A Lei Geral de Proteção de Dados e sua importância no âmbito do consumo por *e-commerce*

Cintia Alves de Macedo Moraes[1]

João Paulo Barbosa de Araújo[2]

Luana Eduardo Magalhães Viana[3]

Maria Thereza Minaré[4]

Recebido em: 18.11.2022

Aprovado em: 15.12.2022

Resumo: A projeção do avanço tecnológico leva a sociedade à uma constante adaptação. Dessa forma, surge a figura do *e-commerce*, que se trata da virtualização das vias consumeristas utilizando a internet, bem como a transferência de dados pessoais solicitados nas plataformas. Diante desse cenário, fez-se necessário a implementação de regulamentos gerais para proporcionar uma via harmônica de trocas – fornecedor e consumidor – surgindo em 2018 a Lei n° 13.709, com o intuito de promover mais segurança aos dados e direitos dos consumidores. Frente a isso, com os cenários pandêmicos, o consumo digital cresceu exponencialmente concomitante com a liberação de dados pessoais, fatores relevantes ao uso da Lei Geral de Proteção de Dados, tendo em vista que tal legislação abre a possibilidade do agente que teve seus dados violados fazer uso da justiça em prol de resguardar seus direitos e prevenir irregularidades. O cerne desta pesquisa é levantar o questionamento acerca da real proteção que a Lei 13.709/18 oferece aos consumidores de *e-commerce*, visando despertar um olhar crítico do leitor para as formas de proteção trazidas pela legislação, bem como a sua eficácia no âmbito hodierno.

1 Graduanda em Direito pela Faculdade de Ensino Superior da Amazônia Reunida- FESAR AFYA. Brasil, macedo.cintia2013@gmail.com. Lattes (2777748298016820). ORCID (0000-0003-3710-7920).

2 Graduando em Direito pela Faculdade de Ensino Superior da Amazonia Reunida- FESAR AFYA. BRASIL, joaopaulobaraujo97@gmail.com. Lattes (4508948462954279). ORCID (0000-0002-1696-8513).

3 Graduanda em Direito pela Faculdade de Ensino Superior da Amazonia Reunida- FESAR AFYA. Brasil, luanaeduardomg@gmail.com. Lattes (3576085883428287). ORCID (0000-0002-3124-2841).

4 Graduada em Direito pela Universidade de Uberaba (1999). Pós-Graduada em Direito Processual Civil pelo Centro Universitário Paulista - UNIRP (2001). mtminare@hotmail.com. Lattes (4818516369571727). ORCID (0000-0001-6147-2229).

Palavras-chave: proteção de dados; comércio eletrônico; responsabilidade; vazamento de dados.

The General Data Protection Law and its importance in the field of e-commerce consumption

Abstract: The projection of technological advance leads society to a constant adaptation. In this way, the figure of e-commerce emerges, which is about the virtualization of consumerist ways using the internet, as well as the transfer of personal data requested on the platforms. In view of this scenario, it was necessary to implement general regulations to provide a harmonious way of exchange - supplier and consumer - arising in 2018, Brazilian Law N° 13,709 in order to promote more security to data and consumer rights. Faced with this, with the pandemic scenarios, digital consumption has grown exponentially concomitantly with the release of personal data, relevant factors for the use of the General Data Protection Law, given that such legislation opens the possibility of the agent who had their data violated. make use of justice in order to protect their rights and prevent irregularities. The core of this research is to raise the question about the real protection that Law 13.709 offers to e-commerce consumers, aiming to awaken a critical eye of the reader for the forms of protection brought by the legislation, as well as its effectiveness in today's context.

Keywords: data protection; *e-commerce*; responsibility; data leakage.

1 INTRODUÇÃO

Com o advento da tecnologia e do acesso ilimitado a sites e redes sociais, as informações pessoais dos usuários encontram-se mais vulneráveis no atual contexto econômico, pois nem sempre as empresas possuem a segurança devida aos cadastros nas organizações que atuam virtualmente.

Durante o cenário pandêmico da COVID-19 no mundo, a sociedade passou a utilizar massivamente a internet para realizar, praticamente, todas as tarefas, principalmente para consumo de produtos ou serviços. Um dos fatores que mais ensejou a criação de mecanismos para propiciar uma melhor proteção às informações pessoais dos cidadãos diz respeito ao crescimento do chamado *e-commerce*, também denominado Comércio Eletrônico.

Tal modalidade consiste na instrumentalização virtual dos meios de consumo através da transmissão eletrônica de dados entre os veículos de comunicação. Com a sua expansão, verificou-se uma necessidade mais exacerbada na criação de

regulamentos a fim de, concomitantemente, proteger os dados e direitos dos consumidores e preservar o livre mercado e o desenvolvimento da economia (LIMA et al, 2021).

Visando regular a proteção e o uso dos dados pessoais da pessoa natural, foi promulgada em 14 de agosto de 2018 a Lei 13.709 (Lei Geral de Proteção de Dados), o que demonstra a importância do tema frente ao mercado de consumo nas vendas pela internet, objeto deste estudo. Com a referida norma será possível responsabilizar civilmente os agentes que cometem ilícitos utilizando-se de dados pessoais de terceiros.

A proteção aos dados não deixa de ser uma amplificação da tutela à privacidade. Já o *e-commerce* é uma evolução do comércio tradicional, que se aproveitou do advento da internet para ter a comercialização de bens e serviços em um ambiente digital. (TEIXEIRA, 2021).

Também instrui Teixeira (2021) que embora a proteção da privacidade (e dos dados) não tenha sido criada em razão da internet (e depois do *e-commerce*), foi pelo desenvolvimento e pela massificação do comércio digital que a preocupação com dados se tornou cada vez maior, dando origem às normas jurídicas que tutelam dados pessoais pelo mundo.

Diante do contexto, o estudo levanta como problema da pesquisa a seguinte indagação: os serviços prestados pelas plataformas de *e-commerce* armazenam os dados dos usuários com a devida proteção conforme prevê a LGPD (Lei 13.709/2018)? Logo, o objetivo geral será compreender a segurança da informação dos dados armazenados com base na Lei 13.709/18 no âmbito das empresas de *e-commerce.*

Para obter êxito no objetivo geral, têm-se os seguintes objetivos específicos: a) Analisar a adaptação feita pelas empresas de *e-commerce* a fim de acomodarem a normativa trazida pela LGPD; b) Apresentar os impactos oriundos da implantação da LGPD na legislação brasileira.

Para tanto, a pesquisa se justifica no cenário atual pelas grandes mudanças que a LGPD trouxe, principalmente no que tange ao âmbito do consumo por meio eletrônico. Para a sociedade como consumidor final, será possível verificar se as empresas e organizações adequaram-se as novas tratativas de proteger os dados pessoais dos usuários, visando a coibir as tentativas de vazamentos de dados, uma vez que a questão do sigilo ainda não é algo absoluto neste meio.

Para o meio acadêmico, frisa-se a importância de explorar como as empresas estão tratando do tema quanto a proteção dos dados fornecidos pelos usuários no comercio eletrônico frente a efetividade da Lei Geral de proteção de dados (LGPD) no âmbito social.

Por fim, o presente artigo apresentará o Referencial Teórico, compondo a literatura que dará suporte ao tema e, em seguida, as considerações finais a título de conclusão. O método utilizado foi o exploratório, onde o procedimento adotado teve como base análise bibliográfica em literatura específica contida em livros, jurisprudências e artigos, explorando assim o universo da LGPD e sua importância no âmbito de consumo por *e-commerce*.

2 REFERENCIAL TEORICO

2.1 Evolução Histórica da Proteção de dados no Ordenamento Jurídico Brasileiro

A discussão sobre a necessidade de haver tutela jurídica para os dados e a privacidade das pessoas iniciou-se na década de 1970 na Europa, que culminou implicando na Diretiva 95/46/CE, que, por sua vez, foi substituída pelo Regulamento 2016/679 (GDPR – General Data Protection Regulation; em português, Regulamento Geral de Proteção de Dados), que entrou em vigor em 2018 (TEIXEIRA, 2021, p.8). No ano de 2016, tal norma europeia, passou a ter forte influência na aprovação de normas de proteção de dados pelo mundo, especialmente no Brasil.

Conquanto, sua iniciativa foi relativamente tardia no Brasil, em comparação ao que ocorreu em outras partes do Ocidente (TAMBOSSI et al, 2021, p.23), uma vez que que somente a partir de 14 de agosto de 2018, passou a ser incorporada ao

ordenamento jurídico brasileiro a Lei n. 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD) (TEIXEIRA, 2021).

A proteção de dados pessoais era mencionada em leis anteriores a LPGD, mesmo que de forma superficial, vejamos: Lei 8.078/90 (Código de Defesa do Consumidor Seção V); Lei 12.414/11 (lei do cadastro positivo); a Lei n° 12.527/11 (lei de Acesso à Informação), "situada na seara do Direito Administrativo, é imbuída do intuito de regulamentar os mandamentos constitucionais voltados à necessidade de transparência e publicidade da Administração Pública com relação aos cidadãos" (TAMBOSSI et al, 2021, p.53); por fim, a Lei 12.965/14, conhecida como o Marco Civil da Internet, da qual estabeleceu princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

O jurista Damásio de Jesus (2014, p.18) entende que as funções advindas do Marco Civil Brasileiro foi gerar segurança jurídica, oferecendo base legal ao Poder Judiciário frente as decisões envolvendo a internet e tecnologia da informação, a fim de evitar decisões contraditórias com temas idênticos.

Contudo, a Lei 12.965/14, conhecida como o Marco Civil na Internet, não garantiu de forma ampla a privacidade e a proteção dos dados pessoais, porque sua criação foi pautada objetivando a responsabilidade do provedor de conexão à internet por danos decorrentes de conteúdo gerado por terceiros e por isso não foi considerada uma norma geral de proteção de dados pessoais.

Para Mesquita (2021), um dos objetivos da LGPD é o tratamento à proteção dos dados pessoais de pessoas físicas e jurídicas com maior abrangência, do que o que se encontra no Marco Civil da Internet e com isso vem as sanções a serem aplicadas nos casos em que forem necessários.

A LGPD n° 13.709/18 veio para alterar de forma significativa a Lei 12.965/14, com o objetivo de proteger dados pessoais das pessoas naturais. Assim, "a LGPD não tem como escopo os dados das empresas (pessoas jurídicas), mas sim os dados que as empresas têm das pessoas físicas, sejam elas funcionárias, terceiras, clientes, acionistas etc."(GARCIA, 2020, p.16).

Vale ressaltar que a proteção de dados gerou efeito significativo nos fatos de vazamento de dados de grande repercussão internacional, como o uso indevido de informações pessoais para influenciar nas eleições dos Estados Unidos no ano de 2016. Dentre os dados coletados incluíam o nome, profissão, local de moradia, além de hábitos e preferências dos participantes que sequer tinham conhecimento das violações que sofriam ao responderem a pesquisa.

No Brasil, o mais recente vazamento de dados ocorreu em 19 de janeiro de 2021, por meio da ação fraudulenta de hackers ao sistema de cadastro do Serasa Experian, atingindo mais de 223 milhões de brasileiros vivos ou mortos, que tiveram suas informações como, CPF, fotos, data de nascimento, expostos pelos criminosos para fins meramente comerciais.

Os dados ganharam uma importância transversal, tornando-se vetores das vidas e das liberdades individuais, assim como da sociedade e da própria democracia (FRAZÃO, 2019, p.24), o que evidência a consequente prioridade que emerge a sua proteção no âmbito jurídico brasileiro.

Destarte, a LGPD foi norteada pelos princípios do respeito a privacidade, na liberdade de expressão, na inviolabilidade da intimidade, na defesa do consumidor e, principalmente, nos direitos humanos.

2.2 A relação de consumo através do e-commerce

O acesso à internet e aos meios digitais, teve um crescimento exponencial nos últimos anos, sendo que o Brasil ocupa a 5ª posição no ranking de países com maior quantidade de internautas, sendo o terceiro no mundo no uso diário de internet (BRASIL, 2021). Tal crescimento foi crucial para consolidação do comércio eletrônico, relação de consumo estabelecida através de negociações *on-line* que já estavam em grande ascensão nos últimos anos e foram amplamente impulsionadas após a pandemia de COVID-19.

Em que pese tenha ocorrido a flexibilização do isolamento social (medida adotada para estimular o confinamento em casa, com o intuito de conter a disseminação do

novo coronavírus), cada vez mais as pessoas se rendem à comodidade de comprar ou contratar serviços via internet (MORAES *et. al*, 2021).

É notório salientar que a expressão *e-commerce* ou comércio eletrônico diz respeito aos negócios que mantém sua estrutura de compra e venda de formas virtuais, realizadas através da internet. Conforme conceito utilizado por Bruno (2001), o comércio eletrônico consiste em uma modalidade de compra a distância, cuja aquisição de bens e/ou serviços ocorre por meio de equipamentos eletrônicos de tratamento e armazenamento de dados, nos quais são transmitidas e recebidas informações.

São claros os efeitos que o uso da tecnologia traz ao desenvolvimento do comércio. Teixeira (2021), destaca que o comércio eletrônico possibilita a diminuição da cadeia distributiva dos bens, possibilita as empresas comercializar seus produtos e serviços em tempo integral, vinte e quatro horas por dia e, principalmente, não existe limitação geográfica para se vender.

Diferentemente do comercio tradicional, nas plataformas de *e-commerce* torna-se impossível realizar uma compra sem o fornecimento de dados pessoais, como nome, CPF, sexo, idade, endereço, telefone e *e-mail*, que são requisitos básicos para possibilitar o consumo de produtos oferecidos no mercado digital. Além disso, informações referentes a navegação, pesquisas por produtos e marcas, dentre outros, também ficam registradas nas preferencias dos usuários.

2.3 Tratamento e proteção de dados no comércio eletrônico

O comércio eletrônico exigiu das empresas uma rápida adaptação ao novo modelo de consumo da sociedade, qual seja as lojas virtuais por meio das vendas *on-line*, comumente conhecidas como mercado digital. Com o aumento deste setor os consumidores passaram a exigir maior segurança no fechamento de compras e negócios na internet, fazendo com que muitos empresários do ramo empregassem maior segurança aos consumidores, como transparência, idoneidade e proteção de dados.

Para tanto, o uso de informações dos usuários permanece relevante dentro das práticas de *marketing* de vendas, haja vista que o consumidor é constantemente "bombardeado" por campanhas publicitárias das mais diversas maneiras e muitas vezes sem o seu consentimento (VIGLIAR, 2022).

Neste ponto, o legislador deixou em evidência o que dispõe o art. 5°, inciso XII, da LGPD, o qual requer o consentimento do titular no uso dos seus dados, ressaltando a manifestação livre, ciente e clara quanto a concordância no tratamento de dados do usuário para fins determinados, não podendo se utilizar destes de forma irregular e/ou irresponsável por qualquer empresa, seja física ou virtual.

Moraes (2021) afirma que, dentre as políticas de tratamento de dados, as empresas devem dispor de autorização do titular para lhes assegurar o direito à privacidade e proteção de dados e, ainda, prestar informações claras a respeito do motivo e finalidade para o uso, bem como nova anuência do titular em caso de transmissão de dados para terceiros. Também deve haver atenção redobrada quanto a coleta de dados que versem sobre raça, etnia, opção sexual ou religião, uma vez que se caracterizam como dados sensíveis e sua solicitação pode ser considerada abusiva.

A LGPD trouxe no Capítulo II a forma e os requisitos para o tratamento de dados pessoais, os quais somente serão realizados seguindo os termos do seu art. 7º, o qual preconiza ser necessária à concessão da vontade de fornecer os dados pelo titular, a realização de obrigações legais e/ou de caráter regulatórios pelo ente controlador e a execução de políticas públicas a cargo da administração pública.

Pode-se citar ainda o emprego de estudos realizados por instituições de pesquisas, assegurando, quando houver a possibilidade, o sigilo dos dados pessoais através da "anonimização", quando houver necessidade à execução de contratos ou procedimentos prévios concernentes a acordos em que o titular seja parte, a seu pedido, para assegurar a proteção do crédito, para garantir o exercício de direito em processos administrativos, arbitral ou extrajudicial, para proteção à vida ou garantia da segurança física de terceiro ou de seu titular, para salvaguardar a saúde, assim como diante da necessidade para fins de atendimento a interesses autênticos do

controlador ou de terceiros, salvo em casos de evidente violação a direitos e/ou liberdades fundamentais.

Em suma, a não observância das condições exigidas pela LGPD torna ilegítima a coleta e tratamento de dados e coloca o fornecedor em situação de risco quanto a aplicação de sanções pela Autoridade Nacional de Proteção de Dados (ANPD) (VIGLIAR, 2022). Os impactos da LGPD nas empresas de *e-commerce* impuseram grandes adequações nas suas rotinas, contudo possuem o intuito de garantir tratamento adequado aos dados pessoais dos clientes, garantindo assim transações comerciais seguras.

2.4 REPERCUSSÕES JURÍDICAS NA IMPLANTAÇÃO DA LGPD

2.4.1 Violação à LGPD: Responsabilidade Objetiva ou Subjetiva?

Na ocorrência do descumprimento dos preceitos estabelecidos na LGPD, responderão pela infração os agentes de tratamento, isto é, o controlador (pessoa jurídica ou física encarregada de coordenar e estabelecer as bases de uso dos dados pessoais, desde a sua coleta até a retirada da base de dados), bem como o operador (pessoa jurídica ou natural atribuída à função de tratamento dos dados em nome do controlador). Aquele responde de forma solidária pelos atos que este incorrer e ocasionar prejuízos à vítima.

Frise-se que, conforme preconizado pelo art. 46 da LGPD, recai perante aos agentes de tratamento a obrigação de adotar medidas de segurança, sejam de caráter técnico, quanto administrativo, que configurem instrumentos capazes de prover proteção aos dados pessoais, protegendo-os de perdas, alterações não solicitadas, vazamentos etc.

Surge, então, o debate acerca da natureza da responsabilidade pelo ato: seria uma responsabilidade subjetiva ou objetiva? A doutrina majoritária entende que a natureza da relação entre vítima e autor deve ser analisada para aferição do caráter da responsabilidade.

Segundo Tambosi (2021), a influência do Código do Consumidor é evidente na seção que trata da responsabilidade civil na LGPD, sobremaneira nos arts. 43 e 44, ambos

conferindo uma ampliação dos requisitos para incidência atrelados ao risco, em prejuízo da culpa. Isto posto, é necessária uma hermenêutica ampliativa para se aferir o núcleo da relação *inter partes.*

Nesse diapasão, em sendo verificado que o mau uso do dado personalíssimo derivou de uma relação de consumo, é de plano verificável a possibilidade de aplicação da responsabilidade objetiva do ente envolvido na relação consumerista, isto é, o fornecedor de produtos e serviços, nos termos do art. 14 do Código do Consumidor, retirando do plano jurídico a imprescindibilidade de existência de culpa ao dano causado.

Por consequência, tratando-se de uma responsabilidade objetiva, há um efeito bastante conhecido nas relações jurídicas consumeristas: a inversão do ônus probatório, nos ditames do art. 6º, VIII do CDC, a qual acarreta na responsabilidade unicamente do autor do dano de comprovar que não houve o nexo causal entre o fato e o dano, e não mais da vítima.

Em sua defesa, para eximir-se da responsabilidade caberá provar que não foi o responsável pelo tratamento dos dados, não desrespeitou as normas da LPPD ou o dano deriva de uma culpa exclusiva do titular do dano ou culpa de terceiros, por força do art. 43 da LGPD.

Lado outro, consigna-se que a responsabilidade subjetiva seria aplicável quando não se verificar uma relação de consumo entre as partes, o que acarretaria na necessidade de se provar a existência de culpa ou dolo do agente, bem como na responsabilidade da vítima de demonstrar o dano e nexo de causalidade entre ambos.

A partir da constatação da existência de violação à LGPD e frutos da responsabilidade atinente, nascem sanções administrativas aos responsáveis pela ilicitude, as quais encontram-se listadas no art. 52 da referida lei, sendo: advertência, multa simples no patamar de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, não inclusos os tributos, sendo limitada, em sua integralidade, ao montante de R$ 50.000.000,00 (cinquenta milhões de reais) por infração, multa

diária, publicidade da infração após sua efetiva apuração e confirmação, bloqueio dos dados pessoais utilizados na infração até esclarecimentos, regularização e a exclusão dos dados pessoais utilizados na infração.

2.4.2 Emenda Constitucional n° 115/2022 e seus efeitos à tutela dos dados pessoais

Promulgou-se no dia 10 de fevereiro de 2022 a Emenda Constitucional nº 115/2022, a qual promoveu uma alteração ao texto da Carta Magna ao incluir a proteção de dados pessoais, inclusive através de meios digitais, no rol dos direitos e garantias fundamentais constitucionais, especificamente no art. 5º, inciso LXXIX, da Constituição Federal.

A LGPD é aplicada a qualquer tratamento de dados realizado por pessoa natural ou jurídica de direito público ou privado, seja por meio digital ou físico, todavia referida lei não abarca o tratamento de dados pessoais quando efetuado por pessoa natural com intuitos exclusivamente particulares e não econômicos (TEIXEIRA, 2021, p. 78). Havia, assim, uma evidente omissão no que diz respeito ao uso de dados para fins diversos do estabelecido na Lei nº 13.709/2018, logo não havendo uma regulamentação clara e robusta abrangendo todas as possibilidades do manuseio de dados.

Até então, a discussão acerca da proteção aos dados pessoais como um direito inerente ao cidadão era apaziguada através do Poder Judiciário, que exercia a sua jurisdição como instrumento norteador à aplicação do direito de sigilo dos dados ao cidadão. Através de demandas judiciais, o exercício forense provia amparo às suas contendas no que tange ao uso indevido dos dados utilizando-se da hermenêutica jurídica dos incisos X e XII do art. 5º da CRFB/88, que nada mais tratam do que as cláusulas gerais do direito constitucional à privacidade.

Vultoso é destacar a Ação Direta de Inconstitucionalidade nº 6387, considerada um marco no reconhecimento do direito a não violação do sigilo de dados pessoais dos cidadãos. Referida ADI acarretou na suspensão da eficácia da Medida Provisória nº 954/2020, a qual foi inserida no mundo jurídico com o propósito de possibilitar que empresas prestadoras de serviços telefônicos ao Instituto Brasileiro de Geografia e

Estatísticas (IBGE) compartilhassem dados de seus usuários com o fito de que se fosse produzida estatísticas oficiais durante a pandemia de Covid-19.

Em seu relatório, a Ministra do Supremo Tribunal Federal Rosa Weber apontou que a MP nº 954/2020 ofende diretamente a prerrogativa de sigilo dos dados, sendo esta oriunda dos efeitos correlatos dos direitos fundamentais à privacidade, desenvolvimento da personalidade, promoção e proteção da liberdade e intimidade, portanto não sujeitos a divulgação e compartilhamento, haja vista a evidente violação à intimidade das pessoas.

Em que pese houvesse entendimento jurisprudencial e doutrinário acerca do reconhecimento do sigilo dos dados como um direito fundamental, essa recognição não tinha como efeito a garantia de sua aplicação imediata, haja vista que a mera pronúncia por vias judiciais deixava à deriva da análise pessoal do aplicador do direito aos casos concretos e, consequentemente, à insegurança jurídica.

Com o advento da EC nº 115/2022, o direito à proteção dos dados pessoais foi incluído no texto explícito da Constituinte no rol de direitos e garantias fundamentais elevando-se ao status de cláusula pétrea, as quais constituem dispositivos não passíveis de alteração ou revogação no sentido de suprimir o quanto estabelecido em seu texto.

Não obstante o caráter inviolável do direito à privacidade e intimidade já possuam natureza de direito imodificável na Constituição Federal, a inovação legislativa trouxe um alicerce de robustez mais categórica ao abranger especificamente em seu texto a tutela aos dados pessoais (RODAS, *et al*., 2022). Assim, atingiu-se patamares que eram alcançáveis apenas após profunda hermenêutica dos dispositivos da Carta Magna.

2.4.3 A Vulnerabilidade do Sistema de Segurança

Praticamente todos os sites que as pessoas procuram para acessar exigem, no mínimo, algum dado pessoal do navegante, como por exemplo*: e-mail*, nome completo, contato telefônico, CPF, endereço, em outros casos, até o cartão de crédito. Nesse contexto, surge a ideia de que a proteção de tais dados deve se dar de maneira

concreta e expressiva, tendo em vista que, em alguns casos, pode chegar até mesmo a causar transtornos para aquele que fornece seus dados e gerar dano moral indenizável.

Com o advento da LGPD, as empresas, em especial as do ramo de *e-commerce*, passaram a se importar mais com essa segurança. No entanto, em se tratando de meios intelectuais, podem haver falhas no sistema de segurança, chegando a vazar informações pessoais daqueles que, porventura, confiaram no próprio site a segurança de seus dados.

Tais vulnerabilidades, também conhecidas como *data breach* ou roubo de dados possuem suas particularidades, que variam de acordo com os objetivos de cada indivíduo em relação à gravidade da violação, que, segundo o site especializado em tecnologia "*Compugraf*" são:

- Pesquisa: o agente procura os pontos vulneráveis no tocante à segurança do site;
- Ataque: o agente inicia utilizando um vetor de ataque;
- Extração: após possuir o acesso ao sistema, ele consegue atacar a rede e abrir caminho até os dados confidenciais empresariais.

Deste modo, é possível observar que *hackers* estudam primeiramente as vítimas, neste caso os consumidores de *e-commerce,* para saber onde e como atacar, por isso há a necessidade de uma grande estrutura de segurança no tocante ao armazenamento de dados.

Grandes empresas já tiveram seus bancos de dados vazados, sendo uma delas a *Netshoes* – empresa no ramo esportivo -, o que resultou na divulgação de dados não bancários específicos de alguns clientes.

Em outro caso, julgado pelo Tribunal de Justiça de São Paulo, a empresa foi condenada a pagar multa de R$2.000,00 (dois mil reais), a título de danos morais, à cliente que teve seus dados expostos, devido a uma falha de segurança. Em síntese, o cliente adquiriu um produto por meio da loja online Sodimac e horas após recebeu

um alerta de terceiro desconhecido, via rede social "*WhatsApp*", relatando que seus dados estavam expostos na internet abertamente, inclusive os de seu cartão de crédito, sendo tal informação comprovada por meio de *prints* de tela.

Tomando ciência do ocorrido, o cliente alterou suas credenciais no site, registrou boletim de ocorrência e após diversas tentativas de contato, o caso só conseguiu ser relatado 3 dias depois a um funcionário da loja. Assim, conforme o desembargador Renato Sartorelli, relator do recurso de apelação, a ré não justificou de forma plausível na contestação o supracitado evento, sendo esta responsável por responder por dano recorrente de falha de segurança.

Mesmo a LGPD tendo um alcance que vai além do *e-commerce*, sem sombra de dúvidas, é nesse ambiente de compras digitais que a lei nacional tem um terreno muito fértil quanto à sua aplicação (SILVA, 2022).

Com evidência, clara a necessidade das empresas de *e-commerce* se voltarem não somente para o "resguardo" dos dados pessoais dos clientes, mas para toda a segurança cibernética em si, tendo em vista que em casos como estes, a empresa sofre danos à reputação da marca, furto de propriedade intelectual, cibervandalismo e queda nos lucros, segundo a empresa de segurança americana "*THE AME group*".

2.4.4 Adequações realizadas pelas empresas de e-commerce

Para que uma empresa possa implementar as novas regras da LGPD é necessário criar políticas de proteção de dados, do qual devem ser informadas aos usuários pelas companhias com o objetivo de esclarecer a este como serão capturados seus dados pessoais e a finalidade para tal.

Dentre tais políticas destacam-se: o reconhecimento das fontes de coletas de dados usadas pelas empresas; o ciclo de vida destes, bem como a confecção do relatório de impacto elaborado pelo controlador de dados, além de treinamentos para toda equipe técnica responsável pelo tratamento de dados.

A empresa que atua no ramo do *e-commerce,* para estar em conformidade com a nova lei, é imprescindível realizar o tratamento de forma correta, protegendo o seu usuário. Deste modo, ao coletar os dados, a organização deve conhecer os princípios que regem

a LGPD (WILLRICH, 2020). Embora, a referida lei tenha sido aprovada no ano de 2018, muitas empresas ainda estão se adaptando a LGPD quanto as exigências no tratamento dos dados, ainda no ano de 2022.

Em pesquisa realizada pelo Fórum empresarial a LGPD no ano de 2021 em parceria com a ABES (Associação brasileira de empresas e *Software*), verificou-se que 94,33% das empresas consultadas iniciaram a adequação à LGPD. Entretanto, 40,44% destas ainda não concluíram o mapeamento de dados pessoais, com identificação das categorias de titulares de dados, finalidade e bases legais para as operações de tratamento, armazenamento e compartilhamento de dados pessoais.

Dentre aquelas, apenas 36,07% das empresas conseguiram concluir a implementação e conclusão das adequações no primeiro semestre de 2022, enquanto 21,86% do total consultado de empresas que iniciaram a adequação disseram que a adaptação completa seria feita até o final do ano de 2021, o que não ocorreu.

A pesquisa revela ainda que a principal dificuldade relatada pelas empresas na gestão de um programa de privacidade e proteção de dados é a organização cultural sobre o tema, a escassez orçamentária e de pessoal para a nova implementação, pois não se considera que as novas técnicas sejam acessíveis a todas as empresas, inclusive as pequenas e médias empresas.

Imperioso observar que há uma constante preocupação das organizações quanto à adequação de pequenas e médias empresas devido as elevadas despesas da transição, o que pode tornar inviável a adequação destas organizações (TANNUS *et. al* (2021).

Isso ocorre porque diversas são as ferramentas aptas a serem utilizadas no projeto de adequação à LGPD, dentre as quais Rodrigues Tristão *et.al* (2021) menciona que se deve debater com os gestores dessas empresas, equipe de tecnologia da informação e os responsáveis pela segurança da informação para que adotem medidas que venham atender as necessidades de forma eficaz, sejam com soluções pagas ou *softwares open source*.

O primeiro desafio nas empresas pequenas está relacionado a montar o processo de implementação institucional da LGPD. Empresas pequenas normalmente tem uma estrutura gerencial familiar, no qual a tomada de decisões pode sofrer influência pessoal e não institucional (CARDOSO, 2022).

Além disso, Cardoso (2022) entende que por mais dificultoso que seja implementar estes procedimentos, as empresas de pequeno porte possuem capacidade de desempenhá-las. O enfrentamento do fluxo de caixa e a necessidade de um profissional a ser contratado, mesmo que gere uma despesa circunstancial, pode ser administrada e gerada dentro da própria empresa.

Outra inovação trazida pela LGPD e que são necessárias para implantação nas empresas, é a nomeação dos agentes de tratamento. Estes serão responsáveis pelo tratamento de dados pessoais, quais sejam: controlador, operador e o encarregado dos dados, que estão descritos no art. 5°, da LGPD. Vejamos:

> VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
>
> VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
>
> VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD) (BRASIL, 2018).

A lei prevê e determina que existam encarregados na proteção de dados pessoais nas organizações, estes são denominados pela GDPR como DPO (Data Protection Officer), onde suas funções são estabelecidas no art. 41 da LGPD, podendo a ANPD complementar suas atribuições.

Willrich (2020) dispõe que o controlador e o operador devem pensar em regras e meios técnicos para proteger os dados pessoais e comprovar sua efetividade nas empresas de e-commerce, seja por aplicação de recursos de anonimização, controle de acesso, procedimentos, política de gestão e treinamentos para equipes.

A gestão de dados impacta diretamente no cumprimento da LGPD, tendo em vista que existem procedimentos que devem ser observados para que se possa assegurar a proteção de dados pessoais e sensíveis, assim como o acesso à informação (CARDOSO, 2022). Portanto, é fundamental que as empresas corporativas visem implementar os sistemas no tratamento de dados, buscando estruturá-los de modo a atender requisitos de segurança, padrões de boas práticas e de governança, bem como aos princípios previstos na LGPD e demais normas regulamentares, conforme determina o art. 49 da norma.

2.4.5. Principais repercussões jurídicas da implantação da LGPD nos últimos anos

A Lei 13.709 entrou em vigor relativo no dia 28 de dezembro de 2018 quanto ao seu aspecto administrativo em relação à Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade. Ao passo que quanto às sanções administrativas apenas entraram em vigor na data de 1° de agosto de 2021. Nesse meio tempo diversos casos já foram ajuizados sob sua vigência, sendo que as suas principais disposições de aplicação no plano prático já começaram a ser delineadas pelo Judiciário.

Segundo a pesquisa da Surfshark, 24,19 milhões de brasileiros tiveram suas informações expostas na internet através de ataques cibernéticos ou falhas em sistemas de segurança entre janeiro a novembro de 2021, estando o Brasil no 6º lugar na lista de países com mais vazamentos anuais de dados.

De acordo com estudo realizado por Paiva (2022), disponível no sítio jurídico JOTA, no ano de 2021 houveram pelo menos 465 decisões acerca do tema, à medida que 77% dessas não resultaram em condenações, tendo sido julgadas improcedentes ou extintas.

Conforme o levantamento realizado por Blum *et al.* (2022), especializado em Direito Digital, os julgamentos de improcedência baseiam-se na demonstração da realização de diligências básicas pelas empresas.

Todavia, nos casos de condenações, as sanções impostas giraram no entorno de R$ 600,00 (seiscentos reais) a R$100.000,00 (cem mil reais), frequentemente

cominadas com obrigações a serem realizadas pelas pessoas jurídicas, tendo o dever de indenização representado tão somente 47% do total das condenações, o qual foi acompanhado da necessidade de efetiva comprovação da lesão sofrida, bem como constituindo um fator de destaque o fato de não ter havido a presunção automática do dever de pagamento de danos morais pelas empresas rés.

Entre as obrigações impostas estão a adoção de boas práticas e governança, como a nomeação de um encarregado para atuar como um meio de comunicação entre o controlador, os titulares dos dados pessoais e a ANPD, o dever de maior transparência e a determinação de exibição de documentos que demonstrem a adoção de medidas de segurança e sigilo de dados.

Com efeito, ao julgar a Ação Direta de Inconstitucionalidade no 6649 e a Arguição de Descumprimento de Preceito Fundamental no 695, o Supremo Tribunal Federal (STF), por maioria de votos, estabeleceu entendimento na direção da possibilidade que órgãos e entidades da administração pública federal compartilhem dados pessoais entre si, todavia devem observar critérios objetivos em se tratando de informações indispensáveis à garantia do interesse público.

Entre os parâmetros a serem observados encontram-se a limitação ao mínimo necessário para atendimento da finalidade a qual foi requerida, o cumprimento integral dos requisitos, garantias e procedimentos estabelecidos na LGPD consonantes com a esfera pública.

Em caso de descumprimento, o Estado responderá objetivamente pelos danos causados às pessoas. Havendo dolo ou culpa, a administração pública poderá mover ação de regresso contra o servidor responsável pela violação, ao passo que o funcionário que dolosamente violar o dever de publicidade estabelecido no artigo 23, I, da LGPD responderá por ato de improbidade administrativa.

3 CONSIDERAÇÕES FINAIS

Conforme expresso ao longo do presente artigo, as comodidades que o comércio eletrônico fornece são ilimitadas e já é uma realidade desfrutada pela sociedade

consumerista, que coloca o Brasil como um dos cinco países com maior quantidade de internautas.

Observando a notoriedade do consumo pelas plataformas virtuais, nasce para o consumidor maior segurança nessas atividades, trazendo maior proteção, pois anteriormente não existiam leis que assegurassem a responsabilidade quando diziam respeito ao vazamento de dados pessoais de forma especifica.

Através da LGPD, é perceptível que qualquer forma de proteção ao consumidor é atrativa. Entretanto, a proteção e responsabilidade dos agentes responsáveis ainda estão vagarosamente caminhando. Empresas ainda estão em processo de aplicação e adequação. Com relação ao judiciário, percebe-se que em casos de vazamento de dados, processos ainda são julgados não conforme a nova lei especifica, mas ainda utilizando, como instrumento legal, o Código Civil e Código do Consumidor.

Observa-se, assim, ainda haver a necessidade de uma maior adequação por parte das empresas aos parâmetros estabelecidos pela LGPD, pois muitas iniciaram, mas ainda não concluíram o processo de compatibilização às novas práticas. Como consequência, surgiu um aumento de demanda do setor de Tecnologia de Informação (TI), haja vista a carência de aperfeiçoamento dos sistemas de segurança responsáveis por guardar e proteger os dados dos usuários, fato que contribuiu mais ainda ao crescimento do referido setor diante da vulnerabilidade digital das empresas não só de *e-commerce*, mas de todas que lidam com quaisquer operações de comunicação de informações e dados.

Pelo exposto, conclui-se que a proteção de dados pessoais consolidada pela LGPD e também na Carta Maior, através da EC n° 115/2022 evidencia que o tema, anteriormente tratado de forma subsidiária em leis anteriores, possui um papel fundamental nas relações de consumo pelo comércio eletrônico. O Brasil ainda tem muito o que avançar neste aspecto, tendo em vista a recorrência de vazamentos de dados pessoais de consumidores de *e-commerce*. Todavia, mudanças e adequações são realizadas gradualmente, uma vez que muitas empresas, em especial as micro e pequenas empresas, não estão habituadas com as inovações exigidas pela nova lei.

REFERÊNCIAS

ALMEIDA, Ursula Ribeiro. A proteção de dados pessoais na Constituição: o impacto da EC 115. *Revista Consultor Jurídico*, 27 fev. 2022. Disponível em: https://www.conjur.com.br/2022-fev-27/almeida-protecao-dados-pessoais-constituicao-ec-115. Acesso em: 11/04/2022.

BBC, News, Brasil. Uso político de dados. 2018. Disponível em: https://www.bbc.com/portuguese/internacional-43461751. Acesso em: 03 maio 2022.

BITTAR, Eduardo C. B. *Metodologia da pesquisa jurídica*: teoria e prática da monografia para cursos de direito. 12 ed. São Paulo: Saraiva, 2014.

BLUM, José Roberto Opice et al. LGPD Lookout: Relatório Anual de Jurimetria 2021. 24 jan. 2022. Apresentação do Power Point. Disponível em: https://images.jota.info/wp-content/uploads/2022/01/relatacc83c2b3rio-anual-jurimetria-24-01-versacc83o-final.pdf. Acesso em: 15.08.2022.

BRASIL. Brasil está entre os cinco países do mundo que mais usam internet. *GOV.BR,* 26 abr. 2021. Disponível em: https://www.gov.br/pt-br/noticias/transito-e-transportes/2021/04/brasil-esta-entre-os-cinco-paises-do-mundo-que-mais-usam-internet. Acesso em: 21 maio 22.

BRASIL. Emenda Constitucional nº 115, de 10 de fevereiro de 2022. Constituição Federal de 1988. Brasília, DF: Presidência da República, 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 10 out. 2022.

BRASIL. Lei n° 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: L13709 (planalto.gov.br). Acesso em: 19 out. 2022.

BRASIL. Supremo Tribunal Federal (1ª Turma). Ação Direta de Inconstitucionalidade nº 6387. Medida Provisória nº 954/2020. Compartilhamento de dados dos usuários do serviço telefônico fixo comutado e do serviço móvel pessoal, pelas empresas prestadoras, com o instituto brasileiro de geografia e estatística. fumus boni juris. periculum in mora. Deferimento. Requerente: Conselho Federal da Ordem dos Advogados do Brasil – CFOAB. Requerido: Presidente da República. Relatora: Min. Rosa Weber, 07 de maio de 2020. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357629. Acesso em: 11 abr. 2022.

BRUNO, Gilberto Marques. As relações do "business to consumer" (B2C) no âmbito do "e-commerce". *Revista Jus Navigandi*, , Teresina, v. 6, n. 52, 1 nov. 2001. Disponível em: https://jus.com.br/artigos/2319. Acesso em: 21 maio 2022.

CARDOSO, Rafaella Ranniele Cândido. LGPD-Lei Geral De Proteção De Dados: o desafio do micro empreendedor individual, das micro e pequenas empresas quanto ao seu custo, adequação e implementação. 2022. Disponível em: https://dspace.uniceplac.edu.br/handle/123456789/1689. Acesso em 19 out. 2022

COMPUGRAF. Os riscos de um vazamento de dados na era da LGPD. Disponível em: https://www.compugraf.com.br/os-riscos-de-um-vazamento-de-dados-na-era-da-lgpd/#4gbev. Acesso em: 04 out. 2022

CORACCINI, Raphael. Fotos e até salários estão entre os dados vazados de 223 milhões de brasileiros. CNN BRASIL, 2021. Disponível em: https://www.cnnbrasil.com.br/business/fotos-e-ate-salarios-estao-entre-os-dados-vazados-de-223-milhoes-de-brasileiros/. Acesso em: 04 maio 22.

DATA BREACH STATISTICS BY COUNTRY IN 2021. Surfshark: 2022. Disponível em: https://surfshark.com/blog/data-breach-statistics-by-country-in-2021. Acesso em: 10 ago. 2022.

FÓRUM LGPD. ABES (Associação Brasileira das empresas de software) 2021.Pesquisa: Panorama de proteção de dados pessoais no Brasil. Disponível em: https://abessoftware.com.br/forumlgpd/. Acesso em 14 out. 2022.

FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais: noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. *Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro*. São Paulo: Thomson Reuters Brasil, 2019. p. 23-52.

GARCIA, Lara R. Lei Geral de Proteção de Dados (LGPD): guia de implantação. São Paulo: Blucher, 2020. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555060164/. Acesso em: 04 maio 2022.

JESUS, Damásio Evangelista D.; OLIVEIRA, José Antônio M. Milagre D. *Marco Civil da Internet: comentários à Lei n. 12.965, de 23 de abril de 2014*. São Paulo: Saraiva, 2014. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502203200/. Acesso em: 03 maio 2022.

LIMA, Ana Paula Moraes Canto de et al. *LGPD aplicada*. São Paulo: Atlas, 2021. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788597026931/. Acesso em: 20 abr. 2022.

MORAES, Frederico Santos Lopes de; ANDRADE, Thais Barbosa; MAIRINK, Carlos Henrique Passos. O comércio eletrônico e as formas alternativas de resolução de conflitos no código de defesa do consumidor sob a ótica da responsabilidade civil dos sites de intermediação. *LIBERTAS: Rev. Ciênci. Soc. Apl.*, Belo Horizonte, v. 11, n.

2, p. 50-93, ago./dez. 2021. Disponível em: http://famigvirtual.com.br/famig-libertas/index.php/libertas/article/view/306. Acesso em: 02 nov. 2022.

PAIVA, Letícia. LGPD: 77% das decisões que citam lei não resultaram em condenação em 2021. *JOTA - São Paulo.* 27 de janeiro de 2022. Disponível em: https://www.jota.info/justica/lgpd-condenacao-77-das-decisoes-nao-27012022. Acesso em: 14 ago. 2022.

PESTANA, Marcio. *Direito Administrativo Brasileiro*. 4. ed. São Paulo: Atlas, 2014.

RODAS, Sérgio; KAMINSKI, Omar. Constitucionalização da proteção de dados é marco e aumenta segurança jurídica. *Revista Consultor Jurídico*, 11 fev. 2022. Disponível em: https://www.conjur.com.br/2022-fev-11/constituciona lizacao-protecao-dados-marco-aumenta-seguranca. Acesso em: 12 abr. 2022.

RODRIGUES TRISTÃO, G.; CAMARGO FIRMINO, M.; AMADO KOZARA, P.; LOPES MOREIRA, W.; ARATA, E. Lei Geral de Proteção de Dados: desafios técnicos enfrentados por microempresas e empresas de pequeno porte. *FatecSeg - Congresso de Segurança da Informação,* [S. l.], v. 1, 2021. Disponível em: https://www.fatecourinhos.edu.br/fatecseg/index.php/fatecseg/article/view/4. Acesso em: 16 out. 2022.

SARLET, Ingo Wolfgang. A EC 115/22 e a proteção de dados pessoais como Direito Fundamental. *Revista Consultor Jurídico*, 11 mar. 2022. Disponível em: https://www.conjur.com.br/2022-mar-11/direitos-fundamentais-ec-11522-protecao-dados-pessoais-direito-fundamental. Acesso em: 11/04/2022.

SILVA, João Pedro Tolentino da. A LGPD como meio de responsabilização nos casos de vazamento de dados pessoais pelas empresas de e-commerce. 2022. Disponível em: https://repositorio.animaeducacao.com.br/handle/ANIMA/23526. Acesso em: 28 set. 2022.

TAMBOSI, Paulo Vitor Petris et al. Responsabilidade civil pelo tratamento de dados pessoais conforme a Lei Geral de Proteção de Dados (LGPD): subjetiva ou objetiva? 2021. Disponível em: https://repositorio.ufsc.br/handle/123456789/223444. Acesso em: 30 mar. 2022.

TANNUS, ALEXANDRE MORAES et al. Segurança da Informação de Pequenas e Médias Empresas conforme a Lei Geral de Proteção de Dados N° 13.709. 2021. Disponível em: http://repositorio.aee.edu.br/bitstream/aee/19661/1/Entrega%2005.pdf. Acesso em: 28 set. 2022.

TEIXEIRA, Tarcísio. *LGPD e E-commerce*. 2. ed. São Paulo: Saraiva Educação, 2021. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786555598155/. Acesso em: 12 abr. 2022.

THE AME GROUP. Data Security Breach: 5 Consequences for Your Business. Disponível em: https://www.theamegroup.com/security-breach/#. Acesso em: 04 out. 2022.

TIME BL CONSULTORIA. TJ-SP condena empresa e aplica multa com base na LGPD Disponível em: https://blconsultoriadigital.com.br/multa-com-base-na-lgpd/#:~:text=Em%20julgado%20proferido%20pela%2026%C2%AA,seguran%C3%A7a%E2%80%9D%20e%20gera%20dano%20moral Acesso em: 04 out. 2022.

VIGLIAR, José Marcelo M. LGPD e a proteção de dados pessoais na sociedade em rede. Grupo Almedina (Portugal), 2022. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786556276373/. Acesso em: 16 nov. 2022.

WILLRICH, Adolfo Chávez. Comércio eletrônico e a regulamentação da lei geral de proteção de dados. *Direito-Florianópolis*, 2020. Disponível em: https://repositorio.animaeducacao.com.br/handle/ANIMA/7329. Acesso em: 28 set. 2022.