CENTRO UNIVERSITÁRIO UNIDADE DE ENSINO SUPERIOR DOM BOSCO – UNDB
CURSO DE DIREITO

THALYTA STHEFANY MENDES MELO

LGPD E DIREITO À PRIVACIDADE EM MEIO A SOCIEDADE DO CONSUMO: o tratamento dos dados pessoais no comércio eletrônico a partir do pseudoconsentimento do consumidor

São Luís
2023

THALYTA STHEFANY MENDES MELO

LGPD E DIREITO À PRIVACIDADE EM MEIO A SOCIEDADE DO CONSUMO: o tratamento dos dados pessoais no comércio eletrônico a partir do pseudoconsentimento do consumidor

Monografia apresentada ao Curso de Graduação em Direito do Centro Universitário Unidade de Ensino Superior Dom Bosco como requisito parcial para obtenção do grau de Bacharela em Direito.

Orientador: Prof ª. Ma. Thaís Emília de Sousa Viegas

São Luís

2023

Dados Internacionais de Catalogação na Publicação (CIP)

Centro Universitário – UNDB / Biblioteca

Melo, Thalyta Sthefany Mendes

Lgpd e direito à privacidade em meio a sociedade do consumo: o tratamento dos dados pessoais no comércio eletrônico a partir do pseudoconsetimento do consumidor./ Thalyta Sthefany Mendes Melo. __ São Luís, 2023.

57 f.

Orientador: Profa. Ma. Thaís Emília de Sousa Viegas.

Monografia (Graduação em Direito) - Curso de Direito – Centro Universitário Unidade de Ensino Superior Dom Bosco – UNDB, 2023.

1. Consumidor. 2. Comércio eletrônico. 3. LGPD. 4. Privacidade. I. Título.

CDU 347.451.31:004.738.5

THALYTA STHEFANY MENDES MELO

LGPD E DIREITO À PRIVACIDADE EM MEIO A SOCIEDADE DO CONSUMO: o tratamento dos dados pessoais no comércio eletrônico a partir do pseudoconsentimento do consumidor

Monografia apresentada ao Curso de Graduação em Direito do Centro Universitário Unidade de Ensino Superior Dom Bosco como requisito parcial para obtenção do grau de Bacharela em Direito.

Aprovada em: 30/11/2023.

BANCA EXAMINADORA

Prof ª. Ma. Thaís Emília de Sousa Viegas (Orientadora)

Centro Universitário Unidade de Ensino Superior Dom Bosco - UNDB

Adv. Esp. Rebeca Laís de Jesus Costa (Membro Externo)

Advogada Especialista

Prof. Me. Roberto de Oliveira Almeida

Centro Universitário Unidade de Ensino Superior Dom Bosco - UNDB

A Deus, meus pais e minha família.

AGRADECIMENTOS

À Deus, por sempre me conceder forças no enfrentamento dos desafios e por abençoar o meu caminho, não só durante esses anos de graduação, mas em toda a minha vida.

Aos meus pais, Emmanuele e Wagner, que sempre se decidiram por mim, mesmo sendo tão novos quando eu cheguei na vida deles. Obrigada por serem incansáveis em me fazer uma pessoa melhor, pelo apoio e amor incondicional que sempre me deram. Devo minha vida a vocês.

À toda a minha família, em especial a família Buscapé, que sempre me apoia e que torce constantemente por mim. Quem tem uma família tem tudo, mas quem tem uma família como vocês tem muito mais. Vocês fazem parte de tudo que eu sou.

Ao meu noivo, Alexandre, por todos os anos de companheirismo e por sempre ter acreditado que eu sou capaz. Obrigada por me ajudar a ser menos dura comigo mesma. Obrigada por lidar pacientemente com os meus estresses ao longo desses anos de graduação e por ter sido compreensivo em todos os momentos.

Aos amigos que fiz durante esses anos de curso: Davi, Júlia, Lays, Márcio, Maria Clara, Melanie e Rodson. A graduação foi muito mais leve e fácil porque encontrei vocês para compartilhar essa caminhada.

De forma particular agradeço a Lays, que é calmaria no meio do caos, tua amizade é um grande presente. Agradeço também a Márcio, que faz uma grande diferença na minha vida e traz pra ela muita alegria e leveza. Obrigada por deixar os perrengues da vida mais leves. E por fim agradeço a Melanie que esteve presente desde o início da graduação, compartilhando juntas todos os momentos de alegrias e de desespero. Obrigada por estar comigo em TODOS os momentos - do corte de cabelo ao pedido de casamento.

À Nathália, minha amiga desde a época da escola, com quem eu compartilho todas as alegrias e angústias. Obrigada por ter me apoiado em todas as etapas e, principalmente, por ter permanecido.

Aos meus companheiros de estágio, Giovanna e Fernando, pela paciência nas inúmeras vezes que eu falava sobre esta pesquisa; e ao meu chefe Carlos Brissac pela troca de ideias, pelo seu tempo e dedicação.

Por fim, à minha orientadora, Thais Viegas, agradeço pela orientação, por ter acreditado no meu projeto, pelo carinho e contribuição na minha pesquisa. Agradeço ainda a professora Aline Fróes por quem sou grata pela paciência e atenção. Obrigada pelas palavras de consolo e apoio.

À todas as pessoas que, apesar de não citadas individualmente, de alguma forma me apoiaram e contribuíram ativamente para a conclusão dessa etapa. Muito Obrigada!

“No presente, as pessoas ficam contentes de ceder seu ativo mais valioso – seus dados pessoais – em troca de serviços de e-mail e vídeos de gatinhos fofos gratuitos.”

Yuval Harari

RESUMO

A fragilidade do consumidor mediante o uso dos seus dados pessoais no ambiente digital, ensejou o surgimento de um instrumento jurídico para regular o tratamento de dados, assim foi sancionada a Lei Geral de Proteção de Dados (LGPD). Diante deste cenário, resta estabelecido como problema de estudo o seguinte questionamento: como o tratamento inadequado dos dados pessoais no comércio eletrônico gera prejuízos ao titular dos dados? Em resposta são levantadas as hipóteses de que o compartilhamento de dados pessoais entre empresas pode levar a uma maior coordenação de preços e práticas comerciais, o que pode resultar em preços mais altos para os consumidores. A disponibilidade de dados pessoais também pode levar ao surgimento de novos modelos de negócios baseados na exploração de informações pessoais, como a venda de dados para terceiros. O presente estudo tem por objetivo analisar as consequências fáticas do uso indiscriminado de dados e a forma de tratamento de dados pessoais no comércio eletrônico pelas empresas. Para tanto, utilizou-se a pesquisa bibliográfica e documental nos procedimentos descritivo e exploratório, com abordagem dedutiva. A partir dessa análise, chegou-se à conclusão de que o tratamento inadequado dos dados pessoais gera prejuízos aos titulares de dados e, consequentemente, aos consumidores-usuários, assim a Lei Geral de Proteção de Dados Pessoais (LGPD) com a criação da Autoridade Nacional de Proteção de Dados Pessoais (ANPD) são indispensáveis para garantir o tratamento adequados aos dados pessoais, colaborando no combate de abusos econômicos, principalmente as práticas de dominação de mercado por meio das publicidades, baseadas no tratamento de dados pessoais.

Palavras-chave: consumidor; comércio eletrônico; LGPD; dados pessoais.

ABSTRACT

The fragility of the consumerist through the use of your personal data in the digital environment, which gives rise to the necessity of a legal instrument to regulate the processing of data, thereby it was sanctioned the General Data Protection Law (GDPL). Given this scenario, it remains established as a study problem the following questioning: how does the processing of personal data influences the increase in online consumption? To answer that, hypotheses are raised that the sharing of personal data between companies can lead to a major price coordination and commercial practices, which can result in higher prices for consumers. The availability of personal data can also give rise to new business models based on the exploitation of personal information, such as selling data to third parties. The present study has the purpose of analyze the consequences of the indiscriminate use of data and the way of processing personal data in e-commerce by companies. To this end, bibliographical and documentary research was used in the descriptive and exploratory procedures, with a deductive approach. Based on this analysis, it was concluded that inadequate handling of personal data lead to losses to data subjects and, consequently, to consumers-user, therefore, the National Data Protection Authority (NDPA) and the General Data Protection Law (GDPL) are indispensable to ensure the proper processing of personal data, contributing to the prevention of economic abuses, mainly the market dominance practices through advertisements, based on the processing of personal data.

Keywords: consumerist; e-commerce; GDPL; personal data.

LISTA DE SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
ANPD	Autoridade Nacional de Proteção de Dados
B2B	Business-to-business
B2C	Business-to-consumer
B2G	Business-to-Government
C2C	Consumer- to-consumer
CDC	Código de Defesa do Consumidor
CE	Conselho Europeu
CNDC	Conselho Nacional de Defesa do Consumidor
DPO	Data Protection Officer
LGPD	Lei Geral de Proteção de Dados
GDPR	General Data Protection Regulation
SENACON	Secretária Nacional do Consumidor
TIC	Tecnologia da Informação e Comunicação

SUMÁRIO

1 INTRODUÇÃO

Na atual sociedade, as pessoas buscam cada vez mais criar laços sociais por meio do consumo. Isso se deve ao fato de que a realidade socioeconômica é dominada pelas experiências proporcionadas pelas mercadorias e pelos valores associados a elas, os quais se tornaram objetos de desejo intrínsecos ao consumidor moderno.

Anteriormente, o valor do consumo estava baseado na aquisição de propriedades, acumulação de bens materiais, segurança, apego e compromisso com a durabilidade e a estabilidade. No entanto, atualmente, ele é pautado pela economia digital, comunicação difusa, individualização crescente e flexibilização das tradições e estruturas sociais. Assim, o consumo atual não se destina mais a satisfazer necessidades biológicas ou alcançar um padrão de vida coletivamente desejado, mas, principalmente, a preencher níveis simbólicos cada vez mais subjetivos (Radfahrer, 2018).

O direito à privacidade assegura que as pessoas tenham controle sobre suas informações pessoais e a devida proteção contra abusos, discriminação e violações da sua intimidade. No contexto da disseminação de dados, o direito à privacidade é especialmente importante para evitar que informações sensíveis e íntimas sejam indevidamente expostas ou usadas de maneira prejudicial.

Os avanços tecnológicos permitiram a disseminação em massa do acesso à informação e a globalização, fazendo com que o ambiente digital se tornasse um local onde as pessoas não apenas consomem informações, mas também são como uma espécie de "produtos" desejados pelas empresas que buscam ampliar suas vendas no comércio eletrônico. Ademais as barreiras que antes separavam os consumidores foram encurtadas, permitindo a comunicação e aproximação independentemente da distância física. Assim, as pessoas podem vender e adquirir produtos independente de onde estejam (Radfahrer, 2018).

Portanto, a publicidade destinada ao público adequado tem o poder de inspirar desejos e se destacar no mercado fazendo com que as informações e, especialmente, os dados, se tornem uma moeda de grande importância na economia. Por conta desse avanço tecnológico, questiona-se: como o tratamento inadequado dos dados pessoais no comércio eletrônico gera prejuízos ao titular dos dados?

A exploração dos limites da privacidade na era da tecnologia é primordial para o uso adequado dos meios digitais, haja vista o monitoramento do usuário estão diretamente ligados a personalização *online*, assim como na influência da economia.

O vazamento e disseminação de dados pessoais podem ser utilizados pelas empresas

para criar campanhas de publicidade altamente segmentadas, que visam diretamente os interesses e necessidades individuais do usuário, aumentando assim a probabilidade de conversão em vendas (Doneda, 2019).

Nesse contexto, o compartilhamento de dados pessoais entre empresas pode levar a uma maior coordenação de preços e práticas comerciais, o que pode resultar em preços mais altos para os consumidores. A disponibilidade de dados pessoais também pode levar ao surgimento de novos modelos de negócios baseados na exploração de informações pessoais (Doneda, 2019).

Constituir pesquisa que aprofunde conhecimentos em um assunto tão importante é ferramenta fundamental de contribuição para a sociedade científica. Assim, notória a importância acadêmica deste estudo que esclarece a realidade por trás do comércio eletrônico em nível nacional, elucida-se a trajetória do meio digital, mostrando como se chegou até o cenário atual, além de elucidar como as empresas que estão no meio eletrônico utilizando dos dados pessoais para crescerem cada vez mais.

Em adição, constitui-se ainda como ferramenta social que deslinda o que a lei efetivamente estabelece e as expectativas futuras a seu respeito, reflexões necessárias que, caso não sejam realizadas, podem gerar desconhecimento populacional sobre um direito fundamental, qual seja, a privacidade e a proteção de dados. Ressalta-se também que esta pesquisa é fator de enriquecimento pessoal e motivação para posteriores atuações no mesmo sentido.

O presente trabalho é de natureza bibliográfica e documental, ou seja, toma por base livros, artigos científicos, trabalhos acadêmicos, legislação e documentos sem prévio tratamento analítico (Gil, 2008). Conta ainda com o procedimento de pesquisa descritivo, que, segundo Gil (2008), ocupa-se de retratar aspectos de uma sociedade ou fenômeno, de modo a estabelecer conexões entre os fatores, bem como do procedimento exploratório. Além disso, terá abordagem dedutiva, uma vez que partirá de premissas maiores para chegar a conclusões por meio da lógica (Severino, 2010).

Esta pesquisa tem por objetivo central analisar as consequências fáticas do uso indiscriminado de dados e a forma de tratamento de dados pessoais no comércio eletrônico pelas empresas. Tem-se como primeiro objetivo específico discutir a privacidade sob a perspectiva constitucional, no contexto de uma sociedade de consumo; o segundo objetivo específico se propõe a compreender aspectos da Lei Geral de Proteção de Dados e o tratamento de dados pessoais no comércio eletrônico; e por fim, esta pesquisa analisa os impactos da não-

observância da LGPD na proteção de dados pessoais e na privacidade no comércio eletrônico frente a publicidade direcionada.

Para tanto, utiliza-se de três capítulos. O primeiro aborda o direito à privacidade enquanto direito fundamental, utilizando, para além da teoria constitucional, uma análise histórica e legislativa. O segundo aborda o papel da LGPD frente a proteção do consumidor e a responsabilização das empresas. Por fim, o terceiro capítulo trata do impacto da não-observância da LGPD na privacidade do consumidor, diante do comércio eletrônico e da publicidade direcionada.

2 O DIREITO À PRIVACIDADE SOB A PERSPECTIVA CONSTITUCIONAL NO CONTEXTO DA SOCIEDADE DE CONSUMO

Este capítulo inaugural apresenta a origem do direito à privacidade e uma contextualização ampla e histórica a seu respeito, primeiramente em nível mundial e posteriormente em nível nacional. Nesse último caso, faz-se uma relação no tocante à sua caracterização enquanto um direito fundamental no contexto contemporâneo da sociedade de consumo. Por fim, o último tópico do presente capítulo apresenta o direito à privacidade e sua trajetória até a elevação da proteção de dados como direito fundamental, evidenciando como os avanços tecnológicos e o novo formato da relação de consumo influenciaram o cenário atual.

2.1 A origem do direito à privacidade e a sua consolidação na legislação brasileira

O desenvolvimento da internet e da tecnologia fez surgir uma nova forma de relacionamento entre os indivíduos. As barreiras da privacidade são cada vez mais ultrapassadas com os avanços tecnológicos, por isso a privacidade tem se distanciado da vida íntima. Nesse sentido, o sociólogo Zygmun Bauman preceituava que a sociedade deixou de ser "sólida" e passou a ser "líquida", estando a liquidez diretamente ligada as evoluções da Tecnologia da Informação e Comunicação (TIC), nos anos 90 (Bauman, 2011).

A ideia da sociedade líquida é intensificada pelos ensinamentos do sociólogo Pierry Levy ao pontuar a cibercultura e os efeitos da utilização da comunicação expressa e por meio da internet. De acordo com Levy, as mudanças na atuação da comunicação humana vêm desde as escritas de cartas e telefonemas - no entanto, há de se observar a diferença principal entre estes meios de comunicação e o objeto de estudo desta pesquisa: a quantidade de receptores da mensagem repassada (*apud* Vieira, 2007).

Na visão de Levy (*apud* Vieira, 2007), enquanto correios e telefonemas se inserem num conceito um-a-um, na internet "um centro emissor envia suas mensagens a um grande número de receptores passivos e dispersos". Aqui cabe também o entendimento de que a internet não é um espaço alheio ao mundo real, sendo parte inerente da vida cotidiana. São expressões de grupos sociais e indivíduos, potencializados pela maior eficiência da internet e da utilização das redes sociais.

A interação e a integração de computadores interligados pela rede da internet abriram caminho para a emergência de um novo domínio geográfico - o *ciberespaço* - que se concretiza

por meio de meios de comunicação tecnológicos e interativos. A noção de *ciberespaço* teve seus primeiros traços em 1894 mesmo antes da existência de uma rede global de internet que conectou máquinas e pessoas em todo o mundo.

Compreendendo a expansão das comunicações através da internet, há de se retomar também o surgimento dos conceitos de privacidade do início da vida privada no Século XVI ao pensamento firmado por John Locke e John Stuart Mill. Locke trouxe a ideia de liberdade como autonomia para dispor de tudo que lhe pertença, enfatizando a ideia de individualidade e espaço privado. Já Mill, apesar do pensamento resultar nos conceitos de privacidade, trouxe a ideia de que o indivíduo é soberano sobre si, sendo suas ações individuais independentes da sociedade como um todo (Vieira, 2007).

Ainda incipiente, as ideias de liberdade e autonomia não mencionam a privacidade em si, somente surgindo após as escritas do alemão David Augusto, em 1846, definindo o direito à privacidade enquanto "incomodar alguém com perguntas indiscretas ou entrar em um aposento sem se fazer anunciar".

Na seara judicial, há a primeira menção ao direito à privacidade, sem que lhe seja propriamente mencionado, no caso *Affaire Rachelix c. O'Connell*, no qual uma atriz fora fotografada no leito de morte e, de forma não autorizada, um desenhista utilizou da foto para elaboração de um desenho que fora posteriormente publicado em um seminário. A família da atriz acionou o Tribunal Civil de Sena e a decisão foi no sentido de não permitir que fosse publicizado ou reproduzido os traços de uma pessoa em seu leito de morte (Cancelier, 2017).

Após os acontecimentos citados, a privacidade foi citada em diversos outros momentos da história e somente expressamente disposta na Declaração Universal dos Direitos do Humanos, em 1948. Percebe-se, então, que o direito à privacidade nada mais é que o exercício da própria liberdade - tantas vezes confundida com a privacidade em si. O primeiro retrata o direito à quietude a escolha de se manter em sua própria solitude, impedindo que se explore a vida particular, quanto o direito à liberdade permite que o indivíduo exerça o direito de escolha em expandir os aspectos de sua vida da maneira que lhe for mais conveniente (Vieira, 2007).

Entre os mais diversos conceitos surgidos acerca da privacidade em si, destacam-se os ensinados por Celso Bastos e por Gilberto Haddad. De modo a se complementar, Bastos afirma que a privacidade é a faculdade de cada pessoa ao impedir acesso de terceiros às informações de sua vida, enquanto Haddad afirma que a escolha também versa acerca das informações que possam revelar aspectos da personalidade da pessoa (Cancelier, 2017).

O ato de impedir o acesso de terceiros é obstado pela intromissão de estranhos na vida pessoal do indivíduo, conforme destaca Paulo José da Costa Júnior:

> Na expressão "direito à intimidade" são tutelados dois interesses, que se somam: o interesse de que a intimidade não venha a sofrer agressões e o de não venha a ser divulgada. O direito, porém, é o mesmo. O que pode assumir uma gama diversa é o interesse protegido pelo direito. São duas esferas de interesses abarcadas no mesmo raio de proteção do mesmo direito. No âmbito do direito à intimidade, portanto, podem ser vislumbrados esses dois aspectos: a invasão e a divulgação não autorizada da intimidade legitimamente conquistada. Em termos de conteúdo, todavia, não deve prevalecer a distinção (Costa Júnior, 2004, p. 32).

Para compreender as diversas formas de violação de privacidade, se faz necessário voltar à contextualização atual da sociedade: sabe-se que os avanços tecnológicos firmaram também uma sociedade de informação - em razão do fácil acesso a informações na sociedade pós-industrial (Doneda, 2006).

A sociedade está imersa em uma era na qual tanto interesses públicos quanto privados frequentemente justificam a contínua violação da privacidade dos cidadãos. Simultaneamente, o comportamento de cada indivíduo torna desafiante a preservação de uma presunção geral de respeito à privacidade. Contudo, sublinhar a significância do direito à privacidade, independentemente da forma como se manifesta, é enaltecer a liberdade, combater a discriminação e salvaguardar as decisões pessoais de cada indivíduo.

O Estado entende, então, que não é possível concentrar o controle de informações nele mesmo, visto que o controle das informações agora vem do titular das ditas informações - um indivíduo ativo nos meios digitais. Os indivíduos detêm, então, o poder e o direito de exercer o controle sobre as alegações que proferem em meios digitais. No entanto, em razão da latente vulnerabilidade técnica na qual grande parte da sociedade está inserida, não é de fácil percepção, para um cidadão comum, a utilização de seus dados pessoais e dados sensíveis de modo indevido, razão pela qual o Estado, apesar de não poder controlar o fluxo de informações que atravessam a internet, criou normas que dispõem acerca da privacidade, da intimidade e da utilização de dados pessoais.

Alguns países não mencionam a privacidade em seu corpo constitucional, como o Reino Unido, que reconhece o direito de modo jurisprudencial. O Brasil inseriu o direito à privacidade no texto da Constituição em 1988, inserindo-o no corpo do artigo 5º (Cancelier, 2017).

Percebe-se que no contexto brasileiro, tanto a Constituição de 88 quanto o Código Civil de 2002 também se abstiveram de usar diretamente o termo, utilizando sinônimos para postular este direito. Nesse sentido, a Constituição faz referência ao sigilo e à inviolabilidade do domicílio, a fim de salvaguardar o direito à privacidade.

Há ainda na Carta Magna outros dispositivos que se debruçam para assegurar e consolidar a privacidade. Alguns incisos do art. 5º asseguram a inviolabilidade e o sigilo da vida privada, bem como o acesso a informações, desde que respeitado o segredo da fonte quando necessário para o exercício profissional. É trazido ainda por este artigo o *habeas data*, instrumento jurídico que garante o direito das pessoas de acessarem informações pessoais armazenadas em bancos de dados, a fim de solidificar o direito à privacidade do âmbito jurídico brasileiro.

2.2 Privacidade e sua caracterização enquanto direito fundamental no contexto contemporâneo da sociedade de consumo

Carlos Alberto Bittar (2001) classifica os direitos da personalidade em três categorias distintas: direitos físicos, direitos psíquicos e direitos morais. A proteção do direito à vida, à integridade física, imagem, voz e ao corpo estariam abarcadas pelos direitos físicos. O direito à liberdade de pensamento e expressão fazem parte dos direitos psíquicos e no que tange os direitos morais, tutelam os direitos à identidade, à honra e o direito às criações intelectuais. Independentemente dessa categorização, o objetivo é um só: a proteção do indivíduo, possibilitando o direito subjetivo de exigir dos outros o respeito à sua existência.

Os direitos de personalidade possuem características distintas de outros direitos ordinários, como: são personalíssimos, gerais, inatos, vitalícios, absolutos, indisponíveis, irrenunciáveis, imprescritíveis e extrapatrimoniais. Ao serem considerados direitos da personalidade, portanto, inatos, cabe ao Estado tutelar um plano de direito positivado, motivo pelo qual o direito à privacidade fora incorporado no artigo 5º da Constituição de 88.

Nas palavras de Robert Alexy (2008) são três os níveis de proteção da privacidade:

> A esfera mais interna, caracterizando-se por ser o âmbito mais íntimo, a esfera íntima intangível, o âmbito núcleo absolutamente protegido da organização da vida privada, compreendendo os assuntos mais secretos que não devem chegar ao conhecimento dos outros devido à sua natureza extremamente reservada; a esfera privada ampla, que abarca o âmbito na medida em que não pertença à esfera mais interna, incluindo assuntos que o indivíduo leva ao conhecimento de outra pessoa de sua confiança, ficando excluído o resto da comunidade; e a esfera social, que engloba tudo o que não for incluído na esfera privada ampla, ou seja todas as matérias relacionadas com as notícias que a pessoa deseja excluir do conhecimento(s) de terceiros (Alexy, 2008).

Apesar da proteção, em todos os níveis conceituados por Alexy, serem considerados direitos fundamentais, há de se ressaltar também o caráter relativo acerca dos direitos fundamentais. Norberto Bobbio (*apud* Doneda, 2006) explica ser raro um direito fundamental

nunca colidir com outro direito fundamental, a depender do contexto de colisão e da titularidade do direito ou mesmo ao recorte populacional ao qual o direito fundamental se direciona (Doneda, 2006).

Em conexão com o meio virtual, cabe a conclusão de um estudo proferido pelo Secretariado de Saúde, Educação e Bem Estar dos Estados Unidos da América, ainda em 1973, sobre a relação entre privacidade e dados pessoais: a privacidade de um indivíduo é diretamente afetada pela maneira com a qual suas informações são divulgadas. Por conta disso, fez-se necessário estipular que aquele titular dos dados deve ter o poder de decisão sobre registro, divulgação ou mesmo utilização de quaisquer dados sob sua titularidade - salvo se autorizados por lei (Siqueira *et al.*, 2021).

Surgem então as noções introdutórias de que o armazenamento de dados, ainda que central, não deveria ser mantido em segredo dos indivíduos titulares dos dados, além da ideia também de que o titular dos dados deveria possuir autonomia para decidir acerca da utilização de seus dados e também de corrigi-los ou retificá-los (Silva, 2019).

Estas ideias iniciais, desenvolvidas no estudo norte americano, foram basilares para a construção do *guideline* da OCDE e na Convenção de Strasbourg. Vale mencionar que os mesmos princípios desenvolvidos neste contexto histórico são utilizados, ainda hoje, através da atual Lei Geral de Proteção de Dados - princípio da publicidade, da exatidão, da finalidade, do livre acesso e da segurança (Silva, 2019).

A Convenção de Strasbourg também conhecida como Convenção Europeia dos Direitos Humanos, estabelece um conjunto abrangente de direitos e liberdades que os Estados signatários buscam respeitar e garantir aos seus cidadãos, como o direito à vida, a liberdade e a segurança pessoal, a exclusão da tortura, a liberdade de pensamento, consciência e religião, a liberdade de expressão, o direito ao respeito à vida privada e familiar, e ao direito à liberdade de reunião e associação.

A partir das definições acima, menciona-se que a Convenção de Strasbourg nº 108 do Conselho Europeu buscou unificar as informações e diretrizes sobre a privacidade no *ciberespaço* em todos os Estados pertencentes ao espaço geopolítico. O primeiro artigo dispôs o seguinte:

> Artigo 1º - Objectivos e finalidades A presente Convenção destina-se a garantir, no território de cada Parte, a todas as pessoas singulares, seja qual for a sua nacionalidade ou residência, o respeito pelos seus direitos e liberdades fundamentais, e especialmente pelo seu direito à vida privada, face ao tratamento automatizado dos dados de carácter pessoal que lhes digam respeito (Conselho Europeu, 1981).

Há uma evidente conexão do direito à privacidade e ao tratamento automatizado de dados, obrigatoriamente adotado por todos em território europeu - não necessariamente por nacionais.

O documento propulsor, originado na Convenção, é datado em 1985, sendo seguido por diversas outras diretrizes, como a Diretiva 95/46/CE do Parlamento Europeu e do Conselho Europeu (CE), 10 anos depois, estabelecendo 72 "diretrizes" sobre coleta e tratamento de dados, considerando o direito à privacidade do titular dos dados (Passos, 2017).

Por fim, em 2000, a Carta dos Direitos Fundamentais da União Europeia dispôs de um artigo exclusivo para proteção de dados pessoais, estabelecendo, por vez, o direito à privacidade no meio digital enquanto um direito fundamental. No Brasil, há de se mencionar que antes de qualquer disposição normativa no sentido da proteção de dados, houve a possibilidade de utilizar do remédio constitucional *habeas data*, cujo objetivo é ser um instrumento para acessos a informações pessoais em bancos de dados de caráter público - em especial àqueles acontecidos durante o regime militar (Doneda, 2011).

Em momentos em que não existia uma legislação específica para a privacidade em meios virtuais, cabe o ensinamento de Danilo Doneda (2011) ao mencionar que "há um hiato que segrega a tutela da privacidade, esta constitucionalmente protegida, da tutela das informações pessoais em si". Essa diferenciação é importante uma vez que há a possibilidade de uma interpretação errônea acerca dos conceitos, fazendo com que o agente interpretador se desobrigue de reputar ofensas à privacidade na hipótese de utilização imprópria dos dados.

Mais uma vez retornando aos primeiros conceitos apresentados na primeira seção, não é plausível desconsiderar o momento líquido e efêmero no qual a sociedade está inserida, no qual a imagem de um indivíduo é valorada através daquilo que é representado a terceiros - motivo pelo qual uma ofensa indireta à privacidade, através do uso inadequado de dados pessoais, é uma ofensa à honra subjetiva, objetiva e ao direito fundamental do indivíduo.

A construção da fundamentalidade do direito à privacidade ocorreu de modo moroso e desafiador, o avanço tecnológico no qual a sociedade estava inserida transcorreu de modo muito rápido. No entanto, a partir das resoluções e estudos advindos, principalmente, da União Europeia, foi possível chegar num tom uníssono em relação à necessidade de absoluta proteção do titular daqueles dados, ainda que em meios virtuais, fazendo com que a existência de Lei Geral de Proteção de dados seja imprescindível para o estabelecer de uma perspectiva social e democrática da privacidade.

Vale destacar que antes da década de 80 o Código Comercial pautava a relação consumerista, logo após, com a abertura democrática e o crescimento econômico, teve origem

o Direito do Consumidor, haja vista o aumento exponencial do consumo no país (Benjamin, 2012). Por meio do Decreto 91.469 criou-se o Conselho Nacional de Defesa do Consumidor (CNDC); seguido pela Lei 8.078/90 que introduziu os primeiros direitos e deveres do consumidor, sendo esta a primeira Lei de Defesa do Consumidor. No final da década de 90, com os avanços tecnológicos, aliado às relações de consumo, surgiu o comércio eletrônico, conhecido também como *e-commerce*. Sendo este um formato de comércio que possibilita a compra e venda pela internet, sendo feito por sites e aplicativos *on-lines* (Sarraf, 2020).

A partir dos anos 2000 com o avanço da internet o comércio eletrônico começou a crescer. O pontapé inicial para que o comércio eletrônico tivesse uma grande visibilidade no Brasil foi dado pela empresa americana Amazon, com a comercialização de livros. A entrada da Amazon no mercado brasileiro aumentou a concorrência e estimulou outras empresas a investirem no comércio eletrônico, desencadeando grandes avanços que fez chegar à magnitude que é atualmente o *e-commerce.*

Compreendendo o contexto, é cristalino dizer que nos dias atuais os dados e informações tomaram um lugar importantíssimo para o funcionamento das empresas. Assim, é indiscutível a necessidade de tratar da forma adequada informações dos consumidores para o uso de dados, visto que se tornaram matéria prima dos negócios (Eliezer *et al.*, 2023). Atualmente, é possível que se obtenha informações de terceiros publicadas mundialmente. Permitindo que sejam identificados “o que” o usuário pesquisa e “como” pesquisa, fazendo ainda um crivo relacionado a frequência (Bueno, 2019).

Diante da falta de informação e despreparo técnico acerca dos contratos de consumo realizados, os consumidores virtuais passaram a ser vulneráveis não somente diante da relação material que é promovida por meio de compra de produtos ou serviços tradicionais, mas principalmente diante das empresas virtuais e pessoas dispostas a utilizarem a plataforma digital para aplicar golpes e utilizarem-se de dados não protegidos pelo fornecedor. A vulnerabilidade se tornou tão notória diante dos mais diversos contratos de adesão pelos quais são obrigados a aceitar, informando seus dados pessoais e demais informações, que diversos mecanismos de proteção, para além do código do consumidor, têm sido criados.

2.3 A trajetória do direito à privacidade até a elevação da proteção de dados como direito fundamental

A Lei Geral de Proteção de Dados demonstra a necessidade de reafirmação do princípio da vulnerabilidade no *ciberespaço* e a tutela dos indivíduos enquanto consumidores virtuais (Siqueira *et al.*, 2021).

A tecnologia deixou de ser um mero componente secundário quando se trata de estratégia nos negócios. Devido a isto, inúmeros dados são fornecidos diariamente a empresas e armazenados nos seus bancos de dados.

Nesse contexto, a Lei Geral de Proteção de Dados (LGPD), ao estabelecer regras para o tratamento de dados pessoais, incluindo aqueles em meios digitais, exige sua aplicação tanto por pessoas jurídicas de direito público quanto privadas. Isso visa proteger os direitos fundamentais e a privacidade dos indivíduos. Além disso, com a criação da Autoridade Nacional de Proteção de Dados (ANPD) por meio da Medida Provisória n°. 869/2018, o Brasil atende aos interesses legais, empresariais e à própria legislação que já previa a necessidade de uma entidade reguladora nesse sentido. Dessa forma, o país passa a se alinhar com políticas públicas internacionais voltadas para a proteção de dados pessoais e da privacidade (Follone; Simão Filho, 2020).

É nesse contexto que as empresas conseguem formar perfis individualizados dos consumidores, uma vez que estes se deparam com uma linguagem complexa e pouco clara, o que dificulta a real compreensão das finalidades e consequências do tratamento de seus dados, o que concorre para o consentimento maculado, não seguindo, portanto, os requisitos da LGPD, a qual diz que o mesmo deve ser: livre, informado e específico para cada finalidade de tratamento (Botelho, 2020).

O utilizador de serviços digitais, sujeito à recolha desmedida, constante e discreta dos seus dados, frequentemente não está ciente desta prática e nem possui os meios para conhecer os resultados ou detê-los. Além disso, é quase impossível determinar quantos outros sites, provedores ou empresas receberam e partilharam os mesmos dados e com que frequência. Isso destaca a preocupante amplitude das possíveis violações dos direitos fundamentais dos consumidores, incluindo até mesmo a possibilidade de atingir bens jurídicos protegidos por lei, devido à exposição e à facilidade resultante do uso indiscriminado da internet, bem como à negligência e ao abuso por parte de provedores e fornecedores de serviços e produtos online (Siqueira *et al.*, 2021).

Apesar do caráter essencial inerente aos direitos fundamentais, estes possuem um viés relativo, haja vista o engessamento imposto pelo Poder Legislativo e Judiciário diante da resolução de casos concretos. Tais situações se evidenciam no confronto entre direitos fundamentais e outros valores constitucionais (Doneda, 2006).

Nesse sentido, Silvia Venosa (2006) aduz acerca da dificuldade de disposição dos direitos da privacidade que tutelam a vida íntima, visto que estes protegem a dignidade da pessoa humana. Contudo, pontua que no atual cenário da sociedade contemporânea surgem

situações que andam lado a lado com a renúncia destes direitos, como ocorre, por exemplo, nos *reality shows*, onde participantes voluntariamente aceitam um contínuo monitoramento e supervisão, abdicando do seu direito à privacidade, expondo a integridade física e psicológica a limites extremos de resistência.

Nesse cenário, o direito à privacidade era tido como um direito individualista, portanto, negativo, o que o insere na perspectiva da primeira geração dos direitos fundamentais, vinculado ao direito de liberdade, já que para ser garantido, necessitava de uma abstenção do Estado. Era necessário que o estado não adentrasse na esfera individual de cada um para que este direito fundamental pudesse ser garantido (Passos, 2017).

Nesse viés, diante dos notórios casos em que os indivíduos vão na contramão da irrenunciabilidade dos direitos à privacidade, se faz cristalina a necessidade de maximizar a proteção deste direito diante da crescente onda dos meios digitais. Deve-se considerar que o indivíduo, aqui titular dos dados, figura uma posição de completa vulnerabilidade dentro dos meios digitais - principalmente em razão da vulnerabilidade técnica, por ser um utilizador regular, até mesmo para o lazer (Eliezer *et al.*, 2023). As novas perspectivas criadas pela era tecnológica conectam a privacidade à proteção de dados.

Nessa seara, é promulgada a Lei Geral de Proteção de Dados, dispondo acerca da obrigação de realizar o tratamento de dados pessoais de forma segura e responsável, tutelando a privacidade digital e direcionando a forma adequada de tratar dados a fim de garantir a confidencialidade, integridade e disponibilidade destes.

A obrigação trazida pela lei se fez vital quando os avanços tecnológicos foram tantos que possibilitaram a singularização de informações, vinculando os dados às pessoas. Nesse sentido, o art. 5º da LGPD dispõe “dado pessoal: informação relacionada a pessoa natural identificada ou identificável” (Brasil, 2018).

A proteção de dados pessoais por muito tempo, foi um direito visto como parte do direito à privacidade, portanto, desprovido de autonomia. No entanto, como o passar dos anos e a descoberta de novas gerações de direitos, aumentou-se o enfoque no titular dos dados pessoais, e inserindo-o cada vez mais no ciclo do tratamento dos seus próprios dados, o que ficou conhecido como Autodeterminação Informativa, o poder do sujeito de ter o controle sobre suas próprias informações.

No continente europeu, evidenciou-se por meio da promulgação do *General Data Protection Regulation* (GDPR), o qual mais tarde iria influenciar a criação e promulgação da Lei Geral de Proteção de Dados (LGPD) no Brasil. É majoritário o entendimento acerca da irrenunciabilidade do direito à privacidade. Assim, é obsoleto adequar o direito à privacidade à

obrigação de privações. Em consonância com as novas perspectivas dadas a este direito, Rodotá (2008) relaciona a privacidade com a autodeterminação informativa. Deste modo, no âmbito da sociedade digital, onde os dados são constantemente vinculados, se fez necessário uma nova forma de proteger os consumidores-usuários, haja vista o novo contexto das relações na sociedade de consumo.

A tecnologia ganha espaço, e o Direito, como produto da realidade social, se adequa a esse novo estilo de vida. Nesse sentido, as tecnologias imaturas e até perigosas estavam sendo colocadas em serviço, principalmente em relação à privacidade e ao uso de dados.

No que tange a privacidade dos dados, é necessário prudência para verificar qual o limite da divulgação das informações pessoais. Nessa seara, o direito fundamental à proteção de dados foi elevado à direito fundamental pela Emenda Constitucional nº 115/2022, estando explícito na Constituição Federal de 1988, atuando, portanto, de maneira autônoma, desvinculado do direito à privacidade.

Dessa forma, a Constituição passou a prever no seu artigo 5º, inciso LXXIX, "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais" (Brasil, 1988).

Conforme demonstrado, a junção da LGPD com o CDC, ou seja, o sistema de proteção de dados e a proteção do consumidor, assegura o consumidor de desequilíbrios de poder que possam prejudicar sua capacidade de tomar decisões autônomas, informadas e livres. Devido ao seu alcance mais abrangente, que abarca diversas situações além do mercado de bens, serviços e consumo, a proteção de dados pessoais aliada ao direito à privacidade e ao CDC, se revela como um mecanismo mais eficaz na salvaguarda da privacidade do consumidor (Follone; Simão Filho, 2020).

Nesse sentido, a proteção de dados pessoais tutela a personalidade do indivíduo, diante dos riscos pela falta de cautela no tratamento de dados pessoais. A finalidade por trás dessa garantia não é a proteção dos dados em si, mas de assegurar a pessoa titular desses dados, haja vista o caráter objetivo deste direito fundamental.

3 O PAPEL DA LGPD: DA PROTEÇÃO DO CONSUMIDOR À RESPONSABILIZAÇÃO DAS EMPRESAS

O presente capítulo ocupa-se em tratar o papel da Lei Geral de Proteção de Dados, abordando a proteção do consumidor e a responsabilização das empresas, estabelecendo, inicialmente, os fundamentos que deram origem à promulgação da lei e os princípios que norteiam a aplicabilidade desta. Além disso, preocupa-se em demonstrar a inter-relação entre o Código de Defesa do Consumidor e a Lei Geral de Proteção de Dados e esclarecer os direitos tutelados quanto ao tratamento de dados do consumidor. Por fim, traz uma análise acerca da responsabilidade e a forma de tratamento das empresas perante os dados pessoais.

3.1 Fundamentos e Princípios da LGPD

Indispensável se faz elucidar acerca dos princípios e fundamentos da Lei Geral de Proteção de Dados. Os fundamentos são aqueles os quais deram origem à lei, ou seja, ensejaram a sua criação e os princípios são a base que norteiam como deve ocorrer a aplicabilidade da legislação. Assim, o artigo 2º da lei dispõe expressamente os fundamentos da proteção de dados, sendo: o respeito à privacidade; à autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião; à inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (Brasil, 2018). Tais fundamentos demonstram a preocupação da lei com a proteção da personalidade, do livre desenvolvimento e da vida digna dos usuários.

O respeito à privacidade, fundamento elencado no inciso I do art. 2º da LGPD, é uma resposta à sociedade na disciplina da proteção de dados que tem sua intimidade cada vez mais violada com o advento dos meios digitais e a superexposição espontânea. Por conseguinte, a autodeterminação informativa estabelece que o titular dos dados pessoais precisa ter transparência e controle da destinação dos seus dados (Pinto, 2023).

Ademais, é indispensável que a lei trate do fundamento da liberdade de expressão, de informação, de comunicação e de opinião (art. 2º, III), haja vista a importância desta garantia constitucional, visto que estas são premissas básicas de um Estado Democrático de Direito. Em consonância com o referido fundamento, tem-se o fundamento da inviolabilidade, da honra e

da imagem (art. 2º, IV), uma vez que esta legislação deve conciliar o direito à liberdade de expressão com a dignidade da pessoa humana.

É vital a harmonia com o desenvolvimento econômico e tecnológico e a inovação (art. 2º, V) “na medida em que a proteção de dados pessoais não pode servir ao obscurantismo” (Pinto, 2023). Os avanços tecnológicos possuem influência direta na urgência da proteção de dados, visto que é necessária a adaptação à nova era tecnológica.

Tem-se ainda a livre iniciativa, a livre concorrência e a defesa do consumidor (art. 2º, VI), o significado deste fundamento é de que a proteção de dados pessoais não pode se sobrepor à livre concorrência e livre iniciativa, ou seja, é necessária a harmonia a fim de possibilitar a coexistência de ambas as garantias.

No que tange os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (art. 2º, VII), este reforça que os direitos fundamentais estão em consonância com os fundamentos da proteção de dados.

> A LGPD, ao fundamentar a sua existência também no livre desenvolvimento da personalidade e na dignidade, demonstra uma robusta preocupação na fidelidade da projeção da personalidade do ser humano, que decorre dos dados tratados do respectivo titular, por exemplo ao prever como direito a correção de dados incompletos, inexatos ou desatualizados (Vainzof, 2019, *apud* Fonseca, 2021, p. 50).

Nesse panorama, o artigo 6º da LGPD elucida, do inciso I ao X quais princípios devem ser observados para o tratamento de dados pessoais, sendo estes os balizadores da lei 13.709/2018, quais sejam: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização prestação de contas e da boa-fé, disposto no *caput* do supracitado artigo.

Este último traz consigo duas vertentes. Podendo ser entendido pela boa-fé objetiva, como o dever de cuidado e boa intenção; e a boa-fé subjetiva que está presente em todo o arcabouço da LGPD, especificamente no art. 52, § 1º, II, a qual aduz que “as sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios: [...] II - a boa-fé do infrator”.

É nesse contexto que surge a necessidade de corrigir, interpretar e delimitar o exercício de direitos trazendo maior segurança aos usuários, visto que a LGPD e os princípios constitucionais brasileiros andam lado a lado.

O primeiro princípio disposto no art 6º é o princípio da finalidade, o qual aduz que o uso dos dados deve estar em consonância com a "propósitos legítimos, específicos, explícitos e informados ao titular", não podendo, portanto, o uso dos dados se distanciar da finalidade que ele foi informado, não podendo também ser usado de acordo com o desejo do controlador. Este princípio ampara o titular dos dados no que tange a delimitação do destino específico informado e consentido, protegendo o titular da possibilidade de uso secundário de dados dos quais ele não esteja ciente, além de proteger do acesso de terceiros (Vainzof, 2019, *apud* Fonseca, 2021, p. 50).

Por isso, qualquer necessidade de mudança da finalidade do uso dos dados, é necessário a comunicação ao titular dos dados, podendo o seu detentor revogar o consentimento, caso discorde das alterações, como dispõe o art 9º, § 2º da LGPD. Assim, de forma cumulativa, o princípio da finalidade deve ser legítimo, específico, explícito e informado possibilitando ao titular o conhecimento do fato gerador, respeitando o contexto em que foram coletados (Feijó; Dutra, 2023, p. 26).

Em seguida, o princípio da adequação regulamenta que o tratamento dos dados deve ser realizado conforme o que foi preestabelecido entre controlador e detentor dos dados. Este princípio traz um complemento do anterior, uma vez que tem o condão de elucidar a materialidade da finalidade e a sua informação, visto que a finalidade sem a adequação seria o mesmo que pedir informações sem o fim determinado que busca o usuário. Deste modo, o princípio da adequação visa compatibilizar o tratamento de dados com a finalidade do detentor de dados (Feijó; Dutra, 2023, p. 26).

Em continuidade, o princípio da necessidade, instituído no inciso III, é o princípio limitador do tratamento de dados, haja vista restringe ao mínimo necessário para a realização da finalidade, devendo ser disponibilizado os dados necessários para a realização da atividade desejada, não podendo extrapolar o uso das informações, o chamado *data minimisation*, proporcionando a menor exposição dos dados pessoais (Brasil, 2018).

Tendo em vista a privacidade do titular, o tratamento de dados se restringe ao mínimo, quanto mais restrito, melhor poderá ser feita proteção dos dados, posto que melhor será ao titular que terá sua privacidade preservada na maior medida e melhor será para os agentes que gerenciarão os dados, visto que este serão mais sucintos (Fonseca, 2021, p. 72).

O princípio do livre acesso, possibilita ao consumidor o acesso livre de todos os seus dados que foi coletado pelo fornecedor, de forma facilitada e gratuita, assim como à forma de execução e duração do tratamento. O supracitado princípio possui correlação ao art. 9º da LGPD, uma vez que este artigo afirma que:

> 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:
>
> I - finalidade específica do tratamento;
>
> II - forma e duração do tratamento, observados os segredos comercial e industrial;
>
> III - identificação do controlador;
>
> IV - informações de contato do controlador;
>
> V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;
>
> VI - responsabilidades dos agentes que realizarão o tratamento; e
>
> VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei

Assim, conforme Fonseca (2021, p. 76) em consonância com o fundamento da autodeterminação informativa e do supracitado princípio do livre acesso, é direito do titular saber quais dados estão sendo tratados pelos agentes e qual será a duração desse tratamento, assim "a boa-fé e a transparência foram alcançadas pela LGPD à condição de princípios fundamentais da proteção de dados pessoais".

O princípio da qualidade de dados traduz a condição de que os dados pertencentes a um banco de dados sejam tratados de forma justa e lícita, sendo adequados e sem excessos no que tange à finalidade, garantindo aos titulares dos dados que as informações serão relevantes e atualizadas. Em caso de violação deste princípio o titular pode requisitar a correção. O referido princípio assegura, portanto, a atualização constante dos dados, evitando que possíveis dados desatualizados não prejudiquem o titular (Fonseca, 2021, p. 76).

Linha contínua, o princípio da transparência, disposto no inciso VI, garante que os dados pessoais sejam claros, relevantes e atualizados "de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento" (Brasil, 2018). Este princípio assegura aos titulares de dados que suas informações não sejam repassadas de forma enganosa ou abusiva, conforme estabelece também o art. 9º, §1 da Lei 13.709/2018.

O princípio da segurança garante a tomada de medidas que assegurem os dados pessoais, com a utilização de medidas técnicas e administrativas visando a proteção de acessos não autorizados, como, por exemplo, invasões por *hackers*. Para Fonseca (2021, p. 79) a segurança no tratamento de dados está para além das barreiras tecnológicas e físicas, mas é necessário a transformação na cultura organizacional, "conscientizando todos os integrantes da organização sobre a importância da proteção de dados pessoais".

O princípio da prevenção instituiu a adoção de medidas preventivas para que não ocorram danos derivados do tratamento de dados, devendo estas medidas serem tomadas desde a concepção do produto ou serviço até a execução. Significa dizer que o serviço a ser prestado deve ter, desde o início, a segurança e a prevenção como norteadores do tratamento de dados, a fim de evitar danos trazidos pelo ineficaz tratamento dos dados, por isso a necessidade do tratamento preventivo.

Ainda no art. 6º da LGPD, tem-se o princípio da não discriminação o qual impossibilita que os dados pessoais sejam tratados com fins discriminatórios ilícitos ou abusivos. Nesse viés, a LGPD aborda ainda na Seção II, do Capítulo II, regras específicas para tratar os dados chamados como sensíveis - visto que são estes que normalmente são usados de forma discriminatória. O objetivo deste princípio é assegurar que, em posse dos dados, os detentores não usaram para fins vexatórios (Fonseca, 2021, p. 80).

> [...] um algoritmo utilizado por uma empresa de *headhunters* para seleção de executivos para grandes empresas, ao ser alimentado com o perfil dos profissionais que normalmente ocupam estes cargos, provavelmente concluirá que o melhor candidato será do sexo masculino, branco, com idade entre quarenta e cinco e sessenta anos. Isso porque os dados que alimentaram o algoritmo mostraram a ele o perfil dos executivos contratados naquele contexto social. Detecta-se, assim, uma decisão enviesada do algoritmo, que deixaria de selecionar pessoas que destoassem do padrão estabelecido (FONSECA, 2021, p. 80).

Dessa forma, é essencial para o adequado tratamento de dados não só o conteúdo que foi armazenado, mas o fim que estes serão destinados. Por isso, é fundamental evitar decisões discriminatórias por parte dos algoritmos.

Por fim, o princípio da responsabilização e prestação de contas é amparado pelo princípio da boa-fé e da transparência. Este princípio obriga a adoção de medidas eficazes no tratamento de dados pelos fornecedores, sendo necessário que estas medidas sejam capazes de assegurar o cumprimento das normas de proteção de dados. Segundo esse princípio, as empresas que coletam dados precisam cumprir de forma integral o que dispõe a LGPD, mas não só, é crucial que demonstrem comprovando e registrando que estão em consonância com a lei (Fonseca, 2021, p. 81).

Em síntese, estes princípios visam facilitar o caminho para a implementação da LGPD, criando diretrizes que devem ser aplicadas e seguidas a fim de garantir o adequado tratamento de dados pelas empresas e a segurança do titular dos dados pessoais, possibilitando que estes sejam usados de forma segura a fim de que os fundamentos que deram origem a LGPD sejam

ampliamento supridos. Assim, o consentimento do titular dos dados deve ser amparado pelo que fora disposto no art. 6º da LGPD.

3.2 A inter-relação entre o CDC e a LGPD e os direitos tutelados quanto ao tratamento de dados do consumidor

Os avanços tecnológicos congruentes à sociedade hiper conectada inspirou o surgimento de regulamentações de proteção de dados pessoais de forma mais consistente e consolidada. O surgimento se deu diante da exposição de informações pelos usuários. Essas informações compartilhadas estabelecem relação com a publicidade direcionada, sendo possível assim, dividir as informações em cadastrais e preferências.

As informações cadastrais dizem respeito aos dados que o usuário precisa fornecer para utilizar os meios digitais; e as informações preferenciais são aquelas que são inerentes as preferências destes usuários, sendo divididas em associativas, ou seja, são as inerentes ao que o usuário gosta de visitar no meio digital e as de navegação são os registros desses acessos, ou seja, o histórico. Com essas informações armazenadas possibilitam a criação de um perfil do usuário que consegue mandar propagandas e anúncios de acordo com o gosto de cada um (Luft; Polli, 2012).

É nesse cenário que é possível conceituar o usuário do *ciberespaço* como consumidor, haja vista o mesmo se enquadra na relação como o destinatário final, estando então abarcado pelo art. 2° do Código de Defesa do Consumidor, estando, consequentemente, a empresa que lucra com o direcionamento dos usuários, encaixada no aduz o CDC sobre fornecedora (Luft; Polli, 2012). Ademais, a Ministra Nancy Andrighi ratifica a relação de consumo existente entre o ciberespaço e seus usuários.

Assim, é inequívoco que a proteção de dados está diretamente vinculada a defesa do consumidor, atuando assim a Autoridade Nacional de Proteção de Dados (ANPD) com os órgãos de defesa do consumidor na proteção dos dados pessoais, essa ideia se faz cristalina no art. 18, § 8° da Lei Geral de Proteção de dados que dispõe “o direito a que se refere o § 1º deste artigo também poderá ser exercido perante os organismos de defesa do consumidor” (Brasil, 2018). Por consequência, tanto a LGPD quanto o CDC possuem uma interligação a fim de garantir os interesses desta relação, como será abordado a seguir.

No que tange a boa-fé, estabelecida tanto no CDC quanto na LGPD, tem-se como um princípio que busca a harmonia dos interesses. Como já fora visto, a Lei Geral de Proteção de

Dados dispõe que o tratamento de dados deve observar a boa-fé, tal qual o art. 4, III do CDC o qual dispõe que a relação entre fornecedor e consumidor deve resguardar a boa-fé.

Este princípio é aplicado no uso de dados mediante o consentimento do titular diante da finalidade no uso dos seus dados, estando estas em consonância com a transparência das informações prestadas ao consumidor. Em vista disso, as relações consumeristas que têm como meio o uso de dados, devem ser pautadas pela boa-fé e canalizada de acordo com a autodeterminação informativa (Miragem, 2019).

Conforme Miragem (2019) é possível vislumbrar ainda está interligação, uma vez que o consentimento elencado pela LGPD, está ligado ao reconhecimento da vulnerabilidade do princípio do consumidor, visto que diante disto se coaduna o dever a informação adequada. Assim, a LGPD em harmonia com o CDC cria caminhos para uma relação de confiança entre consumidor e fornecedor, afinal as duas têm como objetivo informar os direitos e a elevação de garantias individuais dos consumidores, seja no meio físico ou virtual.

Desse modo, a proteção dada pelo CDC e os caminhos criados por esta legislação, propiciou a criação pela LGPD acerca dos direitos tutelados pelos consumidores.

A exigência desta proteção possui relação com o progresso dos negócios digitais que passou a depender das bases de dados (Pinheiro, 2020). No que tange a relação consumerista e o tratamento de dados, é cristalino afirmar que o consumidor também é vulnerável tanto técnico, visto que este possui ausência de conhecimento ou informação técnica; quanto jurídico, visto que parte do pressuposto que o consumidor tem eminentemente carência de informações sobre os direitos que lhe são resguardados; e fático visto que são ainda mais expostos a práticas ilícitas.

É nesse contexto que o art. 43 do Código de Defesa do Consumidor ampara o consumidor no que tange a privacidade dos seus dados, possibilitando a ele acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes (Brasil, 1990).

Diante dos riscos no ambiente digital, a proteção de dados é o instituto que ampara e assegura o consumidor diante da sua vulnerabilidade, assegurando a autodeterminação informativa conjuntamente com o CDC. Desse modo, diante da autoexposição na qual o consumidor, ou seja, o titular dos dados se expõe, é necessário a garantia do armazenamento apropriado, sendo fundamental para a sociedade atual a proteção dos dados (Mendes, 2014).

Nessa toada, a LGPD protege a pessoa natural, resguardando a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade. Os dados pessoais são tratados a partir de operações informatizadas, conforme

preceitua o Princípio da Segurança disposto na LGPD, sendo este feito através de conversação, adaptação e organização dos dados. Conforme o art. 18 da Lei 13.709/2018, o titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição informações dos seus dados.

O supracitado artigo em seu inciso I dispõe acerca do direito do titular de ter a confirmação da existência de tratamento, significa dizer que o consumidor tem o direito de saber se seus dados estão sendo tratados, isso se dá consequente a requisição de informações pelo fornecedor. Este inciso abrange o direito do consumidor de saber da existência dos bancos de dados com seus dados. É nessa circunstância que se encaixa o princípio da transparência, para que o titular possa preservar a sua privacidade, conhecendo a identidade do responsável pelo tratamento e o objetivo deste (Mendes, 2014).

O acesso aos dados garante ao titular conhecimento dos dados que estão sendo usados pelo controlador. Sendo que tanto este quanto o direito de confirmação o titular deve fazer um requerimento expresso, os quais devem estar disponibilizados no site dos agentes de tratamento de dados, o que é ampliamento disciplinado pela Autoridade Nacional de Proteção de Dados (ANPD) (Grinover *et al*., 2019).

Em seguida é disposto o direito à correção de dados incompletos, inexatos ou desatualizados (Art. 18, III), este direito se enquadra caso o titular dos dados perceba equívocos nos seus dados, solicitando a correção, a qual deve ser feita imediatamente. Concomitante, tem-se o "direito de anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei" (Art. 18, IV).

Dados anônimos são aqueles que não é possível atribuir os mesmos ao titular; quanto ao bloqueio ou eliminação é cabível quando os dados que foram disponibilizados forem excessivos estando, portanto, em discordância com o que dispõe a LGPD; sendo cabível ainda quando decorre do tratamento ilícito. Esses direitos estão em consonância com o que preceitua os princípios da finalidade, adequação e necessidade, pleiteando, portanto, a eliminação dos dados excessivos, previsto no inciso VI (Grinover *et al*., 2019).

Tem-se ainda o direito de ter conhecimento acerca da transferência dos seus dados para outro agente de tratamento de dados, sendo informado quais dados foram registrados, feito também através de requerimento expresso, sendo este conhecido como o direito à portabilidade (art. 18, V).

Linha contínua, a Lei Geral de Proteção de Dados institui ainda nos incisos VII, VIII e IX o direito de informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; direito de informação sobre a possibilidade de não fornecer

consentimento e sobre as consequências da negativa; e direito de revogação do consentimento (Brasil, 2018).

3.3 Responsabilidade das empresas perante os dados pessoais

As constantes evoluções da sociedade no que tange o meio digital, fez surgir a necessidade de um maior cuidado com o tratamento de dados das redes sociais e também o tratamento de dados das empresas, possibilitando que os sujeitos sejam inseridos na relação jurídica e na proteção jurídica dos seus direitos.

Nesse contexto, as empresas precisaram readequar seus cuidados com as informações dos consumidores-usuários, tanto no meio físico quanto no digital. Deste modo, Demócrito (2002) já preceituava que diferentemente de como ocorria anteriormente que apenas as agências governamentais coletavam dados das pessoas, atualmente grande parte das empresas privadas sabem como "coletar, manipular, armazenar e transmitir dados de uma forma simples e a um custo relativamente baixo".

Assim, a LGPD pressupõe que para a segurança e sigilo dos dados os agentes de tratamentos devem aderir medidas de segurança a fim de proteger os dados pessoais dos usuários contra situações ilícitas ou acidentais, sendo necessário que essas medidas sejam adotadas desde a fase de concepção do produto ou do serviço até a sua execução (Brasil, 2018).

Segundo disposto por Lima (2020), a Lei Geral de Proteção de Dados é cristalina acerca da necessidade de proteção de dados pelos agentes de tratamento, sendo estes o controlador e operador. Podendo ser pessoas físicas ou jurídicas, sendo necessário o desempenho das funções. Deste modo, a LGDP dispõe no art. 42 sobre a responsabilidade civil destes agentes de tratamento:

> Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.
>
> § 1o A fim de assegurar a efetiva indenização ao titular dos dados:
>
> I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;
>
> II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.

> § 2o O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.
>
> § 3o As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente.
>
> § 4o Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.

Nesse cenário, buscando evitar problemas relativos à captação e tratamento de dados em uma empresa e evitar multas de compliance digital e outras penalidades por descumprimento da LGPD, foi criado o *Data Protection Officer* - DPO, também denominado de "Encarregado", sendo este a pessoa indicada pelo controlador e operador para atuar como comunicador entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD) (Brasil, 2018).

O encarregado deve ter conhecimento sobre a legislação, assim como deve conhecer a empresa que fará o tratamento dos dados, a fim de evitar prejuízos a empresa. Ele é o vínculo entre cliente, usuário e a empresa. Sendo que entre as suas atividades estão a aceitação de reclamações e comunicação dos titulares, receber comunicações da autoridade nacional e adotar providências, orientar aos funcionários e aos contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais e executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares (Brasil, 2018). Apesar da promulgação da LGPD o DPO ainda não é uma realidade comum nas empresas brasileiras.

Nesse sentido, a Resolução CD/ANPD N° 2 dispõe sobre como essas empresas devem realizar os tratamentos de dados, estabelecendo que estas têm o dever de elaborar e fazer a manutenção das operações de tratamentos dos dados pessoais, apesar disso, estas empresas não são obrigadas a indicar a pessoa encarregada. Para além, são também obrigações das empresas de pequeno porte:

> Art. 13. Os agentes de tratamento de pequeno porte pode estabelecer política simplificada de segurança da informação, que contemple requisitos essenciais e necessários para o tratamento de dados pessoais, com o objetivo de protegê-los de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.
>
> Art. 14. Aos agentes de tratamento de pequeno porte será concedido prazo em dobro:

> I - no atendimento das solicitações dos titulares referentes ao tratamento de seus dados pessoais, conforme previsto no art. 18, §§ 3o e 5o da LGPD, nos termos de regulamentação específica;
>
> II - na comunicação à ANPD e ao titular da ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, nos termos de regulamentação específica, exceto quando houver potencial comprometimento à integridade física ou moral dos titulares ou à segurança nacional, devendo, nesses casos, a comunicação atender aos prazos conferidos aos demais agentes de tratamento, conforme os termos da mencionada regulamentação;
>
> III - no fornecimento de declaração clara e completa, prevista no art. 19, II da LGPD;
>
> IV - em relação aos prazos estabelecidos nos normativos próprios para a apresentação de informações, documentos, relatórios e registros solicitados pela ANPD a outros agentes de tratamento (Brasil, 2018).

Por outro lado, as empresas multinacionais e de grande porte se adaptaram de forma mais fácil, visto que devido a sua abrangência estas empresas buscaram se antecipar com a promulgação da LGPD, buscando se adequar às exigências dispostas pela legislação, evitando a aplicação de sanções.

Por tanto, é necessário que as empresas sejam cautelosas na solicitação de dados e criteriosas no seu armazenamento, seguindo o que dispõe o princípio da necessidade. Nessa conjuntura, faz-se necessário também a observância do princípio da qualidade, garantindo ao consumidor-usuário que apenas os dados que são de fatos necessários serão pedidos a ele. Contudo, caso isso não ocorra o titular tem o direito de pedir a correção deste, conforme preceitua Lima (2020):

> Conforme vemos na própria Lei Geral de Proteção de Dados, o titular dos dados tem o direito de correção de dados incompletos, inexatos ou desatualizados e, ainda, informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados e sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa.

Nos termos do princípio da segurança as empresas e órgão públicos devem garantir a integridade do banco de dados, buscando a proteção contra o vazamento que estiverem sob o seu domínio, visto que a depender do caso concreto os vazamentos de dados podem causar sanções administrativas e judiciais. A responsabilidade das empresas perante os dados pessoais passa pelo treinamento de pessoas que possam melhor garantir a proteção dos dados, para que os cuidados estejam em conformidade com a LGPD (Fonseca, 2021).

Portanto, para que as empresas possam aderir a LGPD da forma adequada é indispensável o domínio sobre as orientações dadas pela lei. Por isso, o fornecedor deve adotar

medidas que sejam eficazes no tratamento de dados, onde o agente deve comprovar a observância e cumprimento das legislações que resguardam os dados pessoais.

4 “NÃO LI E ACEITO”: os impactos da não-observância da LGPD na proteção de dados pessoais e na privacidade no comércio eletrônico frente a publicidade direcionada

O presente capítulo apresenta, inicialmente, as relações de consumo no ambiente eletrônico e as técnicas de publicidade comportamental. Posteriormente, apresenta-se a análise dos casos de coleta de dados para o direcionamento de publicidade comportamental, com prejuízos aos usuários devido a inobservância da Lei Geral de Proteção de Dados. Por fim, a pesquisa analisa não apenas as implicações do tratamento inadequado dos dados, mas também a adequação à LGPD, assim como a fiscalização do tratamento adequado dos dados pela Autoridade Nacional de Proteção de Dados (ANPD) e os órgãos regulamentadores e as práticas necessárias para a segurança e o sigilo dos dados.

4.1 Relações de consumo no ambiente eletrônico e o uso da publicidade direcionada

O comércio eletrônico tem suas raízes na formação da internet, surgindo nos anos 60 através do compartilhamento de documentos entre empresas, quando empresas e instituições acadêmicas começaram a utilizar a rede para comprar suprimentos e compartilhar informações, sendo inicialmente de natureza B2B (*business-to-business*) (Patel, 2019).

A partir dos anos 90 com os avanços tecnológicos surgiram as empresas pioneiras no comércio eletrônico na relação fornecedor e consumidor, quais sejam a Amazon e o eBay. A Amazon iniciou neste ramo com a venda de livros pela internet; enquanto o eBay criou uma plataforma de leilões *online* que permitia que os consumidores comprassem e vendessem produtos usados. A globalização desempenhou um papel importante, uma vez que a internet removeu fronteiras geográficas, facilitando transações internacionais (Patel, 2019).

Patel (2019) aduz que o comércio eletrônico teve uma adesão inimaginável. A possibilidade de “efetuar compras sete dias por semana e 24 horas por dia”, foi o que ocasionou o sucesso desta modalidade, possibilitando o alcance internacional. No final da década de 90 surgiu o formato dos bancos digitais. Contudo, no início dos anos 2000 o meio eletrônico sofreu com a falta de confiabilidade dos investidores. Foi a partir disto que os usuários passaram a movimentar o meio eletrônico, passando a ser os produtores de conteúdo na internet.

Posteriormente, com o aumento no uso de smartphones e tablets, ocorreu a proliferação do comércio eletrônico, permitindo que os consumidores realizassem compras em qualquer lugar e a qualquer momento. Este uso contínuo possibilitou que as empresas ligadas ao

ambiente virtual capturassem e armazenassem as informações relacionadas aos consumidores-usuários (Sarraf, 2020).

A rapidez com que ocorreram os avanços tecnológicos foi um divisor para o *e-commerce*, haja vista a inserção de milhares de usuários por dia no meio digital. Com esses avanços, diversos ramos do mercado aderiram ao comércio eletrônico, tornando este ambiente ainda mais diversificado que o meio físico. A migração para o meio virtual possibilitou um menor custo nas transações, assim como reduziu os custos com novos contratantes, fazendo com que o *e-commerce* crescesse cada vez mais (Sarraf, 2020).

Para Cláudia Lima Marques (2002) o comércio eletrônico possui duas definições. A primeira é definida de maneira estrita como contratação não-presencial ou à distância por meio eletrônico; a segunda é definida de maneira ampla como "novo método de fazer negócios através de sistemas e redes eletrônicas", abrangendo nesta última qualquer forma de transação e englobando todas as atividades negociais.

Assim, os contratos eletrônicos possuem relação entre comerciantes e o Estado (B2G); entre empresários (B2B); entre relações consumeristas (B2C); por fim entre consumidores (C2C), dentre as quais são consideradas relações de consumo apenas B2C, visto que possuem uma relação de vulnerabilidade do consumidor frente ao fornecedor. Nos contratos eletrônicos as relações são amparadas igualmente pela legislação cível e consumerista, tendo em vista que as situações que ocorrem nos contratos físicos se assemelham aos contratos eletrônicos, sendo necessário para a validade de ambos a declaração da vontade (Martins, 2016).

Contudo, a relação de consumo no meio virtual vai além da compra e venda de mercadorias, vez que, apenas o acesso ao site pelo consumidor-usuário expõe este à coleta de dados que são aceitos por ele, visto que para o acesso é indispensável a concordância com os cookies, gerando a adesão à Política de Privacidade da empresa. Diante disso, mesmo que o acesso do consumidor tenha sido, por exemplo, apenas para saber o preço, o fornecedor já possui a concordância necessária para a coleta dos dados do usuário.

Portanto, é inequívoco afirmar que o comércio eletrônico estabelece uma relação de ganho, pois independente da compra no site visitado, o consumidor será bombardeado por publicidade direcionada para que o fornecedor consiga persuadir o visitante a comprar seu produto. Nesse sentido, a concorrência sofre impacto, devido a formação de uma arquitetura descentralizada, diante da vantagem que algumas empresas estabelecem quando adquirem os dados pessoais, que direcionam as escolhas dos consumidores (Schwuartz, 2016).

A publicidade é outro meio ligado ao marketing digital, sendo mais abrangente que a propaganda. Ademais, com o espaço que o meio digital tem ocupado na sociedade tem ocorrido

também a mudança no meio publicitário a fim de acompanhar a dinamicidade social na internet (Carvalho, 2013).

Para Bruno Bioni (2020) a publicidade direcionada possui três divisões: publicidade contextual, segmentada e comportamental. Para ele, a publicidade contextual é a publicidade que visa o interesse do público com base no contexto em que estão inseridos. Já a publicidade segmentada tem seu foco no público que será alcançado, sem se importar com o meio em que esta será veiculada, feitas a partir das características do usuário.

Por conseguinte tem a publicidade comportamental *online*, que possui correlação com a coleta de dados do usuário, a partir disso são descobertos os seus interesses e assim os anúncios são direcionados. Este meio de publicidade possui um menor custo, visto que os anúncios estão diretamente ligados aos interesses do consumidor usuário, tendo, portanto, maior chance de êxito (Bioni, 2020).

Ocorre que, com a autoexposição dos usuários na internet, estes passam a ser moeda de troca para a personalização dos anúncios. É devido à autoexposição que houve as percepções acerca de determinada publicidade tem ocorrido de forma mais rápida, assim ocorre os *profiling*, que são a criação de perfis a partir da análise comportamental de acordo com os gostos dos consumidores (Mendes, 2014). Para Bioni (2020) *profiling* é a prática em que "os dados pessoais de um indivíduo formam um perfil a seu respeito para a tomada de inúmeras decisões. Tudo é calibrado com base nesses estereótipos; inclusive, o próprio conteúdo acessado na Internet".

Com a utilização desses dados para a correlação, a privacidade do usuário é colocada em segundo plano, visto que outros dados sensíveis podem ser coletados, tais como dados referentes à vida política, sexual e dados genéticos, colocando em risco a autonomia humana.

Nesse cenário, além dos princípios já elencados que norteiam o Código de Defesa do Consumidor, com o crescimento do comércio eletrônico, os princípios do CDC se adequaram às relações de consumo no meio virtual.

Assim, em relação ao comércio eletrônico é indispensável mencionar o princípio da informação, visto que por meio deste é assegurada aos consumidores uma relação clara. Nesse sentido, o Código de Defesa do Consumidor dispõe em seu art. 6º, inciso III acerca do direito do consumidor "a informação adequada e clara sobre os diferentes produtos e serviços, com especificação correta de quantidade, características, composição, qualidade, tributos incidentes e preço, bem como sobre os riscos que apresentem".

Indispensável se faz ainda citar o princípio do equilíbrio contratual o qual aduz, em seu art. 4°, inciso III do CDC, acerca do "equilíbrio nas relações entre consumidores e

fornecedores". Conforme o art. 51, inciso XV as cláusulas contratuais que estejam em desacordo com o sistema de proteção ao consumidor são nulas. Nessa conjectura, em caso de desrespeito aos princípios do consumidor, são nulas as disposições que ponham em desequilíbrio a equivalência entre as partes. Conforme o art. 51°, §1°:

> Art. 51. São nulas de pleno direito, entre outras, as cláusulas contratuais relativas ao fornecimento de produtos e serviços que:
>
> § 1º Presume-se exagerada, entre outros casos, a vantagem que:
>
> I - ofende os princípios fundamentais do sistema jurídico a que pertence;
>
> II - restringe direitos ou obrigações fundamentais inerentes à natureza do contrato, de tal modo a ameaçar seu objeto ou equilíbrio contratual;
>
> III - se mostra excessivamente onerosa para o consumidor, considerando-se a natureza e conteúdo do contrato, o interesse das partes e outras circunstâncias peculiares ao caso (Brasil, 1990).

Para além, o comércio eletrônico possui grandes benefícios, tais como: vendas com amplo acesso, troca de informações e interativo com os consumidores, o desenvolvimento de ofertas de produtos e serviços direcionadas para um público mais específico.

Por outro lado, há também desafios, estando entre estes a proteção do consumidor, visto que apesar das legislações promulgadas, o ambiente virtual ainda causa uma grande desconfiança para o consumidor, visto que a distância física gera a sensação de insegurança, tornando o consumidor ainda mais vulnerável (Schwuartz, 2016).

A coleta de dados pelas empresas no ambiente virtual também apresenta um desafio, haja vista a capacidade que as empresas de grande porte possuem de tratar os dados de forma adequada frente às empresas de menor porte, sendo um obstáculo não só para a proteção de dados, mas para o equilíbrio concorrencial do mercado (Canut, 2007).

O tratamento de dados exerce um papel indispensável na criação de publicidade para o desenvolvimento de produtos e serviços que estão em consonância com as buscas dos consumidores. Assim, considerando que a proteção de dados é um direito fundamental e um direito da personalidade que atualmente sofre grande exposição, a grande problemática do comércio eletrônico gira em torno da quantidade de dados coletados, vez que esta coleta expõe aspectos muito mais abrangentes do indivíduo que apenas as suas preferências de consumo.

4.2 Análise dos casos de coletas de dados para o uso da publicidade direcionada com prejuízo aos consumidores-usuários devido a inobservância da LGPD

Os dados podem ser classificados como o principal insumo do meio virtual. É nesse sentido que os usuários são obrigados a aceitar as políticas de sites para poder navegar, estando por trás deste aceite um pseudoconsentimento que é velado pelo “Li e Aceito”.

Nesse cenário, os consumidores-usuários deixam rastros que possibilitam a sua identificação, esses dados são coletados para o retorno ao consumidor em forma de publicidade. É através desse consentimento maculado que as empresas conseguem formar perfis comportamentais dos usuários, o qual põe em xeque a privacidade destes, vez que sofrem com manipulação de dados para *profiling* (Mendes, 2014).

As pequenas ações feitas na internet colocam a vida do usuário nas mãos das empresas privadas. Nesse contexto de exposição diante dos fornecedores, surgiu o conceito do consumidor de vidro, dado por Suzan Lace, visto que o consumidor se torna uma pessoa que possui características visíveis, transparentes, incluindo suas emoções (Lace, 2005 *apud* Bioni, 2019).

O que os fornecedores fazem com essas informações é descobrir as ânsias da geração e transformá-las em objeto de desejo. Por isso que os dados se tornaram relevantes, para garantir a satisfação do desejo gerado no consumidor. Esse desejo é personalizado através do que é coletado, tratado e armazenado pelas empresas.

Assim insta mencionar sobre do *big data*. Para Bioni (2020), o *big data* é uma nova metodologia que estrutura os dados e mediante essa estruturação é feito o cálculo da probabilidade de ocorrência de certo evento referente ao consumidor que disponibilizou seus dados. Podendo ser elencada como uma revolução para a nova forma publicitária, por isso quanto maior for o volume dos dados, melhor será o retorno dado pelos algoritmos.

Os dados são o principal aliado do marketing, contudo, com os avanços da era digital, os dados tornaram-se ainda mais lucrativos e indispensáveis para a publicidade direcionada. Isso justifica a necessidade de coletar o maior volume de dados. Para isso, em troca destes é prometido ao consumidor o acesso em plataformas de recompensas que prometem acumular pontos em troca de benefícios e até mesmo descontos em produtos (The Intercept, 2021).

Devidos os avanços no uso de dados, atualmente, há uma controvérsia que sustenta o papel do marketing: um lado acredita na capacitação e autonomia dos consumidores; já o outro acredita que através do marketing há total controle e manipulação de suas decisões, possuindo poder naquilo que o consumidor irá fazer e comprar. A proliferação de dados e a disponibilidade de ferramentas e habilidades analíticas no ambiente de negócios contemporâneo têm reconfigurado as estratégias de marketing.

Contudo, devido a enorme quantidade de dados coletados, é necessário o uso de tarefas tecno-analíticas como, por exemplo, mineração de dados, conhecida também como *data mining*, expressão utilizada para designar a atividade de extrair padrões de determinados conjuntos de dados, relegando os candidatos a certos perfis comportamentais; corretagem de informações, também chamada de *data brokers*, que são uma indústria que consiste na troca de dados entre diversas empresas, fornecendo dados umas as outras, seja vendendo ou combinando; inteligência de mercado e *consumer insights*, empregando monitoramento automático, detecção e produção de perfis com o objetivo de gerar *data brokers* (Bioni, 2020).

Diante desse cenário, foram escolhidos dois casos para exemplificar acerca do uso inadequado de dados pessoais na publicidade comportamental, o caso do grupo Raia-Drogasil e o da Decolar.com que se destacaram por colocar em risco a privacidade dos consumidores-usuários e demasiados riscos de manipulação de dados para *profiling*. A seguir será feito um histórico dos casos, bem como seus desdobramentos e as multas recebidas pela inobservância da LGPD.

Devido às mudanças no marketing digital e na constante disputa pelos dados pessoais dos consumidores, o grupo Raia-Drogasil viralizou no meio digital devido a sua política de extração de dados dos consumidores utilizando a coleta biométrica. A rede já possuía acesso aos dados sensíveis dos usuários através do programa, conhecido como Stix que prometiam descontos - em troca dos dados. Ocorre que a intenção do grupo ia além, com isso objetivaram coletar a biometria dos seus consumidores. Desta vez, a solicitação da digital não se justificava com a troca por descontos, mas sim garantir ao consumidor que seus dados estariam protegidos, ou seja, a adequação à Lei Geral de Proteção de Dados, através do recadastramento com a biometria (The Intercept, 2021).

Ocorre que, como já mencionado, um dos princípios da LGPD é o princípio da finalidade que garante que os dados serão usados para a finalidade informada, assim coaduna com a necessidade de minimizar a coleta dos dados - ao contrário do que estava fazendo o grupo. Vez que a política de privacidade da Raia-Drogasil estabelece a possibilidade de compartilhamento de informações com parceiros do mesmo grupo, sem, contudo, deixar claro para o consumidor quais dados serão repassados e quem são esses parceiros. Assim, ao permitir a coleta da biometria, o consumidor consente com o compartilhamento dos seus dados com todas as empresas que fazem parte do grupo econômico da Raia-Drogasil (The Intercept, 2021).

Assim é possível perceber que a finalidade não condiz com o tratamento de dados que de fato é realizado (princípio da adequação, art. 6º, II) e indícios de coleta excessiva de dados pessoais, incluindo dados sensíveis (princípio da necessidade, art. 6º, III). Ademais, no que

tange a políticas de privacidade e informações disponibilizadas, percebe-se a carência de informações claras, precisas e facilmente acessíveis, especialmente quando relacionadas ao programa de fidelidade Stix (princípio da transparência, art. 6º, VI) junto a informações como finalidade, identificação de agentes de tratamento e compartilhamento de dados, que não são facilmente disponibilizadas a titulares (direito de acesso, art. 9º).

A política de privacidade da Stix afirma que utiliza como bases legais "o legítimo interesse, o consentimento, a execução de contrato e o cumprimento de obrigação legal, em diferentes finalidades". Entre os diversos dados relacionados à finalidade de tratamento para personalização de ofertas, estão os dados de geolocalização e o histórico comportamental de acúmulo de pontos e resgate. A política dispõe ainda que a base legal do histórico comportamental de acúmulos de pontos é o legítimo interesse e não a finalidade. Informando que apenas a realização do cadastro na plataforma utiliza o consentimento como base legal (Sou Stix, 2023).

A situação se agrava visto que as empresas que receberam os dados, trataram e coletaram inúmeros dados sensíveis dos consumidores de forma irregular, o que ameaça não só a privacidade dos consumidores que tiveram seus dados compartilhados, mas de toda a sociedade, visto que em algum momento todos já foram vulneráveis (Silva *et al.*, 2021).

A rede de farmácias recebeu então uma multa no valor de R$572.680,71 (quinhentos e setenta e dois mil seiscentos e oitenta reais e setenta e um centavos) pelo Procon Estadual de Mato Grosso. Foi realizada uma fiscalização nas farmácias a qual constatou a irregularidade através da solicitação do Ministério Público de Mato Grosso, mediante denúncias feitas pelos consumidores (Oliveira, 2022).

Ficou provado na fiscalização que além das farmácias estarem obtendo o consentimento dos consumidores sem prestar a informação clara, percebeu-se ainda a inadequação de informações sobre o recadastramento e autorização para o tratamento de dados pessoais em todas as unidades vistoriadas, conforme disse o coordenador da fiscalização em para o Procon-MT, Ivo Vinicius Firmo:

> Ficou comprovado que o principal objetivo da atualização cadastral é conseguir a autorização para o tratamento de dados, prevalecendo-se da ignorância do consumidor, e não apenas garantir a participação em programas de descontos e benefícios, como era informado aos clientes durante o recadastramento.

Nesse contexto, é inequívoca a falta de adequação e de atualização do grupo farmacêutico em relação à LGPD e a regimes de adequação corporativa. Assim com a falta de

transparência e com a escassa operacionalização do direito de acesso (art. 9º, LGPD) restou clara a dificuldade de os titulares se oporem ao tratamento de seus dados pessoais, em grande parte sensíveis, como por exemplo, a coleta de biometria. Vez que as informações não eram disponibilizadas de maneira clara e facilitada sobre as fases do tratamento de dados, como finalidade ou identificação dos agentes de tratamento (Nota Técnica n° 4/2022/CGTP/ANPD).

Ademais, em outubro de 2023 a Secretaria Nacional do Consumidor (Senacon) notificou a empresa Raia-Drogasil devido tratamento indevido de dados pessoais sensíveis dos consumidores, relacionados à saúde. Segundo matéria do site do governo federal, a empresa foi notificada devido uma matéria publicada no portal UOL, a qual dizia que empresas do Grupo Raia-Drogasil estariam, mais uma vez, coletando informações com o consentimento inadequado dos clientes e comercializando as informações para terceiros anunciantes.

A notícia do Governo Federal diz ainda que:

> A reportagem denuncia que um empresa do grupo, a RD Ads, estaria realizando publicidade direcionada a determinados perfis de consumidores (por exemplo, considerando a faixa etária, o sexo, os problemas de saúde) com base nos dados indevidamente coletados e classificados, entre outras operações de tratamento. A publicidade seria feita não apenas para empresas do grupo econômico, mas também para terceiros, levando a empresa a "ganhar dinheiro", conforme a matéria. Ainda de acordo com o texto, os consumidores seriam induzidos a conceder seus dados pessoais com a promessa de obter descontos em preços de produtos e serviços, especialmente medicamentos (Brasil, 2023).

Apesar deste ser um caso de uso inadequado dos dados sensíveis no meio físico, possui grandes reflexos da correlação em análises de dados automatizados. Visto que a intenção do grupo Raia-Drogasil era de compartilhar os dados como meio de angariar o consumidor para outras empresas do grupo econômico a fim de criar campanhas de publicidade altamente segmentadas. Assim, insta dizer que a atitude da rede vai de encontro com à autodeterminação informativa, conceito já mencionado anteriormente e demonstrar a falta de cuidado com a Lei Geral de Proteção de Dados.

Outro caso que demonstra o uso inadequado dos dados para a publicidade direcionada é o da empresa Decolar.com e a discriminação de preços por cidade através do tratamento de dados de geolocalização. A empresa beneficiava clientes estrangeiros com melhores ofertas, essa diferenciação era feita com base na localização do consumidor na hora da compra, fazendo a ocultação das acomodações para consumidores brasileiros. Para explicitar tal prática foi feita simulações com pesquisas de preço e disponibilidade de hotéis por meio de computadores localizados em São Paulo e Buenos Aires (Marchetti, 2018).

Saber a localização do seu consumidor e onde eles estão concentrados é essencial para o marketing digital para que as campanhas publicitárias possam ter maior êxito e possam angariar mais consumidores. Nesse cenário foi aprimorado o uso do GPS (*Global Positioning System*) nos dispositivos móveis, a fim de facilitar a descoberta de consumidores em potencial através da localização (Bioni, 2020).

Desde a década de 70 a análise de dados demográficos contribui para a publicidade e juntamente com estes são analisados o salário, gênero e etnia, filtrando grupos alvos, visto que perceberam que pessoas da mesma raça e com mesmos salários geralmente moravam na mesma região. O uso da localização para a publicidade acontece inclusive no meio físico, visto que os outdoors são posicionados estrategicamente objetivando captar o consumidor ao se locomover (Bioni, 2020).

Por meio da localização dos usuários a empresa fazia a diferenciação através de dois sistemas conhecidos como geodiscriminação. O primeiro é conhecido como *geoblocking*, o qual estabelece perfis dos consumidores, restringindo acesso a determinado conteúdo devido a sua localidade. O segundo sistema é conhecido como *geopricing* que analisa os perfis dos consumidores e diferencia os valores de um mesmo produto com preços diferentes a depender da sua localidade.

Foi fazendo o uso indevido desses dados que a Decolar.com utilizou estas técnicas para obter maior lucro na venda de reserva dos hotéis. A empresa ofertava reservas a preços diferentes, a depender da localização do consumidor (*geopricing*). A Decolar teria ainda ocultado a disponibilidade de acomodações a consumidores brasileiros, em favor de consumidores estrangeiros (*geoblocking*). As situações foram descobertas através de denúncia do Booking - empresa que atua no mercado de hospedagem como intermediária entre estabelecimentos hoteleiros e consumidores - ao Departamento de Proteção e Defesa do Consumidor (DPDC) do Ministério da Justiça, por meio do processo administrativo n° 08012.002116/2016-21 (Nota Técnica nº 92/2018).

Diante desse cenário, a Nota Técnica n° 92/2018 explicitou sobre a vulnerabilidade do consumidor nos seus três âmbitos - a técnica, a jurídica e a fática. Assim, concluiu que as práticas de *geoblocking* e *geopricing* são abusivas, dispostas, respectivamente, no art. 39, inciso IX e X do CDC:

> **Art. 39.** É vedado ao fornecedor de produtos ou serviços, dentre outras práticas abusivas:

> **IX** - recusar a venda de bens ou a prestação de serviços, diretamente a quem se disponha a adquiri-los mediante pronto pagamento, ressalvados os casos de intermediação regulados em leis especiais;
>
> **X** - elevar sem justa causa o preço de produtos ou serviços.

No caso em comento, ocorre inequívoco desrespeito não só ao Código de Defesa do Consumidor, mas também à Lei Geral de Proteção de Dados, vez que o consumidor não sabe que, por meio de seu IP, pode fornecer esses dados à Decolar - esbarrando assim no princípio da finalidade. Ademais, o uso dessas práticas também esbarra no princípio da não-discriminação, previsto no art. 6, IX da LGPD, uma vez que o uso dessas técnicas discrimina os consumidores por causa da sua localização geográfica. Conclui-se, portanto, que a política de privacidade do site não é clara, nem satisfatoriamente informativa, o que vai de encontro ao princípio da transparência, previsto no art. 6, inciso VI da LGPD.

Devido a isso, o Departamento de Proteção e Defesa do Consumidor (DPDC) multou a empresa em R$ 2.500.000,00 (dois milhões e quinhentos mil reais) por diferenciação de preço nas reservas dos hotéis (*geopricing*) e negativa de oferta de vagas (*geoblocking*), de acordo com a localização geográfica do consumidor, sendo consideradas práticas abusivas e discriminatórias (Despacho n° 299/2018).

Nesse contexto, é notória à urgência da adequação à Lei Geral de Proteção de Dados a fim de prevenir situações futuras, de forma a preservar a livre determinação dos usuários enquanto cidadãos no mundo digital, visto que o compartilhamento de dados pessoais entre empresas pode levar a uma maior coordenação de preços e práticas comerciais, o que pode resultar em preços mais altos para os consumidores.

4.3 A adequação à Lei Geral de Proteção de Dados (LGPD), sanções aplicadas pela inobservância desta lei e as práticas necessárias pelos agentes de tratamento para a segurança e o sigilo dos dados

Anterior à promulgação da Lei Geral de Proteção de Dados, o Código de Defesa do Consumidor, a Lei de Acesso à Informação e o Marco Civil da Internet regulamentavam a proteção de dados. Contudo, foi a partir da LGPD que ocorreu a definição dos personagens em torno do tratamento de dados, assim como a diferenciação do que seria dado pessoal, dado pessoal sensível, dado anonimizado e banco de dados, a fim de tornar a lei mais cristalina e a adequada aplicação. Para fins desta pesquisa serão abordadas apenas as definições que estabelecem correlação com o consumidor e o comércio eletrônico.

Assim, a LGPD traz a definição de dado pessoal, como a informação relacionada a pessoa natural identificada ou identificável. Para Bioni (2020) este conceito é elemento central para o aperfeiçoamento da normatização, assim a lei buscou generalizar a interpretação acerca de dados pessoais através dos critérios reducionistas e expansionistas. Estando o primeiro relacionado a dados que possam identificar de imediato a pessoa; e o segundo seriam os dados que, apesar de serem inerentes à pessoa, não as individualizam.

Por conseguinte, a lei trata acerca dos dados anonimizados, definindo-os no art. 5, inciso III como dados relativos a titular que não possa ser identificado, a partir da utilização de meios disponíveis no seu tratamento. A anonimização é feita por meio de diferentes técnicas que identificam quais elementos poderiam ser modificados para que dificulte a identificação. Bioni (2020) exemplifica as técnicas diante dos casos concretos, da seguinte maneira: a supressão, generalização, randomização e a pseudoanonimização.

A supressão vem a ser a técnica adequada ao CPF, visto que por ser um dado que possibilita a identificação imediata sua disponibilização, ainda que parcial, não seria adequada; a generalização é a técnica usada nos casos de localização geográfica, a qual seria disponibilizada apenas os primeiros dígitos do CEP e não o número completo, quebrando o vínculo da identificação; a randomização é um processo de seleção em que as probabilidades são atribuídas a todos de forma igualitária; e por fim a pseudoanonimização é a técnica que substitui apenas os identificadores diretos do dado por pseudônimos (Bioni, 2020, p. 62).

Faz-se necessário mencionar ainda o conceito de banco de dados, que segundo a LGPD é o "conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico". Após o tratamento, o banco de dados deve ser eliminado, sendo possível a conservação para as finalidades previstas em lei, como: cumprimento de obrigação legal ou regulatória pelo controlador; estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados (Brasil, 2018).

Para fins da relação feita nesta pesquisa, insta mencionar ainda a conceituação de agentes de tratamento, o controlador e operador responsáveis pelo tratamento dos dados (Brasil, 2018).

O controlador deve tratar os dados pessoais de acordo com as finalidades aceitas pelo titular. Como já fora explicado no capítulo anterior desta pesquisa, a LGPD prevê que o tratamento dos dados só será feito mediante consentimento do titular. Ademais, o art. 8º aduz

que o consentimento deverá ser fornecido por meio que demonstre a manifestação de vontade do titular.

No cenário digital a especificação dos direitos do titular de dados é indispensável para a interpretação adequada e sistemática da lei. Assim, se fez necessário a criação de uma autoridade de proteção dos dados pessoais, que está prevista no art. 5°, inciso VIII e XIX da LGPD, fazendo parte da definição de encarregado:

> VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);
>
> XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional (Brasil, 2018).

Apesar da compreensão atual da importância da Autoridade Nacional de Proteção de Dados (ANPD), se deu de forma morosa, visto que não foi aceita de primeira. A ANPD foi criada através da Medida Provisória nº 869/2018, convertida na Lei n° 13.853/2019, tendo função normativa, deliberativa, fiscalizadora e sancionatória para a efetiva proteção de dados em todo o território nacional.

O tratamento de dados pessoais é inerente aos estados contemporâneos, contribuindo principalmente para o avanço da segurança da informação, porém, essa prática deve ser conduzida de forma cautelosa e efetiva.

Por isso, faz-se necessário mencionar as boas práticas que podem ser adotadas pelos agentes de tratamento para 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.

Vez que, conforme o art. 47 da LGPD, são estes os agentes de tratamento que têm a função de garantir a segurança da informação em relação aos dados pessoais, mesmo após o seu término. A LGPD busca com essas práticas evitar eventos invasivos antes que aconteçam, ou seja, preventiva e não corretiva. Assim, o controlador deve comunicar a autoridade nacional e ao seu titular a possibilidade de ações que coloquem em risco a segurança do titular, devendo dispor acerca da descrição da natureza dos dados pessoais afetados, as informações sobre os titulares envolvidos, a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial, os riscos e as medidas que podem ser adotadas para reverter ou diminuir os prejuízos.

O art. 49 aduz ainda que os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais da lei e às demais normas regulamentares.

Nesse sentido, buscando assegurar a proteção de dados, é função da ANPD, conforme art. 55-J da LGPD, a elaboração de estudos sobre práticas nacionais e internacional de proteção de dados pessoais e privacidade, assim como elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade, fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento a legislação, mediante processo administrativo, sendo indispensável também o estímulo a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais (Brasil, 2018).

O art. 55-K da LGPD aduz que compete exclusivamente à ANPD a aplicação das sanções, assim os agentes de tratamento ficam sujeitos a sanções no caso do cometimento de infrações, conforme dispõe o art. 52º da LGPD:

> 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;
>
> IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
>
> 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;
>
> 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;
>
> 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;
>
> XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Para além, a Autoridade Nacional de Proteção de Dados, apesar de ser o órgão central não precisará cumprir suas funções necessariamente sozinha, ela pode atuar juntamente com outros órgãos e entidades com competências sancionatórias e normativas que possuam interesses na proteção de dados (Brasil, 2018).

Considerando que o Brasil está caminhando para ser um país que tem como cultura a proteção de dados, as sanções de publicização da infração, disposta no inciso IV, do art 52º da LGPD, pode obter um efeito corretivo e educacional mais adequado do que efetivamente obrigar ao pagamento de multas. Por isso, segundo Stefano Rodotá (2018), as sanções elencadas pela LGPD possuem um caráter preventivo e não somente reparatório, a fim de evitar prejuízos futuros. Assim, considerando o cenário da proteção de dados no Brasil que visa juntamente a defesa do consumidor, ocorre a atuação conjunta entre a Secretaria Nacional do Consumidor (SENACON) e a ANPD.

Assim, no Brasil, a Lei Geral de Proteção de Dados ainda é um tema considerado novo, passando por processos de aplicabilidade nas empresas privadas e públicas. Considerando os casos citados anteriormente nesta pesquisa, percebe-se que ainda não houve a criação da cultura de proteção de dados pessoais e, consequentemente, a real preocupação com a necessidade do tratamento adequados dos dados pessoais nem o meio físico e nem no digital. Por isso os dados ainda são utilizados de forma inadequada a fim de criarem campanhas de publicidade altamente segmentadas, que visam diretamente os interesses e necessidades individuais do usuário, aumentando assim a probabilidade de preços mais altos aos consumidores.

Em linhas gerais, é indispensável a atenção para os riscos que se materializam para o consumidor-usuário em relação a violação da privacidade e ao tratamento inadequado dos dados pessoais, a fim de que possa garantir a aplicabilidade da LGPD e a criação da cultura no Brasil de proteção aos dados pessoais.

5 CONCLUSÃO

O direito à privacidade é um direito fundamental, e sua importância não se restringe ao fim em si mesmo, mas abrange também a garantia de uma diversidade de outros direitos inerentes a intimidade da vida humana, conforme exposto ao longo desta pesquisa. A sociedade do consumo e os avanços tecnológicos fizeram surgir novas situações de violação da vida privada, como a coleta, o tratamento e o compartilhamento indevidos dos dados pessoais dos indivíduos, sobretudo no meio digital. Assim, as novas perspectivas criadas pela era tecnológica conectaram a privacidade à proteção de dados. Foi nessa perspectiva que ocorreu a elevação da proteção de dados como direito fundamental. A relevância do presente estudo se materializa não apenas no esclarecimento de um tema tão importante, mas também na compreensão de que é preciso estar atento aos meios utilizados para se atingir um objetivo final.

Diante disso, foram abordadas as implicações causadas pelo uso das novas tecnologias e pelo tratamento em massa de dados pessoais no comércio eletrônico. Nesse cenário ocorreu a promulgação da Lei Geral de Proteção de Dados (LGPD) frente as constantes violações da intimidade dos indivíduos por meio dos dados pessoais. A LGPD vem disciplinar sobre como tratar os dados pessoais, protegendo o consumidor nestas ações, pois como detentor desses dados, passa a ter o direito de confirmação da existência de processamento de seus dados e de poder acessá-los; pode ainda coibir o seu tratamento, por meio da recusa em fornecer o consentimento; cabe também ao indivíduo solicitar que cancelem ou excluam dados irrelevantes, exagerados ou com seu tratamento em divergência com a lei.

Nesse sentido, foi estabelecida a inter-relação entre o Código de Defesa do Consumidor e a LGPD no que tange o tratamento de dados do consumidor, visto que o CDC foi o precursor no que concerne à proteção dos dados pessoais do consumidor, assim como foi estabelecida a responsabilidade das empresas perante os dados pessoais.

No decorrer desta análise, foi tratado como o compartilhamento de dados pessoais entre empresas pode levar a uma maior coordenação de preços e práticas comerciais, o que pode resultar em preços mais altos para os consumidores.

A partir das análises feitas, percebeu-se que o titular dos dados pessoais, na maioria dos casos, não possui conhecimento tecnológico adequado e não compreende os potenciais riscos por trás do consentimento maculado, além de ser vulnerável, seja em razão da complexidade da arquitetura tecnológica empregada em um sistema, seja em razão da opacidade encontrada nos dados coletados e suas combinações. Comprovando isto, foi citado ao longo desta pesquisa casos como o da Raia-Drogasil e da Decolar.com que elucidam os riscos da não-observância

da LGPD, assim como os prejuízos sofridos pelos consumidores-usuários com o tratamento inadequado dos seus dados.

Por isso, foi abordado ao longo desta pesquisa a importância da criação da Autoridade Nacional de Proteção de Dados Pessoais (ANPD) que serve para tutelar a proteção de dados pessoais e é responsável por regulamentar, implementar e fiscalizar o cumprimento da LGPD no Brasil. Percebeu-se que além da ANPD outros órgãos como a Secretaria Nacional do Consumidor (SENACON) possuem o objetivo de construir no país a cultura de proteção de dados pessoais, divulgação de procedimentos e estudos, fundamentados em boas práticas nacionais e internacionais em empresas públicas e privadas.

Ficou demonstrado que o fato de a LGPD ser uma regulamentação principiológica possibilita que a interpretação da lei seja ajustada aos novos cenários tecnológicos que já estão surgindo, impedindo dessa forma, que a lei se torne ultrapassada em pouco tempo.

Desse modo, esta pesquisa propôs-se essencialmente a analisar como o uso indevido de dados pessoais e a violação do direito à privacidade por parte das empresas influencia no comportamento do usuário para o aumento do consumo na internet, objetivo que foi atingido, visto que, além da análise teórica da LGPD, foi possível apresentar o contexto do direito à privacidade e da proteção de dados, assim como a sua caracterização enquanto direito fundamental no contexto contemporâneo da sociedade de consumo.

Ademais, este estudo confirmou a hipótese apresentada, de que a disponibilidade de dados pessoais pode levar ao surgimento de novos modelos de negócios baseados na exploração de informações pessoais e que o compartilhamento de dados pessoais entre empresas pode levar a uma maior coordenação de preços e práticas comerciais através da publicidade direcionada, acarretando prejuízos aos consumidores.

REFERÊNCIAS

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Nota Técnica n° 4/2022/CGTP/ANPD.** Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/NotaTcnican4.2022.CGTP.ANPD.pdf . Acesso em: 12 out. 2023.

BOTELHO, Marcos Cesar. A proteção de dados pessoais enquanto direito fundamental: considerações sobre a Lei Geral de Proteção de Dados Pessoais. **Argumenta Journal Law**, Jacarezinho, n. 32, p. 191-207, abr. 2020. Disponível em: https://core.ac.uk/reader/327193050. Acesso em: 30 ago. 2023.

BRASIL. **ANPD**: Documentos e publicações. Disponível em: https://www.gov.br/anpd/ptbr/documentos-e-publicacoes. Acesso em: 19 nov. 2022.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 31 ago. 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). **Diário Oficial da União**, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 31 ago. 2023.

BRASIL. RESOLUÇÃO CD/ANPD Nº 2, DE 27 DE JANEIRO DE 2022**. Diário Oficial da União**, Brasília, DF, ed.20, s. 1, p. 6, 28 jan. 2022. Disponível em: www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019#wrapper. Acesso em: 1 out. 2023.

BRASIL. **Senacon notifica RaiaDrogasil sobre tratamento indevido de dados pessoais dos consumidores.** 23 out. 2023. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/senacon-notifica-raiadrogasil-sobre-tratamento-indevido-de-dados-pessoais-dos-consumidores. Acesso em: 19 out. 2023.

CANCELIER, Mikhail Vieira de Lorenzi. O direito à privacidade hoje: perspectiva histórica e o cenário brasileiro**. Sequência: Estudos Jurídicos e Políticos**, [*s. l.*], v. 38, n. 76, p. 213, 20 set. 2017. Universidade Federal de Santa Catarina (UFSC). Disponível em: https://www.scielo.br/j/seq/a/ZNmgSYVR8kfvZGYWW7g6nJD/?format=pdf&lang=pt. Acesso em: 30 ago. 2023.

CANUT, Letícia. **Proteção do Consumidor no Comércio Eletrônico:** uma questão de inteligência coletiva que ultrapassa o direito tradicional. [*s. l.*], [*s. d.*]. Disponível em: publicadireito.com.br/conpedi/manaus/arquivos/anais/XIVCongresso/011.pdf#. Acesso em: 20 out. 2023.

CARVALHO, Cristiane Mafacioli. Gênero, linguagem e estratégias do discurso publicitário da atualidade. **Revista Famecos,** [*s. l.*], v. 19, n. 3. p. 821-838, 2 jan. 2013. EDIPUCRS. p. 822. Disponível em: http://dx.doi.org/10.15448/1980-3729.2012.3.12903. Acesso em: 25 out. 2023.

CONSELHO EUROPEU. COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS. **Convenção nº 108.** Disponível em: https://rm.coe.int/cm-convention-108-portuguese-version-2756-1476-7367-1/1680aa72a2. Acesso em: 30 ago. 2023.

DIAS, Tatiana. Não cadastre sua biometria na Droga Raia – e nem em qualquer farmácia. **The Intercept Brasil,** 5 jul. 2021. Disponível em: https://theintercept.com/2021/07/05/nao-cadastre-biometria-na-droga-raia/. Acesso em: 21 de out. de 2023.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal Of Law** [Ejjl], Joaçaba, v. 12, n. 2, p. 91-108, jul. 2011. Disponível em: https://periodicos.unoesc.edu.br/espacojuridico/article/view/1315/658. Acesso em: 30 ago. 2023.

DONEDA, Danilo. **Da privacidade a proteção de dados pessoais**. São Paulo: Renovar, 2006. 448 p.

ELIEZER, Cristina Rezende *et al.* (org.). **Estudos contemporâneos de direito do consumidor.** Santo Ângelo: Editora Metrics, 2023. 406 p.

FEIJÓ, Alexsandro Rahbani Aragão; DUTRA, Thayse Caldas Galvão. **A proteção de dados pessoais e o direito à saúde.** Curitiba: Crv, 2023.

FOLLONE, Renata Aparecida; SIMÃO FILHO, Adalberto. A conexão da LGPD e CDC: a proteção de dados pessoais nas relações consumeristas e a sua concretização como direito fundamental. **Anais do Congresso Brasileiro de Processo Coletivo e Cidadania**, [*s. l.*], n. 8, p. 937–959, 2020. Disponível em: https://revistas.unaerp.br/cbpcc/article/view/2112. Acesso em: 1 set. 2023.

FONSECA, Edson Pires da. **Lei Geral de Proteção de Dados-LGPD.** Salvador: Juspodivm, 2021. LIMA, Lindamaria. Os 10 princípios para tratamento de dados da LGPD**.** 2020. Disponível em: https://triplait.com/principios-para-tratamento-de-dados-da-lgpd/ . Acesso em: 1 out. 2023.

GRINOVER, Ada Pellegrini; BENJAMIN, Antônio Herman de V.; FINK, Daniel Roberto; FILOMENO, José Geraldo Brito; WATANABE, Kazuo; NERY JUNIOR, Nelson; DENARI, Zelmo. **Código Brasileiro de Defesa do Consumidor: comentado pelos autores do anteprojeto:** direito material e processo coletivo: volume único. 12. ed. Rio de Janeiro: Forense, 2019.

LUFT, Mayumi Iguchi; POLLI, Fernando Gabbi. Sociedade de Informação, ambiente virtual e Código de Defesa do Consumidor: possibilidade de responsabilização das redes sociais em razão dos danos causados aos usuários através da ótica consumerista. **Revista Eletrônica do Curso de Direito da UFMS.** v. 7, n. 2, 2012. Disponível em: https://periodicos.ufsm.br/revistadireito/citationstylelanguage/get/apa?submissionId=7425&publicationId=5503. Acesso em: 28 set. 2023.

MARCHETTI, Brunno. **Como Decolar.com e outras empresas mudam preços de acordo com seus dados**. 1 mar. 2018. Disponível em: https://brunobioni.com.br/blog/namidia/como-decolar-com-e-outras-empresas-mudam-precos-de-acordo-com-seus-dados/. Acesso em: 08 nov. 2023.

MARQUES, Cláudia Lima. **Contratos no código de defesa do consumidor:** o novo regime das relações contratuais. 2002. Disponível em: https://edisciplinas.usp.br/pluginfile.php/5547102/mod_resource/content/1/MARQUES%2C%20Cl%C3%A1udia%20Lima%20%20Contratos%20no%20C%C3%83%C2%B3digo%20de%20Defesa%20do%20Consumidor%20-%20P.%20251-334.pdf. Acesso em: 19 out. 2023.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor:** linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MINISTÉRIO DA JUSTIÇA. Despacho n° 299/2018. **Diário Oficial da União**, Brasília, DF, ed. 115, s. 1, p. 73, 18 jun. 2018. Disponível em: http://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/26176368/do1-2018-06-18-despacho-n-299-2018-26176301. Acesso em: 3 out. 2019.

MINISTÉRIO DA JUSTIÇA. **Nota Técnica nº 92/2018/CSA-SENACON/CGCTSA/GAB-DPDC/DPDC/ SENACON/MJ**. Disponível em: http://tiny.cc/x4hwdz. Acesso em: 3 out. 2019.

MIRAGEM, Bruno. A Lei Geral de Proteção de dados (Lei 13.709/2018) e o direito do consumidor. **Revista dos Tribunais**, v. 1009, nov., 2019. Disponível em: https://www.brunomiragem.com.br/wp-content/uploads/2020/06/002-LGPD-e-o-direito-do-consumidor.pdf. Acesso em: 28 set. 2022.

PASSOS, Bruno Ricardo dos Santos. **O direito à privacidade e a proteção aos dados pessoais na sociedade da informação**: uma abordagem acerca de um novo direito fundamental. 2017. 105 f. Dissertação (Mestrado) - Curso de Faculdade de Direito, Universidade Federal da Bahia, Salvador, 2017. Disponível em: https://repositorio.ufba.br/bitstream/ri/22478/1/Bruno%20Ricardo%20dos%20Santos%20Passos.pdf. Acesso em: 29 ago. 2023.

PINTO, Eduardo Régis Girão de Castro. **A responsabilidade civil do fornecedor pela quebra do dever de proteção de dados pessoais dos consumidores: metodologia da análise de decisões proferidas entre 2018 e 2022**. Disponível em: https://biblioteca.sophia.com.br/terminalri/9575/acervo/detalhe/129854. Acesso em: 25 out. 2023.

RODOTÁ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje.** Tradução: Danilo Doneda. São Paulo: Ed. Perspectiva, 2018. Disponível em: https://pt.scribd.com/document/288104762/A-Vida-Na-Sociedade-Da-Vigilancia#. Acesso em: 20 de abr. 2023

SCHWUARTZ, Fabio. **A Defensoria Pública e a proteção dos (hiper) vulneráveis no mercado de consumo.** Consultor Jurídico, 19 jul. 2016. Disponível em: https://www.conjur.com.br/2016-jul-19/protecao-hipervulneraveis-mercado-consum. Acesso em: 1 maio de 2022.

SILVA, André Luiz Barbosa da. A sociedade contemporânea**:** a visão de Zygmunt Bauman. **Revista Extraprensa**, [*s. l.*], v. 4, n. 2, p. 31-37, 2011. DOI: 10.11606/extraprensa2011.77237. Disponível em: https://www.revistas.usp.br/extraprensa/article/view/77237. Acesso em: 1 set. 2023.

SILVA, Vanessa Junior da. **Proteção Geral de Dados**: comunidade europeia x Brasil. 2019. 81 f. Monografia (Graduação) - Curso de Curso de Direito, Universidade Univates, Lajeado, 2019. Disponível em: https://www.univates.br/bduserver/api/core/bitstreams/cb6348ff-35c6-4e20-aa9a-5fcfbb029b4d/content. Acesso em: 29 ago. 2023.

SIQUEIRA, Oniye Nashara *et al*. A (hiper)vulnerabilidade do consumidor no ciberespaço e as perspectivas da LGPD. **Revista Eletrônica Pesquiseduca**, [*s. l.*], v. 13, n. 29, p. 236-255, 21 mar. 2021. Universidade Católica de Santos. Disponível em: https://periodicos.unisantos.br/pesquiseduca/article/view/1029. Acesso em: 29 ago. 2023.

SOU STIX. **Política de Privacidade e Cookies**. 2023 Disponível em: https://www.soustix.com.br/politicas-de-privacidade. Acesso em: 23 out. 2023.

VENOSA, Silvio de Salvo. **Direito Civil**: parte geral. 6ª ed. São Paulo: Atlas, 2006.

VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade de informação:** efetividade desse direito fundamental diante dos avanços da tecnologia da informação. 2007. 297 f. Dissertação (Mestrado) - Curso de Direito, Estado e Sociedade, Faculdade de Direito, Universidade de Brasília, Brasília, 2007. Disponível em: https://repositorio.unb.br/bitstream/10482/3358/1/2007_TatianaMaltaVieira.pdf. Acesso em: 27 ago. 2023.

VIEIRA, Waleska Duque Estrada. A privacidade no ambiente cibernético: direito fundamental do usuário. **Revista da Esmesc**, [*s. l.*], v. 24, n. 30, p. 197, 14 dez. 2017. Lepidus Tecnologia. DOI: http://dx.doi.org/10.14295/revistadaesmesc.v24i30.p197. Disponível em: https://esmesc.emnuvens.com.br/re/article/view/167/141. Acesso em: 31 ago. 2023.