Pontifícia Universidade Católica de Goiás Prof. (a) Orientadora: Profa. Dra. Maria Cristina Vidotte B. Tárrega

GOIÂNIA-GO
2023

VINÍCIUS FERNANDES ARAÚJO

A LEI GERAL DE PROTEÇÃO DE DADOS NO E-COMMERCE

Data da Defesa: 31 de maio de 2023

BANCA EXAMINADORA

_____

Orientador (a): Prof. (a): Dra. Maria Cristina Vidotte B. Tárrega Nota

_____

Examinador (a) Convidado (a): Prof. (a): Dra. Cláudia Luiz Lourenço Nota

A LEI GERAL DE PROTEÇÃO DE DADOS NO E-COMMERCE

Vinícius Fernandes Araújo[1]

Em decorrência das novas tecnologias, emergiu o e-commerce, uma nova forma de comercialização onde todo o processo de compra e venda de produtos e serviços são efetuados de forma *online.* Todo esse contexto expõe, de forma significativa, os dados pessoais dos usuários, os quais ficam mais vulneráveis aos crimes *cibernéticos.* Para tanto, a discussão de novas formas de assegurar essas informações pessoais é sempre pertinente. Assim, o objetivo da presente pesquisa foi pesquisar o que trazem as atuais pesquisas acerca das contribuições relacionadas à Lei Geral de Proteção de Dados Pessoais no que tange a minimização do sequestro de dados no *e-commerce*. Para sua realização, a metodologia selecionada foi a revisão de literatura, os dados foram coletados por meio de revisões distribuídas em livros, artigos científicos, trabalhos de conclusão de curso e teses. Ademais, conclui-se que, temos em nosso ordenamento jurídico um instituto processual principal para a defesa do consumidor nos casos de sequestros de seus dados: a Lei Geral de Proteção de Dados Pessoais, a qual dispõe de penalidades para aqueles que apresentarem algum ato ilícito com os dados de outrem.

Palavras-chave: E-commerce. Proteção. Dados. Tecnologia.

[1]Acadêmico no curso de Direito pela Pontifícia Universidade Católica de Goiás.

SUMÁRIO

INTRODUÇÃO

Com a significativa ascensão das novas tecnologias e dos meios midiáticos, notoriamente, foi possível identificar a disponibilização de um rol de dados pessoais de usuários nas plataformas *onlines*, tornando essas informações suscetíveis aos mais variados riscos, haja vista que, na maioria dos casos não é realizado o processo de *criptografia,* oferecendo, dessa forma, mínima segurança aos indivíduos.

Alude-se ainda a respeito do *e-commerce*, o qual vêm se destacando em proporções demasiadas, partindo do pressuposto de que as pessoas têm priorizado as compras de forma totalmente *online,* diante disso, perceptivelmente os índices de sequestro de dados, golpes e fraudes também apresentou um crescimento bastante notável e significativo (COUTO, 2017).

Em meio a grande vulnerabilidade das informações pessoais dos usuários, passou-se a ter a premissa da necessidade de proteção desses dados, garantindo maior confiabilidade dos clientes para disponibilização de suas informações pessoais. Atrelado a isso, em decorrência dos casos de crimes cibernéticos, houve também a imprescindibilidade do âmbito jurídico propor aparatos legais para evitar as respectivas ocorrências.

Concomitante a isso, a criação de instrumentos legais visava, sobretudo, garantir a proteção dos dados, bem como dos direitos dos usuários e, em consonância a isso, garantir que houvesse o livre desenvolvimento da economia e do mercado. A partir disso, a jurisprudência promulgou em 2018 a Lei de nº 13.709 (MORAES *et al.,* 2022).

Dessa forma, a Lei Geral de Proteção de Dados Pessoais se mostra extremamente importante, principalmente no cenário das comercializações de forma virtual, isto porque através dela os agentes apresentam condutas errôneas que devem ser responsabilizados civilmente e juridicamente. Neste viés, sem dúvidas, essa lei é uma ampliação da tutela ao direito da privacidade.

Neste sentido, surge então uma questão problematizadora que norteou o presente estudo: quais as principais contribuições advindas com a Lei Geral de Proteção de Dados Pessoais no contexto do *e-commerce*? Para tanto, para responder a seguinte problemática foram propostos os objetivos gerais e

específicos do trabalho.

O objetivo geral da presente pesquisa foi pesquisar o que trazem as atuais pesquisas acerca das contribuições relacionadas à Lei Geral de Proteção de Dados Pessoais no que tange a minimização do sequestro de dados no e-commerce. Seguido dos objetivos específicos: realizar uma abordagem acerca do contexto histórico do *e-commerce*, contextualizar a Lei Geral de Proteção de Dados Pessoais e sua importância no *e-commerce.*

Para tanto, a metodologia utilizada no presente trabalho foi de cunho estritamente bibliográfico de natureza qualitativa enriquecida com uma revisão literária em livros, artigos científicos, teses e trabalhos de conclusão que abordavam sobre o tema debatido.

1 CONTEXTO HISTÓRICO *E-COMMERCE*

Inegavelmente, com o advento da globalização e a emergência das novas tecnologias, ficou notório que houve uma série de modificações inerentes às formas como os consumidores compram seus produtos. Concomitante a isso, nos dias atuais, percebe-se que os meios tecnológicos estão cada vez mais presentes na vida das pessoas e apresentam interferências das mais variadas formas.

Neste mesmo ínterim, ao analisar o *e-commerce* sob uma óptica histórica é perceptível que, a partir da primeira fase da Revolução Industrial um rol de mudanças permearam o consumo, sendo este influenciado por distintos aspectos e fatores, neste mesmo viés, a partir do final do século XX passou a ser perceptível a emergência da sociedade da informação, a qual caracterizava-se principalmente pelo consumo exacerbado atrelado ao avanços tecnológicos e em decorrência ao acesso dos novos meios midiáticos viabilizados pela *internet*, derivando assim, o estabelecimento de novas formas de se consumir através dos meios digitais (MENDONÇA, 2016).

Neste mesmo viés, surgiu o *E-commerce*, sua tradução quer dizer “comércio eletrônico” e caracteriza-se como sendo um meio viável de compra ou venda através de um equipamento eletrônico, utilizando-se da *internet,* onde o

consumidor pode ter acesso aos mais variados produtos e optar por aquele que mostra maior viabilidade e melhor custo-benefício.

Sem dúvidas, os novos meios de comunicação, a forma como os consumidores compram os serviços, bem como as novas formas contratos foram fatores que sofreram alterações notórias em decorrência do estabelecimento da *internet*, a qual possibilitou a expansão dos relacionamentos interpessoais, permitindo que pessoas de diferentes regiões se comuniquem instantaneamente, interpolando as barreiras geográficas e tornando possível a troca de informações de indivíduos dos mais variados lugares (RIBEIRO e FREITAS, 2021).

Sob uma perspectiva histórica, denota-se que o *E-commerce* iniciou-se no Estados Unidos, em 1995, chegando ao Brasil em 2000, apresentando crescimento significativo e contínuo ao longo dos anos, fato este derivado pelos benefícios desse tipo de comércio, sobretudo, pela sua facilidade, há ainda a percepção de que alguns sujeitos preferem realizar suas compras de forma *online* em detrimento das compras presenciais.

É possível encontrar ainda uma série de conceptualizações abordadas pelos doutrinadores a respeito do comércio eletrônico, os quais partem do pressuposto de que há uma expansão significativa de uma nova modalidade de comunicação, onde o consumidor passa a se aproximar dos serviços e produtos de forma síncrona, com transações efetuadas à distância, garantindo assim maior rapidez nas atividades e redução de custos. Não obstante, cabe ainda enfatizar que o comércio eletrônico não restringe-se somente a disponibilizar compras e vendas de forma *on-line*, mas também presta informações e serviços.

Assim, conforme aponta Jensen e Ferreira (2012), o *e-commerce* pode ainda ser entendido como uma nova forma de se estabelecer relações jurídicas por intermédio do meio virtual, utilizando-se de documentos de forma eletrônica, podendo ser realizados de forma remota, com contratantes localizados a longos quilômetros de distância.

A partir disso, depreende-se então que, as negociações jurídicas efetivas de forma remota são concluídas sem implicar na necessidade de haver, de fato, a presença física do fornecedor e cliente no mesmo ambiente, sendo esses contratos realizados a distância, fato este que é possibilitado, originalmente, pelo comércio eletrônico.

Atrelado a isso, ressalta-se ainda que, o *e-commerce* deve ser regulado pelo direito comercial, no entanto, em conformidade as relações de consumo pré-estabelecidas entre o cliente e o fornecedor, é possível notar que o direito do consumidor passa a ser atribuído pela regulamentação das relações supracitadas.

Voltando a discussão para a evolução do *e-commerce* ao longo dos anos, é possível ressaltar que desde o ano de 2020 essa nova modalidade tem crescido demasiadamente, sendo impulsionada principalmente devido a pandemia do novo corona Vírus. Isto porque durante a crise pandêmica, houve uma série de impactos na sociedade que não se restringiram somente ao caráter epidemiológico, mas, sobretudo, na economia e nas formas que os consumidores têm comprado seus produtos.

Dessa forma, com o isolamento social, perceptivelmente o comércio precisou reinventar novas formas de relações com os clientes, e o *e-commerce* passou então a ser denotado como uma alternativa viável e que poderia expandir as possibilidades de vendas. E, de fato, através das vendas *on-lines* é possível estabelecer uma maior interação com os clientes, receber *feedbacks*, facilitar os processos de compra e venda, entre outras vantagens que se mostram pertinentes. No entanto, apesar das vantagens das compras por meio *on-line,* não é possível camuflar ou omitir os riscos em que os consumidores são constantemente expostos, como é o caso da exposição de dados pessoais, aumentando assim os riscos de fraudes e, sobretudo, do sequestro de dados.

1.1 SEQUESTRO DE DADOS NO *E-COMMERCE*

Inegavelmente, os avanços relacionados à nova era tecnológica corroboram demasiadamente para o constante aumento do processamento e armazenamento dos dados, principalmente no mercado digital. Neste ínterim, são coletadas várias informações, incluindo os dados pessoais dos indivíduos, colocando-os assim, em risco.

O sequestro de dados no e-commerce ocorre quando hackers invadem um sistema de loja virtual e acessam informações sensíveis dos clientes, como números de cartão de crédito, endereços de e-mail e senhas. Esses dados podem ser usados para uma série de fins maliciosos, como fraudes financeiras

ou roubo de identidade. Para evitar o sequestro de dados, os proprietários de sites de e-commerce devem implementar medidas de segurança robustas, como o uso de criptografia de dados e a verificação de segurança de terceiros. Também é importante que os clientes sejam educados sobre como proteger suas informações pessoais e financeiras.

Associado a isso, salienta-se ainda que essas informações são coletadas diariamente no ambiente virtual, quais sejam: endereço, nome, dados de cartões de créditos, informações bancárias, entre outras. Concomitante a isso, a exposição exacerbada dos indivíduos no espaço *on-line* corrobora para a vulnerabilidade desses sujeitos para os mais variados crimes cibernéticos, sendo os mais comuns: sequestro de dados e roubo (SÁ, 2021).

O sequestro de dados tem se destacado no que concerne a ser um dos principais crimes praticados na esfera digital, o qual caracteriza-se como sendo uma forma em que o sujeito instala algum código no equipamento eletrônico na vítima, sendo então possível a criptografia das informações que estão contidas neste equipamento, trazendo assim prejuízos irreversíveis, tornando-se então imprescindível que haja atribuições legais efetivas, bem como punições penais sob à luz do direito penal para quem comete esses crimes. Não obstante, emerge ainda a necessidade de oferecer aos consumidores maior segurança de seus dados, minimizando a vulnerabilidade e riscos do sequestro dessas informações.

Inegavelmente, a grande disponibilidade de informações, sobretudo, de dados pessoais dos clientes no meio digital aumenta as possibilidades para ocorrência dos crimes cibernéticos. Um dos principais vírus que têm sido relevante no sequestro de dados é chamado *ransomware*, extremamente utilizado por ter a capacidade de codificar, sem a autorização do usuário, todos os dados do equipamento eletrônico.

Normalmente, esses *malwares* não demonstram nenhum sinal, por isso representam um grande risco. Para além disso, é válido ressaltar que, a empresa não irá conseguir ter acesso a mais nenhum de seus dados, isto porque será solicitado uma senha criada pelo *hacker.* É justamente a partir disso que os criminosos agem, solicitando um valor x para a liberação da respectiva senha e, consequentemente, dos dados do computador, então, esses sujeitos conseguem obter lucros altíssimos para devolução de informações do dono legítimo (COUTO, 2017).

Dessa forma, os *hackers* passam a enviar mensagens para a empresa pedindo quantias altíssimas em moedas virtuais, denominadas como *Bitcoin* (significativamente difíceis de serem rastreadas após ocorrer o processo de criptografia dos dados). Assim a restauração dos dados e o funcionamento normal do sistema só volta a acontecer após o pagamento.

Devido à grande incidência desses casos no âmbito global, notoriamente, tem-se a percepção que empreendedores e comerciantes do mercado eletrônico vêm se preocupando expressivamente, uma vez que, estão cotidianamente submetidos a estes respectivos riscos. Não obstante, visivelmente o cliente, de certa forma, se expõe também à ameaça de ter suas informações pessoais divulgadas, podendo então ser vítima de fraude (MORAES *et al.,* 2022).

Dessa forma, torna-se cada vez mais emergente que as organizações empresariais que atuam no âmbito do *e-commerce* e disponibiliza seus produtos ou serviços através das redes sociais ou *websites* estejam abstraídas as questões relacionadas ao sequestro de dados, partindo do pressuposto de que são mais vulneráveis e vêm sendo alvo dessas práticas constantemente. Concomitante a isso, há ainda a imprescindibilidade de garantir aos consumidores que as suas informações serão armazenadas de forma segura, estando, portanto, isentos de qualquer prática que violem os seus direitos.

Assim, discussões perduraram durante longos anos no ordenamento jurídico brasileiro, buscando formas de solucionar a referida problemática. Diante desse cenário, foi então sancionada a Lei de Proteção de Dados Pessoais, visando coibir tais condutas.

2 LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS: UMA CONTEXTUALIZAÇÃO

De forma inegável, debates acerca da proteção de dados pessoais têm sido uma das temáticas discutidas nos últimos anos, decorrentes de significativos avanços tecnológicos e fácil acesso de informações. Principalmente, devido às grandes problemáticas relacionadas à violação de informações pessoais dos indivíduos, tornou-se então emergente a necessidade

de implementar uma lei que abordasse, de forma específica, a segurança de dados no Brasil (TRINDADE, 2022).

Analogamente, era perceptível que havia uma escassez significativa de legislações que tratassem especificamente a respeito do crime de sequestro de dados, havia ainda a ausência de medidas que se objetivaram em combater e prevenir tal prática. Assim, foram propostas algumas legislações que tratavam de forma superficial e abstrata essa prática, a saber: a Lei nº 12.737/2012, denominada popularmente como a Lei Carolina Dieckmann (BRASIL, 2012).

Em consonância a isso, foi então publicada em 14 de agosto de 2018 a denominada Lei Geral de Proteção de Dados Pessoais (LGPD), de nº 13.709/2018, representando, desta forma, um importante passo para garantir maior segurança no comércio eletrônico e mitigação dos índices exorbitantes de sequestros de dados. Neste contexto:

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (BRASIL, 2018).

Neste ínterim, pode-se então aludir que, a Lei foi implementada no ordenamento jurídico brasileiro com o objetivo genuíno de propor regulamentações viáveis para os meios que realizam a coleta e armazenamento de dados no Brasil. Paralelo a isso, ressalta-se ainda que foram determinadas algumas normas a serem cumpridas pelas empresas, seja de médio ou grande porte, que fazem uso de informações em suas atividades, de modo a garantir maior seguridade aos clientes que disponibilizam seus dados pessoais.

De modo sucinto, a referida lei supracitada caracteriza a privacidade como sendo um direito civil e, em decorrência disso, só poderá haver a utilização dos dados mediante autorização, para tanto, a lei aplica-se para todas as empresas que detém dessas informações, não obstante, dispõe ainda de um rol de penalidades para os indivíduos que não seguirem os requisitos legais de proteção. Quanto à forma de tratamento de dados pessoais, o art. 5º da referida lei, em seu inciso X, aborda uma conceptualização relevante, enfatizando que:

> Art. 5º Para os fins desta Lei, considera-se:
>
> X- Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da

> informação, modificação, comunicação, transferência, difusão ou extração (BRASIL, 2018).

Para tanto, existem penalidades que são aplicadas no caso de tratamento indevido dos dados pessoais, isto implica dizer que há advertências, aplicações de multas e de prazos para que sejam feitas as correções dos erros, perceptivelmente, é implementada ainda uma fiscalização para monitoramento do cumprimento da LGPD, a qual deve efetivada por um órgão Federal que foi instituído Inter especificamente para esta função, denominado como Autoridade Nacional de Proteção de Dados (ANPD) (BRASIL, 2018).

Concomitantemente, o art. 52º enfatiza as penalidades a quem cometer alguma infração referente ao tratamento dos dados pessoais:

> Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
> I - advertência, com indicação de prazo para adoção de medidas corretivas;
> II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração.
> (BRASIL, 2018).

Pautado nisto, denota-se então que a relevância da LGPD está elencada na minimização de ataques em distintas dimensões, desde aqueles que se mostram relativamente pequenos, até mesmo aqueles casos que trazem prejuízos financeiros irreversíveis para o indivíduo. Além disso, perceptivelmente, este aparato legal garante maior confiança por parte dos clientes aos sistemas.

Com a LGPD, as empresas são obrigadas a informar aos seus clientes quais dados estão sendo coletados e para que são utilizados, além de garantir a segurança dessas informações. Além disso, os consumidores têm o direito de acessar, corrigir e excluir seus dados pessoais quando desejarem.

Como já citado anteriormente, a LGPD também estabelece penalidades para as empresas que descumprirem a lei, podendo gerar multas de até 2% do faturamento da empresa, limitado a R$ 50 milhões. É importante destacar que a LGPD não afeta apenas as empresas, mas também os órgãos públicos. Todas as entidades que lidam com dados pessoais devem estar em conformidade com a Lei, garantindo que os direitos dos cidadãos sejam respeitados.

Em um mundo cada vez mais digital, a LGPD é essencial para garantir a privacidade e a proteção dos dados dos indivíduos. Por isso, é fundamental que as empresas e órgãos públicos estejam atentos às novas regras para evitar as penalidades previstas na Lei.

3 LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E *E-COMMERCE*

De fato, com a emergência das novas tecnologias e as novas formas de comercialização no mercado digital houve uma expansão significativa da vulnerabilidade do consumidor em relação ao risco de captura de seus dados pessoais. É justamente sob esse viés, que percebe-se a imprescindibilidade de implementar a Lei Geral de Proteção de Dados Pessoais.

Neste contexto, vale então elencar o inciso XII do art. 5º, o qual deixa claro que o consentimento do titular é uma premissa básica e indispensável para a utilização dos seus dados, destaca-se ainda a livre manifestação, de forma clara no que tange a concordância para o tratamento de dados para determinados objetivos, sem haver, portanto, a possibilidade de usá-lo irregularmente pelas empresas.

Aduz-se ainda acerca dos princípios da LGPD, os quais elencam a forma que os dados deverão ser tratados e em quais princípios devem basear-se, salienta-se que eles mostram-se crucialmente relevantes no sentido de reduzir a possibilidades do consumidor ter seus dados sequestrados.

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades (BRASIL, 2018).

O princípio de finalidade da lei de proteção de dados estabelece que os dados pessoais devem ser coletados e processados apenas para finalidades específicas e legítimas, que devem ser determinadas no momento da coleta. As finalidades devem ser explícitas, claras e informadas ao titular dos dados, que deve consentir expressamente com o seu uso.

Além disso, os dados devem ser adequados, relevantes e limitados ao necessário para atingir a finalidade específica, e não podem ser utilizados para

finalidades que não sejam compatíveis com aquela para a qual foram coletados. Esse princípio visa proteger os direitos fundamentais dos titulares dos dados, como a privacidade e a autodeterminação informativa, garantindo que os seus dados sejam utilizados de forma justa e transparente.

> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
>
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
>
> IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
>
> V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
>
> VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
>
> VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
>
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais (BRASIL, 2018).

Torna-se então perceptível o quão importantes são os respectivos princípios supracitados anteriormente para garantir o direito civil de privacidade aos cidadãos, com maior seguridade de que estes serão tratados de forma adequada e, sobretudo, o titular deverá estar ciente de toda e qualquer informação.

Diante o exposto, é possível considerar que a LGPD emerge como um contexto favorável e viável no que concerne a garantia de menores riscos de fraudes e crimes cibernéticos no *e-commerce*, em consonância a isso, convém ressaltar que sua aplicabilidade deve ser efetivada com êxito, uma vez que, o comércio digital tem se expandido demasiadamente, e atrelado a isso, têm sido percepto também um aumento significativo nos números de casos de sequestro de dados (MORAES *et al.,* 2022).

Neste caso, os dados pessoais dos clientes deve ser um direito a ser tutelado pelo ordenamento jurídico brasileiro, garantindo confidencialidade e, principalmente, a restrição da divulgação desses, sobretudo, a impossibilidade para uso de outros fins que não seja de conhecimento do titular.

Inegavelmente, a proteção dos dados está intrinsecamente relacionada com a segurança da privacidade do indivíduo. A partir do pressuposto, evita-se dessa forma, o uso indevido dos dados, inviabilizando que as pessoas tenham danos morais, psicológicos ou financeiros decorrentes dessas condutas repudiadas.

Dessa forma, sucintamente, pode-se então ressaltar que com a entrada em vigor da Lei Geral de Proteção de Dados (LGPD), em setembro de 2020, as empresas tiveram que se adequar a novos requisitos para garantir a privacidade e a segurança dos dados pessoais de seus clientes.

No contexto do comércio eletrônico, a LGPD tem grande importância, uma vez que essa modalidade de negócio lida diretamente com dados sensíveis dos consumidores, como nome, CPF, endereço, e-mail, telefone, entre outros. É fundamental, portanto, que os e-commerce’s estejam em conformidade com as normas estabelecidas pela LGPD para evitar sanções e garantir a confiança dos usuários em suas plataformas.

Dentre as obrigações que as empresas têm na Lei de Proteção de Dados, está a necessidade de obter o consentimento expresso do consumidor para o uso de seus dados pessoais, informando claramente qual é a finalidade do tratamento dessas informações. Além disso, as empresas devem adotar medidas de segurança para proteger esses dados de eventuais vazamentos, roubos ou acessos indevidos.

Nesse sentido, o e-commerce precisa investir em tecnologias e processos seguros para garantir a privacidade dos consumidores. Caso ocorra algum incidente de segurança, a empresa deverá reportar imediatamente à autoridade competente e aos próprios usuários afetados, bem como tomar medidas para minimizar os possíveis danos.

Por fim, é importante lembrar que a LGPD aplica-se a todas as empresas que tratam dados pessoais, independente do seu porte ou ramo de atuação. No caso do comércio eletrônico, essa regulamentação é ainda mais relevante, já que as informações dos usuários são a base desse modelo de negócio. Por isso,

investir na proteção de dados pessoais pode ser uma forma estratégica de garantir a competitividade e a fidelização dos clientes.

CONCLUSÃO

A partir da presente pesquisa ficou perceptível o quanto os novos meios tecnológicos abriram um rol de possibilidades para novas formas de relações entre as pessoas, interferindo ainda nos modos de comercialização de produtos e serviços, os quais atualmente ocorrem frequentemente pelos meios digitais.

Exposto o significativo avanço das novas tecnologias, cabe então evidenciar o e-commerce e como este novo meio de comercialização pode impactar os consumidores, além disso, os principais riscos advindos com esta ferramenta. Dessa forma, percebe-se então que, há uma grande viabilidade de acesso aos mais variados dados de clientes inseridos nos sistemas, isto corrobora para que estes estejam expostos ao risco intrínseco de violação dessas informações pessoais.

O objetivo do presente trabalho foi pesquisar o que trazem as atuais pesquisas acerca das contribuições relacionadas à Lei Geral de Proteção de Dados Pessoais no que tange a minimização do sequestro de dados no *e-commerce*. Sendo assim, infere-se ressaltar ainda que, os objetivos da pesquisa foram alcançados com êxito desde a etapa de coleta de dados por intermédio de uma pesquisa na literatura, até a discussão desses resultados ao longo do desenvolvimento da pesquisa.

Quanto a metodologia adotada para a realização da pesquisa, pode-se inferir que ela apresentou grande importância e se mostrou eficaz, foi a pesquisa de revisão de literatura, através dela foi possível aprofundar-se e debater sobre o tema proposto no trabalho, de modo que, foi possível ainda ter conhecimento sobre o que outros autores já tinham debatido acerca do assunto. As pesquisas bibliográficas permitem que sejam feitos debates e reflexões acerca do que os autores abordam.

Ficou constatado a partir da pesquisa que, é perceptível uma redução significativa dos riscos de sequestro de dados de clientes a partir da promulgação da LGPD, isto porque ela dispõe de penalidades para quem descumprir o correto tratamento de dados, além disso, explica, de forma

detalhada, como devem ser tratados essas informações, estando estas tuteladas pela jurisprudência. Além disso, a referida lei garante maior segurança e confiabilidade por parte dos clientes.

REFERÊNCIAS

BRASIL. **Lei nº 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: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 10 de jan. 2023.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm**.** Acesso em: 13 de jan. 2023.

COUTO, Marta Lais dos Santos Alegria. **O e-commerce à luz do direito: análise do regulamento geral da proteção de dados: a uniformização da União Europeia**. 2017. Tese de Doutorado.

JENSEN, Vinicius Souza; FERREIRA, Vitor Hugo do Amaral. Relações virtuais de consumo: perspectivas de direitos no e-commerce. **Revista Direitos Emergentes na Sociedade Global**, v. 1, n. 1, p. 94-119, 2012.

MENDONÇA, Herbert Garcia. E-commerce. **Revista Inovação, Projetos e Tecnologias**, v. 4, n. 2, p. 240-251, 2016.

MORAES, Cintia Alves de Macedo *et al.* A Lei Geral de Proteção de Dados e sua importância no âmbito do consumo por e-commerce. **LIBERTAS: Revista de Ciências Sociais Aplicadas**, v. 12, n. 2, 2022.

RIBEIRO, Frantchesca Eduarda Soares; FREITAS, Marcio. E-commerce. **Seminário De Tecnologia Gestão e Educação**, v. 3, n. 1, 2021.

SÁ, Marina Ferraz Da R. A publicidade do e-commerce nas redes sociais e os limites legais frente à vigência da lei geral de proteção de dados (L. 13.709/2018). **Portal de Trabalhos Acadêmicos**, v. 8, n. 2, 2021.

TRINDADE, Larissa Freitas da Silva. **Impactos da Lei Geral de Proteção de Dados nas relações *e-commerce***. Trabalho de Conclusão de Curso (Bacharelado em Direito)–Faculdade Nacional de Direito, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2022.