

## 1 INTRODUÇÃO

A sociedade atual é permeada por transformações no âmbito digital e tecnológico, com alterações nas formas como as informações são captadas e compartilhadas. De maneira associativa, a tecnologia proporciona para as pessoas a construção de relações, o desenvolvimento de conhecimentos e oportuniza comodidades cotidianas, além de novos meios de efetivar o comércio, consubstanciando a chamada sociedade da informação, que tece todo esse emaranhado inovacional.

Os dados e as informações sempre tiverem relevância, mas nos meios digitais passaram a ser vistos com mais atenção, diante da dinâmica desenfreada no qual os mesmos são inseridos nesses sistemas eletrônicos, seguindo para as formas em que são manejados, tratados, armazenados, compartilhados, que podem resultar em afronta aos direitos das pessoas. Tendo em vista, que a tecnologia vem se instaurando cada vez mais no âmbito social e no cotidiano das pessoas, há como decorrência a vulnerabilidade tanto dos dispositivos e sistemas conectados à internet como dos usuários, em virtude de haver potencial risco de exposição de informações e cibercrimes.

Ademais, o *e-commerce* tornou-se mais aparente e usual, porém nem todas as empresas tratam os dados com segurança e atenção, resultando em preocupação para com os titulares no que tange ao que está sendo realizado a partir das suas informações pessoais, além disso, tais manejos irregulares também podem causar afronta aos direitos humanos e fundamentais. Dessa forma, a proteção de dados, esta por sua vez, não se resume e nem se limita a apenas aos dados, abarca-se esses direitos mencionados dos titulares quando estes são violados, ou seja, quando se atinge às liberdades individuais, privacidade, personalidade, entre outros. Então, a LGPD reflete expressivamente no âmbito social e digital, sendo necessário que tal regramento seja aplicado adequadamente, caso contrário haverá o ensejo de responsabilização da empresa, aos operadores e controladores de dados.

O artigo tem por objetivo problematizar sobre as implicações causadas pela Lei Geral de Proteção de Dados no exercício do *e-commerce*, com análise da responsabilidade das empresas frente aos possíveis vazamentos de dados.

A temática se justifica pela atualidade, relevância social e importância da LGPD e da responsabilidade das empresas no atual contexto nacional e internacional.

A pesquisa utiliza-se do método analítico com base bibliográfica e da legislação.

O desenvolvimento temático foi subdividido de modo a inserir a abordagem de conteúdos versando sobre os aspectos gerais da proteção de dados, implicações da LGPD para o *e-commerce*, responsabilidade das empresas e considerações finais.

## **2 ASPECTOS GERAIS SOBRE A PROTEÇÃO DE DADOS**

A internet adentrou ao âmbito social mundial no ano de 1970, e com isso, gerou modificações nos mais diversos âmbitos sociais, renovando as maneiras de se obter informações e estas, por conseguinte passaram a serem inseridas acentuadamente nas plataformas digitais e conseqüentemente muitas vezes são compartilhadas sem o conhecimento e a autorização do titular. Ainda, essa conectividade promove que variadas associações sociais interagem, originando um novo modelo de se relacionar entre as pessoas, governos, empresas, entre outros, o que fomenta o alcance para qualquer lugar do mundo, sem quaisquer barreiras ou impedimentos. Dessa forma, além da modificação das formas de se originar a conexão interpessoal, também tal, atingiu as esferas econômicas, de comércio, consumo, entre outros, que por conta da tecnologia, fora abarcada outras características que afetam o contexto mundial (DE FAZIO, 2012, p. 77; MARINELLI, 2019, 19).

A partir destas transformações e da conectividade originada, a sociedade passou a ser conhecida como “sociedade da informação”, que para Bioni (2020, p. 5) se refere às informações elencadas no contexto social, e são estas que contribuem para a constituição da sociedade. Em complemento, Marinelli (2019, p. 27) argumenta que com o desenvolvimento das tecnologias como por exemplo, nas formas de comunicação e obtenção informacional, houve a redefinição da sociedade, ou seja, o cenário é representado por uma permanente conexão. Sendo que a informação passou a ser cada vez mais, o centro principal que se movimenta em todos os campos sociais interligados à tecnologia.

Nesse cenário, foram pensadas e criadas diversas legislações que tratam especificamente sobre o tema proteção de dados ou que os abordam em seu rol de forma pormenorizada, como por exemplo, o Marco Civil da Internet, o Código de Defesa do Consumidor, o Código Civil, entre outras. Além disso, há o Decreto n. 7.962/2013 que dispõe de normatizações específicas sobre o *e-commerce* no que tange a sua utilização.

Para tanto, referente às normatizações comentadas sobre proteção de dados, buscou-se por um sistema de regramentos que seja apto a proteger não só as tecnologias e regulamentá-las, mas também que estabeleça diretrizes de funcionamento e meios eficazes de sanar os usos desregulares, protegendo, por conseguinte os direitos fundamentais e humanos

além dos próprios dados das pessoas. Nisto, criou-se a Lei Geral de Proteção de Dados que passou a vigorar no ano de 2018, se tornando um marco importante para o direito brasileiro no que tange a temática, em virtude de seu caráter inovador e diferenciados, a qual obteve influência da legislação europeia denominada *General Data Protection Regulation* (GDPR).

Diante do foco do presente escrito, a abordagem se limita às normatizações previstas na LGPD, que tem o viés de dispor “[...] 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<sup>1</sup>”. Assim, cumpre salientar que a mesma, possui um rol de fundamentos e princípios que abarcam os direitos dos sujeitos; é delineado sobre o consentimento e autodeterminação dos dados; é esclarecido as peculiaridades dos variados tipos de dados bem como sua respectiva asseguarção; comenta-se sobre a responsabilidade; e assim por diante (BRASIL, 2018).

Nota-se que a tecnologia passa por constantes transmutações, com interesses principais ligados à informação, sendo aparente em variados setores, como no âmbito trabalhista, na educação, na economia e assim por diante, por isso, cabe-nos conceituar alguns pontos essenciais sobre dados para o entendimento da temática. Então, após a inserção na internet com mais assiduidade, houve um alargamento de índices informacionais e de dados colocados nas redes. Assim, o dado nada mais é que a origem da informação por assim dizer, são episódios primitivos que geram o saber a partir do momento em que são estruturados. Nesse sentido, os dados e suas informações estão relacionados aos sujeitos, de maneira específica e pormenorizada, que revelam por exemplo, questões ligadas às suas ações, suas características, peculiaridades referentes ao íntimo, à economia, ao consumo, entre outros (BIONI, 2020, p. 31-32; DONEDA, 2011, p. 93).

Quanto ao dado pessoal, este é a “informação relacionada a pessoa natural identificada ou identificável<sup>2</sup>”, cita-se como exemplo, o nome, endereço residencial ou eletrônico, localização, perfil de compras, número do Internet Protocol (IP), dentre outros, os quais referem-se a distinção de uma pessoa; os dados pessoais sensíveis são um “dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biomédico, quando vinculado a uma pessoa natural<sup>3</sup>”; e os dados

---

<sup>1</sup> Art. 1º, caput da Lei n. 13.709/18;

<sup>2</sup> Art. 5º, I da Lei n. 13.709/18;

<sup>3</sup> Art. 5º, II da Lei n. 13.709/18.

anonimizados são um “dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento<sup>4</sup>”. Após a captação dessas informações, de maneira digital, são criados os bancos de dados que se referem como:

[...] não são somente um agrupamento lógico e inter-relacionado do estado primitivo da informação, mas são, também, um ferramental que deve tomar uma interface para quem o manipula analisar e descobrir informações para tomada de decisões (BIONI. 2020, p. 34).

Quanto aos fundamentos<sup>5</sup> abordados na LGPD, a proteção de dados será consubstanciada quando se é visado à privacidade; à autodeterminação informativa; as liberdades relacionadas a expressão, informação, opinião e comunicação; que não haja violações à intimidade, honra e imagem, assim como a preservação dos direitos humanos, entre outros.

Também o tratamento de dados precisa ser acatado em todo trajeto perpassado pelos dados neste contexto, atentando-se assim, aos princípios<sup>6</sup> previstos na LGPD, o primeiro deles é o da boa-fé; também, haverá o princípio da finalidade, ou seja, que haja a determinação de intuito claro, específico e de conhecimento do titular; o princípio da adequação, estabelece que o tratamento seja realizado apropriadamente e que as finalidades sejam repassadas ao titular; o princípio da necessidade pressupõe que o tratamento precisa ser essencial e utilizar apenas os dados pertinentes; sobre o princípio do livre acesso, os titulares deverão ter liberdade para verificar o que está sendo realizado no tratamento e aos seus dados; e o princípio da qualidade dos dados, significa dizer, que essas informações precisam ser atualizadas.

Em continuidade aos princípios, tudo que envolve o tratamento, inclusive os envolvidos, deverão ser apresentados de maneira clara ao titular, ou seja, se alinhando ao princípio da transparência; ademais, o princípio da segurança determina que os procedimentos realizados terão que se atentar a seguridade, aplicando critérios técnicos e administrativos para proteger os dados nos casos de acessos de terceiros não autorizados ou demais circunstâncias que puderem ensejar riscos as informações; já o princípio da prevenção, diz respeito a estabelecer maneiras que poderão prevenir situações danosas; quanto ao princípio da não discriminação, se resume em que o tratamento não poderá possuir teor discriminatório;

---

<sup>4</sup> Art. 5º, III da Lei n. 13.709/18;

<sup>5</sup> Art. 2º da Lei n. 13.709/18;

<sup>6</sup> Art. 6º da Lei n. 13.709/18.

e por fim, o princípio da responsabilização e prestação de contas, é o papel do agente em cumprir com os regramentos protetivos de dados.

Ainda, outro ponto importante trazido pela LGPD que contribui para a consubstanciação da proteção de dados, isso inclusive no âmbito do *e-commerce* é o instituto do consentimento, este sucede duas conjecturas. Inicialmente, o consentimento é a representação da autodeterminação. Posteriormente, o consentimento serve como instrumento de legitimação de informações que podem ser ou que foram vazadas. Então em resumo, o consentimento é a manifestação expressa da vontade do titular em relação à disposição, aplicação, tratamento e compartilhamento de seus dados, podendo este consentimento ser revogado a qualquer momento (DONEDA, 2019, 293-296; 302-303).

O tratamento que for empregado aos dados das pessoas precisa seguir os preceitos elencados no rol da LGPD, então os agentes de tratamento precisaram inserir “medidas de segurança, técnicas e administrativas para a proteção de dados pessoais quanto a acessos não autorizados [...] e a situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito”. (TEIXEIRA, 2021b, p. 94).

A LGPD também aborda sobre a Autoridade Nacional de Proteção de Dados Pessoais (ANPD), que é “uma autarquia de natureza especial, vinculada ao Ministério da Justiça e Segurança Pública, responsável por zelar pela proteção de dados pessoais e por regulamentar, implementar e fiscalizar o cumprimento da LGPD no Brasil”. Então basicamente a ANPD tem o intuito de supervisionar para que as empresas por exemplo, adaptem seus regimentos seguindo os preceitos da proteção de dados e efetivamente os aplique nas relações, garantindo maior seguridade tanto para a empresa quanto para as pessoas correlacionadas (MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA, 2021, n.p.).

Com a captação e armazenamento contínuo de dados pessoais pelas empresas, bem como diante da aplicabilidade destas informações que muitas vezes é desconhecida pelo titular, ou até mesmo quando estes dados são compartilhados para locais diversos aos consentido inicialmente, gera por conseguinte o ferimento de direitos inerentes e pessoais, isso porque, os dados representam um desdobramento destes direitos, necessitando de um respectivo anteparo jurídico, em prol de promover a liberdade e a igualdade (MENDES, 2014, p. 33).

Com isso, percebe-se que os dados atualmente são aplicados em diversas áreas, inclusive no âmbito do *e-commerce*. Conseqüentemente para a utilização pelas empresas das informações pessoais, é necessário visar a proteção de dados a fim de evitar vazamentos e compartilhamentos indevidos, que são capazes de gerar afronta aos direitos humanos dos titulares, sendo importante seguir alguns pontos, como os fundamentos e princípios previstos na LGPD assim como o consentimento do titular, tornando a prática do comércio digital mais segura e lucrativa tanto para a empresa como para os consumidores.

### **3 IMPLICAÇÕES CAUSADAS PELA LGPD NO ÂMBITO DO E-COMMERCE**

A partir da inserção da internet no contexto mundial, além do avanço da tecnologia, as relações comerciais passaram a serem realizadas por diferentes formas, incluindo através dos meios digitais, originando o e-commerce. Nesse novo cenário, os dados e as informações se tornaram cada vez mais importantes, visto que estes são adicionados na internet por meio dos apetrechos eletrônicos, sendo o procedimento realizado pelo titular ou através de cadastros em sites por exemplo, com isso, podem se tornar visíveis e utilizáveis por terceiros, ou seja, a partir do momento pelo qual o titular cede suas informações para obter uma vantagem ou uma possibilidade de seu interesse, seus dados depois de apanhados podem ser compartilhados de maneira não consentida, em outras palavras, quando os dados são colocados na rede, são manuseados e visualizados por muitas pessoas.

Conforme Bioni (2020, p. 16), “cada vez mais, os usuários da Internet subvertem-se em consumidores”, complementa-se tal afirmação a partir de notícias retratadas no ano de 2023, a qual destaca que o comércio eletrônico realizado a partir da internet está em crescente avanço, e vem estando em ascensão desde o ano de 2020 até os dias de hoje (DINO, 2023, n.p.). Importante conceituar o que seria o *e-commerce* (comércio eletrônico) conforme Teixeira (2021b, p. 11):

[...] é uma extensão do comércio convencional [...], tratando-se de um ambiente digital em que as operações de troca, compra e venda e prestação de serviço ocorrem com suporte de equipamentos e programas de informática, por meio dos quais se possibilita realizar a negociação, a conclusão e até a execução do contrato [...].

Cumprе salientar, que na atualidade, as grandes empresas através do sistema de *e-commerce* passaram a obter lucros através desse sistema de dados. Uma das formas de captura de dados, é pelas próprias pessoas, quando estas os concedem voluntariamente, originando então os denominados perfis de consumo, e com estes é possível analisar as tendências de mercado e identificar os gostos, assim conduzindo os seus produtos a essas

pessoas de forma certa. Além disso, é estimado diversas coisas, como os horários, as movimentações financeiras e assim por diante, que impulsionam os sistemas de compra e venda pelos meios digitais (MOROZOV, 2018, p. 165; SILVEIRA, 2017, p. 16).

Ainda, com o mesmo intuito acima comentado, outro método utilizado para a obtenção de dados é por meio da atribuição da inteligência artificial e procedimentos tecnológicos o qual possibilita averiguar os comportamentos pessoais realizados através de computadores, celulares e demais dispositivos conectados à internet, processo esse celebrado por interceptações, suscitando na extração de dados e informações por meio das “pegadas digitais<sup>7</sup>, dos *cookies*<sup>8</sup>, pixels<sup>9</sup> [...], mas também de processamento e análise dos dados captados e cruzados com outras bases de dados [...]” (SILVEIRA, 2017, p. 43). Em suma, o comércio eletrônico pode ser visto como uma ampliação no modo de difundir e anunciar o comércio de bens e serviços através da efetivação do negócio de maneira digital e à distância (TEIXEIRA, 2021b, p. 13).

Cabe salientar, que no caso do *e-commerce*, independente da forma de obtenção de dados, seja através da disposição pelo próprio titular ou da aplicação de métodos tecnológicos, haverá benefícios para ambas as partes. Ou seja, no primeiro caso, ao informar seus dados, o titular tem essa ação com o intuito de obter bens e serviços através das plataformas digitais no comércio eletrônico. Já no segundo caso, as empresas captam os dados quando as pessoas adentram nos sites, e-mails e demais portais relacionados a empresa em si ou ao seus associados, com o intuito de personalizar o conteúdo que chegará a cada pessoa de forma específica e direcionada com base nas informações deixadas através de seus buscadores, conseqüentemente gerando interesse das pessoas para com os produtos e serviços ofertados pela empresa e posteriormente há grandes possibilidades de ser consubstanciado a compra por exemplo.

Dito isso, compreende-se que as tecnologias possuem o condão de transformar as informações em um meio de gerar capital financeiro. Como o próprio titular dispõe de seus dados de forma livre em variados ambientes, e posteriormente após essa coleta, os dados são guardados e esquecidos, tornando difícil a proteção dos mesmos. Com a entrega

---

<sup>7</sup> Pegada Digital: “[...] às vezes chamada de sombra digital ou pegada eletrônica, refere-se ao rastro de dados que você deixa ao usar a Internet. Inclui sites que você visita, e-mails que você envia e informações que você envia online. Uma pegada digital pode ser usada para rastrear as atividades e os dispositivos online de uma pessoa” (KASPERSKY, c2023, online);

<sup>8</sup> *Cookies*: “são pequenos textos enviados ao navegador por um site que você acessa. Eles ajudam o site a se lembrar de informações sobre a visita, o que pode facilitar o próximo acesso e deixar o site mais útil [...]” (PRIVACIDADE & TERMOS, s.d, n.p.);

<sup>9</sup> Pixels: são “pequenos arquivos que permitem identificar os computadores nas redes” (SILVEIRA, 2017, p. 43).

despretensiosa dos dados pessoais, favorece um meio de controle, ou seja, as condutas das pessoas, bem como o encaminhamento de conteúdos variados, se tornam bem determinados e deliberados pelos controladores, por meio da verificação dos gostos, das inclinações, dos desejos dos usuários (LIMBERGER, 2008, p. 139-140).

Quanto ao *e-commerce*, este por sua vez perpassa pelas execuções realizadas em aparelhos eletrônicos e por meio da internet (PINHEIRO, 2021 p. 52). O comércio eletrônico está avançando constantemente, com isso, os acessantes da internet estão se transformando em consumidores. Dessa forma, a ciência do marketing verificou que a internet pode oferecer oportunidades, ou seja, é possível gerar uma publicidade eficaz através de variados métodos tecnológicos, como por meio dos *cookies*, que permite que haja um rastreamento dos acessos das pessoas nesse ambiente online e assim se extraia os interesses dos mesmos podendo tal ser interligado ao comercial publicitário que fomenta o *e-commerce*. (BIONI, 2020, p. 16-17). Diante das facilidades proporcionadas por esse sistema de compra e venda, surge a questão referente a imprescindibilidade em asseverar a segurança das pessoas e de suas respectivas informações (PINHEIRO, 2021, p. 53).

Assim, percebe-se que as pessoas estão vivenciando novas práticas comerciais, consequentemente aumentando-se o percentual de consumidores no âmbito digital, e havendo a essencialidade de se haver um regramento que aborde tal dinâmica. Por isso, de um modo geral, o tratamento de dados conforme os ditames da LGPD, gira em torno da coleta dos dados, da sua aplicabilidade, armazenamento, processamento, compartilhamento, transferência e eliminação destas informações. Então todas as movimentações efetuadas pelo *e-commerce* no que se refere a dados se enquadram na lei em questão. Por isso, as empresas deverão atuar de maneira preventiva e repressiva, ou seja, será necessário proteger os dados contra violações, perdas, vazamentos, bem como, requerer o devido consentimento do titular e seguir conforme o que for autorizado.

Cumprido comentar, que no Decreto 7.962/2013, este que regulamenta o comércio eletrônico, em seu art. 4º, inc. VII estabelece que o fornecedor adote meios de segurança adequados para o pagamento e o tratamento de dados do titular consumidor. Tendo em vista que o foco da pesquisa é a análise da LGPD, destaca-se alguns pontos. Primeiramente, quanto ao art. 5º, inc. XII da LGPD, este dispõe sobre o consentimento, que deverá ser representado pela “[...] manifestação livre, informada e inequívoca [...]”, ou seja, o titular aceita o tratamento de dados ofertado dentro das finalidades apresentadas naquele momento.



Conforme explicado no primeiro tópico do presente artigo, o processamento envolve variados tipos de dados, dos quais possuem particularidades normatizadas e específicas. Quanto aos dados pessoais sensíveis, por exemplo, estes dizem respeito a características personalíssimas e íntimas das pessoas, ensejando, por conseguinte, uma proteção mais efetiva e elevada quanto ao sigilo dessas informações no decorrer do tratamento, por isso, a LGPD estabelece um tratamento delineado a essa espécie de dados. O art. 11 da LGPD aponta que o processamento de dados sensíveis só será efetuado após prévio consentimento autorizativo do titular, devendo ser este, específico e claro, com finalidade estabelecida. O parágrafo terceiro do mesmo artigo mencionado, impede a comunicação e uso compartilhado destes dados pelos controladores, nos casos em que é visado o interesse de alcançar vantagens pecuniárias.

Ademais, no artigo 11, inciso II e respectivas alíneas da LGPD, há casos em que haverá a dispensa do consentimento, quando por exemplo, for em relação a implementação de obrigação legal; para questões relacionadas a administração pública; para estudos efetuados por órgãos de pesquisa; quando for referente a processos judiciais, administrativos ou arbitrais; quando o intuito seja proteger a vida do titular ou terceiro, bem como a sua saúde; e nos casos em que for necessário para evitar fraudes e prevenir a segurança do titular no âmbito dos sistemas eletrônicos.

As relações efetivadas por meio do comércio eletrônico se derivam na constituição de contrato, este pelo qual, é um instrumento jurídico que institui as obrigações e os direitos das partes, bem como apresenta os dados pessoais necessários para a realização de tal negócio. Neste caso, o art. 7º, inc. V da LGPD<sup>10</sup> destaca que os dados elencados no contrato são essenciais e podem passar por tratamento para efetivar o comércio empresarial pretendido. Sendo assim, as empresas precisam seguir tanto os preceitos legais dispostos na Lei Geral de Proteção de Dados, como aquilo que foi estipulado em contrato acordado pelo titular, se atentando quanto às finalidades, necessidades, interesse legítimo, consentimento e demais princípios e fundamentos legais anteriormente comentados.

Dentre as principais implicações trazidas pela LGPD, além das destacadas nos tópicos da presente pesquisa, ressalta-se novamente a questão do consentimento, pois o titular será requisito para manifestá-lo; às empresas reanalisar as documentações em seu poder, e posteriormente implementar nos sistemas e no cotidiano, políticas de privacidade e segurança, políticas que abarcam possíveis incidentes cibernéticos, além disso, que todas as obtenções de

---

<sup>10</sup> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: [...] V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados.

dados sejam respaldadas pela prévia autorização do titular; ainda, que haja uma conscientização a respeito da segurança e transparência nessas relações comerciais; quaisquer vazamentos precisam ser comunicados à Autoridade Nacional de Proteção de Dados (PERINA, 2021, n.p.).

Outro ponto importante, é que as empresas estabeleçam um plano de governança para os dados, ou seja, que seja atribuído meios para a administração dos dados pessoais; para o suporte aos titulares; ademais que haja “[...] atualização e a melhoria dos padrões e instrumentos, técnicos e administrativos, relacionados à privacidade e proteção de dados” de maneira contínua (TEIXEIRA, 2021a, n.p.).

As empresas de comércio digital, em seus sistemas, também precisam definir um profissional responsável pela proteção de dados (sendo o DPO - Data Protection Officer), que além de demonstrar lisura na relação comercial, também atuará como prestador de contar aos órgãos incumbidos em realizar as fiscalizações sobre a temática, bem como, este também terá como encargo lidar com os incidentes e sanar as dúvidas das pessoas. Ademais, outro ponto importante, é destacar as possibilidades em que o titular poderá retirar sua autorização, e ainda, estabelecer todas as finalidades da obtenção de informações, sejam aquelas relacionadas aos *cookies*, cadastros, da coleta de dados, dentre outros (PERINA, 2021, n.p.).

Dessa maneira, a proteção de dados é realmente consubstanciada quando tutela os sujeitos e dispõe de deveres, obrigações e até mesmo sanções aos incumbidos de realizar o tratamento dos dados, é presente também quando são atribuídos direitos aos proprietários dos dados, nesse sentido, com esse ato protetivo “não se está meramente regulando um objeto externo à pessoa, porém uma representação própria pessoa” (DONEDA, 2010, p. 52). Entretanto, ainda que existam regulamentações para tanto, muitas vezes não são atribuídas eficazmente aos processamentos de dados e de informações, pois são considerados privilégios particulares ou de natureza financeira.

Assim, torna-se essencial resguardar os dados pessoais e sensíveis tanto nos meios de armazenamento e processamento físico e digital, em razão de que atualmente, tais dados representam montantes monetários para o meio dos negócios, tendo em vista que com o atual sistema de captação e cadastros realizados são conduzidos serviços e produtos de modo personalizado. Sendo assim, diante dessa demanda de dados no âmbito empresarial por conta da elevada obtenção destes a todo momento, passaram essas informações no viés da sociedade digital a serem apontados como o “novo petróleo”, decorrendo a partir do momento em que o dado é processado, concebendo valor. Então, a necessidade de uma proteção de dados

pertinente, concerne ao propósito de caracterizar um parâmetro entre as particularidades e a privacidade do titular relacionado e também visando a liberdade comercial e conversação (MENDES, 2014, p. 33; TEIXEIRA; GUERREIRO, 2022, p. 12).

Diante dessa breve explanação, verifica-se que os dados e as informações estão presentes no nosso cotidiano e nas ações que realizamos regularmente ao utilizarmos a internet, sendo que tais, são compartilhados, guardados, tratados, compartilhados e aplicados em seguindo diversas formas, como para fins econômicos. Por isso, os dados atualmente tidos como “bens” demonstram grande importância nos mais variados contextos e principalmente são essenciais para o titular, ou seja, carecem de uma respectiva e adequada proteção.

#### **4 RESPONSABILIDADE DAS EMPRESAS AOS POSSÍVEIS VAZAMENTOS DE DADOS ORIUNDOS DO E-COMMERCE**

Diante desse novo sistema de prática comercial realizado pelas empresas, bem como da obtenção de dados e informações pessoais e respectivo manuseio, armazenamento, compartilhamento e aplicação, as empresas passaram a ter um encargo mais elevado no que tange a manter tais bancos de dados protegidos, e caso haja possíveis vazamentos dos mesmos, a Lei Geral de Proteção de Dados estimulou regramentos referentes a responsabilidade de tais empresas em razão do e-commerce.

O comércio eletrônico ocorre no âmbito digital, nisto cotidianamente há a intensa coleta de dados, referentes à por exemplo, a identificação pessoal, endereço, dados bancários e de crédito, para o desempenho de ações que passarem a serem possíveis de serem realizadas de forma online. Dentre essas atividades ocorridas na internet, pode-se comentar, sobre a compra e venda de bens e serviços, o acesso e respectivas transações bancárias por meio dos dispositivos móveis, a adesão de aplicativos e sites, dentre outros. Em resultado, os acessantes desses ambientes digitais, acabam se expondo, convertendo-se em vulnerabilidade diante dos possíveis cibercrimes que podem ocorrer nestes locais.

Por isso, há a imprescindibilidade de todas as empresas em adequar protocolos efetivos para proteger ao máximo possível as informações dos titulares aliada a LGPD, em razão de que tais envolvem tantos dados pessoais como dados pessoais sensíveis, ou seja, se associando aos direitos humanos e fundamentais, que caso estes sejam vazados, poderá resultar em uso por terceiros desconhecidos de forma maliciosa e discriminatória (SARLET; RUARO, 2021, p. 100-101).

Tendo em vista, que qualquer pessoa que esteja responsável por realizar o manejo e o tratamento de dados possa incorrer em erros, gerando responsabilidade tanto pessoal como para a empresa, é essencial que seja estabelecido métodos para a segurança informacional, para pelo menos, diminuir os resultados negativos decorrentes de alguma irregularidade. As empresas que realizam essa prática comercial pelos sistemas digitais, precisam se atentar quanto as criptografias empregadas a seus sites, além disso, é importante que haja a presença de boas práticas no cotidiano dos funcionários e demais envolvidos no tratamento de dados, em prol de evitar que estes sejam visualizados por pessoas não autorizadas, “situações acidentais ou ilícitos de destruição” (TEIXEIRA, 2021b, p. 94).

Conforme Araújo e Figueredo (2020, p. 343), “a responsabilidade civil ocorre a partir do cometimento do ato ilícito, ou seja, da violação de uma obrigação, podendo ela ser contratual ou extracontratual, e tem por objetivo tornar indene o prejudicado, restabelecer à vítima situação em que estaria sem a ocorrência do fato danoso”. Nisto alude-se o que se preceitua no art. 46 da LGPD, o qual estabelece que os “agentes de tratamento devem adotar medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito”, ou seja, os agentes não estão isentos de responsabilidade, porém precisam atuar com o caráter preventivo e adotar tais medidas comentadas.

Então quando houver um tratamento de dados irregular ao acordado e ao que é estabelecido pela LGPD, resultando em prejuízos ao titular, tanto o controlador<sup>11</sup> como o operador<sup>12</sup> dos dados serão solidariamente responsáveis. O operador será responsabilizado de forma solidária quando não seguir as normatizações oriundas da LGPD ou não seguir as instruções do controlador<sup>13</sup>. E quando se trata de controladores conjuntos, haverá a solidariedade aos danos gerados ao titular<sup>14</sup>. Conforme o art. 43 da LGPD, há casos em que o controlador e operador não serão responsáveis pelos dados aos titulares, isso quando provarem que: não tenham efetuado o tratamento ordenado; que mesmo tendo realizado o tratamento ordenado, não houve afronta a LGPD; que o dano ocorrido foi culpa unicamente do titular ou de algum terceiro (BRASIL, 2018).

---

<sup>11</sup> Art. 5º, inc. VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

<sup>12</sup> Art. 5º, inc. VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

<sup>13</sup> Art. 42, §1º, inc. I da Lei n. 13.709/18;

<sup>14</sup> Art. 42, §1º, inc. II da Lei n. 13.709/18.

Ademais, o parágrafo único do art. 44 da lei em comento, estabelece que os encarregados pelo tratamento de dados também serão responsabilizados, quando não aderirem os métodos de segurança e isto der causa ao dano ao titular consumidor dos serviços da empresa. Assim, o art. 46 da LGPD dispõe que os agentes de tratamento, neste caso as empresas, possuem a obrigação de acatar as medidas de segurança, técnicas e administrativas, adequadas para a promoção do anteparo aos dados e aos acessos não irregulares, bem como as circunstâncias ilegítimas ou acidentais “[...] de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito” perante as informações pessoais.

Será, portanto, aplicada a responsabilidade civil objetiva, alinhando as disposições da LGPD (art. 43, inc. II) e do Código de Defesa do Consumidor (art. 14, §3º), em razão da vulnerabilidade do titular consumidor, fazendo com que a empresa fornecedora tenha ônus probatório do dano, mesmo que não haja culpa. Sendo que tal entendimento também pode ser observado na jurisprudência abaixo:

APELAÇÃO CÍVEL. AÇÃO CIVIL PÚBLICA. DISPONIBILIZAÇÃO INDEVIDA DE BANCO DE DADOS DE CONSUMIDORES NA REDE MUNDIAL DE COMPUTADORES. [...] APLICABILIDADE DO CÓDIGO DE DEFESA DO CONSUMIDOR. LEGITIMIDADE PASSIVA DE TODOS OS FORNECEDORES DE SERVIÇOS E PRODUTOS QUE INTEGRAM A CADEIA DE CONSUMO PARA RESPONDER PELOS DANOS CAUSADOS PELA FALHA NA PRESTAÇÃO DOS SERVIÇOS. RESPONSABILIDADE OBJETIVA. TEORIA DO RISCO DO EMPREENDIMENTO. [...] DIVULGAÇÃO INDEVIDA DE DADOS. OFENSA A DIREITOS PERSONALÍSSIMOS DOS CONSUMIDORES E EM ESPECIAL DAQUELES INTEGRANTES DO BANCO DE DADOS MANTIDO OU UTILIZADO PELAS RÉS. DIREITO À INTIMIDADE E AO SIGILO DE DADOS VIOLADO. DANO MORAL COLETIVO. DANO MORAL IN RE IPSA. DESNECESSIDADE DA DEMONSTRAÇÃO DE PREJUÍZOS CONCRETOS OU DE EFETIVO ABALO MORAL. PRECEDENTES DA CORTE SUPERIOR. VALOR INDENIZATÓRIO QUE SE MOSTRA RAZOÁVEL E CONDIZENTE COM A RELEVÂNCIA DO TEMA E COM O CARÁTER REPRESSOR DA INDENIZAÇÃO. [...] RECURSO DESPROVIDO. (TJRJ- 0418456-71.2013.8.19.0001- Apelação. Primeira Câmara Cível. Des(o). Fábio Dutra - Julgamento: 23/02/2021 - Data de Publicação: 10/03/2021).

Na presente pesquisa, pode-se citar algumas formas, além das até aqui comentadas, que irão proporcionar maior segurança no *e-commerce* e conseqüentemente evitar sanções às empresas. Primeiramente, que haja a inserção de boas práticas e de governança no cotidiano empresarial, em prol de evitar desvantagens monetárias, desonerar-se de sanções administrativas ou judiciais, viabilizando os direitos humanos e fundamentais dos consumidores (TEIXEIRA, 2021a, n.p.).

Também, seria interessante a implementação de “certificados de segurança SSL (Secure Sockets Layer), este por sua vez, é um protocolo de criptografia que visa resguardar

os dados compartilhados dos acessantes e dos servidores dos sites, com isso, impedindo a visualização de terceiros não autorizados. Os funcionários que atuam diretamente nos procedimentos que envolvem as informações pessoais, precisam ser treinados para que possam gerir tais dados de maneira adequada a fim de evitar possíveis transgressões, bem como, orientá-los os procedimentos a serem empregados caso haja tais vazamentos (ASSIS, 2023, n.p.).

Os agentes de tratamento de dados podem adotar: a) os sistemas de gestão e segurança da informação (SGSI) dentro das políticas de privacidade no interior dos sistemas da empresa; b) estabelecer deveres e obrigações aos enredados no tratamento; c) asseverar a confirmação dos direitos pessoais; d) informar os colaboradores da empresa sobre as práticas de segurança para os dados (PINHEIRO; LOTUFO, 2021, p. 31, 33, 34).

Caso a empresa não siga os ditames da LGPD e não prezar pela segurança dos dados e os direitos dos titulares, haverá conforme o art. 42 deste mesmo ordenamento legal, o ensejo da responsabilidade civil e a aplicação de sanções administrativas ou judiciais, resultando em condenação da empresa a indenizar os titulares atingidos, em razão das falhas de segurança e vazamento de dados pessoais.

## **5 CONSIDERAÇÕES FINAIS**

A sociedade informacional gerou novas perspectivas, inclusive no âmbito empresarial, isso porque, a partir da internet e das tecnologias é possível realizar trocas comerciais que fomentam a economia atual. Então criou-se a Lei Geral de Proteção de Dados com o intuito de, por exemplo, regulamentar tais transações no que tange às informações pessoais, trazendo definições importantes a respeito dos dados, do tratamento destes, do consentimento necessário para isto, sobre as transferências, armazenamento, responsabilidade, dentre outros.

Os dados e as informações constantes nas ações diárias realizadas pelas pessoas no meio digital, sendo que os mesmos, são compartilhados, armazenados, tratados e aplicados nos mais diversos ramos, remontando a economia. Cumpre salientar que os mesmos são utilizados no comércio digital e as empresas precisam observar a proteção destes dados, em prol de distanciar situações envolvendo vazamentos ou compartilhamentos inadequados, que poderiam atingir os direitos humanos dos titulares

Embora haja diferentes nuances interpretativas na aplicação da normatização da LGPD no âmbito das empresas, tal movimento pode ser observado não apenas como uma

obrigação legal, mas também como uma ferramenta que irá aprimorar a figura da empresa para os consumidores, bem como irá aperfeiçoar os procedimentos inerentes, além dos produtos e serviços ofertados, promovendo ampliação do mercado e das possibilidades. Isso porque, a aceitação do titular remete a um negócio jurídico consubstanciado no site, portanto um ambiente comercial digital seguro, fomentando a confiança para com os consumidores e acessantes. Além disso, englobar a LGPD nestas relações, remete em segurança não só para os usuários como também para as empresas que realizam todo e qualquer tipo de obtenção, movimentação, tratamento e armazenamento destes dados, tornando-as mais fidedigno assim como o *e-commerce* mais eficiente.

Então, é de responsabilidade civil objetiva da empresa que efetua o tratamento de dados, atribuir uma segurança adequada para com os titulares, para evitar possíveis vazamentos e também seguir com as finalidades propostas e consentidas no momento da coleta destes dados. Cabe salientar que, a LGPD aborda direitos e obrigações para todos os relacionados, seja para os titulares, empresas, agentes de tratamento, entre outros, estipulando responsabilização e sanções na hipótese destes preceitos serem violados e gerarem danos.

Por isso, conclui-se que para o tratamento de dados estar em conformidade a LGPD, no âmbito do *e-commerce*, é necessário seguir os seguintes requisitos: Primeiramente, que estes dados só sejam tratados após a manifestação do consentimento pelo titular, concordando com o que fora proposto; que sejam seguidos os preceitos referentes aos princípios e fundamentos da lei em comento; que haja a implementação de boas práticas e de governança no dia a dia das empresas; que seja viabilizado os direitos humanos e fundamentais em prol dos consumidores titulares dos dados; que os agentes que realizam esse tratamento incluam um sistema de gestão e segurança informacional, implementando também protocolos de criptografia para proteger os dados de acessos não autorizados; que sejam estipulados obrigações e deveres a estes agentes; que os direitos pessoais sejam reafirmados; que os colaboradores da empresa sejam informados a respeito das práticas de segurança para os dados.

## REFERÊNCIAS

ARAÚJO, Vitor Eduardo Lacerda de; FIGUEREDO, Douglas Dias Vieira de. **Análise jurídica dos incidentes de segurança e a responsabilidade civil no Brasil.** in GROSSI, Bernardo Menicucci (org.). **Lei Geral de Proteção de Dados: Uma análise preliminar da Lei 13.709/2018 e da experiência de sua implantação no contexto empresarial.** Porto Alegre: Editora Fi, 2020. p. 337-358. *E-book*. ISBN 978-65-87340-21-0.

ASSIS, Alexandre. **LGPD e segurança de dados dentro do e-commerce**. E-commerce Brasil, 2023. Disponível em: <https://www.ecommercebrasil.com.br/artigos/lgpd-e-seguranca-de-dados-dentro-do-e-commerce>. Acesso em: 19 ago. 2023.

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

BRASIL. **Decreto n. 7.962, de 15 de março de 2013**. Regulamenta a Lei n. 8.078, de 11 de setembro de 1990, para dispor sobre a contratação no comércio eletrônico. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2013/decreto/d7962.htm](https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/decreto/d7962.htm). Acesso em: 14 ago. 2023.

BRASIL. **Lei n. 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/leis/18078compilado.htm](https://www.planalto.gov.br/ccivil_03/leis/18078compilado.htm). Acesso em: 12 fev. 2023.

BRASIL. **Lei n. 10.406, de 10 de janeiro de 2002**. Instituiu o Código Civil. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/leis/2002/110406compilada.htm](https://www.planalto.gov.br/ccivil_03/leis/2002/110406compilada.htm). Acesso em: 24 nov. 2020.

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/112965.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm). Acesso em: 23 nov. 2020.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/L13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm). Acesso em: 25 nov. 2020.

BRASIL. **Tribunal de Justiça do Rio de Janeiro**. Apelação cível n. 0418456-71.2013.8.19.0001. Apelante: Smarty Solutions Treinamento Profissional LTDA.ME e outros. Apelada: Ministério Público. Relator (a): Fabio Dutra, julgamento: 23/02/2021-Data de Publicação: 10/03/2021. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-rj/1204645702>. Acesso em 13 ago. 2023.

DE FAZIO, Marcia Cristina Puydinger. **A sociedade civil global e a rede: Resistência à globalização desde cima?** Ijuí: Unijuí, 2012. p. 59-109.

DONEDA, Danilo. **A proteção de dados pessoais nas relações de consumo: para além da informação creditícia**. Escola Nacional de Defesa do Consumidor. Brasília: SDE/DPDC, 2010. Disponível em: <https://www.justica.gov.br/seus-direitos/consumidor/Anexos/manual-de-protecao-de-dados-pessoais.pdf>. Acesso em: 27 nov. 2020.

DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental**. Joaçaba: Espaço Jurídico, 2011. Disponível em: <https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315/658>. Acesso em: 27 maio 2021.



DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais**. São Paulo: Thomson Reuters Brasil, 2019. ISBN: 978-85-5321-957-5.

DINO. **E-commerce segue em constante ascensão desde 2020**. O Globo, 16 ago. 2023. Disponível em: <https://oglobo.globo.com/patrocinado/dino/noticia/2023/08/16/e-commerce-segue-em-constante-ascensao-desde-2020.ghtml>. Acesso em: 18 ago. 2023.

KASPERSKY. **O que é uma pegada digital?** E como protegê-la de hackers. c2023. Disponível em: <https://www.kaspersky.com.br/resource-center/definitions/whats-is-a-digital-footprint>. Acesso em: 10 fev. 2023.

LIMBERGER, Têmis. **Da Evolução do Direito a ser deixado em paz à Proteção dos Dados Pessoais**. Revista do Direito, edição 30, 2008. p. 138-160. DOI: <https://doi.org/10.17058/rdunisc.v0i30.580>. Disponível em: <https://online.unisc.br/seer/index.php/direito/article/view/580>. Acesso em: 26 nov. 2020.

MARINELI, Marcelo Romão. **Privacidade e Redes Sociais Virtuais: Sob a égide da Lei 12.965/2014 – Marco Civil da Internet e da Lei 13.709/2018 – Lei Geral de Proteção de Dados Pessoais**. São Paulo: Thomson Reuters Brasil, 2019. ISBN 978-85-5321-730-4.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: Linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788502218987/>. Acesso em: 20 out. 2020. ISBN: 9788502218987.

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA. **Autoridade Nacional de Proteção de Dados: Perguntas Frequentes - ANPD**. 2021. Disponível em: <https://www.gov.br/anpd/pt-br/acao-a-informacao/perguntas-frequentes-2013-anpd#inicio>. Acesso em: 17 ago. 2023.

MOROZOV, Evgeny. **Big Tech a ascensão dos dados e a morte da política**. São Paulo: Ubu Editora, 2018. p. 144-181.

PERINA, Gustavo. **Quais foram os impactos da LGPD no E-commerce?**. E-commerce Brasil, 2021. Disponível em: <https://www.ecommercebrasil.com.br/artigos/quais-foram-os-impactos-da-lgpd-no-e-commerce>. Acesso em: 19 ago, 2023.

PINHEIRO, Patrícia Peck. **#Direito digital**. São Paulo: Saraiva, 2021. ISBN 9786555598438. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786555598438/>. Acesso em: 18 mar. 2023.

PINHEIRO, Patrícia Peck. LOTUFO, Larissa. **Proteção de dados pessoais**. In: PINHEIRO, Patrícia Peck. **Segurança Digital: Proteção de dados nas empresas**. São Paulo: Atlas, 2021. p. 31-40. *E-book*. ISBN 9788597026405. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788597026405/>. Acesso em: 13 ago. 2023.

PRIVACIDADE & TERMOS. **Como a GOOGLE usa os cookies.** [S.l., s.d]. Disponível em: <https://policies.google.com/technologies/cookies?hl=pr-BR>. Acesso em: 09 fev. 2023.

SARLET, Gabrielle Bezerra Saler; RUARO, Regina Linden. **A proteção de dados sensíveis no sistema normativo brasileiro sob o enfoque da lei geral de proteção de dados (LGPD) - L.13.709/2018.** Revista de Direitos Fundamentais e Democracia. Curitiba, v. 26, n. 2, p. 81-106, 2021. DOI: <https://doi.org/10.25192/issn.1982-0496.rdfd.v26i22172>. Disponível em: [revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/article/view/2172](http://revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/article/view/2172). Acesso em: 18 abr. 2023.

SILVEIRA, Sergio Amadeu da. **Tudo sobre tod@s: redes digitais, privacidade e venda de dados pessoais.** São Paulo, 2017. Disponível em: [https://mudancatecnologicaedinamicacapitalista.files.wordpress.com/2019/02/tudo-sobre-tod40s\\_-redes-digitais-privacid-sergio-amadeu-da-silveira-1.pdf](https://mudancatecnologicaedinamicacapitalista.files.wordpress.com/2019/02/tudo-sobre-tod40s_-redes-digitais-privacid-sergio-amadeu-da-silveira-1.pdf). Acesso em: 27 nov. 2021. ISBN: 978-85-9493-028-6.

TEIXEIRA, João Pedro Ferraz. **E-commerce: Como se adequar à LGPD?**. 2021a. Disponível em: [jusbrasil.com.br/artigos/e-commerce-como-se-adequar-a-lgpd/1181332143](http://jusbrasil.com.br/artigos/e-commerce-como-se-adequar-a-lgpd/1181332143). Acesso em: 19 abr. 2023.

TEIXEIRA, Tarcísio. **A LGPD e o e-commerce.** São Paulo: Saraiva, 2021b. *E-book*. ISBN 9786555598155. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786555598155/>. Acesso em: 09 fev. 2023.

TEIXEIRA, Tarcísio; GUEREIRO, Ruth M. **Lei Geral de Proteção de Dados Pessoais (LGPD): Comentada Artigo por Artigo.** São Paulo: SaraivaJur, 2022. ISBN 978-65-5559-901-5. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786555599015/>. Acesso em: 09 fev. 2023.