



FACULDADE EVANGÉLICA DE GOIANÉSIA
BACHAREL EM DIREITO

**A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E AS RELAÇÕES
JURÍDICAS NO ÂMBITO DO DIREITO DO CONSUMIDOR**

CACILIANA DA SILVA RECALDE

GOIANÉSIA/GO
2022

CACILIANA DA SILVA RECALDE

**A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E AS RELAÇÕES
JURÍDICAS NO ÂMBITO DO DIREITO DO CONSUMIDOR**

Artigo Científico apresentado junto ao Curso de Direito da FACEG (Faculdade Evangélica de Goianésia), como exigência parcial para a obtenção do grau de Bacharel em Direito.

Orientadora: Me^a Prof.^a Simone Maria da Silva

GOIANÉSIA/GO
2022

FOLHA DE APROVAÇÃO

**A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E AS RELAÇÕES
JURÍDICAS NO ÂMBITO DO DIREITO DO CONSUMIDOR**

Este Artigo Científico foi julgado adequado para a obtenção do título de Bacharel em
Direito e aprovado em sua forma final pela banca examinadora da Faculdade
Evangélica de Goianésia/GO- FACEG

Aprovada em, ____ de ____ de 2022

Nota Final ____

Banca Examinadora

Prof.^a Doutoranda Simone Maria da Silva
Orientador

Prof.^a. Esp. Mariana Ferreira Martins
Professor convidado 1

Prof. Mestre Adonis de Castro Oliveira
Professor convidado 2

AGRADECIMENTOS

Primeiramente agradeço a Deus por ter me dado iniciativa e condições para cursar a faculdade de Direito. Aos meus pais *in memorian*, os quais tenho a missão de honrar.

Dedico esse trabalho ao meu amigo Alam Aparecido de Mattos Tombini *in memorian*, a sua amizade engrandeceu a minha vida.

Dedico esse trabalho em homenagem ao nosso amigo Gustavo Siqueira Correia *in memorian* pela companhia nos primeiros anos do Direito, um jovem alegre e trabalhador que deixou saudade em nossos corações e nas aulas.

Agradecer meus colegas de turma, especialmente a Carliana Elias da Silva Santos. Na turma fiz grandes amigos e agradeço cada um que trilhou essa jornada comigo.

Meus agradecimentos a minha orientadora Prof.^a Me^a Simone Maria da Silva pela dedicação nos ensinamentos, disponibilidade na orientação e brilhantismo na condução desse trabalho de conclusão de curso. Minha admiração por ela ter lutado bravamente pela vida contra a Covid 19.

A profa. Dra. Maisa França Teixeira por ser uma excelente profissional e ainda ter um coração sensível a todos os alunos do Direito.

A Nádía Mariel Farias do NAI (Núcleo de Assuntos Internacionais) pelo apoio fundamental para meu intercambio em Valladolid – Espanha.

EPÍGRAFE

Poemas pra não ler

Menino do mato

Nasci com o cheiro do mato

Primeiro me rastejava de lá pra cá parecendo um bicho preguiça

Depois fui dando meus primeiros passos como um potrinho desajeitado logo depois de nascer

Minhas primeiras aventuras foram no lombo de um cavalo solto pelos campos

Aprendi a nadar com os peixes

Aprendi a voar com os sabiás

Me camuflava na brincadeira de esconde esconde como um filhotinho de quero quero

Meu doce mais doce era o da jabuticaba

Minha grande surpresa era achar um bicho na goiaba

Meu primeiro carro foi uma carroça

Meu grande herói puxava sempre cantando uma enxada

Minha rainha não tem coroa, mas tem mais luz que todo tesouro de todas elas

Leite quente na caneca

Procurar o ninho da marreca

Se fui feliz?

Minha resposta é uma lágrima caindo devagarinho quando ouço um canto de perdiz.

Alam Tombini *in Memoriam*

A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E AS RELAÇÕES JURÍDICAS NO ÂMBITO DO DIREITO DO CONSUMIDOR

THE GENERAL PERSONAL DATA PROTECTION LAW AND LEGAL RELATIONS IN THE SCOPE OF CONSUMER LAW

CACILIANA DA SILVA RECALDE¹

SIMONE MARIA DA SILVA²

¹Discente do curso de Direito da Faculdade Evangélica de Goianésia- e-mail: caciliana@gmail.com

²Docente do curso de Direito da Faculdade Evangélica de Goianésia- e-mail: smsr.direito@hotmail.com

RESUMO: A presente pesquisa, intitulada: A Lei Geral de Proteção de Dados Pessoais e as Relações Jurídicas no Âmbito do Direito do Consumidor, buscou discorrer sobre as inovações da LGPD e os impactos no Direito do Consumidor. O tema abordado se justifica tendo em vista que a respectiva legislação tem o propósito de proteger direitos fundamentais como privacidade, intimidade, honra, direito de imagem e dignidade, que a partir da implantação da respectiva legislação os mesmos deverão ser observados com mais rigor. O problema que se buscou responder foi: Como permanece a proteção dos dados pessoais dos consumidores após a entrada em vigor da Lei 13.709/2018?. O objetivo geral da pesquisa foi verificar a aplicação da LGPD na proteção de dados, além de trazer suas definições e princípios. A metodologia utilizada foi pesquisa bibliográfica e documental. Demonstrou que o consentimento por parte do titular muitas vezes não reflete a realidade porque estes na grande maioria não leem as políticas de privacidade, para tanto se propõe o uso do modelo *European Data Protection Board (EDPB)* em não permitir que as empresas bloqueiem o acesso à prestação do serviço caso o titular não realize o aceite, para que as empresas não possam utilizar indevidamente seus dados. Como conclusão para aplicação das sanções frente a lei é necessário que os titulares dos dados tenham conhecimento do fluxo de utilização de seus dados, também caso ocorra danos causados na esfera consumerista ficará a critério da aplicação das normas do Código de Defesa do Consumidor.

Palavras-Chave: LGPD. Consumidor. Inovações.

Abstract: *This research, entitled: The General Data Protection Law (LGPD, in portuguese) and the Legal Relationships in the Field of Consumer Law, sought to discuss the innovations of LGPD and its impacts on Consumer Law. The approached theme is justified considering that the respective legislation has the purpose of protecting fundamental rights such as privacy, intimacy, honor, image rights and dignity, which, after the implementation of the respective legislation, should be more strictly observed. The problem that was sought to answer was: How does the protection of consumers' personal data remains after the entry into force of the Law no. 13.709/2018. The main objective of this research was to verify the application of the LGPD in data protection matter, in addition to bringing its definitions and principles. The methodology used was bibliographic and documentary research. It showed that the consent of the owner of the data often does not reflect the reality because most of them do not read the privacy policies, so it is proposed the use of the European Data Protection Board (EDPB) model in not allowing companies to block access to the provision of the service if the owner does not accept, so that companies cannot misuse their data. In conclusion, in order to apply the sanctions against the law, it is necessary that the owners of the data are aware of the flow of use of their data, and also in the event of damage caused in the consumer sphere, it will be at the discretion the application of the rules of the Consumer Protection Code.*

Keywords: LGPD. Consumer. Innovations.

INTRODUÇÃO

A Lei Geral de Proteção de Dados é uma norma que foi criada para regulamentar e proteger os dados dos usuários, esta proteção se tornou necessária frente aos direitos fundamentais de privacidade e liberdade, devido ao grande valor que as informações de usuários valem no mercado da publicidade.

A Lei Geral de Proteção de Dados, conhecida pela sigla LGPD “É uma regulamentação que traz princípios, direitos e obrigações relacionados ao uso de bases de dados das pessoas” (PINHEIRO, 2021, p.9). Os riscos a privacidade inerentes a utilização das tecnologias da informação, relativos ao direito do consumidor fez com que os países cada vez mais criassem ferramentas de proteção e conseqüentemente normatização.

A LGPD possui uma série de penalidades como advertência, multa, publicização da infração, bloqueio dos dados pessoais, suspensão parcial do funcionamento do banco de dados, suspensão do exercício da atividade de tratamento dos dados pessoais e proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Por isso é necessário realizar esse estudo para que se possa verificar aplicação da lei, como ela pode influenciar na vida do consumidor e o papel das empresas que fazem o tratamento dos dados. Assim respeitar os princípios fundamentais que regem a lei resguardando as pessoas em sua personalidade, privacidade, intimidade e honra.

Dessa forma, a presente pesquisa busca discorrer sobre a LGPD e sua aplicação frente ao Direito do Consumidor. O tema abordado justifica-se, tendo em vista que a respectiva legislação tem o propósito de proteger direitos fundamentais como privacidade, intimidade, honra, direito de imagem e dignidade. Posto isso, a problematização desta pesquisa se resume da seguinte forma: Como permanece a proteção dos dados pessoais dos consumidores após a entrada em vigor da Lei 13.709/2018?

Assim, o objetivo geral da pesquisa foi verificar a aplicação da LGPD na proteção de dados, além de trazer suas definições e princípios. Dentre os objetivos específicos destacou-se relatar o que as empresas fizeram para adequar e cumprir as

determinações da LGPD na entrada da vigência da Lei; descrever as sanções que as empresas podem ter diante do não cumprimento da LGPD frente ao direito do consumidor; discutir o papel das entidades de defesa do consumidor com possíveis violações a proteção de dados dos consumidores.

A metodologia utilizada foi pesquisa bibliográfica e documental, dentre artigos científicos, dissertações, teses. Os autores que serviram como fontes foram: Sarlet (2018), Corrêa (2019), Miragem (2019), Capanema (2020), Pinheiro (2021), Bioni (2021), Fornasier; Knebel (2021), dentre outros.

O trabalho foi dividido em três partes. O primeiro tópico discorrerá sobre os aspectos históricos da LGPD, demonstrando toda trajetória da criação da legislação até a vigência da mesma. O segundo tópico, abordará sobre os Princípios aplicados a LGPD e Tratamento de Dados, asseverando quais os princípios adotados pela legislação e como deverá ocorrer o tratamento dos dados em todas as relações de consumo.

Já no terceiro tópico será apresentado as Implicações Jurídicas da LGPD no Direito do Consumidor, onde abordará casos de vazamento de dados, as consequências jurídicas aplicadas dentre outros. E para finalizar as considerações finais sobre o assunto tratado, relatando as conclusões do estudo realizado.

1 ASPECTOS HISTÓRICOS DA LEI GERAL DE PROTEÇÃO DE DADOS- LGPD

Inicialmente como relata Bioni (2021) a sociedade se organizava através de riquezas provindas da terra dela aconteciam as trocas comerciais conhecida como escambo, sendo a primeira forma de organização comercial da chamada Sociedade Agrícola.

Posteriormente “sobreviu a criação das máquinas a vapor e da eletricidade que detiveram papel central na produção fabril e, por conseguinte, na formação das riquezas (sociedade industrial)” (BIONI, 2021, p. 3). Após a Segunda Guerra Mundial a sociedade pós industrial organizava-se através dos serviços que podiam oferecer, sendo de grande relevância para desenvolvimento da economia. Conforme Bioni (2021, p. 3) “como exemplo os setores bancário, securitário, educacional, de assistência

médica e de consultoria jurídica/legal”.

Atualmente o fator importante para o desenvolvimento econômico é a informação. A evolução tecnológica criou ferramentas de difusão das informações com velocidade o que fez com que o binômio tempo e espaço superasse os obstáculos das distâncias antes enfrentada. Permitindo assim uma maior interação social e desenvolvimento da economia global. “A informação é o (novo) elemento estruturante que (re)organiza a sociedade, tal como o fizeram a terra, as máquinas a vapor e a eletricidade, bem como os serviços, respectivamente, nas sociedades agrícola, industrial e pós-industrial” (BIONI, 2021, p. 3).

O armazenamento das informações de mercado através das redes de computadores permite fazer um mapeamento dos dados pessoais, o que é consumido, preferências, necessidades e demanda comercial. Todos esses dados alimentam as empresas que passam a produzir de acordo com o que o mercado necessita ou exige.

Essa utilização dos dados é conhecida pelo capitalismo de vigilância estudado por Shoshana Zuboff, autora norte americana que descreve uma transformação econômica com o capitalismo objetivando a exploração do comportamento das pessoas, compilações dos dados em todos os aspectos da vida cotidiana (FORNASIER; KNEBEL, 2021).

Nesse contexto surge a necessidade de proteger o consumidor já que os seus dados se tornaram um ativo valioso no mercado digital. De acordo com Sarlet (2018) a proteção de dados é relatada na história através de acontecimentos relacionados a proteção do direito de personalidade e também do direito ao esquecimento.

No Direito estrangeiro a proteção de dados não é algo novo, mesmo não sendo usada essa terminologia já estava na literatura e nas esferas jurisprudenciais, como relatado por Sarlet (2018, p.492) “Note-se que, em termos gerais, aspectos relevantes do que atualmente se entenda ser objeto de proteção de um direito ao esquecimento já podem ser encontrados em decisões bem mais antigas, que, todavia, não fazem menção direta a tal direito”.

Importante apresentar uma evolução histórica dos direitos que vieram posteriormente a serem relacionados com a proteção de dados, como se pode observar na Declaração Universal dos Direitos Humanos de 1948 que expressa em seu artigo 12

o direito à privacidade, sendo assim implicitamente uma proteção dos dados, que pode ser observado na leitura do artigo:

“Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei” (DECLARAÇÃO UNIVERSAL DOS DIREITOS HUMANOS, 1948).

O Brasil a partir do Decreto nº 678 de 06/11/1992 promulga a Convenção Americana sobre Direitos Humanos (Pacto de São José da Costa Rica), de 22 de novembro de 1969. A proteção à privacidade está presente no Pacto de São José da Costa Rica com objetivo de garantir direito ao respeito a honra, a dignidade, a vida privada com ressalva que quanto essas ingerências terão proteção da lei. É o que está exposto em seu artigo 11:

Proteção da Honra e da Dignidade

1. Toda pessoa tem direito ao respeito de sua honra e ao reconhecimento de sua dignidade.
2. Ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, na de sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra ou reputação.
3. Toda pessoa tem direito à proteção da lei contra tais ingerências ou tais ofensas. (PACTO DE SÃO JOSE DA COSTA RICA, 1969).

Na Europa conforme Quintiliano (2021) a Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais, tem de forma genérica uma proteção à privacidade. Datada de 1950, em seu artigo 8º, tem se a seguinte leitura:

Direito ao respeito pela vida privada e familiar

1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência.
2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar econômico do país, a defesa da ordem e a prevenção das infrações penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros (CONSELHO DA EUROPA, 1950).

Em 1981 o Conselho Europeu realizou a primeira Convenção para a Proteção Pessoal em relação ao Tratamento Automatizado de Dados de Caráter Pessoal, adotada em 28 de janeiro de 1981 (QUINTILIANO, 2021). Entre os fundamentos estabeleceram a importância de relacionar os valores fundamentais do respeito à vida

privada e da livre circulação de informação entre os povos. No ano de 2020 o Brasil foi convidado a participar desta reunião pela Agência Nacional de Proteção de Dados (ANPD) na condição de observador.

Mudanças no modelo de economia digital a partir dos anos de 1990 com o maior fluxo internacional de bases de dados relacionados às pessoas desencadearam o surgimento de regulamentações de proteção de dados pessoais (PINHEIRO, 2021). Os avanços tecnológicos e da globalização foram fatores preponderantes para demanda em proteção de dados pessoais, uma vez que as pessoas passaram a disponibilizar dados nas redes para os mais diversos usos.

“As organizações passaram a ter compromisso de resgatar e repactuar à proteção e à garantia dos direitos humanos fundamentais, como o da privacidade, já celebrados desde a Declaração Universal dos Direitos Humanos (DUDH) de 1948” (PINHEIRO, 2021, p.10). No ano de 1995 a União Europeia elaborou a Diretiva 95/46/CE com objetivo de assegurar a proteção dos dados pessoais no âmbito das instituições e dos órgãos da União Europeia, prevendo: Disposições que garantem um nível de proteção elevado aos dados pessoais tratados pelas instituições e pelos órgãos comunitários; “A criação de uma instância de fiscalização independente encarregada do controle da aplicação dessas disposições” (UNIÃO EUROPEIA, 1995).

A Diretiva 95/46/CE traz em seu artigo segundo um fundamento importante de que os meios estão a serviço do homem, assim devem respeitar as liberdades e direitos fundamentais das pessoas, ao contrário não é o homem que está a serviço dos meios para os quais os dados possuem uma grande relevância. Entende-se que os serviços prestados pelas instituições não podem violar direitos com intuítos mercadológicos, mas que o homem deve se utilizar desses serviços para melhoria da qualidade de vida.

“Considerando que os sistemas de tratamento de dados estão ao serviço do Homem; que devem respeitar as liberdades e os direitos fundamentais das pessoas singulares independentemente da sua nacionalidade ou da sua residência, especialmente a vida privada, e contribuir para o progresso econômico e social, o desenvolvimento do comércio e o bem-estar dos indivíduos” (UNIÃO EUROPEIA, 1995).

De acordo com Quintiliano (2021) a promulgação da Carta de Direitos Fundamentais no ano de 2000 fez com que a União Europeia reconhecesse esses direitos como fundamentos limitadores do poder da entidade. Passando a ser

vinculativo como direito primário da União Europeia em 2009, com a entrada em vigor do Tratado de Lisboa.

A proteção de dados tornou-se um tema de grande relevância deste a criação pela União Europeia do Regulamento Europeu de Proteção de Dados Pessoais, também conhecido pela sigla *GDPR* (*General Data Protection Regulation*). Ele foi aprovado em 27 de abril de 2016 sendo que foi concedido um prazo até 25 de maio de 2018 para as adequações antes de iniciar as penalidades (PINHEIRO, 2021).

Após a vigência do *GDPR* na União Europeia eles passaram a exigir de outros países que tivessem uma legislação no mesmo nível para que pudessem continuar realizando atividades comerciais, os países rapidamente procuraram se adequar com propósito de não sofrer sanções comerciais. Pode se dizer que os efeitos do *GDPR* são principalmente econômicos, sociais e políticos.

O Brasil com o propósito de se adequar e não sofrer embargos comerciais com países que já tem uma legislação vigente quanto a proteção de dados, como por exemplo os países da União Europeia, buscou de acordo com Pinheiro (2021) uma norma compatível com o Regulamento Europeu de Proteção de Dados Pessoais. Nesse sentido o país buscou uma norma que pudesse atender essas demandas econômicas, sociais e políticas para se adequar com atributos qualitativos na proteção de dados pessoais com o fim de não sofrer penalidades.

Embora como relata Lugati e Almeida (2020) “o assunto de proteção de dados já era indiretamente tratado em legislações esparsas como o Código de Defesa do Consumidor e a Lei do Cadastro Positivo (Lei nº 12.414/2011) e o Marco Civil da Internet”. No entanto não existia uma norma que atendesse a proteção de dados de forma mais específica como a LGPD.

A Lei Geral de Proteção de dados, conhecida pela sigla LGPD “É uma regulamentação que traz princípios, direitos e obrigações relacionados ao uso de bases de dados das pessoas” (PINHEIRO, 2021, p. 09). Os riscos a privacidade inerentes a utilização das tecnologias da informação, relativos ao direito do consumidor fez com que os países cada vez mais criassem ferramentas de proteção e conseqüentemente normatização.

A LGPD se tornou um mecanismo de controle para regulamentar as relações no meio digital amplamente explorado e utilizado no comércio atual. “A LGPD é apenas uma das muitas regulamentações que vão surgir na busca por trazer mecanismos de controle para equilibrar as relações em um cenário de negócios digitais sem fronteiras”. (PINHEIRO, 2021, p.10).

A utilização do comércio eletrônico faz com que o consumidor tenha uma expressão de liberdade e poder de escolha, mas na verdade, as empresas têm acesso a toda informação e aproveitam para explorar o consumidor. Importante nesse sentido é a atuação das empresas no contexto digital com a criação de mecanismos de regulação e proteção dos dados pessoais. “Toda situação ou ação realizada no ambiente virtual faz parte da realidade de qualquer pessoa, portanto os direitos garantidos no “mundo *offline*” devem ser assegurados também no espaço virtual” (PINHEIRO, 2021, p. 29).

Conforme explanado os países foram se preocupando com mecanismos de regulação do uso e tratamento dos dados, sendo assim muito importante conhecer os princípios aplicados nessa legislação e também saber como é realizado o tratamento dos dados.

2 BREVE ESTUDO SOBRE OS PRINCÍPIOS APLICADOS A LGPD E TRATAMENTO DE DADOS

O tratamento de dados permite uma segmentação dos consumidores, é possível realizar uma análise das informações para diversos usos conhecendo para quem direcionar uma propaganda, perfil das pessoas, uma análise de risco para contratações, eficiência para uso das informações, neste sentido que os dados são importantes ativos no mercado (BIONI, 2021).

As normas de proteção de dados são baseadas em princípios norteadores o que significa dizer que para serem atendidos é preciso olhar se os princípios aplicados na lei estão sendo cumpridos. A Lei Geral de Proteção de dados é considerada principiológica que implica dizer de acordo com Pinheiro (2021, p. 18) que “a melhor forma de analisar a lei é pela verificação da conformidade dos itens de controle, ou seja, se o controle não está presente, aplicado e implementado, logo o princípio não está atendido”.

A LGPD em seu artigo primeiro caput estabelece a que se dispõe a lei, conforme pode ser observado:

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

Pode-se dizer que neste artigo a lei estabelece o tratamento de dados pessoais no ambiente digital com o propósito de proteger os direitos fundamentais de liberdade e privacidade e o desenvolvimento livre da personalidade da pessoa natural. Posteriormente estabelece quais são os fundamentos da lei, quais sejam:

“I - o respeito à privacidade; II - a autodeterminação informativa; III - a liberdade de expressão, de informação, de comunicação e de opinião; IV - a inviolabilidade da intimidade, da honra e da imagem; V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais” (BRASIL, 2018)

Conhecidos os objetivos da LGPD e seus fundamentos, faz-se necessário o conhecimento e compreensão dos princípios que permite disciplinar a proteção de dados e a forma com que podem ser utilizados seguindo os critérios definidos na legislação. A seguir será realizado um breve estudo de cada um dos princípios aplicados a LGPD e posteriormente será abordado o tratamento de dados.

O art. 6º, caput, da LGPD estabelece que as atividades de tratamento de dados observarão a boa-fé que disciplina as relações de direito público e privada, respeitando os objetivos das partes envolvidas nas relações jurídicas.

A boa-fé terá objetivo de delinear com transparência as reais intenções do controlador dos dados a quem está sendo prestada as informações. Importante salientar que o controlador deve indicar para quais fins serão usados os dados e que não haja um desvio do que se foi acordado no consentimento. De acordo com o que está definido no art. 9º, § 3º, da LGPD: “Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato...” (BRASIL, 2018).

Sendo assim para o tratamento de dados pessoais dependerá do consentimento

do portador de dados e do esclarecimento pelo controlador quanto a finalidade, que não poderá ser diversa do que se foi acordado, cumprindo assim o princípio da boa-fé.

Após abordagem da boa-fé serão elencados os 10 incisos do art. 6º que contém os dez princípios da LGPD que devem ser observados para cumprimento da lei no tratamento de dados.

O Princípio da finalidade está diretamente relacionada com a utilização dos dados pessoais pelo controlador, sendo um requisito do consentimento pelo titular dos dados, de forma que ela deve ser expressa de acordo com o art. 6º, I, da LGPD: “realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades” (BRASIL, 2018).

Desta forma protege o proprietário dos dados pessoais de possíveis desvios na finalidade consentida, o que permite responsabilização pelo uso indevido ou tratamento dos dados pessoais não autorizado, como por exemplo a transferência dos dados para terceiros.

O princípio da adequação no tratamento de dados pessoais é definido pela “compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento” (art. 6º, inciso II, da LGPD). Tem o objetivo de vincular o consentimento do titular para o tratamento de dados de acordo com as finalidades legais que devem ser informadas, caracterizada pela confiança no atendimento do uso informado (MIRAGEM, 2019).

O princípio da necessidade em consonância com o conceito da norma é a “limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados” (art. 6º inciso III, da LGPD). Para Miragem (2019) como o tratamento de dados pessoais está vinculado a um direito fundamental de proteção de acordo com o consentimento do titular e o fim legítimo do uso da informação, faz-se necessário uma limitação do uso mínimo que atenda a finalidade determinada.

Significa dizer que deve existir uma proporcionalidade entre os meios e fins, não sendo excessivos em relação as finalidades do tratamento de dados. Pois sabe se que

existe um grande processamento de dados que torna importante a regulação da proteção de dados de forma a limitar o uso de acordo com o princípio da necessidade.

O princípio do livre acesso conforme o art. 6º inciso IV, da LGPD estabelece a “garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais” (BRASIL, 2018). Esse princípio garante aos titulares dos dados consulta sobre a forma como os dados são tratados, tempo em que isso ocorre, podendo terem acesso para correção de informações ou mesmo solicitar cópia dos registros existentes (MIRAGEM, 2019).

No art. 9º da LGPD foram listados um rol de características que garantem e asseguram ao titular dos dados o direito do livre acesso, que também é reforçado como direito no art. 18º inciso II, da LGPD. No caso em que ocorra a falta de atendimento a solicitação do titular para o acesso aos dados o controlador (empresa que possui os dados), pode sofrer sanções pela LGPD ou também responsabilização por danos causados.

A qualidade dos dados está na LGPD em seu art. 6º inciso V “garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento” (BRASIL, 2018). Importante salientar nesse princípio a relevância da atualização dos dados, pois se sabe que as informações a respeito do titular vão mudando e para ter seu direito garantido o controlador deve se preocupar em ter dados de forma exata para que não ocorra em uma circunstância que o fato relacionado ao titular não corresponda mais a realidade.

A própria Constituição estabelece concessão do instituto Habeas data para a obtenção de dados cadastrados em registros ou banco de dados de entidades governamentais e para retificação de tais dados (CORRÊA, 2019, p. 27).

Dessa forma pontua Miragem (2019, p.11) “a relevância dos dados, talvez esta seja, em termos práticos, o critério de mais difícil precisão quanto à qualidade dos dados”. A noção de relevância se define em acordo com a finalidade do tratamento dos dados”. O controlador deve demonstrar a correlação entre a finalidade e a relevância dos dados, isto geralmente é demonstrado através de estatística.

O princípio da transparência exibido em seu art. 6º inciso VI da LGPD a “garantia,

aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial” (BRASIL, 2018).

As empresas detentoras de dados pessoais dos titulares de acordo com a LGPD devem ter transparência na prestação de informações sobre como os dados são tratados no limite de suas finalidades, respeitando assim um direito fundamental resguardado pela Constituição Federal de que todos tem direito a obter informações de seu interesse conforme o que está no art. 5º inciso XXXIII da CF 1988.

A segurança é dos princípios de maior importância para o titular de dados, uma vez que a legislação de proteção dos dados tem como objetivo oferecer uma prevenção de riscos relacionados ao tratamento de dados. O princípio da segurança estabelece de acordo com o art. 6º inciso VII, da LGPD “utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão” (BRASIL, 2018).

Em suma esse princípio protege o titular de dados que tenha sofrido qualquer ato ilícito relacionado com seus dados na atividade de tratamento tendo assim como consequência a responsabilização por parte do controlador.

A disponibilização de dados pessoais apresenta riscos para os titulares, pois estes podem ser usados indevidamente, sendo assim a LGPD em seu art. 6º inciso VIII descreve a “adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais” (BRASIL, 2018). Estabelecendo assim o princípio da prevenção.

As empresas controladoras de dados pessoais devem oferecer a privacidade do consumidor no oferecimento de produtos e serviços, o que também demanda segurança dos dados. Conforme Miragem (2019, p.13) destaca na “conservação, descarte e precisão dos dados, realizando o gerenciamento de dados durante todo ciclo de vida de seus produtos e serviços”.

O princípio da não discriminação de acordo com a definição legal no art. 6º inciso IX, da LGPD a “impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos” (BRASIL, 2018). Este artigo tem como objetivo proibir que o

tratamento de dados tenha como resultado a ação discriminatória e abusiva contra o consumidor, pois sabe-se que o próprio tratamento tem como funcionalidade segmentar e personalizar os dados, assim podendo discriminar, separar e diferenciar, por isso não pode ser utilizado com este objetivo.

Para tanto a Constituição Federal apresenta artigos que proíbem quaisquer formas de discriminação. Em seu art. 3º inciso IV dispõe “promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação” (BRASIL, 1988). A CFRB/ 1988 estabelece em seu art. 5º inciso VIII “ninguém será privado de direitos por motivo de crença religiosa ou convicção filosófica ou política” (BRASIL, 1988).

A LGPD determina em seu art. 21 “os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo” (BRASIL, 2018). Reforçando o princípio da não discriminação que pode ser realizado tanto para não oferecer um serviço, um produto como também não permitir que determinado consumidor tenha acesso a determinados interesses legítimos, caracterizando uma desigualdade de tratamento.

O princípio da responsabilização e prestação de contas finaliza no artigo sexto inciso X da LGPD mais um dever do titular de dados de “demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas” (BRASIL, 2018).

Esse princípio está em conformidade com a transparência e a prevenção, para que todos aqueles que são titulares de dados estejam alinhados com a legislação de forma que possam responsabilizar-se por eventuais desvios de conduta e também que estejam preparados para prestar contas caso não estejam agindo em conformidade com as normas jurídicas.

A aplicação dos fundamentos da Lei Geral de Proteção de Dados conforme apresentado permite que a norma cumpra seu objetivo principal que para Pinheiro (2021, p. 18) é “a proteção da privacidade do titular dos dados, a liberdade de expressão, de informação, de opinião e de comunicação, a inviolabilidade da intimidade, da honra e da imagem e o desenvolvimento econômico e tecnológico”.

Portanto para analisar se a lei aplicada está em conformidade é necessário verificar os itens de controle, se estão presentes, aplicado e implementado (PINHEIRO, 2021). Isso permite avaliar se o princípio da norma foi atendido de acordo com o que está preconizado. O conhecimento dos princípios fornece ferramentas para proteção dos dados e consequentemente evita danos aos consumidores.

No que se refere ao consentimento por parte do titular para que seus dados possam ser utilizados pelas empresas prestadoras de serviços, atendendo LGPD, elas precisam disponibilizar a política de privacidade. Que seriam os termos de serviços utilizados na internet, um instrumento de implementação de privacidade. Conforme Freitas (2019) “*privacy by design* ou “privacidade desde a concepção” que é uma abordagem ligada à Engenharia de Sistemas e que preza pela privacidade do usuário durante todo o processo de construção de uma solução”.

Esse documento é para a proteção de dados, tem o objetivo de dar transparência ao tratamento de dados pessoais em um determinado serviço, sistema ou *site*, em suma é a forma em que o titular realiza o consentimento para o uso do serviço e a empresa disponibiliza nos termos qual é a política de privacidade e para qual finalidade utiliza os dados pessoais.

De acordo com Lugati e Almeida (2020) no que se refere aos termos de aceite eles representam uma imposição para o uso dos serviços, já que muitas vezes não são lidos, por serem textos muito grandes, também pela rapidez com que se almeja utilizar os serviços, assim o “eu aceito” não reflete a realidade da vontade do titular de dados. Em um estudo da Universidade de Stanford foi constatado que 97% dos usuários não liam a política de privacidade antes de realizar o aceite (LUGATI; ALMEIDA, 2020 *apud* SANSANA, 2018, p. 16).

Esse contexto fez com que o *European Data Protection Board (EDPB)*, que é o órgão responsável pela aplicação da norma europeia, modificasse suas diretrizes de consentimento exigindo que um prestador de serviço não pode impedir um titular de dados de acessar um serviço em razão de não ter dado seu consentimento (LUGATI; ALMEIDA, 2020).

Atualmente o que se verifica ao realizar acesso nos mais diversos tipos de *site* é que para navegação faz se necessário aceitar as políticas de privacidade. Futuramente

a Agência Nacional de Proteção de dados brasileira pode adotar diretrizes semelhantes à do *EDPB* para evitar o não fornecimento dos serviços, o consentimento pelo titular de forma “falsa”, no sentido de desconhecimento de qual tipo de tratamento será realizado com seus dados pessoais.

3 IMPLICAÇÕES JURÍDICAS DA LGPD NO DIREITO DO CONSUMIDOR

A Lei Geral de Proteção de Dados (LGPD), entrou em vigor no dia 18 de setembro 2020 para regulamentar o uso, a proteção e a transferência de dados pessoais, assim as empresas que não se adequaram quanto a utilização dos dados no que se refere as hipóteses de tratamento previstas na Lei estão passíveis de serem sancionados administrativamente, podendo ser com multas de até 2% do faturamento da empresa e até a suspensão do funcionamento das atividades da pessoa jurídica. As sanções administrativas podem ser observadas no art. 52 ao art. 54 da LGPD e aplicadas a partir de 1º de agosto de 2021.

O tratamento de dados oferece muitas possibilidades sendo uma ferramenta para as empresas no capitalismo de vigilância pois como já abordado ele permite uma exploração do comportamento das pessoas e uma compilação dos dados em todos os aspectos da vida cotidiana. Dessa forma a LGPD tem por objetivo dispor sobre o tratamento de dados pessoais para proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (BRASIL, 2018).

Importante nesse momento dissertar sobre as implicações jurídicas da LGPD no direito do consumidor, para isso deve-se esclarecer que a lei possui em seus fundamentos no art. 2º inciso VI “a livre-iniciativa, a livre concorrência e a defesa do consumidor” (BRASIL, 2018), relevante fundamento na defesa do consumidor.

A lei estabelece em seu art. 18 § 1º que o titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional, assim como no § 8º que o direito a que se refere o § 1º deste artigo também poderá ser exercido perante os organismos de defesa do consumidor.

Demonstra-se a relação da LGPD com o direito do consumidor pois a lei

expressa ainda em seu art. 45 que “as hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente” (BRASIL, 2018). A LGPD trata ainda da responsabilidade civil frente a violações dos direitos que protegem os dados das pessoas nos seus artigos 42 a 45, como será dissertado.

Em seu artigo 42 estabelece que a violação a legislação pertinente a proteção de dados por parte do controlador ou operador, que cause dano patrimonial, moral, individual ou coletivo é obrigado a reparar. Por “violação a legislação pertinente” na LGPD Capanema (2020) faz uma analogia ao estabelecido no art. 96 do CTN (Código Tributário Nacional) que defini legislação tributária todo arcabouço de leis, decretos, convenções e tratados que poderão ser utilizadas e que versem sobre o tema, assim como ocorre na LGPD, onde o legislador deixou claro que para reparação poderão ser utilizadas outras leis, onde se encontra também o Código de Defesa do Consumidor.

Uma interpretação do art. 42 e art. 44 da LGPD conforme Capanema (2020) permite identificar dois tipos de violações uma de normas jurídicas, do microssistema de proteção de dados e uma segunda que seria de normas técnicas, voltadas à segurança e proteção de dados pessoais. Caracterizando formas de responsabilidade civil que podem ser identificadas na lei para possíveis reparações em caso de descumprimento das normas. Assim qualquer tipo de violação que trazer dano material ou moral para o titular de dados poderá ser responsabilizado civilmente.

Recentemente um Juiz de São Paulo condenou um gerente de farmácia a indenizar o Médico David Uip em R\$ 11 mil reais. Ele foi responsável por divulgar uma receita do infectologista David Uip, que foi ex-coordenador do Centro de Contingência do Coronavírus em São Paulo. Após divulgação do conteúdo da receita por grupos de *WhatsApp* e outras redes sociais, o Médico e sua família foram hostilizados com uma série de críticas. Segundo advogado do caso a grande repercussão deste episódio criminoso deve refletir uma punição, um ônus, que o acusado suporta, para que não reitere no cometimento de seu crime e sirva de exemplo à sociedade (ANGELO, 2021).

Embora o gerente tenha sido condenado por violação de sigilo profissional de acordo com o artigo 154 do Código Penal observa-se neste fato uma violação ao direito de intimidade, da honra e da imagem fundamentos presente na LGPD de acordo com o

art. 2 inciso IV da referida Lei, em que cabe reparação dos danos causados.

Inicialmente serão apresentados casos de violação da LGPD que poderiam ter sido evitados se as empresas já tivessem implantado e implementado um programa de conformidade com a lei. O vazamento de dados tratados com a LGPD possibilita a verificação da não adequação das empresas às normas nesse contexto que desencadeou as punições registradas no sistema judiciário.

CASO 1) Vazamento de atestado médico indicando que o funcionário era portador de *HIV* pelo RH da empresa (EJURADMIN, 2020):

Através de uso comum de uma impressora utilizada pelo setor de recursos humanos e demais membros da empresa, um funcionário ao ter acesso a um atestado médico em que constava ser um colega portador do vírus *HIV* (*Human Immunodeficiency Virus*), este compartilhou os dados fazendo com que essa informação interferisse na interação social e laboral do funcionário que teve sua informação pessoal vazada. Dados referentes a saúde da pessoa é considerado um dado sensível pela LGPD.

A LGPD estabelece em seu art. 5º inciso II o conceito de dado pessoal sensível que é o:

dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (BRASIL, 2018);

Sendo assim uma violação quanto ao uso do dado pessoal sensível referente a saúde do funcionário portador de *HIV*. Se a empresa contasse com um programa de conformidade com a LGPD poderia ter afastado tal risco e evitado o ocorrido que lesou fortemente a intimidade e privacidade do funcionário em questão, podendo levar a reparação por danos causados. A seguir um caso relacionado a uma construtora que compartilhou dados sobre a compra de um imóvel por um cliente.

CASO 2) Construtora compartilha dados pessoais de clientes e é multada (EJURADMIN, 2020):

A juíza da 13ª Vara Cível de São Paulo multou uma construtora por compartilhar com outras empresas os dados de um cliente que havia comprado um imóvel. Este acionou o judiciário por ser importunado por telefone, *WhatsApp* e *e-mail* por diversas empresas. A juíza entendeu que o compartilhamento dos dados pessoais do comprador

feriu preceitos como a honra e privacidade do cliente, além de violar sua intimidade ao revelar seus dados e detalhes da compra do imóvel.

Conforme apresentado os princípios que regem a LGPD observa-se que a transferência de dados pessoais é considerada uma forma de tratamento, como consta no conceito do art. 5º inciso X:

Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (BRASIL, 2018);

O conhecimento da lei no que se refere aos limites e deveres do uso dos dados possibilita evitar erros na publicidade e possíveis sanções, pois para o tratamento dos dados a empresa deve contar com o consentimento do cliente de acordo com art. 7º inciso I da LGPD “O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I - mediante o fornecimento de consentimento pelo titular;” (BRASIL, 2018). Posteriormente tem se o caso três o qual trata de uso de número de telefone celular de uma funcionária pelo *site* da empresa em que trabalhava.

Caso 3) Doceria usou o número de uma funcionária como contato oficial e foi condenada a pagar 5 mil reais em indenização:

Uma Filial da Cacau Show em Ponte Nova MG foi condenada a pagar uma indenização de R\$ 5 mil reais por danos morais a uma ex funcionária por ter usado número de telefone dela no *site* como oficial da loja sem autorização.

A empresa chegou a entrar com recurso para anular a indenização por danos morais, porém o relator do processo e juiz Ricardo Marcelo Silva, negou que fosse impossível de reconhecer a funcionária apenas pelo celular. De acordo com Knoth (2021) para o magistrado, o *site* não dava essa informação, mas os clientes conseguiam identificá-la ao ligar para o número. Sendo assim a divulgação é uma violação a privacidade da funcionária, configurando uma irregularidade na LGPD, pois o telefone celular é um dado pessoal.

Na sequência serão apresentados alguns casos de empresas que foram condenadas por violar o *GDPR (General Data Protection Regulation)* norma vigente na União Europeia desde 2016. Importante ressaltar que o Brasil para ter normas

compatíveis e assim não sofrer embargos mercadológicos criou a Lei Geral de Proteção de Dados (LGPD).

O *Google* realizou mudanças na política de privacidade e proteção dos dados dos usuários, criou uma página para esclarecimentos sobre as novas regras. Porém foi multado na França em 2019 em 50 milhões de euros. Segundo *site Softwall* (2021) a empresa não forneceu aos usuários informações suficientes sobre a política de consentimento para o tratamento de dados.

O *Facebook* usou de forma indevida informações de 87 milhões de usuários da rede social, no que ficou conhecido escândalo “*Cambridge Analytica*”, a empresa foi condenada a pagar 5 bilhões de dólares, também realizou um acordo de restrições de atuação e análise trimestral de seus serviços e produtos. De acordo com *site Softwall* (2021) a rede social de Mark Zuckerberg falhou em proteger os dados de seus usuários de empresas terceirizadas e teria ocultado de seus clientes a informação de que os sistemas de reconhecimento facial estavam desativados por padrão.

A *Uber* escondeu um vazamento de dados que aconteceu em sua plataforma, conforme *site Softwall* (2021) esse episódio afetou 7 milhões de motoristas e 57 milhões de usuários – destes, 196 mil eram brasileiros. O vazamento aconteceu devido a um ataque de *hackers* no sistema da empresa, está com intuito de esconder o problema ofereceu 100 mil dólares para os *hackers* responsáveis. Porém em uma auditoria externa no setor, foi descoberto o vazamento de telefones, nomes, e-mails e carteiras de motoristas.

A revelação do ataque tornou-se público quando o ex-diretor de segurança da empresa foi demitido, posteriormente durante uma auditoria foi constatado o vazamento, a empresa foi punida em 2018 com uma multa de 148 milhões de dólares.

Os fatos relatados demonstram a importância da aplicação da LGPD na proteção dos dados pessoais, uma vez que a constatação da violação permite ao titular requerer do controlador a responsabilização por possíveis danos causados.

A responsabilidade e o ressarcimento de danos deverão observar as regras expostas na lei nos artigos 42 a 45, porém o Código Civil estabelece em seu art. 944 que “A indenização mede-se pela extensão do dano”. Logo a extensão do dano no que se refere a proteção de dados poderá levar em consideração os seguintes critérios:

a) a quantidade de dados pessoais afetados; b) a natureza dos dados pessoais afetados: o vazamento de dados pessoais sensíveis, por exemplo, determinará uma indenização maior, especialmente por se tratar de dados biométricos, que não podem ser substituídos; c) a reincidência da conduta; d) a omissão em tomar medidas de segurança e técnicas para minorar o dano ou em colaborar com a Autoridade Nacional de Proteção de Dados; e) a ausência de notificação dos usuários da ocorrência do incidente; f) a comprovada utilização dos dados pessoais vazados de titulares por terceiros (CAPANEMA, 2020, p. 168);

Nas relações de consumo a LGPD estabelece que a responsabilização permanece sujeitas às regras previstas na legislação pertinente portanto para Capanema (2020, p.166) “se a relação jurídica do titular com o controlador e o operador for de natureza consumerista, serão aplicadas as normas de responsabilidade solidária dos artigos 12 e 18 do CDC (Código de Defesa do Consumidor)”.

Diante dos casos apresentados foi possível verificar uma série de violações na proteção de dados pelas empresas, como vazamento de uma receita médica, atestado médico, compartilhamento de dados de compra de imóvel, uso de número de telefone, ou qualquer dado considerado pessoal como as transgressões a lei por empresas como *Google*, *Facebook* e *Uber*. O conhecimento dos princípios aplicados pode favorecer os titulares no que tange aos sistemas jurídicos pela aplicação de proteção de dados.

A legislação brasileira de proteção de dados pessoais está relacionada a proteger a privacidade do titular dos dados e também a sua liberdade pessoal nas relações de consumo, bem como em sentido mais amplo no exercício de seus direitos fundamentais em geral.

A LGPD estabelece que haverá uma interação com as normas de proteção do consumidor, pois em seu art. 64 estabelece a possibilidade de diálogo de fontes. Para Miragem (2019, p. 28) “a Autoridade Nacional de Proteção de Dados e outros órgãos com competência sancionatória, inclusive os de proteção do consumidor em seu art. 55-K, parágrafo único”.

Assim nas relações cotidianas e no uso das tecnologias da informação e internet nas relações de consumo, o Brasil com a eficácia da Lei Geral de Proteção de Dados (LGPD) estabelece um novo patamar na proteção de dados favorecendo o desenvolvimento nas relações de consumo e efetividade na proteção dos interesses do consumidor.

CONSIDERAÇÕES FINAIS

A LGPD representa uma inovação importante para o Brasil na proteção de dados apresentando uma equiparação com legislações estrangeiras como *General Data Protection Regulation (GDPR)* que inspirou a lei brasileira favorecendo uma equivalência e uma demonstração para os países da União Europeia que o país dispõe de uma norma compatível. Consequentemente para não sofrer embargos comerciais.

O desenvolvimento da informação permitiu que o binômio tempo e espaço fosse superado favorecendo a economia global e a interação social, reorganizando a sociedade. Esse grande fluxo de informações e armazenamento de dados contribuiu para o capitalismo de vigilância pois as empresas através do mapeamento dos dados pessoais sabem o que é consumido, as necessidades, as preferencias e toda demanda comercial.

Através desse modelo de capitalismo faz-se necessário proteger os titulares dos dados pessoais frente a violações por parte do controlador, nesse contexto a lei estabeleceu requisitos para o tratamento dos dados que seguem os fundamentos da lei estudados neste trabalho. Esses fundamentos permitem que o titular disponha de ferramentas para exigir sua autodeterminação informacional que é o conhecimento do que é feito com seus dados, respeitando assim princípios como privacidade, intimidade e honra do cidadão.

Nesse contexto tem se a aplicação do consentimento por parte das empresas para o titular o que se observou no presente trabalho é que elas muitas vezes não refletem um verdadeiro consentimento, mas apenas uma formalidade para cumprimento das normas, já que o titular para se utilizar dos serviços realiza o “eu aceito” sem a leitura das políticas de privacidade.

Para tanto propõe se que o modelo do *European Data Protection Board (EDPB)* em não permitir que as empresas bloqueiem o acesso a prestação do serviço caso o titular não realize o aceite pode ser uma alternativa de exigência para que estas não utilizem do consentimento para o armazenamento e uso indevido dos dados pessoais.

Por fim o presente trabalho trouxe exemplos de aplicações da LGPD no Brasil e suas consequências jurídicas como multa por danos morais. Apresentou que podem haver dois tipos de violações à LGPD, uma de ordem jurídica e outra técnica, sendo a primeira do microssistema de proteção de dados e a segunda que seria de voltada à segurança e proteção de dados pessoais. Ambas podem caracterizar formas de responsabilização civil se comprovado o dano ao titular. Os maiores exemplos ficaram por conta de grandes empresas como *Google* e *Facebook* por terem violado direitos dos consumidores, deixando evidente que a LGPD no Brasil terá grande aplicação na esfera jurídica.

Portanto para aplicação das sanções frente a lei é necessário que os titulares dos dados tenham conhecimento do fluxo de utilização de seus dados e da aplicação da lei. Como abordado no trabalho se os danos causados forem na esfera consumerista ficará a critério da aplicação das normas do Código de Defesa do Consumidor.

REFERÊNCIA BIBLIOGRÁFICA

ANGELO, T. **Farmacêutico é condenado a pagar R\$ 11 mil por vazar receita de cloroquina de Uip.** Disponível em: <https://www.conjur.com.br/2021-mar-12/farmaceutico-pagara-11-mil-vazar-receita-david-uip> acesso em 21/05/2022. Acesso em: 23/05/2022

ASSEMBLEIA GERAL DA ONU. **Declaração Universal dos Direitos Humanos.** 1948. Disponível em: <<https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos>. Acesso em: 10/04/2022.

BIONI, B. R. **Proteção de Dados Pessoais - A Função e os Limites do Consentimento.** Rio de Janeiro: Grupo GEN, 2021. 9788530994105. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788530994105/>. Acesso em: 17 mar. 2022.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil.** Texto constitucional promulgado em 5 de outubro de 1988, 57ª edição do Texto Constitucional promulgado em 5 de outubro de 1988, com as alterações adotadas pelas Emendas constitucionais nºs 1/1992 a 110/2021, pelo Decreto legislativo nº 186/2008 e pelas Emendas constitucionais de revisão nºs 1 a 6/1994. Disponível em: <https://www2.camara.leg.br/atividade->

legislativa/legislacao/constituicao1988/arquivos/ConstituicaoTextoAtualizado_EC%20112.pdf. Acesso em: 05 /12 /2021.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados**. Diário Oficial da União, Brasília, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 07/11/2021

BRASIL, Decreto nº 678 de 06 de novembro de 1992. **Promulga a Convenção Americana sobre Direitos Humanos (Pacto de São José da Costa Rica)**, de 22 de novembro de 1969. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/d0678.htm. Acesso em: 10/04/2022.

CAPANEMA, W. A. **A responsabilidade civil na Lei Geral de Proteção de Dados**. Cadernos Jurídicos, São Paulo, ano 21, nº 53, p. 163-170, Janeiro-Março/2020.

CONSELHO EUROPEU. **Convenção Europeia dos Direitos do Homem**. Roma, 1950. Disponível em: <https://www.echr.coe.int> Acesso em: 20/03/2022.

CORRÊA, A. C. M. **Análise do consentimento na Lei de Proteção de Dados Pessoais no Brasil e sua aplicação no mundo jurídico**. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Universidade Presbiteriana Mackenzie, São Paulo, 2019.

EAJURADMIN. **3 Casos de vazamento de dados que lhe mostrarão que a aplicação da LGPD não está tão distante da realidade do seu negócio**. Outubro /2020. Disponível em: <https://ejur.com.br/blog/3-casos-de-vazamento-de-dados-que-mostram-a-aplicacao-da-lgpd/>. Acesso em: 15/05/2022.

FORNASIER, M. O. KNEBEL, N.M. **O titular de dados como sujeito de direito no capitalismo de vigilância e mercantilização dos dados na Lei Geral de Proteção de Dados**. Rev. Direito e Práxis, Rio de Janeiro, Vol. 12, N. 2, 2021, p. 1002-1033.

FREITAS, C. **Como elaborar uma política de privacidade aderente a LGPD?** Disponível em: <https://www.serpro.gov.br/lgpd/noticias/2019/elabora-politica-privacidade-aderente-lgpd-dados-pessoais>. Acesso em: 15/04/2022.

KNOTH, P. **Empresa é condenada em R\$ 5 mil por violar LGPD com celular de funcionária.** Disponível em: <https://tecnoblog.net/noticias/2021/11/16/empresa-e-condenada-em-r-5-mil-por-violar-lgpd-com-celular-de-funcionaria/>. Acesso em 23/05/2022

LUGATI, L.N. ALMEIDA, J.E. **Da evolução das Legislações sobre proteção de dados: a necessidade de reavaliação do papel do consentimento como garantidor da autodeterminação informativa.** Revista De Direito. Viçosa. ISSN 2527-0389. V.12 N.02 2020.

MIRAGEM, B. **A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o Direito do Consumidor.** Revista dos Tribunais. vol. 1009/2019. Nov. 2019.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS, **Convenção Americana de Direitos Humanos (“Pacto de San José de Costa Rica”)**, 1969. Disponível em: <http://www.dhnet.org.br/direitos/sip/oea/oeasjose.htm>. Acesso em: 10/04/2022.

QUINTILIANO, L. **Contexto histórico e finalidade da Lei Geral de Proteção de Dados (LGPD).** Março 2021. Disponível em: <https://iapd.org.br/contexto-historico-e-finalidade-da-lei-geral-de-protacao-de-dados-lgpd/>. Acesso em: 20/03/2022

SARLET, I. W. **Proteção da personalidade no ambiente digital: uma análise à luz do caso do assim chamado direito ao esquecimento no Brasil.** Joaçaba, v. 19, n. 2, p. 491-530, maio/ago. 2018.

SOFTWALL. **8 casos de vazamentos de dados tratados com a LGPD.** Disponível em: <https://www.softwall.com.br/blog/vazamentos-de-dados-tratados-com-a-lgpd/>. Acesso em: 23/05/2022.

UNIÃO EUROPEIA. **Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.** Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. Disponível em: <https://eur-lex.europa.eu/legalcontent/PT/TXT/?uri=celex%3A32016R0679>. Acesso em: 20/03/2022.

UNIAO EUROPEIA. **Proteção dos dados pessoais.** Diretiva 95/46/CE. Dezembro 1995. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/LSU/?uri=celex:31995L0046>. Acesso em: 20/03/2022.