PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO
NÚCLEO DE PRÁTICA JURÍDICA
COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO
ARTIGO CIENTÍFICO

IMPACTO DA LEI GERAL DE PROTEÇÃO DE DADOS NO E-COMMERCE E MARKETPLACE

ORIENTANDA: JÉSSYCA ALVES DE SOUZA CUNHA
ORIENTADORA: PROFª: Ma. ÉVELYN CINTRA ARAÚJO

GOIÂNIA
2024

JÉSSYCA ALVES DE SOUZA CUNHA

IMPACTO DA LEI GERAL DE PROTEÇÃO DE DADOS NO E-COMMERCE E MARKETPLACE

Artigo Científico apresentado à disciplina Trabalho de Curso II, da Escola de Direito, Negócios e Comunicação, Curso de Direito, da Pontifícia Universidade Católica de Goiás (PUCGOIÁS).

Prof.(a) Orientadora: Ma. Évelyn Cintra Araújo.

GOIÂNIA

2024

JÉSSYCA ALVES DE SOUZA CUNHA

IMPACTO DA LEI GERAL DE PROTEÇÃO DE DADOS NO E-COMMERCE E MARKETPLACE

Data da Defesa: ____ de _____ de _____

BANCA EXAMINADORA

_____

Orientadora: Profa: Ma. Évelyn Cintra Araújo Nota

_____

Examinador (a) Convidado (a): Prof. (a): Ma. Neire Divina Nota

SUMÁRIO

IMPACTO DA LEI GERAL DE PROTEÇÃO DE DADOS NO E-COMMERCE E MARKETPLACE

Jéssyca Alves de Souza Cunha[1]

RESUMO

A pesquisa analisou o impacto da Lei Geral de Proteção de Dados (LGPD) no e-commerce e marketplaces, utilizando o método hipotético-dedutivo. O estudo mostrou que a evolução histórica da legislação, incluindo o Marco Civil da Internet, estabeleceu fundamentos legais que moldaram os requisitos da LGPD. O princípio da proteção de dados foi identificado como essencial no e-commerce, definindo bases legais para o tratamento de dados pessoais. A pesquisa evidenciou que os custos de manutenção e implementação das normas exigiram adaptações significativas das empresas, impactando a experiência do usuário, que passou a se sentir mais seguro ao interagir com plataformas online. Contudo, as empresas enfrentam desafios relacionados a multas e sanções por descumprimento, o que levou a uma reavaliação de suas práticas de privacidade. As conclusões apontaram que a LGPD não apenas promoveu um ambiente digital mais seguro, mas também impôs uma mudança de cultura nas empresas, que passaram a valorizar mais a transparência e a proteção dos dados dos consumidores. Esse novo cenário demandou um equilíbrio entre compliance e inovação no setor, reafirmando a importância de adaptar estratégias de negócios à legislação vigente.

Palavras-chave: LGPD. E-commerce. Proteção de dados. Compliance. Experiência do usuário.

[1] Estudante do 10º período do curso de Direito da Faculdade Pontifícia Universidade Católica de Goiás.

INTRODUÇÃO

A presente pesquisa tem por objeto a Lei Geral de Proteção de Dados que foi implementada no País tempos depois da população já utilizar deste meio digital, a pesquisa realizada TIC Domicílios em 2019, fez um importante levantamento sobre o acesso a tecnologias da informação e comunicação, realizada pelo Centro Regional para o Desenvolvimento de Estudos sobre a Sociedade da Informação (Cetic.br), vinculado ao comitê Gestor da Internet no Brasil, aponta que três em cada quatro brasileiros acessam a internet, o que equivale a 134 milhões de pessoas. Em se tratando de uma era completamente digital o avanço nos números de usuários com acessos a internet se tornou necessário tomar medidas que proteja a população.

A Lei Geral de Proteção de dados (LGPD), tem como proposito garantir princípios cruciais para a coleta e armazenamento de dados pessoais dos usuários, conforme o seu escopo definido no artigo 1º da Lei nº 13.709/2018: Está Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

A Lei Geral de Proteção de dados traz uma proteção ainda maior em seu artigo 5º, inciso II, onde é abordado dado pessoal sensível: dado pessoal sobre a 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 biométrico, quando vinculado a uma pessoa natural.

Em virtude de tudo isso, em princípio, surgem as seguintes dúvidas a serem solucionadas no transcorrer da pesquisa: a) quais são as medidas adotadas pelas empresas para garantir a eficácia das políticas de proteção de dados; b) quais são as divergências da Lei geral de proteção de dados com o Marco Civil na Internet; c) a falta de conscientização de colaboradores e parceiros para estar em conformidade com a (LGDP) pode gerar riscos; d) o E-commerce e Marketplace realiza análises de riscos para identificar possíveis vulnerabilidades de segurança; e) O órgão regulamentador Autoridade Nacional de Proteção de Dados (ANPD) possui recursos para garantir a funcionalidade da (LGPD).

Para tanto, poder-se-ia supor, respectivamente, o seguinte: a) O compliance comercial propõe-se garantir que as empresas sigam a prática e o decurso da

referida Lei (LGPD) e seus regulamentos internos, adequação está necessária para garantir a segurança do tratamento de dados captados; b) tanto (LGPD) quanto o (MCI) possuem o mesmo objetivo, proteger os indivíduos e garantir a segurança de seus dados e a sua privacidade. O Marco Civil da Internet foi fundamental para um debate relacionado aos crimes cibernéticos. Já Lei Geral de Proteção de Dados vai além, garantindo a máxima proteção dos dados, estabelecendo regras e padrões a serem cumpridos, preenchendo lacunas deixadas anteriormente deixadas.; c) é indispensável que as empresas de E-commerce e Marketplace promovam a conscientização de seus colaboradores e parceiros, estabelecendo um controle de mapeamento e tratamento de dados aquedado para evitar vazamentos e proteger a privacidade do cliente, visto que a empresa tem um nome a preservar.; d) as plataformas de E-commerce e Marketplace adotam medidas breves para sanar possíveis vulnerabilidades. Ferramentas que podem empregar a verificação em duas etapas (exigindo que o usuário confirme o cadastro por e-mail) ou o recaptcha no momento de cadastro, monitoramento contínuo para garantir o nível de segurança das páginas de E-commerce e Marketplace; e) a ANPD trata-se de uma autarquia vinculada ao Ministério da Justiça e de Segurança Pública, possui uma missão de garantir de a LGPD seja cumprida à risca no Brasil, em seu artigo 55, com isso a ANPD tem o dever de fiscalizar, advertir e até mesmo multar.

Utilizando-se uma metodologia adotada será o método hipotético-dedutivo, o qual envolve a escolha de um problema hipotético com base em conhecimentos prévios e viáveis. Esse método busca preencher lacunas no conhecimento científico, formulando suposições para serem posteriormente testadas e refutadas por meio de coleta e interpretação de dados.

Ter-se-á por objetivo principal garantir a coleta, o tratamento e o armazenamento dos dados pessoais sensíveis ou não, priorizando a credibilidade entre o comércio eletrônico e o usuário.

Como resultado deste trabalho, visa primeiramente explicar os princípios básicos de proteção de dados pessoais estabelecidos pela Lei Geral de Proteção de Dados (LGPD) e subsidiar análises posteriores focadas especificamente nas obrigações de proteção de dados. Processamento de dados.

A seguir, são analisadas as sanções administrativas previstas na LGPD, incluindo seu conceito, adequação, aplicabilidade e, principalmente, seu impacto nos responsáveis pelo tratamento de dados pessoais.

Por fim, definir e estudar as características regulatórias e fiscalizadoras da Autoridade Nacional de Proteção de Dados (ANPD), buscando a melhor explicação possível sobre sua atuação na proteção dos direitos dos titulares dos dados e na conformidade organizacional, bem como nas suas decisões relativas ao tratamento de dados pessoais no Brasil.

Nesse diapasão, em razão da dificuldade de sua compreensão e consequentes discussões a respeito dessas exceções, torna-se interessante, conveniente e viável a LGPD foi uma Lei pensada com um intuito de estabelecer regras entre empresas de E-commerce e Marketplace, visando a proteção singular no armazenamento de dados, onde as empresas precisou tomar novas medidas e políticas de privacidade para o seu funcionamento, muitas lojas virtuais terceirizam diversos serviços como exemplo o plataforma de pagamento, ou seja, além do site que irá armazenar as informações cadastrais.

1. ASPECTOS DA LEI GERAL DE PROTEÇÃO DE DADOS

1.1 EVOLUÇÃO HISTÓRICA E FUNDAMENTOS DA LGPD

A proteção de dados se tornou um tema de crescente importância nas últimas décadas, com o avanço tecnológico e a chegada da internet, com o surgimento de novas ferramentas tecnologias de comunicação e informação que revolucionaram o sistema de coleta e armazenamento de dados e a utilização destes.

A Constituição Federal traz em seu artigo 5º inciso X e XII:

> X - São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
> XII - e inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

A proteção de dados é um dos direitos fundamentais mais valiosos em uma sociedade igualitária, sendo fundamental para a independência e o crescimento pessoal e a manutenção da dignidade humana que possui amparo Constitucional, conforme aponta o artigo 1º inciso III, da Constituição Federativa do Brasil (CF/88):

> Art. 1º A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito e tem como fundamentos:
> (...)
> III- a dignidade da pessoa humana;

A dignidade humana está intimamente relacionada aos direitos fundamentais inerentes à condição humana, sendo assim:

> O direito à vida privada, à intimidade, à honra, à imagem, dentre outros, aparecem como consequência imediata da consagração da dignidade da pessoa humana como fundamento da República Federativa do Brasil. Esse fundamento afasta a ideia de predomínio das concepções transpessoalistas de Estado e nação, em detrimento da liberdade individual (DE MORAES, 2003, p. 60).

O referido tema apresenta ser relativamente novo, mas esse assunto antecede a própria formalização dos direitos humanos, realizada após a Segunda Guerra Mundial, com o surgimento dos primeiros computadores e o aumento de

processamento de dados na década de 60/70. Com a primeira Convenção Internacional no contexto: A Convenção para a Proteção Pessoal em relação ao tratamento automatizado de dados de caráter pessoal realizada pelo Conselho Europeu em 1981. A partir do século XXI, a proteção de dados ganhou espaço na agenda Global, com a publicação de Leis e regulamentos em diversos países para proteger a privacidade de todos os usuários de forma severa.

Antes da promulgação da Lei geral de proteção de Dados (LGPD), o Marco Civil da Internet foi um marco regulatório para a Internet no Brasil, estabelecendo diretrizes para garantir a proteção da privacidade e a neutralização da rede, mas o Marco Civil da internet não tratou de maneira especifica a questão dos dados pessoais, sendo assim, somente após 30 anos da promulgação Constituição Federal Brasileira foi aprovada a Lei nº 13.709/2018 lei regulamentadora da proteção de dados no Brasil, após vigorosos debates e negociações no Congresso Nacional. A Lei Geral de Proteção de Dados foi motivada por legislações estrangeiras, como a Regulamentação Geral de Proteção de Dados (GDPR) em passou a vigorar em 2018 na União Europeia.

O Art. 2º da Lei Geral de Proteção de Dados traz os princípios fundamentais a serem seguidos pelas instituições e empresas relacionados a coleta e o tratamento dos dados pessoais:

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
> I - o respeito à privacidade;
> II - a autodeterminação informativa;
> III - a liberdade de expressão, de informação, de comunicação e de opinião;
> IV - a inviolabilidade da intimidade, da honra e da imagem;
> V - o desenvolvimento econômico e tecnológico e a inovação;
> VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

A referida lei traz uma proteção ainda maior em seu artigo 5º, inciso II, onde é abordado dado pessoal sensível: dado pessoal sobre a 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 biométrico, quando vinculado a uma pessoa natural.

1.1.1 Marco civil da internet

O Marco Civil da Internet (Lei n.12.965/2014) foi predecessora em se tratando do uso da internet no Brasil, estabelecendo princípios, garantias, direitos e deveres, lei esta que foi celebrada por se tornar a primeira lei a disciplinar os direitos e deveres dos usuários na rede, criada com o intuito de assegurar a liberdade de expressão, a privacidade dos usuários, a neutralidade da rede e a proteção dos dados pessoais na internet, trazendo assim limites para o que muitos usuários consideram a internet uma terra sem lei, se tornou a "internet livre" como defende Souza e Lemos (2016, p. 18):

> O Marco Civil da Internet apresenta um novo cenário no qual o conceito de "Internet livre" está ligado não à ausência de leis, mas sim à existência de leis que possam garantir e preservar as liberdades que são usufruídas por todos justamente por causa da tecnologia e mais especificamente pelo desenvolvimento da Internet.

Para Tomasevicius (2015, p. 276):

> (...) não se perceberão mudanças substanciais, uma vez que esta não acrescentou praticamente nada à legislação vigente. A expectativa criada com a discussão dessa lei deu-se pela crença errônea de que as normas contidas na Constituição Federal, no Código Civil, no Código Penal, nos Códigos de Processo Civil e Penal, no Código de Defesa do Consumidor, no Estatuto da Criança e do Adolescente e na lei sobre interceptação de comunicações (Lei n.9.296/96) não teriam aplicação nas relações jurídicas estabelecidas na internet.

A internet reconfigurou a separação entre a esfera social e alterou as diferenciações entre esses espaços, tornando possível a qualquer momento ou lugar acessar a rede, ser visto ou ouvido por todos como exemplo as redes sociais Facebook, Instagram, Whatsapp, tornando possível até mesmo a prestação de serviço por Home Office, entre outras redes socais ou ferramentas comerciais. Eduardo Tomasevicius (2015, p. 272) aponta que: "essas transformações resultantes do uso livre da internet geram perplexidade nas pessoas, que ainda não sabem ao certo como comportar-se nessa "terceira esfera de ação humana", equivocadamente denominada de "ciberespaço".

A Lei n.12.965/2014 conhecida como Marco Civil da Internet considerou diversos princípios e garantias quanto ao uso da internet, organizou a atuação do

Poder Público relacionado ao desenvolvimento da internet no Brasil, destacando- se em três artigos, realizando uma análise inicial em seu artigo 2 º da lei citada:

> Art. 2º A disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão, bem como:
> I - o reconhecimento da escala mundial da rede;
> II - os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais;
> III - a pluralidade e a diversidade;
> IV - a abertura e a colaboração;
> V - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VI - a finalidade social da rede.

Com relação aos princípios apontados no artigo 3:

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
> I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
> II - proteção da privacidade;
> III - proteção dos dados pessoais, na forma da lei;
> IV - preservação e garantia da neutralidade de rede;
> V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
> VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
> VII - preservação da natureza participativa da rede;
> VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.

No que diz respeito à proteção, o artigo 7º apresenta os direitos do usuário:

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
> I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
> II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
> III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;
> IV - não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização;
> V - manutenção da qualidade contratada da conexão à internet;
> VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;
> VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
> VIII - informações claras e completas sobre coleta, uso,

> armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
> a) justifiquem sua coleta;
> b) não sejam vedadas pela legislação; e
> c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;
> IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;
> X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei e na que dispõe sobre a proteção de dados pessoais. (Lei no 12.965/2014).

Precedentemente não existia legislação com intuito de regular o uso da internet e impor limites que asseguram os direitos dos navegadores online de forma detalhada, sendo assim foi identificado a fragilidade Código Penal com relação aos cibercrimes. Contudo, diversos estudiosos, incluindo José Luis Bolzan de Morais e Elias Jacob de Menezes Neto, não acreditavam que essa fosse a melhor solução para o problema. Abaixo está um trecho de um artigo dos autores mencionados, que analisa o assunto:

> [...] forma reducionista como vem sendo tratada a questão da privacidade, apenas como sinônimo de vida particular, ou seja, de intromissão nas comunicações privadas armazenadas (vide inciso III); segundo os problemas
> oriundos da modernidade liquida não são resolvidos a partir de soluções dependentes da territorialidade, como é o caso do marco civil. ((BOLZAN DE
> MORAIS; JACOB DE MENEZES NETO, 2014, p. 13)

Após duas das maiores redes sociais, sendo elas o Facebook e o Google terem os seus nomes utilizados a vazamento e venda de dados pessoais, sendo um cenário antecedente a Lei Geral de Proteção de Dados, a criação da Lei 12.965/14 Marco civil da internet ser insuficiente para proteger os dados dos usuários dessas redes, os legisladores compreenderam a necessidade de elaborar uma lei que estivesse alinhada aos padrões da União Europeia, conforme estabelecido pelo Regulamento Geral de Proteção de Dados (GDPR). Análise Silva (2008).

> [...] O Brasil encontra-se em situação delicada, principalmente após os escândalos de espionagem norte-americana – caso Snowden – quando voi possível constatar que o país está despreparado para lidar com as possíveis violações de dados pessoais, mesmo que a jurisprudência já tenha se posicionado acerca de casos sobre dados pessoais e algumas leis já tenham articulado sobre o assunto, as decisões ainda são contraditórias e

> as leis abordam o tema de forma superficial ou específicas para apenas um setor, deixando todos os outros casos desprotegidos. Silva, 2008.

O Marco Civil da Internet, formalizado pela Lei 12.965/2014, estabelece os princípios, garantias, direitos e obrigações para o uso da Internet no Brasil e representa a legislação básica para a governança da Internet no país. Dentre seus diversos dispositivos, o artigo 10 da referida lei trata da proteção dos registros de conexão e de acesso a aplicações na Internet, no qual reforça a importância de manter o sigilo e a segurança dos dados coletados pelos provedores de internet, impondo obrigações claras sobre a guarda e o fornecimento desses registros. O artigo 11 desta mesma lei, aborda a aplicação da lei brasileira no âmbito da internet, destacando a extensão territorial das normas do Marco Civil. Ambos desempenham papel crucial na proteção dos dados dos usuários e na aplicação da legislação brasileira no ambiente digital.

> Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
> § 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º .
> § 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º .
> § 3º O disposto no caput não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.
> § 4º As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais.
> Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.
> § 1º O disposto no caput aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.
> § 2º O disposto no caput aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço

> ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.
> § 3º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações.
> § 4º Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo.

Em conjunto, os Artigos 10 e 11 do Marco Civil da Internet criam uma base sólida para a proteção dos dados pessoais e a aplicação da lei brasileira, fortalecendo a autoridade do Brasil na governança da internet e garantindo os direitos dos usuários.

O artigo 12 é uma das disposições fundamentais que define as responsabilidades dos fornecedores de serviços de Internet na proteção de dados pessoais e na cooperação com as autoridades públicas. Este documento reflete preocupações fundamentais sobre a privacidade e segurança dos usuários, estabelecendo diretrizes claras para a custódia e proteção dos registros de conexão e acesso por aplicações de Internet.

> Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa:
> I - advertência, com indicação de prazo para adoção de medidas corretivas;
> II - multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;
> III - suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou
> IV - proibição de exercício das atividades que envolvam os atos previstos no art. 11.
> Parágrafo único. Tratando-se de empresa estrangeira, responde solidariamente pelo pagamento da multa de que trata o caput sua filial, sucursal, escritório ou estabelecimento situado no País.

Estabelece obrigações aos fornecedores de serviços de Internet para proteger os dados pessoais dos utilizadores. Isto inclui a adoção de medidas técnicas e administrativas capazes de garantir a segurança dos dados pessoais registados e armazenados conectados contra acessos não autorizados, bem como contra a destruição, perda, alteração, comunicação acidental ou ilícita ou qualquer forma de tratamento impróprio ou ilícito. Outro aspecto importante do artigo 12 é a

obrigação do prestador de cooperar com as autoridades públicas na forma e na medida previstas pela legislação

Esta legislação foi muito importante para que houvesse o desenvolvimento de uma legislação que de fato protegesse os dados pessoais e os dados sensíveis, e o exigir clareza na coleta e armazenamento desses dados.

2.FUNDAMENTOS LEGAIS E REQUISITOS DA LGPD PARA O E-COMMERCE E MARKETPLACE

2.1 PRINCÍPIOS DA PROTEÇÃO DE DADOS APLICÁVEIS AO COMÉRCIO ELETRÔNICO

A proteção de dados definida pela Lei Geral de Proteção de Dados (LGPD) Lei nº 13.709/2018, é essencial para garantir o tratamento adequado dos dados e manter seguro todas as informações coletadas no comércio eletrônico. Princípios estes que devem ser observados, ou seja, as plataformas digitais e empresas (e-commerce e marketplace) precisam coletar, armazenar, usar e compartilhar esses dados, de maneira que respeite a política de privacidade, assegurando a proteção dos dados de maneira ética e transparente, garantindo que os dados coletados estejam em comum acordo com a legislação.

O art. 6 º da Lei Geral de Proteção de Dados (LGPD) prevê uma série de medidas cautelares relacionadas ao tratamento de dados pessoais no Brasil, que requer uma análise cautelosa e servem como diretrizes, sendo eles:

> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
> IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
> V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

> VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
> VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
> X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

O tratamento de dados pessoais no e-commerce e Marketplace se indispensável para a criação de um vínculo de confiança entre consumidores e empresas, pois possibilita a personalização da experiência de compra e segurança nas transações de pagamento e o cumprimento das obrigações legais. Esse processo inclui desde o registro inicial dos usuários, no qual são coletados dados pessoais, até mesmo informações sensíveis até a conclusão do pagamento, vale ressaltar que a proteção de dados financeiros é de suma importância.

2.1.1 Bases legais para o tratamento de dados

As bases legais para o tratamento de dados são requisitos estabelecidos diretamente pela Lei Geral de Proteção de Dados (LGPD), com o intuito de garantir a proteção e a privacidade dos dados pessoais, sejam eles sensíveis ou comuns. Dessa maneira, o usuário tem a possibilidade de controlar o uso, o compartilhamento e o armazenamento de suas informações.

Em relação ao tratamento de dados, o consentimento ocorre com o consentimento de forma livre por parte usuário para o tratamento de dados no qual é fornecido para um objeto específico como regra, conforme consta no “Artigo 7º: O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I - mediante o fornecimento de consentimento pelo titular;”

No caso de dados sensíveis foi consolidada normas mais rígidas conforme o Artigo 11: “O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;”.

A legislação destaca em seu art. 9 º, § 3 º, também estabelece:

> Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:
> (...)
> § 3º Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18 desta Lei

A Lei Geral de Proteção de Dados (LGPD) trata com mais rigor e cautela quando se refere à coleta de dados pessoais de crianças, no qual foi adicionado uma hipótese de tratamento de dados sem o consentimento dos pais ou responsável legal no art. 14, §1º e 3º.

> Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.
> § 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.
> (...)
> § 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo.

Para Teffé Chiara Sapadaccini (2020, p. 6):

> O maior cuidado com o consentimento do titular mostra-se de grande relevância no cenário tecnológico atual, no qual se verifica a coleta em massa de dados pessoais (...). Nesse sentido, defende-se que a interpretação do consentimento deverá ocorrer de forma restritiva, não podendo o agente estender a autorização concedida a ele para o tratamento de dados para outros meios além daqueles pactuados, para momento posterior ou para finalidade diversa.

A Lei Geral de Proteção de Dados (LGPD) oferece outras bases legais, além do consentimento que permite o tratamento de dados pessoais sem a necessidade de autorização expressa do titular. Essas bases incluem o cumprimento de obrigações legais ou regulatórias, a implementação de políticas públicas e até a proteção da vida ou da incolumidade física do titular ou de terceiros. Isso significa

que, sem o consentimento prévio do titular, dados pessoais podem ser tratados em situações específicas, como em emergências médicas ou para cumprir obrigações contratuais.

A lei visa equilibrar o direito à privacidade com as necessidades operacionais e sociais das empresas, desde que o tratamento de dados ocorra dentro dos limites legais e respeite os princípios da transparência e da finalidade. Dessa maneira, a LGPD assegura que os dados coletados mesmo onde não houve consentimento sejam tratados de forma responsável e segura, preservando o direito dos titulares.

3. IMPACTO ECONÔMICO, OPERACIONAL E SANÇÕES DA LGPD NO E-COMMERCE E MARKETPLACES

3.1 CUSTO DE IMPLEMENTAÇÃO E MANUTENÇÃO DA CONFORMIDADE

A Lei Geral de Proteção da Dados instituída em 2018, trouxe uma nova realidade no qual pegou muitas empresas de surpresa, mas essa lei entrou em vigor somente em 2020, as empresas que operam principalmente com o comércio eletrônico (e-commerce) e o Marketplace precisaram adequar-se. Esta legislação tem como princípio garantir a proteção dos dados pessoais sensíveis ou não dos consumidores, promovendo uma transparência relacionada a coleta desses dados e um tratamento adequado para tal coleta.

Contudo adequar-se às exigências da Lei Geral de Proteção de Dados (LGPD) gera custos consideráveis, cobrindo tanto a fase de implementação inicial quanto a supervisão contínua das práticas de conformidade.

Para Tigeira Claro et al. em sua obra: Aplicação Inovadora da LGDP na Segurança da Informação em Empresas de Desenvolvimento de SOFTWARE:

> Com toda essa dificuldade econômica as empresas precisam se adequar, revisitando seus processos, atualizando ou contratando sistemas e treinando os colaboradores, todo esse esforço geram custos, que no caso de startups, pequenas e médias empresas de desenvolvimento de software, tornam-se grandes limitadores, gerando um enorme impacto nos investimentos (...). (TIGEIRA CLARO et al. 2022 p. 88).

Para se adequar a conformidade da LGPD é preciso a realização de um estudo adequado para a realização de um diagnóstico detalhado sobre o tratamento dos dados coletados nas empresas de e-commerce e marketplace. Este processo abrange a identificação dos usuários e dados coletados, forma de armazenamento, quem pode manusear essas informações e sua finalidade.

> É possível implementar a Lei Geral de Proteção de Dados (LGPD) com custo “suportável” para as empresas de médio a grande porte, uma empresa brasileira de grande porte em média gasta cerca de 5,8 milhões para se adequar aos conformes da LGPD, esse valor teve inclusão de consultoria jurídica e transformação de TI, que pode ser a parte mais complicada de lidar. São utilizados cerca de 158 softwares para se adaptar a LGPD, e dentro desses softwares muitos são de empresas estrangeiras o que torna os preços mais altos devido a inflação e também acaba dificultado as negociações, empresas como Oracle e SAP por terem seus softwares de tamanho global elas decidem não fazer adaptações regionais exclusivas para o Brasil ou qualquer outro país adepto a LGPD. (GLENDA EDUARDA et al. 2021. p. 42)

Após esse diagnóstico inicial, é necessário mapear todo o fluxo de dados dentro da empresa, desde o momento da coleta de dados sensíveis ou não, o tratamento e o seu armazenamento. Com esse sistema de mapeamento é possível que a empresa analise cada passo daquele usuário, partindo apenas de um cadastro, compras, atendimento ao cliente, entre outras. Com isso é possível identificar se a empresa está em conformidade com a Lei Geral de Proteção de Dados, com a limitação mínima necessária de dados coletados para aquela prestação de serviço e o consentimento explícito do usuário para o tratamento de dados.

A adoção de medidas técnicas e organizacionais é primordial para garantir a proteção dos dados coletados, incluindo o uso de criptografia para o armazenamento seguro e controle de acesso restrito por funcionários não habilitados. A política de privacidade e termos de uso devem ser criadas para que o usuário compreenda como seus dados serão tratados e possam exercer seus direitos, como acesso, correção ou exclusão dos dados fornecidos.

Adicionalmente, é crucial que a empresa desenvolva uma cultura interna de proteção de dados, oferecendo treinamentos contínuos aos colaboradores e revisando regularmente as práticas adotadas. A LGPD, em seu artigo 41, estabelece a obrigatoriedade de designar um Encarregado de Proteção de Dados (DPO) para organizações operacionais que lidam com o tratamento de dados pessoais.

> Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.
> § 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.
> § 2º As atividades do encarregado consistem em:
> I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
> II - receber comunicações da autoridade nacional e adotar providências;
> III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
> IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.
> § 3º A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.

O processo de conformidade com a LGPD deve ser encarado como um esforço contínuo de governança e segurança, garantindo a adesão às normas de forma constante e não apenas como uma ação isolada. Isso implica que a governança de dados se torne um pilar essencial para a sustentabilidade da empresa, diminuindo riscos legais, financeiros e reputacionais, além disso, reforçando a confiança dos clientes e empresas parceiras.

3.1.1 Impacto na experiência do usuário e nas estratégias do e-commerce e marketplace

Com o constante crescimento da digitalização do comércio e a evolução da coleta, tratamento e armazenamento de dados modifica a experiência do usuário, e se faz necessário alterar a tática do Marketing no e-commerce e no marketplace.

Estar em conformidade com a Lei Geral de Proteção de Dados indica a responsabilidade de uma empresa com relação a proteção dos dados, além disso, faz com que os usuários (clientes) desse comércio eletrônico, criem uma relação de vínculo, e se sintam seguros para fornecer seus dados pessoais sensíveis ou não, no qual irá ser depositando total confiança e manter um relacionamento positivo com essa empresa seja ela do e-commerce ou marketplace.

Sobre o tema Laura Schertel Bruna Lins e Pietra Quinelato (apud Claudemir do Nascimento, 2022, p. 231):

> [O] ambiente virtual é propenso às violações da privacidade, de uma forma mais imperceptível e silenciosa que o ambiente físico. Isso porque o espaço físico possibilita a constatação mais nítida do nível de privacidade disponível e permite que a pessoa tome as decisões a fim de aumentar ou diminuir a sua privacidade, o que nem sempre é possível no espaço virtual, uma vez que não se sabe quais informações estão sendo capturadas, nem o momento em que esse controle é realizado.

O marketing desse comércio é uma peça chave para passar credibilidade, pois através do sistema de tráfego será responsável por demonstrar a seriedade e comprometimento da empresa, criando uma reputação cada vez melhor no mercado digital, além disso, clientes (usuários) preferem empresas digitais que prezam pelo zelo e tratamento adequado pelos seus dados, e assim gerando grande concorrência com as demais plataformas digitais apenas por estar em conformidade com a legislação.

Com o avanço do comércio e as exigência da Lei Geral de Proteção de Dados algumas medidas foram implantadas, no qual inicialmente podemos claramente citar os “cookies”, que se trata de uma ferramenta de armazenamento de dados pelos quais os usuários da internet tem interesse, com isso será entregue com mais frequência para aquele Lead determinados anúncios relacionados ao conteúdo pesquisado anteriormente através do tráfego pago, ferramenta essa utilizada pelas agências de marketing para impulsionar vendas para plataformas de e-commerce e marketplace, sendo assim será criado um perfil de consumo para aquele cliente (usuário).

Sob essa abordagem, é relevante mencionar a interpretação de Lins e Quinelato (*apud* Nascimento, 2022, p. 234):

> Um consentimento informado e inequívoco deve ser proveniente de um indivíduo que sabe exatamente com o que está consentindo e sua manifestação deve ser expressa, sem deixar dúvidas ou possíveis interpretações. Assim, o titular dos dados deve receber a quantidade suficiente de informação para que ele possa decidir se vai ou não consentir com aquele tratamento dos seus dados, já que excessos podem confundir mais do que informar.

Outrossim, é fundamental a validação do legítimo interesse por parte do usuário a fim de equiparar os direitos, pois, tanto o portador daqueles dados, como o encarregado de proteção de dados (DOP) fará o controle adequado e o tratamento necessário para aquela coleta realizada. Portanto o uso anárquico desses dados

pode trazer riscos, multas e sanções a empresa de e-commerce e marketplace, prejudicando todo o relacionamento entre cliente (usuário) e empresa digital.

3.1.2 Multas e sanções previstas pela lei geral de proteção de dados

A Lei Geral de Proteção de Dados (LGPD), Lei n 13.709/2018 foi estabelecida com o intuito de regulamentar o tratamento de dados pessoais no Brasil, garantindo a proteção da privacidade e dos direitos dos titulares desses dados. Entre suas diretrizes, a Lei Geral de Proteção de Dados impõe uma série de deliberações e análise para empresas que desrespeitem a suas normas, destacando a responsabilidade e a urgência.

Para garantir a efetividade dessa norma e assegurar a proteção aos direitos dos titulares. A LGPD contém um rol que disposições e prevê advertências, multas pecuniárias e que podem incluir medidas mais rigorosas, como o bloqueio ou a exclusão de dados em caso de inobservância da Lei Geral de Proteção de Dados. As multas e sanções estabelecidas pela LGPD têm como objetivo promover a conformidade e a responsabilização organizacional, buscando equilibrar a inovação tecnológica com a proteção dos direitos fundamentais à privacidade e à proteção de dados. O art. 52 da referida Lei, prevê multas e sanções:

> Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
> I - advertência, com indicação de prazo para adoção de medidas corretivas;
> II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
> III - multa diária, observado o limite total a que se refere o inciso II;
> (...)
> V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
> VI - eliminação dos dados pessoais a que se refere a infração;
> A Autoridade Nacional de Proteção de Dados (ANDP) foi instituída pela Lei Geral de Proteção de Dados (LGPD) como entidade responsável por garantir a proteção de dados dos pessoais no Brasil, a ANDP é uma autarquia federal, vinculada ao Ministério da Justiça e Segurança Pública, com proposito primordial na supervisão e implementação das normas de proteção de dados, estabelecendo um ambiente seguro que proteja os direitos dos titulares e garantir que as organizações estejam em conformidade e eficácia da legislação LGPD.
> (...)
> X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual

> período, até a regularização da atividade de tratamento pelo controlador; (Incluído pela Lei nº 13.853, de 2019)
> XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; (Incluído pela Lei nº 13.853, de 2019)
> XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. (Incluído pela Lei nº 13.853, de 2019)
> (...)

A ANDP apresenta uma gama de atribuições que são cruciais para a proteção de dados no Brasil. De acordo com o que está previsto no Artigo 55-J da Lei n 13.709/2018. Entre suas funções principais destacam-se:

Art. 55-J. Compete à ANPD:

> I - zelar pela proteção dos dados pessoais, nos termos da legislação; (Incluído pela Lei nº 13.853, de 2019)
> II - zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º desta Lei; (Incluído pela Lei nº 13.853, de 2019)
> III - elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade; (Incluído pela Lei nº 13.853, de 2019)
> IV - fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso; (Incluído pela Lei nº 13.853, de 2019)
> V - apreciar petições de titular contra controlador após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação; (Incluído pela Lei nº 13.853, de 2019)
> VI - promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança;
> (...)

Desde a sua criação, a Autoridade Nacional de Proteção de Dados (ANDP) enfrenta dificuldades de implementação da LGPD, um impasse relacionado a conscientização das organizações sobre a relevância com a proteção de dados e a exigência de se adequarem às novas demandas, pois muitas empresas ainda não estão de acordo com a Lei Geral de Proteção de Dados, o que intensifica a relevância da ANDP ainda mais essencial.

CONCLUSÃO

Desse modo, o estudo destaca a relevância da proteção de dados no contexto do comércio eletrônico e marketplace, demonstrando o impacto direto da Lei Geral de Proteção de Dados (LGPD) Lei n. 13.709/2018 no tratamento de dados pessoais. Juntamente com legislações anteriores, como o Marco Civil da Internet, Lei n. 12.965/2014, a Lei Geral de Proteção de Dados desempenha um papel fundamental na salvaguarda dos direitos dos usuários e na regulação das atividades online como a coleta, o tratamento e o armazenamento dos dados coletados. Este trabalho demonstra que a proteção de dados não é apenas uma questão jurídica, mas se faz necessária para construir a confiança e credibilidade entre consumidores, pois um consumidor informado tende a ser mais fiel, contribuindo para o sucesso das empresas de e-commerce e marketplace, com base na troca de informações pessoais que ocorrem constantemente.

Os resultados indicam que a implementação dos princípios da LGPD pelas empresas do setor digital é crucial para a transparência e segurança do processamento de dados, ou seja, todas as empresas que tiveram o cuidado em estar em comum acordo com a legislação se torna uma empresa digital de referência, levando em consideração a importância daquele cliente para o sucesso dessa empresa seja ela e-commerce ou marketplace. Destaca também a importância de bases jurídicas sólidas, como o consentimento informado e o cumprimento das obrigações legais, para que as empresas possam coletar, armazenar e processar dados de forma ética, no qual visam proteger os direitos dos titulares desses dados, prevenindo abusos ou vazamento de dados que podem ser considerados como incidentes de segurança. Dessa forma, esses vazamentos não apenas comprometem a privacidade dos indivíduos afetados, mas também resultam na perda de confiança por parte do cliente (usuário), além disso, pode acarretar em consequências mais severas para empresas digitais responsáveis pelo tratamento desses dados.

Sendo assim, o Marketing tem um papel essencial para o sucesso do comércio digital, no qual possui várias responsabilidades, principalmente no que diz a respeito da coleta e tratamento de dados pessoais fornecido por consumidores, partindo da premissa de uma coleta de número telefônico ou e-mail o que torna esse consumidor um lead para aquela empresa digital. Os dados coletados são

importantes para a produção de ofertas e campanhas de marketing, além do mais, possui o intuito de entregar um informativo para aquele usuário do mercado digital que as empresas digitais estão em conformidade com a Lei Geral de Proteção de Dados e trabalha de forma clara e transparente com aquele cliente.

Uma análise dos dispositivos da Lei Geral de Proteção de Dados (LGPD) revela a importância fundamental da base legal para o tratamento de dados pessoais, enfatizando a proteção e a privacidade das pessoas físicas. Ao estabelecer o controle dos usuários sobre suas informações, a LGPD não apenas garante a transparência no uso dos dados, mas também promove o processamento ético e responsável.

As normas específicas para dados sensíveis e as proteções adicionais para as informações das crianças refletem a seriedade com que a legislação aborda as questões de privacidade. Além do consentimento, a possibilidade de tratamento de dados em circunstâncias especiais, como o cumprimento de obrigações legais, demonstra o necessário equilíbrio entre os direitos do titular dos dados e as necessidades sociais e operacionais. Em suma, a LGPD não só protege os direitos dos cidadãos, mas também estabelece um quadro regulamentar que permite às empresas operarem de forma responsável.

Com a constante evolução da coleta, tratamento e armazenamento dos dados pessoais e o crescimento do comércio eletrônico, a experiência do usuário é primordial para o bom funcionamento e sucesso do e-commerce ou marketplace, no qual exige mudanças e uso de software capaz de fazer a coleta e armazenamento adequado, no qual permite que as empresas construam uma reputação sólida. Além do mais a plataforma digital no qual é mais propenso a violação de privacidade deve ser realizada sempre com cautela e transparência, o uso de “Cookies” é uma forma de personalizar a experiência do usuário, mas deve ser realizado com o consentimento informado e inequívoco dos titulares dos dados. Sendo assim, é preciso a designação de um encarregado de proteção de dados (DOP), no qual fará um tratamento e controle adequado para os dados coletados.

A Lei Geral de Proteção de Dados trouxe um processo desafiador para todas as empresas quando entrou em vigor a referida lei em 2020, pois, exigiu que todo o comércio realizasse uma análise e um mapeamento profundo em relação aos seus processos de coleta, tratamento e armazenamento de dados, priorizando a transparência e a segurança desses dados sensíveis ou não. Apesar do custo

significativo para essas adequações, a adequação com a legislação é inadiável. A implementação de medidas técnicas e treinamentos adequados dentro das empresas de e-commerce e marketplace são cruciais para garantir que as práticas estão em comum acordo com a Lei Geral de Proteção de Dados (LGPD). Portanto, deve ser vista como um compromisso estratégico e contínuo que vai além de uma mera adequação pontual.

Contudo, a Lei Geral de Proteção de Dados, além de redefinir a forma como as empresas digitais tratam os dados pessoais, estabelece novas responsabilidades para as organizações. A Autoridade Nacional de Proteção de Dados (ANPD) funciona como um órgão regulador que fiscaliza a aplicação da legislação e promove a educação sobre a proteção de dados. A atuação da ANPD é imprescindível para garantir que as empresas cumpram as normas da Lei Geral de Proteção de Dados (LGPD), mas também compreendam o valor da privacidade e proteção de dados. Não se trata apenas de monitorar e aplicar sanções, mas também de promover boas práticas e desenvolver orientações para ajudar as empresas digitais a passar pelo complexo ambiente da LGPD.

Portanto, a adaptação à LGPD, a integração da ANPD deve ser vista como uma oportunidade para as empresas do e-commerce e marketplace evitarem penalidades e também aumentarem a confiança dos consumidores e se diferenciarem no mercado. O compromisso com a proteção de dados deve ser contínuo, incluindo a atualização contínua de processos e a formação de equipes para transformar a conformidade numa vantagem competitiva. Dessa forma, a Lei Geral de Proteção de Dados (LGPD) e a Autoridade Nacional de Proteção de Dados (ANPD) trazem uma oportunidade para inovar e melhorar o relacionamento com os clientes, garantindo um futuro mais seguro e responsável na utilização de dados pessoais.

REFERÊNCIAS

BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, [2016]. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 12 jun. 2024.

BRASIL. [Lei. 13.709/2018]. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, [2018]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 12 jun. 2024.

BRASIL. [Lei. 12.965/2014]. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, [2014]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 12 jun. 2024.

NASCIMENTO, Claudemir. A aplicabilidade das bases kegais da LGPD na estratégia de funil de vendas perpétuo no mercado digital: uma análise do consentimento e legítimo interesse. Res. Severa Verum Gaudium v.7, n1, (2022). Disponível em: https://seer.ufrgs.br/index.php/resseveraverumgaudium/article/view/125569/87251. Acesso em: 16 out. 2024.

DE MORAES, Alexandre. Direitos humanos fundamentais. 5. ed. São Paulo: Atlas, 2003.

MORAIS, Jose Luis; NETO, Elias. SURVEILLANCE E ESTADO-NAÇÃO: AS INADEQUADAS TENTATIVAS DE CONTROLAR OS FLUXOS DE DADOS ATRAVÉS DO MARCO CIVIL DA INTERNET E DA CPI DA ESPIONAGEM, [S. l.], p. 13, 2014. Disponível em: http://publicadireito.com.br/artigos/?cod=2f7eaf16eceec07f. Acesso em: 11 jun. 2024.

SILVA, M. A. C. et al. Cultura Inovativa e Formação de Ambiente Inovador. XVII

SEMEAD Seminários em Administração, ISSN 2177-3866. São Paulo: out. 2014.

SOUZA, Carlos Affonso. Marco civil da internet: construção e aplicação / Carlos Affonso Souza e Ronaldo Lemos, Juiz de Fora: Editar Editora Associada Ltda, 2016.

TEIJEIRA CLARO, Roberto; GARCIA, Domingos Sávio da Cunha; ARAÚJO, Leonardo Amorim de; LEAL, Carlos Artur Alevato; ASSUNÇÃO, ArthurNascimento; MACHADO, Lisleandra. Aplicação Inovadora da LGPD na Segurança da Informação em Empresas de Desenvolvimento de Software.
Disponível em: https:// Vista do Aplicação Inovadora da LGPD na Segurança da Informação em Empresas de Desenvolvimento de Software (ifc.edu.br).
Acesso em: 16 de OUT. 2024.
TEFFÉ,Chiara Spadaccini de; VIOLA,Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. Civilistica.com. Rio de Janeiro, a. 9, n. 1, 2020. Disponível em:

<http://civilistica.com/tratamento-de-dados-pessoais-na-lgpd/>. Acesso em: 21 set. 2024

TOMASEVICIUS. EDUARDO. F. Marco Civil da Internet: uma lei sem conteúdo Normativo. Disponível em: https:// www.scielo.br/j/ea/a/n87YsBGnphdHHBSMpCK7zSN/?format=pdf&lang=pt. Acesso em: 11 de jun. 2024.