UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO DE CIÊNCIAS JURÍDICAS
DEPARTAMENTO DE DIREITO
CURSO DE DIREITO

EVELIM DOS SANTOS CARDOSO

# **A vulnerabilidade do direito à informação nas relações de consumo pelos meios digitais:** uma análise sobre a necessidade de consentimento e controle do consumidor sobre o destino de seus dados pessoais.

Florianópolis/SC
2022

EVELIM DOS SANTOS CARDOSO

# **A vulnerabilidade do direito à informação nas relações de consumo pelos meios digitais:** uma análise sobre a necessidade de consentimento e controle do consumidor sobre o destino de seus dados pessoais.

Trabalho Conclusão do Curso de Graduação em Direito do Centro de Ciências Jurídicas da Universidade Federal de Santa Catarina como requisito para a obtenção do título de Bacharel em Direito.
Orientador: Prof.ª Dr.ª Belinda Pereira da Cunha

Florianópolis
2022

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Cardoso , Evelim dos Santos
A vulnerabilidade do direito à informação nas relações de consumo pelos meios digitais : uma análise sobre a necessidade de consentimento e controle do consumidor sobre o destino de seus dados pessoais / Evelim dos Santos Cardoso ; orientador, Belinda Pereira da Cunha , 2022.
90 p.

Trabalho de Conclusão de Curso (graduação) - Universidade Federal de Santa Catarina, Centro de Ciências Jurídicas, Graduação em Direito, Florianópolis, 2022.

Inclui referências.

1. Direito. 2. Vulnerabilidade do consumidor, Proteção de dados pessoais , direito à informação . I. Cunha , Belinda Pereira da . II. Universidade Federal de Santa Catarina. Graduação em Direito. III. Titulo.

UNIVERSIDADE FEDERAL DE SANTA CATARINA

CENTRO DE CIÊNCIAS JURÍDICAS

COLEGIADO DO CURSO DE GRADUAÇÃO EM DIREITO

# TERMO DE APROVAÇÃO

O presente Trabalho de Conclusão de Curso, intitulado **A vulnerabilidade do direito à informação nas relações de consumo pelos meios digitais:** uma análise sobre a necessidade de consentimento e controle do consumidor sobre o destino de seus dados pessoais, elaborado pelo(a) acadêmico(a) Evelim dos Santos Cardoso, defendido em 21/03/2022 e aprovado pela Banca Examinadora composta pelos membros abaixo assinados, obteve aprovação com nota **10(dez)**, cumprindo o requisito legal previsto no art. 10 da Resolução nº 09/2004/CES/CNE, regulamentado pela Universidade Federal de Santa Catarina, através da Resolução nº 01/CCGD/CCJ/2014.

Florianópolis, 21 de março de 2022.

Documento assinado digitalmente
Belinda Pereira da Cunha
Data: 21/03/2022 18:02:42-0300
CPF: 044.141.298-00
Verifique as assinaturas em https://v.ufsc.br

**Belinda Pereira da Cunha**
Professor Orientador

Documento assinado digitalmente
gov.br
JOSE IRIVALDO ALVES OLIVEIRA SILVA
Data: 21/03/2022 18:27:28-0300
Verifique em https://verificador.iti.br

**José Irivaldo Alves de Oliveira Silva**
Membro de Banca

Documento assinado digitalmente
Guilherme Edson Merege de Mello Cruz Pinto
Data: 22/03/2022 10:55:05-0300
CPF: 085.089.449-26
Verifique as assinaturas em https://v.ufsc.br

**Guilherme E. Mello**
Membro de Banca

**Universidade Federal de Santa Catarina**

**Centro de Ciências Jurídicas**

**COORDENADORIA DO CURSO DE DIREITO**

TERMO DE RESPONSABILIDADE PELO INEDITISMO DO TCC E ORIENTAÇÃO IDEOLÓGICA

Aluna: Evelim dos Santos Cardoso
RG: 5.937.218 SSP/SC
CPF: 091.839.619-09
Matrícula: 16106490
Título do TCC: **A vulnerabilidade do direito à informação nas relações de consumo pelos meios digitais:** uma análise sobre a necessidade de consentimento e controle do consumidor sobre o destino de seus dados pessoais
Orientadora: Prof.ª Dr.ª Belinda Pereira da Cunha

Eu, Evelim dos Santos Cardoso, acima qualificado(a); venho, pelo presente termo, assumir integral responsabilidade pela originalidade e conteúdo ideológico apresentado no TCC de minha autoria, acima referido

Florianópolis, 21 de março de 2022

Documento assinado digitalmente
Evelim dos Santos Cardoso
Data: 22/03/2022 18:31:49-0300
CPF: 091.839.619-09
Verifique as assinaturas em https://v.ufsc.br

Evelim dos Santos Cardoso

Este trabalho é dedicado à minha querida mãe, pois sem o seu amparo eu não teria chegado até aqui.

## AGRADECIMENTOS

Sou muito grata por estar realizando um de meus maiores sonhos: me formar no curso de Direito e em uma Universidade pública, gratuita e de qualidade. De fato, essa conquista há alguns anos atrás parecia ser impossível diante dos percalços da vida.

Agradeço a Deus e à Nossa Senhora Aparecida, por terem me guiado até aqui e cuidado de mim até mesmo e meus momentos de pouca fé.

À minha mãe, Josefina Eli Cordeiro dos Santos, que sempre cuidou de mim e confiou no meu potencial. Muito obrigada mãe, por ter desempenhado o papel de mãe e pai com maestria.

Ao meu "amore", Guilherme Schvambach, por estar juntinho de mim nesses 11 anos de namoro, me amparar nos momentos difíceis e confiar no meu potencial desde o começo.

À Eugênia Maria Bergmann, minha querida amiga de vida, de graduação e futura colega de profissão, agradeço pelas risadas, pela compreensão e apoio.

Aos meus amigos e colegas da UFSC, especialmente à Angélica e Nicole, pela amizade e pelas risadas proporcionadas no CCJ.

Ao Projeto Integrar, um projeto voltado à educação comunitária focado na inclusão de trabalhadores e trabalhadoras que assim como eu, se preparam para o vestibular conciliando trabalho e estudo.

À minha orientadora, Professora Doutora Belinda Pereira da Cunha, por ser uma pessoa fantástica e acreditar no meu potencial para o desenvolvimento deste trabalho.

E aos membros da banca, Prof. Dr. José Irivaldo Alves de Oliveira Silva e Guilherme E. Mello, que gentilmente aceitaram avaliar o presente trabalho.

## RESUMO

O amplo acesso ao uso da internet, o desenvolvimento da tecnologia e a facilitação da relação de consumo no ambiente virtual contribuíram para que surgisse um novo tipo de produto no mercado: informações pessoais. A informação então tornou-se um dos produtos mais valiosos e, em decorrência disso, o mercado passou a desenvolver técnicas para sua coleta, armazenamento e tratamento de dados pessoais. Sem controle por parte do titular das informações pessoais, elas passaram a ser utilizadas de forma indiscriminada, motivo pelo qual se fez necessário desenvolver novas leis para que o consumidor tivesse a proteção da sua privacidade e de seus dados pessoais garantida. Para isso, será necessário analisar o Código de Defesa e sua importância na defesa do consumidor; a lei do Marco Civil da Internet, a primeira lei que traz garantia aos cidadãos sobre a utilização da internet no Brasil e a Lei Geral de Proteção de Dados Pessoais, que traz com uma de suas principais bases a necessidade de consentimento por parte do titular dos dados pessoais para que suas informações possam ser utilizadas pelo agente de tratamento de dados. Neste sentido, o objetivo do presente trabalho será demonstrar que a vulnerabilidade do consumidor é agravada no ambiente digital e analisar se a necessidade de consentimento por parte do titular realmente é eficaz para que não haja o tratamento de seus dados de forma indiscriminada. O método utilizado é o dedutivo e a conclusão é de que os contornos dados à necessidade de consentimento ao titular dos dados pessoais pela legislação são insuficientes para a efetiva proteção da sua decisão, tendo em vista que a legislação não regulou como deveria ocorrer o processo de consentimento do titular para garantir a sua eficácia e a sua verdadeira vontade.



**Palavras-chave:** Dados pessoais. Lei Geral de Proteção de Dados. Consumidor. Consentimento. Direitos fundamentais. Tratamento de dados pessoais.

## ABSTRACT

Wide access to the use of the internet, the development of technology and the facilitation of the consumption relationship in the virtual environment contributed to the emergence of a new type of product on the market: personal information. Information then became one of the most valuable products and, as a result, the market began to develop techniques for collecting, storing and processing personal data. Without control by the holder of personal information, they started to be used indiscriminately, which is why it was necessary to develop new laws so that the consumer had the protection of their privacy and their personal data guaranteed. For this, it will be necessary to analyze the Defense Code and its importance in consumer protection; the Marco Civil da Internet law, the first law that guarantees citizens the use of the internet in Brazil and the General Law for the Protection of Personal Data, which has as one of its main bases the need for consent on the part of the holder of the personal data so that your information can be used by the data processing agent. In this vein, the objective of this work will be to demonstrate that consumer vulnerability is aggravated in the digital environment and to analyze whether the need for consent on the part of the holder is really effective so that there is no treatment of their data indiscriminately. The method used is deductive and the conclusion is that the contours given to the need for consent to the holder of personal data by the legislation are insufficient for the effective protection of their decision, given that the legislation did not regulate how the process of consent of the holder to guarantee its effectiveness and its true will.



**Keywords**: Personal data. General Data Protection Act. Consumer. Consent. Fundamental rights. Processing of personal data.

## LISTA DE ABREVIATURAS E SIGLAS

| | |
|---|---|
| ADCT | Ato das Disposições transitórias |
| ANATEL | Agência Nacional de Telecomunicações |
| ART | Artigo |
| CDC | Código de Defesa do Consumidor |
| CPF | Cadastro de Pessoa física |
| CRFB | Constituição da República Federativa do Brasil |
| DEC | Decreto |
| FUNTTEL | Fundo para o Desenvolvimento Tecnológico das Telecomunicações |
| IBGE | Instituto Brasileiro de Geografia e Estatística |
| IP | Internet Protocol |
| LGPD | Lei Geral de Proteção de Dados |
| MCI | Marco Civil da Internet |
| MDB | Movimento Democrático Brasileiro |
| MP | Medida Provisória |
| PEC | Proposta de Emenda à Constituição |
| PNBL | Plano Nacional de Banda Larga |
| PPP | Provedores de Pequeno Porte |
| PT | Partido dos Trabalhadores |
| RG | Registro Geral |
| SGCD | Satélite Geoestacionário de Defesa e Comunicações Estratégicas |
| STF | Supremo Tribunal Federal |
| TELEBRAS | Telecomunicações Brasileiras S.A. |
| WWW | World Wide Web |
| CGI | Comitê Gestor de Internet |
| IP | Internet Protocol ou Protocolo de Internet |
| STJ | Superior Tribunal de Justiça |

**SUMÁRIO**

# 1 INTRODUÇÃO

Com o surgimento de novas tecnologias, o mercado digital tornou-se um meio rápido e eficaz para o consumo. No entanto, toda essa rapidez e comodidade trazida ao consumidor, levou a possibilidade de exposição indiscriminada de seus dados pessoais no ambiente virtual, local em que seus dados viraram um produto lucrativo e que abriu margem para um novo tipo de mercado: a venda de dados pessoais.

O consumidor aderiu a um novo modo de consumo pelo meio digital que, embora ofereça um acesso prático e rápido ao consumo, também o coloca em posição vulnerável diante da grande indústria de venda de informações pessoais para grandes empresas. Como trata-se de um tema novo para o Direito, é necessário tentar entender como o meio jurídico deve atuar na efetiva proteção do usuário/consumidor e se as novas leis serão realmente eficazes no combate a essa prática indiscriminada, que até a entrada em vigor da Lei Geral de Proteção de dados não tinha uma normativa que atribuísse ao cidadão  o poder de decisão sobre a finalidade a que seus dados pessoais serão submetidos.

A regulamentação do uso, proteção e transferência de dados pessoais no Brasil é algo muito recente e, como o mercado digital tem crescido exponencialmente, é necessário abrirmos os olhos para o direito dos consumidores neste tipo de contrato de consumo, pois, as informações, na maioria das vezes, acabam sendo imprecisas e agravam a situação de vulnerabilidade do consumidor.

O princípio da vulnerabilidade é um dos princípios basilares do Código de Defesa do Consumidor, reconhecendo e regulando seu tratamento diferenciado a fim de que proporcione meios que sejam eficazes para reequilibrar a relação de consumo ante a existência de disparidade entre as duas figuras (fornecedor e consumidor) e, por isso, é tão importante a existência de uma legislação específica para a proteção do consumidor.

Com relação ao ambiente virtual e o consumo através do comércio eletrônico, nota-se que a falta de contato direto entre as partes ocasiona dependência do consumidor com relação às informações prestadas pelo fornecedor na oferta, pois, quem escolhe quais informações estarão disponíveis na oferta será o próprio fornecedor.

Diante da falta de normativa que tratasse das relações de consumo no ambiente virtual (comércio eletrônico), a então Presidente Dilma Rousseff expediu o Decreto nº 7962/2013 para

regulamentar o CDC sobre a contratação no comércio eletrônico, trazendo uma série de regras que devem ser observadas pelo fornecedor.

Essa preocupação com a utilização de novas tecnologias e da relação de consumo no ambiente digital se deve à ampliação do acesso à internet no Brasil, que ao longo dos vários governos tentou incentivar o seu acesso através de políticas públicas. Atualmente, a política pública em vigor é prevista pelo decreto nº 9612/2018, que possui como um de seus objetivos (art. 2º) expandir e ampliar o acesso à internet em banda larga e promover inclusão digital à população.

Será diante dessa nova perspectiva de acesso à tecnologia e uso da internet, que o país passará a delinear normativas de sua utilização e sobre as consequências que esse novo mercado pode gerar para a utilização dos dados pessoais dos indivíduos, isso tendo em vista que como citado anteriormente, os dados pessoais tornam-se mais um produto à venda no mercado virtual. Por este motivo, são criadas legislações importantes como: o Marco Civil da Internet ( lei nº 12965/2014) como meio de garantir aos cidadãos direitos ao utilizar a internet e prever princípios estruturantes que resguardem seu direito à privacidade e proteção de seus dados pessoais e a Lei Geral de Proteção de Dados Pessoais para garantir ao titular dos dados pessoais regulamentação sobre o uso e tratamento de seus dados e assegurar seu poder de decisão sobre o destino a que serão submetidos os seus dados pessoais.

A importância do tema se deve com base nas mudanças significativas trazidas com a ampliação do acesso à internet no Brasil, da crescente utilização do comércio eletrônico pelo consumidor e das legislações que passam a regulamentar o tema.

O presente trabalho busca analisar a necessidade de consentimento e controle do consumidor sobre o destino de seus dados pessoais e traz como problema: o consentimento do consumidor no ambiente digital é instrumento eficaz para que seus dados pessoais não sejam comercializados ou utilizados indevidamente por terceiros?

Conduz como hipótese básica que o destino dos dados pessoais do consumidor no ambiente digital precisa obrigatoriamente ser informado e consentido expressamente pelo usuário, de modo que existam mecanismos que auxiliem no efetivo cumprimento de sua vontade e fiscalizem a sua utilização pelos agentes de tratamento. E possui como objetivo específico (i) demonstrar a vulnerabilidade dos dados pessoais do consumidor no meio digital e a obrigatoriedade de informação sobre a finalidade a que serão submetidos no primeiro capítulo, (ii) analisar os procedimentos trazidos pela legislação para que o consumidor não tenha seus dados utilizados de forma abusiva e indiscriminada no segundo capítulo e (iii) definir

se o papel do consentimento tem sido eficaz na autodeterminação do titular dos dados pessoais e quais mecanismos podem auxiliar o efetivo cumprimento do consentimento para que sua vontade seja efetivamente cumprida.

Ademais, a atualidade do tema se deve em decorrência da exposição indiscriminada dos dados pessoais do consumidor no ambiente digital, que, consequentemente, também é um ambiente de consumo que tem mercantilizado essas informações pessoais. A importância do tema surge porque é preciso entender as novidades trazidas pela LGPD e se realmente ela é eficaz no combate a essa prática. E a novidade do tema, de acordo com o que já foi exposto, decorre do fato que a regulamentação do uso, proteção e transferência de dados pessoais no Brasil é algo muito recente e precisa ser debatida a fim de que proporcione aos cidadãos entendimento sobre o papel importante que seus dados pessoais possuem na sociedade.

## 2 RELAÇÃO DE CONSUMO NO AMBIENTE DIGITAL E A PROTEÇÃO DOS CONSUMIDORES

Ao longo dos anos o ambiente em que o consumidor passou a realizar suas relações de consumo extrapolou o limite físico e territorial. Se antes era necessário que consumidor e fornecedor se deslocassem até uma loja física para realizar a compra e venda de produtos, atualmente basta que o consumidor tenha acesso à internet, um computador/tablet ou smartphone, que poderá inserir-se no mercado digital e de forma facilitada realizar a compra de qualquer produto ou serviço disponível no mercado. Isso desde um cachorro-quente por plataformas como o ifood, até a compra de um teste de ancestralidade[1].

Toda essa facilitação da compra on-line teve um caminho árduo até chegar ao patamar atual, passando pela criação de diversas políticas públicas na tentativa de auxiliar a acessibilidade dos cidadãos brasileiros à internet.

Como o Código de Defesa do Consumidor foi promulgado em 1990 e o mercado virtual ainda não existia no Brasil, impossível que o Código trouxesse previsões específicas quanto à comercialização de bens e serviços de forma on-line, muito menos prever que mais tarde ocuparia lugar de destaque na economia brasileira. A proteção do consumidor trazida pelo CDC refere-se a uma legislação geral e, portanto, extensível às relações de consumo em qualquer ambiente, seja ele físico ou eletrônico. Basta que tenha um fornecedor disposto a

[1] O *site* do laboratório Genera disponibiliza a venda de teste de ancestralidade que pode ser feito pelo próprio usuário em sua casa da seguinte forma: o usuário compra o teste de ancestralidade e recebe em casa um kit de coleta com instruções para que ele mesmo colha o material e depois envie para o laboratório (GENERA, s.d.)

vender um produto e um consumidor que seja destinatário final na relação de consumo disposto a comprá-lo, que serão aplicadas as regras do Código. Essas regras observam a necessidade de proteção do consumidor e fundamentam-se em princípios e direitos básicos que alcançam o setor econômico e a personalidade do consumidor (MENDES, 2008).

Em que pese o CDC não tenha previsão específica sobre a relação de consumo no ambiente virtual, ao longo dos anos mostrou-se apto a acompanhar as necessidades do consumidor no mercado digital, o que segundo Santos e Silva (2011) se deve por atribuir proteção especial ao consumidor e utilizar normas flexíveis a fim de que possam protegê-lo frente às mudanças da sociedade e a evolução das necessidades do consumidor.

Somente em 2013, que o legislador regulamenta o CDC através do Decreto n º 7962/2013 no que tange a relação de consumo no âmbito do comércio eletrônico e, no ano seguinte, disciplina o Marco Civil da Internet (MCI) – lei nº 12.965/2014 – enfatizando a aplicabilidade do CDC nas relações de consumo ocorridas no ambiente virtual em seu capítulo que fala a respeito dos Direitos e Garantias dos Usuários, especificamente em seu artigo 7º, inciso XIII[2]. Quatro anos depois, é promulgada a tão esperada lei nº 13.709/2018 denominada Lei Geral de Proteção de Dados Pessoais (LGPD) que veio para assegurar os direitos dos usuários sobre os seus dados pessoais e proteger seu direito à liberdade, privacidade e o livre desenvolvimento da pessoa natural[3], uma lei estruturada e focada em normativas que regulamentam a forma com que os dados serão capturados, armazenados e tratados (FERNEDA; FERRAZ; GUIMARÃES FILHO, 2020).

Os dados pessoais, embora sejam privativos do usuário, passam a ser de domínio do fornecedor após serem disponibilizados durante a relação de consumo. E essas informações deixadas pelo consumidor no ambiente virtual, sejam os seus dados pessoais ou até mesmo as páginas que visita, agora são objeto de monitoramento por empresas que utilizam de tecnologias de armazenamento para lucrar com o perfil individualizado de consumidor e o redirecionamento de propagandas:

---

[2] Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
[…] XIII - aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet. (BRASIL, 2014).

[3] Art. 1º 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. Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios. (BRASIL, 2018).

> A utilização de sistemas informatizados em diversas etapas da cadeia de produção e de consumo, à qual hoje já estamos nos habituando, trouxe consigo uma possibilidade concreta de mudança nesta equação: os sistemas informatizados de hoje têm uma capacidade muito grande de armazenar cada detalhe e sutileza das ações que ajudam a realizar. O consumidor de hoje existe em um ambiente onde muitas de suas ações são, ao menos tecnicamente, passíveis de registro e de posterior utilização (DONEDA, 2010, p. 9)

Todo esse avanço tecnológico traz à tona a fragilidade do consumidor e a violação constante das informações deixadas por ele no ambiente virtual. Este capítulo servirá como base de apoio para entendermos o contexto ao qual o consumo digital foi inserido no Brasil; como a relação de consumo ultrapassou o limite físico e passou a ser possível no ambiente virtual; explicar o motivo dos dados pessoais terem virado um produto lucrativo às várias empresas e como essa venda desenfreada repercute na vida do consumidor; enfatizar a importância do princípio da vulnerabilidade nas relações consumeristas trazido pelo Código de Defesa do Consumidor, com a observância de que o ambiente digital agrava a sua vulnerabilidade.

## 2.1 A VULNERABILIDADE DOS DADOS PESSOAIS DO CONSUMIDOR NO AMBIENTE DIGITAL

O desenvolvimento das tecnologias da informação ao longo dos últimos anos – principalmente a computação e as telecomunicações – e a crescente facilitação do acesso ao uso da internet abriu margem à exploração do mercado de compra e venda de bens de consumo no ambiente digital. Os consumidores, que em sua maioria tinham acesso somente aos serviços e produtos do mercado local, puderam começar a realizar suas compras de forma totalmente digital, obtendo um amplo acesso aos diversos tipos de ofertas de serviços e produtos, além da praticidade por não precisar deslocar-se até uma loja física para a realização da compra das mercadorias, que podem ser entregues diretamente no endereço fornecido pelo próprio consumidor na hora da compra, poupando seu tempo de deslocamento.

Além da comodidade adquirida pelo consumidor em poder realizar suas compras de qualquer lugar e a qualquer momento, "[…] há uma ampliação da oferta de consumo, de maneira global, em tempo real" (BASAN, 2021, p. 66). O aumento do número de pessoas conectadas à internet oportunizou o aperfeiçoamento e desenvolvimento da tecnologia, inclusive aquelas tecnologias voltadas ao controle do usuário que são do interesse de governos e do comércio, que, por consequência, restringem a liberdade do usuário (MENDES, 2008).

Os dados dos usuários então passaram a ser informações úteis à exploração de um novo tipo de produto: a venda de dados pessoais dos usuários/consumidores no meio eletrônico.

É com o intuito de capturar os dados pessoais dos usuários na indústria de mineração e sua posterior comercialização, que a lógica de consumo se alterna e faz com que os próprios consumidores passem a ser o próprio produto (FERNEDA; FERRAZ; GUIMARÃES FILHO, 2020).

Essa mercantilização, por não ser informada de forma didática ao consumidor no momento de disponibilização dos dados, coloca-o em posição de desvantagem. Doneda (2010) expõe que o acesso a essas informações pelo fornecedor será capaz de causar desequilíbrio da relação de consumo e gerar assimetria informacional, deixando o usuário sem suporte para entender o que acontece com seus dados pessoais no mundo virtual.

Foi em razão da falta de equilíbrio nas relações de consumo que a Constituição Federal previu em seu artigo 5º, inciso XXXII[4], a garantia legal da defesa do consumidor como um direito fundamental e tratou a necessidade de sua defesa com um dos Princípios Gerais da Atividade Econômica disposto no artigo 170, inciso V, Título VII, que trata da Ordem Econômica e Financeira (BRASIL, 1988). Além disso, a própria Carta Magna reconheceu a necessidade de uma lei que tratasse dos direitos do consumidor e previu em seu artigo 48 do Ato das Disposições transitórias (ADCT), que após os 120 dias de sua promulgação teria que ser elaborado o Código de Defesa do Consumidor – CDC, que posteriormente virou a lei nº 8.078 de 11 de setembro de 1990 (CUNHA, 2011).

Segundo Humberto Theodoro Júnior (2021), a necessidade de criação do Direito do Consumidor como uma disciplina autônoma, ocorreu pela inequívoca superioridade do fornecedor sobre o consumidor nas relações contratuais e pelo fato do mercado não conseguir superar sozinho esse desequilíbrio. Por isso a necessidade de intervenção do Estado e criação de uma lei que proteja integralmente a relação de consumo e que alcance todas as especificidades do mercado.

No intuito de suprir as lacunas existentes no mercado e a relação díspar entre fornecedor e consumidor, o CDC trouxe alguns princípios norteadores às relações de consumo, dentre eles o da vulnerabilidade, previsto em seu artigo 4º[5], inciso I. A vulnerabilidade do

[4] Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes
[...]XXXII - o Estado promoverá, na forma da lei, a defesa do consumidor; (BRASIL, 1988)

[5] Art. 4º A Política Nacional das Relações de Consumo tem por objetivo o atendimento das necessidades dos consumidores, o respeito à sua dignidade, saúde e segurança, a proteção de seus interesses econômicos, a melhoria da sua qualidade de vida, bem como a transparência e harmonia das relações de consumo, atendidos os seguintes princípios:
I - reconhecimento da vulnerabilidade do consumidor no mercado de consumo;
II - ação governamental no sentido de proteger efetivamente o consumidor:

consumidor pessoa física, deve ser entendida como um dos princípios basilares do Código. Segundo Almeida e Lenza (2020) este princípio reconhece a existência de desigualdade na relação de consumo, enfatiza a posição do consumidor como parte mais fraca da relação contratual e assegura tratamento diferenciado por meio de instrumentos jurídicos que sejam capazes de reequilibrar a relação entre fornecedor e consumidor. Importante frisar que a vulnerabilidade de que tratam os artigos citados acima não deve ser confundida com a hipervulnerabilidade, pois essa última refere-se a um grupo específico de consumidores com características pessoais que os tornam ainda mais sensíveis às relações de consumo:

> […] a vulnerabilidade inerente à relação de consumo é somada a uma vulnerabilidade intrínseca à pessoa do consumidor, seja em virtude de sua idade (crianças e idosos), de seu estado de saúde (doentes), de suas necessidades especiais (deficientes) ou de seu nível de escolaridade (analfabetos), tornando-o mais suscetível de ceder às pressões promovidas pelos fornecedores. Com isso, constata-se que a hipervulnerabilidade decorre de uma sobreposição de certas características pessoais que fragilizam o indivíduo – averiguáveis no caso concreto – à vulnerabilidade relacional do consumidor, tendo como resultado um consumidor-criança, consumidor-idoso, consumidor-doente, consumidordeficiente ou consumidor-analfabeto que necessita de atenção especial do Estado, que deve operar por intermédio de suas casas legislativas, dos órgãos públicos responsáveis pelo controle e fiscalização das atividades econômicas no mercado de consumo e dos magistrados chamados a decidir causas que envolvam esses atores, sempre observando essas hipervulnerabilidades como diretriz de sua atuação(CANTO, 2014, p. 76 e 77).

No que se refere ao reconhecimento da vulnerabilidade informacional, o artigo 6º, III, do CDC traz como direito básico do consumidor o acesso à informação clara e adequada sobre os diferentes produtos e serviços, com especificação correta de quantidade, características,

---

a) por iniciativa direta;
b) por incentivos à criação e desenvolvimento de associações representativas;
c) pela presença do Estado no mercado de consumo;
d) pela garantia dos produtos e serviços com padrões adequados de qualidade, segurança, durabilidade e desempenho.
III - harmonização dos interesses dos participantes das relações de consumo e compatibilização da proteção do consumidor com a necessidade de desenvolvimento econômico e tecnológico, de modo a viabilizar os princípios nos quais se funda a ordem econômica (art. 170, da Constituição Federal), sempre com base na boa-fé e equilíbrio nas relações entre consumidores e fornecedores;
IV - educação e informação de fornecedores e consumidores, quanto aos seus direitos e deveres, com vistas à melhoria do mercado de consumo;
V - incentivo à criação pelos fornecedores de meios eficientes de controle de qualidade e segurança de produtos e serviços, assim como de mecanismos alternativos de solução de conflitos de consumo;
VI - coibição e repressão eficientes de todos os abusos praticados no mercado de consumo, inclusive a concorrência desleal e utilização indevida de inventos e criações industriais das marcas e nomes comerciais e signos distintivos, que possam causar prejuízos aos consumidores;
VII - racionalização e melhoria dos serviços públicos;
VIII - estudo constante das modificações do mercado de consumo.
IX - fomento de ações direcionadas à educação financeira e ambiental dos consumidores;
X - prevenção e tratamento do superendividamento como forma de evitar a exclusão social do consumidor (BRASIL,1990)

composição, qualidade, tributos incidentes e preço, bem como sobre os riscos que apresentem (BRASIL,1990), assegurando em seu artigo 43º[6] o acesso às informações existentes em cadastros, fichas, registros e dados pessoais, e que todas as informações sejam disponibilizadas em formatos acessíveis, mediante solicitação do consumidor.

O que muitas vezes acontece no ambiente virtual e agrava a condição do consumidor como parte vulnerável da relação de consumo é que a falta de contato presencial entre as partes deixa o consumidor mais suscetível a falta de informações, correndo o risco de suas dúvidas serem sanadas pelo fornecedor. Mesmo que o CDC traga a previsão legal de que o consumidor possui direito ao acesso à informação clara e adequada sobre os produtos e serviços ofertados pelo fornecedor, tais informações acabam sendo colocadas de maneira insuficiente ou camufladas, sem que o consumidor consiga dialogar diretamente com o fornecedor na relação consumerista digital. Consequentemente, se as informações inerentes aos produtos por muitas vezes não são publicizadas no anúncio, quem dirá a divulgação da finalidade a que são submetidos os dados pessoais disponibilizados pelo consumidor no momento da realização do contrato de compra. Além do mais, pouquíssimos são os consumidores que possuem conhecimento da mina de ouro que pode ser a disponibilização de seus dados e da necessidade em preservá-los.

Portanto, tendo em vista a vulnerabilidade a que o consumidor está exposto no ambiente virtual quanto a divulgação e comercialização de seus dados, é necessário entender como funciona a lógica do mercado eletrônico e como ocorre de fato a relação de consumo.

---

[6] Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.
§ 1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.
§ 2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.
§ 3° O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.
§ 4° Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.
§ 5° Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores.
§ 6º Todas as informações de que trata o **caput** deste artigo devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor. (grifo nosso) (BRASIL, 1990).

## 2.2 RELAÇÃO DE CONSUMO NO COMÉRCIO ELETRÔNICO

Para entender como funciona a relação de consumo no comércio eletrônico, necessário entender quais os elementos que a caracterizam como relação jurídica de consumo: "[…] poderá ser definida como aquela relação firmada entre consumidor e fornecedor, a qual possui como objeto a aquisição de um produto ou a contratação de um serviço"(ALMEIDA; LENZA, 2020, p. 92). O Código de defesa do consumidor (CDC), por sua vez, não traz o conceito relação de consumo – até o momento também não existe conceituação para a relação de consumo ocorrida digitalmente –, no entanto, tal definição não se faz necessária, tendo em vista que o Código obteve êxito ao distinguir quais seriam os sujeitos necessários para que a relação de consumo possa ser configurada, além do que, a doutrina também contribuiu criando teorias que pudessem explicar o conceito amplo de destinatário final trazido pelo CDC. Portanto, a relação de consumo será configurada quando de um lado estiver presente consumidor[7] e do outro lado, o fornecedor de produto ou serviços[8]; um disposto a comprar um produto ou serviço, e o outro disposto a oferecer.

Consumidor será aquele que adquire produto ou serviço como destinatário final – há discussão doutrinária sobre o conceito de consumidor e a abrangência do uso da expressão "destinatário final"[9] – e fornecedor aquele que compõe o outro lado da relação contratual fornecendo ou vendendo produto/serviço ao destinatário final (consumidor).

---

[7] Art. 2° Consumidor é toda pessoa física ou jurídica que adquire ou utiliza produto ou serviço como destinatário final.
Parágrafo único. Equipara-se a consumidor a coletividade de pessoas, ainda que indetermináveis, que haja intervindo nas relações de consumo. (BRASIL,1990).

[8] Art. 3° Fornecedor é toda pessoa física ou jurídica, pública ou privada, nacional ou estrangeira, bem como os entes despersonalizados, que desenvolvem atividade de produção, montagem, criação, construção, transformação, importação, exportação, distribuição ou comercialização de produtos ou prestação de serviços. (BRASIL,1990).
§ 1° Produto é qualquer bem, móvel ou imóvel, material ou imaterial.
§ 2° Serviço é qualquer atividade fornecida no mercado de consumo, mediante remuneração, inclusive as de natureza bancária, financeira, de crédito e securitária, salvo as decorrentes das relações de caráter trabalhista. (BRASIL,1990).

[9] A compreensão do conceito de consumidor como destinatário final deu origem ao surgimento de duas teorias doutrinárias: a maximalista e a finalista. A teoria finalista compreende que destinatário final seja o destinatário econômico do bem, ou seja, consumidor seria aquele que compra o produto/serviço com a finalidade de uso próprio ou de sua família. Quanto a teoria maximalista, o entendimento é de que o conceito de consumidor trazido pelo CDC em seu art. 2º deve ser interpretado abrangentemente, de modo que destinatário final é quem consome o produto/serviço ao retirá-lo do mercado, não importando se a finalidade a que se destinará o produto possa ser intermediária para a construção de produto ou serviço que se reverterá em lucro (BENJAMIN; BESSA; MARQUES, 2021).
Existe também uma teoria recente chamada finalismo aprofundado que fica em posição intermediária nas teorias originárias. Essa teoria amplia o conceito de consumidor, expondo a necessidade de analisar a situação de vulnerabilidade a que o consumidor está exposto, seja ele pessoa física ou jurídica, não sendo necessário que

Quanto ao termo comércio eletrônico ou *e-commerce,* ou comércio virtual, como também é conhecido, podemos entendê-lo "como o conjunto de relações travadas entre fornecedor e consumidor, realizada em um estabelecimento empresarial virtual, através, ou não, da *internet"* (NEVES, 2014, p. 155), portanto, basta que a relação consumerista aconteça no ambiente virtual e com transmissão de dados através de uma rede de computadores, sem necessidade de conexão à *internet*. "No Brasil, a primeira empresa que comercializou produtos a partir de sites na internet foi a Livraria Cultura, começando suas atividades em 1995" (TOMÉ, 2018, p. 1). Então é o ambiente virtual um facilitador ao comércio e à redução de custos para as empresas, que não precisam arcar com as despesas de um ambiente físico e com a contratação de vendedores, porque são os próprios consumidores que irão se servir das ofertas e escolher qual delas será mais atrativa à sua necessidade.

De forma mais ampla, "o comércio eletrônico é a realização de toda a cadeia de valores dos processos de negócio num ambiente eletrônico, por meio da aplicação intensa das tecnologias de comunicação e de informação, atendendo aos objetivos de negócio" (OLIVEIRA; SOBHIE, 2013, p.88). O produto ou serviço dependerá desse processo de negócio para a venda ser realizada, sendo tanto a venda quanto a compra realizada on-line. Para que a compra seja realizada, o fornecedor obrigatoriamente precisa especificar as informações sobre o produto a fim de que o consumidor consiga ter certeza que está comprando o que realmente deseja, no entanto, o que acontece com frequência é que as informações disponibilizadas muitas vezes são insuficientes e a comunicação entre consumidor e fornecedor resta prejudicada pela grande demanda de compras virtuais e a falta de disponibilização por parte do fornecedor de um serviço de atendimento ao cliente que resolva de forma eficiente as dúvidas dos usuários consumidores.

No que se refere a regulamentação da defesa do consumidor trazida pelo CDC, sua promulgação ocorreu no ano de 1990, momento em que sequer havia estrutura e regulamentação para a atuação dos provedores de serviços de internet comercial no Brasil. O acesso à internet até existia nesse período, mas era restrito ao uso acadêmico. Segundo Carvalho (2006), somente em 1995, com a entrada do governo de Fernando Henrique Cardoso, que houve a criação do Comitê Gestor da Internet (CGI), instituído pela Portaria Interministerial nº 147 para tratar da regulamentação da *internet* comercial no Brasil. Ainda neste ano, também houve a edição da norma 004/95 objetivando regular a Rede Pública de telecomunicações para o

ele seja o destinatário final da relação de consumo, mas sim que seja esteja exposto a uma posição de desvantagem e, portanto, sendo a parte vulnerável da relação de consumo (THEODORO JÚNIOR, 2021).

provimento e utilização de Serviços de Conexão à Internet e definir alguns termos e conceitos a respeito do serviço de internet no Brasil (ANATEL, 1995).

Carvalho (2006) chama a atenção para o fato de que embora tenha havido uma regulamentação, a infraestrutura continuou precária e sem capacidade de atender a todos os usuários, tendo em vista que o número de redes telefônicas era insuficiente para o acesso dos computadores à *internet.* Além disso, não eram todas as pessoas que tinham cacife para comprar um computador e pagar a conta telefônica, já que o uso da internet era cobrado de acordo com o custo da ligação telefônica.

Nesse meio tempo, no ano de 1997, é criada a Lei nº 9742/1997, denominada Lei Geral de Telecomunicações, com o intuito de regular a competência da União para organizar a exploração dos serviços de telecomunicações e seu artigo 1º; os direitos e deveres do usuário dos serviços das telecomunicações em seu artigo 3º e 4º, a criação da Agência Nacional de Telecomunicações como órgão regulador das telecomunicações (ANATEL) entre outras previsões sobre a organização dos serviços de telecomunicações.

No que tange a falta de estrutura e o difícil acesso à internet, o governo tentou investir em políticas públicas a fim de tornar viável o uso da internet e beneficiar a sociedade brasileira com a sua aplicação, tendo instituído o Programa Sociedade da informação através do decreto nº 3.294, de 15 de dezembro de 1999, política que não foi implementado por faltar ações concretas por parte do governo que viabilizassem a expansão do acesso ao serviço e firmasse o propósito de universalização do acesso à internet (FONTES, 2014). Ainda segundo Fontes (2014), após esse Decreto, o governo ainda tentou implementar outras políticas públicas: o Programa GESAC (Governo Eletrônico Serviço de Atendimento ao Cidadão) pela portaria nº 256/2002; o Projeto Casa Brasil em 2003; Projeto Cidadão Conectado pelo Decreto nº 5.542/2005; o Programa de inclusão digital pela Lei nº 11.196/2005.

No ano seguinte, foi criada a lei nº 10.052, de 28 de novembro de 2000, criando o Fundo para o Desenvolvimento Tecnológico das Telecomunicações (FUNTTEL), delimitando

como seria constituído o Conselho Gestor[10] e sua competência[11], além de estabelecer como seriam arrecadadas as receitas do fundo[12] prevendo que a aplicação dos recursos arrecadados pelo Fundo devem ocorrer exclusivamente no interesse do setor de telecomunicações.

Fontes (2014) destaca que a exclusão digital no Brasil era extremamente acentuada no ano de 2009 e que as inúmeras tentativas de criação de políticas públicas que viabilizassem o acesso dos cidadãos às telecomunicações não foram eficazes. Motivo pelo qual em 2010 o governo lançou o Plano Nacional de Banda Larga (PNBL):

> Em 2010, o então Presidente Luiz Inácio Lula da Silva (PT) editou o decreto n. 7.175, que instituiu o Programa Nacional de Banda Larga (PNBL), com o objetivo de promover a inclusão digital, entre outras finalidades. Na ocasião, a estatal Telebrás foi acionada para promover a infraestrutura necessária ao projeto. Caberia à Anatel a regulação do serviço. Um termo de compromisso foi assinado entre o então Ministério

[10] Art. 2º O Fundo para o Desenvolvimento Tecnológico das Telecomunicações será administrado por um Conselho Gestor e terá como agentes financeiros o Banco Nacional de Desenvolvimento Econômico e Social – BNDES e a Empresa Financiadora de Estudos e Projetos – Finep.
§ 1º O Conselho Gestor será constituído pelos seguintes membros:
I – um representante do Ministério das Comunicações;
II – um representante do Ministério da Ciência e Tecnologia;
III – um representante do Ministério do Desenvolvimento, Indústria e Comércio Exterior;
IV – um representante da Agência Nacional de Telecomunicações – Anatel;
V – um representante do Banco Nacional de Desenvolvimento Econômico e Social – BNDES;
VI – um representante da Empresa Financiadora de Estudos e Projetos – Finep.
§ 2º Cabe ao Poder Executivo nomear os membros do Conselho Gestor do Funttel, devendo a primeira investidura ocorrer no prazo de até noventa dias a partir da publicação desta Lei.
§ 3º O Conselho Gestor será presidido pelo representante do Ministério das Comunicações e decidirá por maioria absoluta.
§ 4º O mandato e a forma de investidura dos conselheiros serão definidos em regulamento. […] (BRASIL, 2000)

[11] Art. 3º Compete ao Conselho Gestor:
I – aprovar as normas de aplicação de recursos do Fundo em programas, projetos e atividades prioritárias na área de telecomunicações, em consonância com o disposto no art. 1º desta Lei;
II – aprovar, acompanhar e fiscalizar a execução do Plano de Aplicação de Recursos submetido pelos agentes financeiros e pela Fundação CPQd;
III – submeter, anualmente, ao Ministério das Comunicações a proposta orçamentária do Funttel, para inclusão no projeto de lei orçamentária anual a que se refere o § 5º DO ART. 165 DA CONSTITUIÇÃO FEDERAL, observados os objetivos definidos no art. 1º desta Lei, as políticas de desenvolvimento tecnológico fixadas pelos Poderes Executivo e Legislativo e a existência de linhas de crédito;
IV – prestar conta da execução orçamentária e financeira do Funttel;
V – propor a regulamentação dos dispositivos desta Lei, no âmbito de sua competência;
VI – aprovar seu regimento interno;
VII – decidir sobre outros assuntos de interesse do Funttel. (BRASIL, 2000).

[12] Art. 4º Constituem receitas do Fundo:
I – dotações consignadas na lei orçamentária anual e seus créditos adicionais;
II – (VETADO)
III – contribuição de meio por cento sobre a receita bruta das empresas prestadoras de serviços de telecomunicações, nos regimes público e privado, excluindo-se, para determinação da base de cálculo, as vendas canceladas, os descontos concedidos, o Imposto sobre Operações relativas à Circulação de Mercadorias e sobre Prestações de Serviços de Transporte Interestadual e Intermunicipal e de Comunicação (ICMS), a contribuição ao Programa de Integração Social (PIS) e a Contribuição para o Financiamento da Seguridade Social (Cofins); [...] (BRASIL, 2000)

> das Comunicações, a Anatel e as empresas Algar Telecom, Oi, Sercomtel e Telefônica/Vivo visando a adoção da internet popular.
> Em 2016, com o encerramento do termo de compromisso, o PNBL chegou ao fim (CHAGAS; FERNANDES, 2019, p.67).

Fontes (2014) aponta que as medidas e metas adotadas pelo governo foram insuficientes, mas que ainda assim um passo importante para o Brasil à época. Outro passo importante para o Brasil nas telecomunicações, ocorreu quando em 05 de julho de 2017, quando colocou em órbita o Satélite Geoestacionário de Defesa e Comunicações Estratégicas (SGCD), no intuito de ampliar o acesso à internet e disponibilizar banda larga em todo o território nacional (CHAGAS; FERNANDES, 2019).

Em 2018, o PNBL (Decreto nº 7.175 de 2010) e o Programa Brasil Inteligente (criado para substituir o PNBL) foram revogados e substituídos pelo Decreto nº 9612, de 17 de dezembro de 2018, para dispor sobre as políticas públicas de telecomunicações que manteve algumas atribuições das Telecomunicações Brasileiras S.A. (Telebrás)[13].

Em que pese o avanço do acesso à internet no Brasil ainda ter muitos desafios, podemos dizer que o crescimento dos provedores regionais ou Provedores de Pequeno Porte (PPP) contribui significativamente para o aumento da cobertura de banda larga fixa (SILVA, 2020), e isso se deve porque "são pequenas e médias empresas de telecomunicação responsáveis

[13] Art. 12. As políticas públicas de telecomunicações de que trata este Decreto substituem, para todos os fins legais, o Programa Nacional de Banda Larga e o Programa Brasil Inteligente, mantidas as seguintes atribuições da Telecomunicações Brasileiras S.A. - Telebrás:
I - implementação da rede privativa de comunicação da administração pública federal;
II - prestação de apoio e suporte às políticas públicas de conexão à internet em banda larga para universidades, centros de pesquisa, escolas, hospitais, postos de atendimento, tele centros comunitários e outros pontos de interesse público;
III - provisão de infraestrutura e de redes de suporte a serviços de telecomunicações prestados por empresas privadas, pelos Estados, pelo Distrito Federal, pelos Municípios e por entidades sem fins lucrativos;
IV - prestação de serviço de conexão à internet em banda larga para usuários finais, apenas em localidades onde inexista oferta adequada daqueles serviços.
§ 1º A Telebrás exercerá suas atividades nos termos da legislação.
§ 2º Os sistemas de tecnologia de informação e comunicação destinados às atividades de que tratam os incisos I e II do **caput** são considerados estratégicos para fins de contratação de bens e serviços relacionados à implantação, à manutenção e ao aperfeiçoamento.
§ 3º A implementação da rede privativa de comunicação da administração pública federal de que trata o inciso I do **caput** consistirá na provisão de serviços, infraestrutura e redes de suporte à comunicação e à transmissão de dados, na forma da legislação em vigor.
§ 4º O Ministério das Comunicações definirá as localidades onde inexista a oferta adequada de serviços de conexão à internet em banda larga a que se refere o inciso IV do **caput**. (REDAÇÃO DADA PELO DECRETO Nº 10.799, DE 2021)
§ 5º A Telebrás permanece autorizada a usar, fruir, operar e manter a infraestrutura e as redes de suporte de serviços de telecomunicações de propriedade ou posse da administração pública federal e a firmar o correspondente contrato de cessão, na hipótese de uso de infraestrutura detida por entidade da administração pública federal indireta.
§ 6º As ações executadas ou em execução com fundamento nos programas indicados no **caput** não serão prejudicadas pela entrada em vigor deste Decreto. [...] (BRASIL, 2018)

por levar banda larga fixa a localidades distantes dos grandes centros e/ou com acessos difíceis, como as regiões da Amazônia, por exemplo (CHAGAS; FERNANDES, 2019, p.69).

Importante entender o contexto que a internet foi inserida no Brasil e como ocorreu a tentativa por parte do governo de universalização do seu uso, para entender os desafios que temos atualmente. O Código de Defesa do Consumidor não trouxe previsões de direitos e deveres específicos das relações de consumo em ambiente virtual, porque em 1990 os cidadãos brasileiros não possuíam acesso à internet. Tirando por base a história das telecomunicações apresentada anteriormente e a dificuldade que o governo tem em ampliar o acesso às regiões distantes dos grandes centros, podemos entender o motivo de estarmos atrasados na criação de leis que regulamentem o uso da internet no Brasil e suas peculiaridades, pois foi somente em 2013, com o Decreto 7.962/2013 que houve a regulamentação da lei nº 8078/1990 (CDC), para dispor sobre a contratação no comércio eletrônico e as garantias do consumidor para a relação de consumo. E a criação da lei nº 12.965, de 23 de abril de 2014, assim denominada Marco Civil da Internet (MCI), a primeira lei a estabelecer o uso da internet e garantir a proteção dos dados pessoais no ambiente digital.

Diante da necessidade de garantir direitos ao consumidor, a ele é atribuída a condição de parte vulnerável da relação de consumo. A falta de conhecimentos específicos, sejam eles de espécie técnica (não possuir conhecimento preciso sobre o produto ou serviço), jurídica (não possuir conhecimento específico sobre a área jurídica, econômica, contábil e reflexos na relação consumerista), fática (carece de poder econômico, psicológico ou físico) e informacional (insuficiência de dados sobre os serviços ou produtos que possam influenciar no momento de realização da compra) (BENJAMIN; BESSA; MARQUES, 2021), colocam o consumidor em posição desfavorável. Por este motivo, “a função principal do Código é reequilibrar as forças dos sujeitos da relação consumerista, diminuir a vulnerabilidade do consumidor e limitar as práticas nocivas de mercado" (THEODORO JÚNIOR, 2021, p.4).

Quando tratamos da relação de consumo por meio de acesso a sites e aplicativos, mesmo que o consumidor domine o acesso à internet, sua vulnerabilidade continuará em evidência. Isso pelo simples fato de que ele não conseguirá ser autossuficiente na relação consumerista e ter acesso a toda e qualquer informação por não possuir capacidade técnica para tanto:

> o meio eletrônico, automatizado e telemático, em si, usado profissionalmente pelos fornecedores para ali oferecerem seus produtos e serviços aos consumidores, representa para os consumidores leigos um desafio extra ou vulnerabilidade técnica. O consumidor não é — mesmo que se considere um especialista ou técnico em

> computadores e na internet. Esta "falha tecnológica" é geral, mas não desanima; ao contrário, fascina a maioria. É típica da pós-modernidade. Apesar da "falha tecnológica" ou vulnerabilidade ante o meio virtual, milhares de consumidores, sem medo, negociam, compram e participam até mesmo de leilões e outros "divertimentos" consumistas sem censura, através da rede mundial da internet. Atuam eles sem conhecimento técnico, sem fronteiras, sem território, sem passado, sem experiência e com uma fluida confiança, justamente no direito "do consumidor", em uma vaga (e muitas vezes inexistente) proteção "internacional" dos mais fracos, confiando nas respostas pelo menos razoáveis que a justiça dará. É um contexto novo de superficialidade, hedonismo consumista e insegurança pós-moderna. (MARQUES, 2016, p. 124 e 125).

Como a informação passa a ser um instrumento organizado, armazenado (criação de grandes bancos de dados para armazenamento de informações) e até mesmo vendido para que possa beneficiar outras práticas de mercado, a exposição do consumidor acentua sua vulnerabilidade e ressalta o abismo existente entre a relação consumerista realizada no ambiente digital.

Uma prática de mercado utilizada para o acesso às informações do consumidor, principalmente as informações individuais que são tratadas como "dados pessoais" é a denominada publicidade comportamental on-line e a utilização de *cookies*, duas formas de monitoramento on-line dos usuários da qual as informações tornam-se uma espécie de produto (MENDES, 2008) – serão explicadas de maneira mais aprofundada nos próximos tópicos. Por isso, é tão importante entendermos como essas práticas de mercado podem ferir a privacidade de cada indivíduo, expondo suas informações pessoais sem que o próprio usuário saiba que essa possibilidade tanto existe, que é prática recorrente nesse tipo de mercado.

Os dados do consumidor tornam-se produtos e podem ser utilizados como moeda de troca, um exemplo disso é o caso das plataformas digitais e aplicativos "gratuitos" sejam: *sites* de busca, *Facebook, Instagram, Spotify, Youtube,* entre outros), que na verdade de gratuitos não possuem nada. Trata-se de nítida relação de consumo, em que há contrapartida do consumidor que paga pelo serviço cedendo à plataforma a utilização de seus dados de consumo. Esse tipo de relação com o usuário é muito interessante para essas empresas, isso tendo em vista que "para uma empresa tecnológica, os dados fornecidos pelo utilizador em troca do bem são em muitos casos muito mais valiosos do que uma contrapartida financeira" (CARVALHO, 2018, p.116). O pagamento, portanto, não é realizado com dinheiro, mas com os seus dados, sejam eles pessoais ou não, aí dependerá do tipo de dado que a plataforma solicita.

Uma coisa interessante e algo a se pensar, é que quando o consumidor realiza uma compra no mercado eletrônico, ele disponibiliza seus dados e paga pelo produto que está adquirindo, seja por boleto, cartão de crédito, cartão de débito, pix ou qualquer outro meio que

não sejam os seus próprios dados pessoais. Neste cenário, os dados cedidos por ele à empresa também se tornam um produto, que possivelmente será explorado pela empresa e/ou vendido a outros fornecedores. Neste sentido, o consumidor acaba pagando duas vezes pela compra realizada. Uma vez, ao realizar a compra do produto e paga por ele monetariamente e outra, de forma mascarada, ao ceder seus dados que serão vendidos a outros setores. O que a nosso ver escancara sua vulnerabilidade e pode ser configurar prática comercial abusiva pelos simples do fornecedor estar vantagem manifestamente excessiva.

## 2.3 PUBLICIDADE COMPORTAMENTAL ON-LINE

Para alguns consumidores pode até parecer estranho que os sites consigam ter acesso sobre as pesquisas que realizam no ambiente digital, sem ter noção alguma de que seus rastros digitais são informações úteis a várias empresas que investem fortemente em um marketing digital que individualiza e personaliza as publicidades de acordo com as preferências do internauta. A publicidade como vemos nos veículos de comunicação pode ser entendida como:

> [...] uma prática comercial de marketing, desenvolvida mediante uma comunicação comercial (feita através de veículos de difusão) que apresenta uma oferta destinada à divulgação, com finalidade econômica, de determinado produto, serviço, marca ou empresa, com o escopo de persuadir consumidores, direta ou indiretamente, provocando ou aumentando a demanda de um determinado produto ou serviço ou em relação a uma determinada marca ou empresa que está sendo objeto do anúncio. (ALVES, 2016, p. 211).

Mendes (2008) explica que foi a instabilidade do mercado sobre a produção em massa de bens padronizados e de baixo custo na década de 70, que contribuiu para o surgimento de um novo modelo econômico baseado na produção de produtos com alta qualidade, especializados conforme a necessidade do mercado e do consumidor, tendo surgido nessa mesma época o interesse do setor privado pelo processamento de dados pessoais dos consumidores do modo como é tratado hoje em dia – coleta de dados que contribuam para o crescimento das vendas e atinja a maior quantidade possível de consumidores.

Como a produção passou a ser focada de acordo com a especificidade de cada tipo de mercado, os consumidores também passaram a ser individualizados de acordo com a sua necessidade de compra. Portanto, à medida que a sociedade passa a aderir às novas tecnologias e a criar produtos, surge o *marketing* para criar estratégias para a venda de produtos e serviços.

Com toda a evolução do mercado e a utilização da *internet* como um ambiente apto para a realização das relações de consumo, “as práticas de monitoramento de dados tornam-se

estratégias constantes para as empresas que operam no comércio virtual, especialmente para determinar o perfil do consumidor e enviar ofertas e serviços direcionados" (SILVA, 2016, p. 80).

Difícil o internauta que navegando entre os sites nunca se deparou com anúncios repetidos incomodando o acesso do mouse à barra de rolagem. Vale dizer que esse tipo de publicidade fundada no comportamento, a depender do modo como é realizada, pode ser configurada com base no 6º, inciso IV,[14] do CDC como uma prática comercial coercitiva e desleal:

> […] tanto quando expõe o consumidor de maneira compulsória a anúncios publicitários em sites que não mantém qualquer espécie de relação direta entre si (método coercitivo), como quando não dá ciência ao consumidor de que seus hábitos comportamentais estão sendo coletados para fins de publicidade (método desleal). (ALVES, 2016, p. 218).

Essa coleta de dados ocorre através de técnicas e *softwares* capazes de coletar informações, como é o caso da Construção de Perfis (*Profiling*), da mineração de dados (*Data Mining)* e do Sistema de avaliação de dados (*Scoring - ou Rating-System*) (MENDES, 2008).

Dessa forma, os meios utilizados para a coleta de dados podem gerar a diminuição da liberdade do indivíduo, pois a pessoa que é dona do dado pessoal acaba perdendo o controle sobre o que sabe sobre si mesma, tendo em vista que seus dados fazem parte da sua personalidade (DONEDA, 2010) e se tais dados são amplamente utilizados e disponibilizados, ela pode perder sua privacidade.

A sugestão de anúncios que são disponibilizados ao internauta com base nas suas pesquisas, podem expor suas buscas a outros usuários que dividem o mesmo computador que ele, por exemplo. Se esse computador é dividido entre um casal, e os dois possuem somente um usuário de entrada no computador e na internet, existirá a possibilidade de um saber o que outro busca na internet sem sequer precisar acessar o seu histórico de navegação, vale ressaltar que para saber disso não precisa ser um expert em *internet,* basta que a pessoa entenda a lógica com que os anúncios são disponibilizados pelos sites. Dessa forma, se a pessoa divide computador com alguém e quer manter em sigilo suas buscas, hoje em dia não basta apagar o histórico de

[14] Art. 6º São direitos básicos do consumidor:
[…] IV- a proteção contra a publicidade enganosa e abusiva, métodos comerciais coercitivos ou desleais, bem como contra práticas e cláusulas abusivas ou impostas no fornecimento de produtos e serviços; […] (BRASIL, 1990).

navegação do computador, pois seus dados já estão sendo refinados para voltar em forma de propaganda direcionada.

Algo importante a refletir, embora não seja o ponto essencial deste trabalho, é a maneira como a publicidade pode ter o poder de afetar negativamente o consumidor para além do debate sobre o direito à autodeterminação de seus dados pessoais. A publicidade também afeta o indivíduo na medida em que os consumidores de baixa renda possuem acesso a uma ampla rede de anúncio de produtos à venda, mas que não podem comprar devido a sua condição social; ou até mesmo aquele consumidor que não possui poder econômico para a compra, mas devido à facilidade com que o crédito é vendido no mercado, acaba comprando produtos que sequer precisa.

Essa enxurrada de anúncios afeta psicologicamente as pessoas, invade sua privacidade e vende seus dados, instiga ao consumismo desenfreado e, ainda por cima, coloca produtos no mercado com a vida útil reduzida propositalmente: a chamada "obsolescência programada". Em que "a vida útil do produto, é reduzida propositalmente pela indústria com o intuito de estimular o consumo e movimentar o mercado industrial" (NASPOLINI; ROSSINI, 2017, p. 54), sem nenhuma preocupação ambiental, visto que a maioria dos resíduos produzidos são descartados inadequadamente. Um sistema falho e que, infelizmente, muitos consumidores ainda não são capazes de observar o problema que isso trará para a nossa geração e as gerações futuras.

Por isso, é importante que o consumidor entenda como funciona a lógica de consumo e como ele (o consumidor) é importante para que o mercado continue em ascensão e, desta forma, continue lucrando.

### 2.3.1 Construção de Perfis

Essa técnica é utilizada com base em informações que a pessoa disponibiliza, seja na hora de realizar algum cadastro em um site ou com base nas informações colhidas normalmente por um software, podendo ser utilizada tanto para individualizar o perfil do usuário, como também para utilização com grupos (MENDES, 2008).

O usuário, ao ter suas informações colhidas, monitoradas e o seu perfil digital traçado, acaba perdendo o seu direito à privacidade, seu poder de decisão sobre o conteúdo das páginas que acessa, pois não tem liberdade de escolha sobre os anúncios que aparecem e não possui

autonomia para fazer tais assuntos cessarem. Visto que é uma tarefa muito difícil desabilitá-los dos sites.

### 2.3.2 Mineração de Dados

É através do acesso a dados brutos armazenados e o seu refinamento, que os serviços de publicidade conseguem ter acesso a consumidores em potencial e a estimativa desses consumidores em potencial através de informações especificadas pelo próprio, que fornece as suas preferências (sem saber que está fornecendo), por meio do seu acesso a sites e de suas buscas na internet (BORGES; VASCONCELOS, 2019). Um problema que deve ser levantado, ainda mais tomando em conta que a Lei Geral de Proteção de Dados já está em vigor, é o fato da obrigatoriedade que a empresa possui em deixar claro ao cliente que está utilizando esse tipo de tecnologia.

Como o seu objetivo é criar padrões a fim de que possibilite a classificação de pessoas ou objetos, essa técnica pode gerar um grande risco de analisar e classificar comportamentos de forma que possibilite a discriminação entre os consumidores na hora de tomada de decisão sobre qual será a finalidade das informações que foram extraídas, ou seja, o problema não é a tecnologia, mas sim como a estimativa de padrões será utilizada e, caso essa decisão gere algum tipo de discriminação, restará configurado um ato ilegal e estará ferindo o direito fundamental à igualdade resguardado pela Constituição Federal em seu artigo 5º[15] (MENDES, 2008).

### 2.3.3 Sistema de Avaliação de Dados Pessoais

Essa forma de avaliação permite à empresa identificar a potencialidade de compra dos seus consumidores sobre os produtos que ela vende. Segundo Mendes (2008), quando a empresa consegue identificar quem, dentre os seus consumidores possui maior potencial de compra, poderá investir em promoções estratégicas de fidelização desses clientes. Neste sentido, Mendes também chama atenção para a existência de um outro lado da moeda, pois, da mesma forma que a avaliação pode ser feita para identificar os melhores consumidores, também pode identificar os piores, o que abre margem à utilização do sistema de forma inadequada e

[15] Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: […] (BRASIL, 1988).

causar danos aos consumidores. Esse sistema de avaliação de dados também serve de base para serviços de disponibilização de crédito aos consumidores.

No mercado de crédito, a avaliação do consumidor servirá como base para definir se ele é um bom pagador ou não. O fornecedor terá amplo acesso a uma base de dados em que estará disponível o histórico de compras e histórico de dívidas.

Segundo Oliva e Viegas (2019), esse sistema de avaliação de risco de inadimplência será um fator levado em consideração pela empresa para definir se há possibilidade de concessão de crédito ao cliente e para definição do percentual de juros que será utilizado no contrato. Uma pessoa considerada boa pagadora, terá mais chances de ter a taxa de juros reduzida, em contrapartida, a pessoa considerada "má pagadora" terá grandes chances de ter o seu crédito recusado ou no caso de aceitação, a taxa de juros aumentada porque de acordo com o seu histórico de créditos, estará mais suscetível a não cumprir com a sua obrigação.

Para os autores, o cadastro considerado positivo será diferenciado do negativo, porque apresentará o histórico completo das compras realizadas pelo consumidor, enquanto o cadastro negativo mostrará os débitos vencidos e ativos do consumidor. Mister destacar que o artigo 43º[16] do CDC prevê o direito de acesso do consumidor às informações constantes em cadastros, registros e seus dados pessoais, resguardando o seu direito de não possuir informações negativas em seus cadastros com período superior a cinco anos e prevendo que a abertura de cadastro dever ser realizada mediante sua comunicação por escrito quando o mesmo não a solicitar.

Normalmente as empresas fazem análise de crédito utilizando o sistema denominado *credit scoring* ou pontuação de crédito em português. Isso acontece, segundo Cortazio (2019), porque as empresas baseiam-se na quantidade de informações disponíveis sobre o potencial comprador/tomador de crédito, portanto, quanto menos informações a empresa tiver sobre o consumidor, menor será a sua confiança para a disponibilização de crédito, e quanto mais informações disponíveis, maior será a probabilidade de o consumidor ser bom pagador.

Como não havia uma lei que cuidasse da regulamentação dos bancos de dados com informações de adimplemento dos consumidores, a lei nº 12.414/2011 chamada de Lei do

[16] Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.
§ 1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.
§ 2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele […]. (BRASIL, 1990).

Cadastro Positivo, entrou em cena para regular a formação e consulta a bancos de dados com informações de adimplemento para formação de histórico de crédito.

Quanto aos bancos de dados, a lei acertadamente específica em seu artigo 3º e parágrafos seguintes[17], que somente poderão ser armazenadas informações claras, objetivas, verdadeiras e de fácil compreensão, além de definir o que seria cada uma dessas informações e proibir anotações de informações sensíveis e excessivas. A LGPD, embora tenha entrado em vigor anos após a promulgação da Lei do Cadastro Positivo, traz a previsão em seu artigo 7º[18], da realização do tratamento de dados pessoais para a proteção de crédito, o que de acordo com Cortazio (2019) reconhece a existência de interesse legítimo no tratamento de dados pessoais para análise da concessão de crédito, à medida que permite o compartilhamento desses dados com outras entidades de proteção ao crédito.

### 2.3.4 Cookies

Talvez o internauta tenha notado que ultimamente é preciso autorizar uma tal "política de privacidade" ou "política de cookies" para que consiga ter acesso a determinados sites. Essa foi a maneira encontrada pelos sites após a entrada em vigor da Lei Geral de Proteção de Dados. Isso ocorre porque a utilização de cookies tem a finalidade de armazenar informações pessoais e, como as informações pessoais são protegidas pela LGPD, os sites possuem o dever de atuar em consonância com a lei, sob risco de sofrer penalidades. Neste momento, o intuito não será analisar a Lei Geral de Proteção de Dados, pois ela será objeto de análise no próximo capítulo,

---

[17] Art. 3º Os bancos de dados poderão conter informações de adimplemento do cadastrado, para a formação do histórico de crédito, nas condições estabelecidas nesta Lei.
§ 1º Para a formação do banco de dados, somente poderão ser armazenadas informações objetivas, claras, verdadeiras e de fácil compreensão, que sejam necessárias para avaliar a situação econômica do cadastrado.
§ 2º Para os fins do disposto no § 1º consideram-se informações:
I - objetivas: aquelas descritivas dos fatos e que não envolvam juízo de valor;
II - claras: aquelas que possibilitem o imediato entendimento do cadastrado independentemente de remissão a anexos, fórmulas, siglas, símbolos, termos técnicos ou nomenclatura específica;
III - verdadeiras: aquelas exatas, completas e sujeitas à comprovação nos termos desta Lei; e
IV - de fácil compreensão: aquelas em sentido comum que assegurem ao cadastrado o pleno conhecimento do conteúdo, do sentido e do alcance dos dados sobre ele anotados.
§ 3º Ficam proibidas as anotações de:
I - informações excessivas, assim consideradas aquelas que não estiverem vinculadas à análise de risco de crédito ao consumidor; e
II - informações sensíveis, assim consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas (BRASIL, 2011)

[18] Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
[…] X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente. […] (BRASIL, 2018)

trataremos de explicar a definição de cookie e como funciona a sua utilização pelas páginas da internet.

De forma resumida, os cookies são pequenos arquivos de dados que ficam armazenados no computador do usuário quando ele visita determinada página da web e que permitem que o servidor tenha acesso aos registros que lá estão armazenados, são esses dados armazenados que irão auxiliar na criação de perfis dos usuários (BASAN, 2021). O autor também vai dizer que as regras do CDC e da LGPD não admitem o uso automático dos cookies em desfavor do consumidor sem que o consumidor tenha acesso a informação da finalidade a que serão submetidos e sem que o consumidor tenha consentido com essa utilização.

O que vinha acontecendo antes da entrada em vigor da LGPD, embora já existisse previsão legal pela lei do MCI sobre a proteção dos dados pessoais e o direito do usuário a ter seus dados pessoais resguardados sem que sejam fornecidos a terceiros, incluindo o acesso a registros de conexão e acesso a aplicações de internet sem autorização, é que os sites continuavam a utilizar dessa ferramenta sem que o consumidor tivesse ciência disso. Os sites até então não haviam se preocupado em ter o consentimento expresso do usuário e a finalidade a que seriam submetidos os cookies, porque até então não existia uma lei que regulamentasse de fato o uso dos dados pessoais, que até então vinham sendo utilizados indiscriminadamente e sem prévia autorização do usuário/consumidor.

Cumpre salientar, que a finalidade original da utilização de cookies, segundo Watfe (2006) era tornar a navegação mais cômoda e flexível pela WWW[19], mas que essa lógica foi alterada quando os responsáveis das páginas web identificaram que poderiam utilizá-los para rastrear seus visitantes. Com essa nova lógica, os cookies passaram de meros auxiliadores dos usuários na web, para potenciais vigilantes do comportamento dos usuários.

Em relação a utilização de cookies, os usuários também possuem a alternativa de bloqueá-los através do seu navegador. Basta saber qual o nome do seu navegador e pesquisar em algum site de busca o passo a passo para mudar as configurações dos cookies e bloqueá-las. No entanto, Barreto (2015) chama atenção para o fato de que as empresas, sabendo dessa facilidade de exclusão por parte do usuário, desenvolveram uma nova técnica para captação de dados: os "*flash cookies*". Sendo a principal diferença entre eles o modo de operação, pois

[19] A internet era uma rede restrita à academia e ao governo antes do desenvolvimento do World Wide Web (conhecido também como WWW, ou Web). O WWW foi desenvolvido em 1989, no laboratório Europeu de Física de Altas Energias (PAESANI, 2013) e consistia em "[…] uma combinação de conteúdos e de referências a outros documentos. Essas referências ou *hyperlinks* podiam apontar para outro ponto da mesma página, para outra página armazenada no mesmo local, o sítio (website ou site) ou para uma página em qualquer outro lugar da rede (ou, diríamos hoje, do mundo virtual)" (LINS, 2013, p. 24).

enquanto o cookie tradicional pode ser facilmente removido através do navegador pelo usuário, o flash cookie torna a sua remoção muito mais difícil.

De acordo com Avelino (2019), foi a empresa de publicidade on-line United Virtualities que em 2005 anunciou o desenvolvimento de um sistema protegido contra ferramentas de exclusão de cookies, isso porque a empresa estava apreensiva com um estudo que apontava que mais de 30% dos usuários de internet naquela época já estava excluindo os cookies ao menos uma vez por mês.

O ramo da publicidade é um mercado que lucra muito e, que segundo Pesquisa realizada pela empresa Deloitte, foi responsável por R$ 418,18 milhões no Produto Interno Brasileiro- PIB em 2020. Essas empresas sempre estarão em busca de novas ferramentas que possibilitem o aumento de seus lucros, o que em contrapartida, reforça a necessidade de regulamentação por parte do legislador de mecanismos que atenuem a vulnerabilidade dos consumidores.

Mas não são todos os cookies que possuem a finalidade de rastreamento, também existem os cookies que são essenciais à web, como é o caso dos que identificam o usuário, dos cookies de segurança (que previnem fraudes online), os que guardam as senhas (MENDES, 2008). Após a entrada em vigor da LGPD, os sites têm avisado antes do acesso dos usuários ao site, quais tipos de cookies utilizam e dão a opção de aceitação ou não, mas não são todos. O site da figura 1, por exemplo, só deixa claro que utiliza cookies para estatísticas de visita e melhora da experiência de navegação do usuário, dando a opção de clicar em "política de privacidade" para saber mais.

Os sites que disponibilizam quais tipos de cookies utilizam e dão a opção de o usuário aceitá-los ou não, normalmente deixam claro que utilizam cookies: essenciais, para publicidades e alguns para estatísticas e podem condicionar o acesso ao site através da aceitação dos cookies. Ramos explica em seu guia como isso pode ocorrer:

> (i) o consentimento implícito – aquele aviso de *cookies* em que o usuário "ao navegar pelo site/aplicativo, aceita automaticamente" – dificilmente será considerado uma boa prática adequada, salvo para cookies essenciais – aquelas *tags* que são estritamente necessárias para o funcionamento da aplicação, como, por exemplo, identificadores que otimizam performance de vídeos ou que previnem fraudes online;
> (ii) mesmo no caso de cookies essenciais, é importante que o aviso de cookies descreva claramente para o usuário que esses identificadores serão utilizados ao utilizar o site ou aplicativo, de forma a permitir o direito de escolha do usuário em não acessar determinada aplicação;
> (iii) embora cookies de publicidade sejam essenciais para financiar as atividades de certos sites e aplicativos e, logo permitir o acesso gratuito pelos usuários, várias autoridades europeias já se posicionaram no sentido de que identificadores de marketing não podem ser considerados cookies essenciais. Todavia, nada impede que

> os *publishers* neguem acesso a usuários que utilizem-se de *adblockers* ou que não aceitem cookies de publicidade, abordagem que tem sido adotada por grandes veículos como o Washington Post (2019, p. 13);

Os cookies podem ser boas ferramentas aos usuários, se utilizados apenas com o intuito de auxiliá-lo – essa era a ideia dos seus precursores. Eles auxiliam o usuário à medida que armazenam as senhas de acesso a determinados sites, exemplo: facebook, instagram, sites de compras como a shopee, gov.br, e-mail e a também servem para personalização de serviços (MENDES, 2008).

O seu uso torna-se preocupante à medida que as empresas passam a utilizá-los como ferramenta para diferenciar os consumidores, discriminá-los e aumentar o lucro das empresas de forma indevida. Um claro exemplo disso no Brasil, foi o caso da condenação da empresa Decolar.com pelo Departamento de Proteção e Defesa do Consumidor (DPDC) em esfera administrativa. A empresa foi condenada em esfera administrativa ao pagamento de multa no valor de R$ 7.500.000,00 (sete milhões e quinhentos mil reais), ao utilizar as técnicas de *geo-blocking*[20] e *geo-pricing*[21]*,* que além de discriminar o consumidor com base nos critérios de localização, também pode ser considerada uma prática desleal de mercado (GUIMARÃES, 2019).

## 3 A PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

Como citado anteriormente, ao consumidor foi reconhecida a condição de vulnerabilidade nas relações de consumo, o que lhe confere tratamento diferenciado a fim de atenuar a relação de disparidade existente entre ele e o mercado. O ambiente digital abriu as portas para o mercado de compra e venda de bens e serviços realizados de forma totalmente virtual. Esse novo mercado, além de proporcionar a compra e venda de bens físicos, fundamenta-se também na compra e venda de informações que são em sua grande maioria deixadas por seus próprios usuários.

Essas informações são de fácil acesso, conforme explicado no capítulo anterior, por causa do desenvolvimento de técnicas que proporcionam o rastreio e tratamento desses dados, pois é dessa forma que eles se tornarão informações úteis aos vários setores do mercado – em

[20] Geo-pricing (geo-precificação) é uma técnica para analisar o perfil de compras do consumidor e variar os preços dos produtos a partir da localização do usuário (CAMURÇA, 2021).

[21] Geo-blocking (bloqueio geográfico) é realizado para que determinados consumidores não tenham acesso a alguns serviços de acordo com a sua região geográfica (CAMURÇA, 2021).

especial o Marketing. O rastro deixado pelos usuários nada mais são do que características pessoais, tais como: seu gosto por determinadas comidas, músicas, sua preferência por determinados produtos.

O usuário, ao passo que faz parte dessa rede de conexões, tem através do seu aparelho uma identificação no ambiente digital que se difere do que é conhecido tradicionalmente como Cadastro de Pessoa Física (CPF) ou Registro Geral (RG). Sua identificação ocorre através do IP (internet protocol ou protocolo de rede traduzindo ao português), "a carteira de identidade do computador na rede" (PAPA, 2011, p. 1), é essa identificação que tornará as ações do usuário identificáveis na internet.

Em relação a definição de dados pessoais, Doneda e Machado (2018) trazem duas conceituações a respeito: a conceituação restrita e a conceituação ampla. A restrita seria a exibição de fato sobre uma pessoa individualizada e identificável, podendo essa identificação ocorrer a partir de elementos de informação chamado de identificadores diretos ou indiretos. Os diretos referem-se ao primeiro sinal que diferencia a individualidade da pessoa e os indiretos seriam aqueles elementos complementares necessários para distinção da pessoa quando os elementos diretos são o bastante para individualizá-la. Em relação ao conceito amplo, esse terá caráter de informação pessoal quando a pessoa mesmo que não seja diretamente identificada, possa eventualmente ser individualizada e, portanto, identificável. Os autores também explicam que existem dados que a primeiro momento podem não ser identificáveis, mas caso sejam tratados com técnicas e dados de apoio, podem também levar a identificação do titular dos dados.

Os autores chamam a atenção para o fato de que a Lei Geral de Proteção de Dados (lei nº 13.709/2018), adotou a conceituação ampla de dados pessoais ao especificar em seu artigo 5º, inciso I que o dado pessoal é a "informação relacionada a pessoa natural identificada ou identificável" (BRASIL, 2018).

## 3.1 A PROTEÇÃO DOS DADOS PESSOAIS COMO DIREITO FUNDAMENTAL – EMENDA CONSTITUCIONAL Nº 115 DE 2022

Muito embora o legislador tenha levado alguns anos para falar sobre a necessidade da proteção de dados no Brasil, não é recente o debate sobre sua extensão ao rol de direitos fundamentais previstos pela Carta Magna. A proteção de dados pessoais é antes de tudo, matéria relacionada aos vários direitos fundamentais expressos pelo artigo 5º da CRFB/88, tais como: proteção à vida e à intimidade (art. 5º, inciso X); a inviolabilidade do sigilo de dados

(art. 5º, inciso XII) e, como a exposição dos dados pode ocasionar discriminação e preconceitos, a proteção de dados é resguardada pela proteção do Estado quando prevê em seu art. 3º, inciso IV da CRFB/88.

O ordenamento jurídico brasileiro, segundo Doneda (2011) traz garantias à liberdade de expressão e ao direito à informação, que precisam ser observadas ao passo que não extrapolem e confrontem a proteção da personalidade e o direito à privacidade. É necessário que, via de regra, hajam barreiras entre a amplitude do direito à informação e a informação de caráter pessoal de cada indivíduo, pois, quando tratamos de informação pessoal, estamos falando da vida e de traços de personalidade do cidadão, informações que não podem estar abertas ao acesso de todos. Quando tratamos de informações pessoais, cabe ao indivíduo consentir quais informações sobre a sua vida podem ser acessadas por terceiros ou não – importante deixar claro que esse limite de acesso às informações pessoais sobre o direito à privacidade diz respeito àquelas informações que não impliquem na vida de outro indivíduo e que não prejudiquem a liberdade individual de outras pessoas, ou seja, com ressalva as exceções encontradas no ordenamento jurídico (em caso de crimes, acesso a dados sigilosos que sejam fundamentais a uma pretensão jurisdicional e etc.).

Dada a relevância do tema, em 2019 houve a Proposta de Emenda à Constituição nº 17/2019 pelo Senado Federal de autoria do Deputado Eduardo Gomes (MDB/TO). A proposta teve o intuito de garantir a proteção de dados pessoais no Brasil como direito fundamental previsto pelo art. 5º da CRFB/88. Um dos fundamentos dessa proposta, segundo o Deputado Eduardo Gomes, é o fato de que vários outros países já possuem legislação que contornam os limites da utilização dos dados pessoais e resguardam o usuário do uso indevido de seus dados pessoais (BRASIL, 2019a)

A União Europeia, por exemplo, há anos vem tratando da regulação dos dados pessoais. Bioni (2021) fala sobre a trajetória do consentimento nas leis gerais de proteção de dados através das gerações de leis que continuam em constante evolução até os dias de hoje, tendo já na década de 80 o Direito Comunitário Europeu normatizado pela primeira vez a proteção dos dados pessoais. Segundo ele, até mesmo o preâmbulo desta norma relacionou a liberdade do fluxo informacional com a proteção dos dados pessoais, que correlaciona até hoje esse entendimento na Diretiva de Europeia de Proteção de Dados 95/46/ EC. Ainda segundo Bioni, a Diretiva Europeia traduz em normas específicas a garantia de controle das informações aos indivíduos, sendo adotada a sua autodeterminação como parâmetro da licitude ou não, de

qualquer operação de tratamento dos dados pessoais, para além do indivíduo, ela também impõe ao processador dos dados pessoais deveres de aperfeiçoamento como estratégia de regulação.

O projeto da PEC teve sua aprovação e passou a vigorar a Emenda Constitucional nº 115/2022, que acrescentou ao artigo 5º, o inciso LXXIX com a seguinte redação: "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais"; acrescentou ao artigo 21 o inciso XXVI para atribuir à União a competência para organizar e fiscalizar sobre os dados pessoais: "organizar e fiscalizar a proteção e o tratamento de dados pessoais, nos termos da lei" e definiu em seu artigo 22 com o acréscimo do inciso XXX, a competência privativa da União em legislar sobre: "proteção e tratamento dos dados pessoais", vale lembrar, que esse artigo em seu parágrafo único prevê que os Estados estarão autorizados a legislar sobre questões específicas da matéria de proteção e tratamento dos dados. Essa Emenda Constitucional entrou em vigor em quando da sua publicação no Diário Oficial da União, em 11 de fevereiro de 2022 (BRASIL, 2022).

Durante a tramitação da PEC, audiências públicas foram realizadas e alguns estudiosos da área de proteção de dados pessoais foram convidados para debater sobre o assunto, dentre eles, alguns autores citados no presente trabalho: Laura Schertel Mendes, Bruno Ricardo Bioni e Danilo Doneda. Laura posicionou-se a favor da criação de inciso separado no artigo 5º da CRFB/88 para a proteção de dados em razão de sua autonomia; Bruno também se posicionou a favor de um inciso separado e indicou que no texto deveria constar a necessidade de uma agência reguladora no texto; Danilo expôs que a União deveria ter a competência privativa para legislar (BRASIL, 2019b).

A proteção de dados pessoais, então passa a ser delineada no ordenamento jurídico brasileiro ao ser definida expressamente como direito fundamental e tornando-se um elemento individual intrínseco ao ser humano, resguardado pela Constituição e que não poderá sofrer alterações ou modificações por parte do Estado. Sarlet (2018) vai dizer que é por opção do Constituinte que determinado direito é bem jurídico relevante a ponto de ser determinado como direito fundamental, exercendo função garantida e decisiva no regime democrático contra desvios que possam ser exercidos pela maioria no poder, podendo serem considerados simultaneamente "pressuposto, garantia e instrumento do princípio democrático de autodeterminação do povo por meio de cada indivíduo" (SARLET, 2018, p. 62)

Essa autonomia da proteção dos dados pessoais conferiu à União o dever de garantia da proteção dos dados pessoais, além de abrir margem ao surgimento de leis complementares autorizando os Estados a legislarem as suas especificidades (art. 22, parágrafo único). Cumpre

salientar, que antes mesmo dos dados pessoais terem entrado expressamente no rol de direitos fundamentais, o STF já os havia reconhecido como direito fundamental, diante do julgamento de Ações Diretas de Inconstitucionalidade que versavam sobre a inconsistência da Medida Provisória nº 954/2020 que autorizava o compartilhamento com o IBGE dos dados pessoais dos usuários de telefonia (o número de telefone e o endereço residencial), durante a situação de emergência pública de Covid-19[22] (FOLLONE; SIMÃO FILHO, 2020). O entendimento firmado pela Suprema Corte foi de suspender a eficácia da PEC, pois o compartilhamento de dados pessoais previstos pela Medida Provisória violaria direitos constitucionais, tais como: direito à intimidade, ao sigilo de dados, e à privacidade, violando, portanto, os dispositivos constitucionais que asseguram a dignidade da pessoa humana (LANZILLO; OLIVEIRA, 2021).

Doneda (2020), já falava sobre o problema que seria encontrado caso a proteção de dados pessoais fosse derivada da privacidade, visto que a distância existente entre ambas limitaria o alcance da tutela dos dados pessoais e sua interpretação seria abordada de forma restrita, levando em conta que os fundamentos da proteção aos dados estariam restritos ao momento da comunicação, o que não alcançaria a informação e sua complexidade.

Essa Emenda Constitucional, portanto, foi um marco para o Brasil. Pois, o desenvolvimento tecnológico anda a passos largos à medida que o acesso à internet no país é cada vez mais ampliado e acessível à grande parte da população, de modo que os consumidores tenham seus dados protegidos e seu consentimento seja o principal instrumento que possibilite tais dados serem utilizados por terceiros.

## 3.2 INFORMAÇÃO PESSOAL E DADOS PESSOAIS

Como citado anteriormente, a informação está presente em todos os setores da sociedade graças ao avanço das tecnologias da informação. Paesani (2013), fala da importância do acesso à informação e como a democracia está comprometida com o modo que as informações circulam. Para ela, em um processo democrático, o grau de democracia pode ser medido pela quantidade e qualidade de informações recebida nesse processo, pois, quanto maior

[22] Art. 1º Esta Medida Provisória dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras do Serviço Telefônico Fixo Comutado - STFC e do Serviço Móvel Pessoal - SMP com a Fundação Instituto Brasileiro de Geografia e Estatística - IBGE.
Parágrafo único. O disposto nesta Medida Provisória se aplica durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020. VIGÊNCIA ENCERRADA (BRASIL, 2020).

a disponibilidade de informação e maior a quantidade de sujeitos que as recebe, melhor será o seu desenvolvimento.

Paesani (2013) ressalta que a liberdade informática, por mais vasta que seja, precisa encontrar limites que garantam o desenvolvimento dos direitos fundamentais dos sujeitos e da sociedade. É de extrema importância que exista uma delimitação sobre essa amplitude da informação quando atingir a esfera individual dos sujeitos de direito, sendo necessário diferenciá-la da informação pessoal que é intrínseca a cada ser humano.

Dentro da esfera da informação pessoal, há uma diferença entre as palavras "dado" e "informação". Doneda (2011) vai explicar os requisitos que devem ser observados para a caracterização de uma informação como pessoal, sendo possível sua identificação através de um vínculo direto existente entre a pessoa e a revelação de algo sobre ela, que pode referir-se às suas características ou suas ações. Segundo o autor, será considerada informação pessoal quando a informação estiver vinculada diretamente a uma pessoa e revelar algo objetivo sobre ela. Em contrapartida, o "dado" estaria associado a uma "pré-informação" que antecede a interpretação da informação.

Portanto, compreende-se que os termos "dado" e "informação" fazem parte de um processo em que o dado fornecido em primeiro momento precisa ser organizado/estruturado a fim de tornar-se uma informação e que essa informação para ser considerada pessoal precisa ter a ver com as características ou ações pessoais do próprio sujeito.

A partir da delimitação de informação pessoal e partindo do pressuposto que a internet abriu caminhos para que as informações sejam disponibilizadas a qualquer tempo, de modo permanente e sem necessitar de autorização (LEONARDI, 2011), surgiu a necessidade de que o Estado regulasse a utilização dos dados pessoais:

> A proteção de dados pessoais surgiu justamente como forma de regular a utilização da informação pessoal durante o seu tratamento, isto é, nas várias operações às quais ela pode ser submetida após ter sido colhida por uma forma qualquer. Perdido o vínculo que poderíamos descrever como "físico" com seu titular, portanto, a informação pessoal manter-se-ia vinculada a ele através de um vínculo jurídico, determinados pelas normas de proteção de dados pessoais e justificadas pela identidade desta informação com a pessoa (DONEDA, 2010, p. 40).

Esse vínculo jurídico foi firmado pela Lei Geral de Proteção de Dados quando trouxe a garantia do direito à autodeterminação informativa ao titular dos dados pessoais. Em relação a compreensão da autodeterminação, ela "corresponde a uma espécie do direito à privacidade, na qual o indivíduo se mostra capacitado e informado o suficiente para exercer sua liberdade

de decisão acerca do tratamento efetuado junto aos seus dados" (FONSECA; NOGUEIRA, 2020, p. 22).

É a partir do momento que os dados dos sujeitos não podem mais ser expostos indiscriminadamente, que o Brasil passa a proporcionar maior segurança jurídica e, consequentemente, passa a ser visto por outros países os quais possuem legislação de proteção de dados mais desenvolvida que a nossa, como um país seguro para seus cidadãos realizarem transações on-line internacionalmente.

O tratamento de dados pessoais é um processo que compreende a captação dos dados (a empresa ou o controlador obtém informações pessoais do consumidor), o seu processamento (em que os dados são refinados através de técnicas que os modificam e transformam em informações úteis para a empresa) e a divulgação dos dados (a depender a finalidade) (MENDES, 2008).

Além disso, é importante entender a delimitação do conceito de dado pessoal, o que segundo Doneda e Machado (2018) será essencial para que haja a devida interpretação das leis de proteção de dados e quais serão os limites previstos em lei da sua aplicação. Segundo os autores, as estruturas legislativas dos países utilizam abordagens distintas de técnicas para conceituação de dados pessoais, eles explicam a existência da construção de conceituação restrita e conceituação ampla.

Na conceituação restrita, o dado pessoal será fatos sobre alguém que podem ser reconhecidos e identificados em meio a um grupo ou coletividade, através de um processo de identificação denominado de identificadores. Esses identificadores podem ser diretos ou indiretos. Diretos quando forem o primeiro sinal que identifique e individualize a pessoa – o nome da pessoa. Já o identificador indireto, são os elementos que compõem a individualidade da pessoa e possibilitam distingui-la quando o identificador direto não for suficiente para essa distinção – o número do CPF, a nacionalidade, o endereço. Essa conceituação, caso seja adotada, poderá ter seus identificadores especificados pela lei.

Quanto à conceituação ampla, essa é definida quando o alcance dos dados pessoais é estendido para dados que em primeiro momento não individualizam e identificam a pessoa, mas que possuem potencial de identificação caso sejam tratados com técnicas acessíveis que em conjunto com dados suplementares podem identificar o titular dos dados. A conceituação adotada pelo direito brasileiro, segundo os autores, é a ampla tendo como base a orientação europeia tendo sido especificada na Lei Geral de Proteção de Dados em seu artigo 5º, I[23].

[23]Art. 5º Para os fins desta Lei, considera-se:

As tecnologias de hoje permitem que os dados armazenados em bancos de dados de consumo – diga-se dados colhidos do próprio consumidor virtualmente – sejam facilmente organizados, estruturados e disponibilizados para o mesmo consumidor que os cedeu (sem saber) em forma de propaganda e publicidade. Embora muito recente a legislação que trata da proteção desses dados, parece que as empresas estão tomando um pouco mais de cuidado com a propagação dos dados de seus clientes, até mesmo aquelas empresas ligadas a área da saúde e que atendem em local físico[24] – a LGPD abrange o tratamento de dados pessoais em meio físico também – que na hora do atendimento de seus clientes lhes dão um termo informando a finalidade a que serão submetidos os dados pessoais de seus pacientes e que até mesmo deixam acessível no site uma política de privacidade de leitura acessível e fácil entendimento.

## 3.3 BANCO DE DADOS PESSOAIS

Um banco de dados é um conjunto de informações estruturadas e organizadas, com critérios determináveis, podendo ser manual ou automatizado, de maneira que facilite uma pesquisa (MENDES, 2008) e que o conhecimento advindo dele possa revertido para tomada de alguma decisão, essa decisão, por exemplo, pode facilitar a identificação do perfil de um consumidor em potencial (BIONI, 2021).

A partir da evolução da informática, os bancos de dados tiveram um novo sentido sobre a importância e a finalidade do armazenamento de informações, eles tornaram-se aliados dos fornecedores de bens e serviços facilitando seu relacionamento com um alto fluxo de pessoas (WATFE, 2006).

Toda essa evolução tecnológica demorou a ser alcançada por uma lei brasileira que regulamentasse o armazenamento e a divulgação desses dados, mesmo que o CDC já previsse normas para a utilização de bancos de dados e cadastros de consumo. Segundo Bioni (2021), a Seção VI do Código de Defesa do Consumidor que trata sobre os bancos de dados e cadastros de consumo e a suas características construídas doutrinariamente, deixam de fazer sentido na sociedade da informação, isto porque, o fluxo de informações torna-se constante e acaba excedendo os elementos caracterizadores utilizados pela própria doutrina para diferenciá-los, isso tendo em vista que os dados agora são coletados a todo momento, de inúmeras fontes e por pessoas que podem ser alheias ou não à relação de consumo. Além do mais, o autor explica que

---

I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável […] (BRASIL, 2018)

[24] A Policlínica São Lucas (clínica e Hospital situada em Palhoça/SC), possui uma política de privacidade de fácil entendimento em seu site, além de disponibilizar aos pacientes um termo de consentimento na hora da consulta que explica a finalidade a que serão submetidos os seus dados (SÃO LUCAS CLÍNICA E HOSPITAL, 2021).

essa facilidade de armazenamento de informações pôde ser proporcionada pelo progresso tecnológico, que contribuiu para a redução dos custos de armazenamento de informações.

E, se hoje existem muitos bancos de dados pessoais com alta capacidade de armazenamento de informações e a todo momento, é graças ao desenvolvimento das tecnologias. Ademais, o interesse pelos dados pessoais de consumidores no ambiente virtual só é possível por causa do surgimento do mercado eletrônico e da facilitação do acesso à internet aos cidadãos – sem o consumo pelo meio digital, o armazenamento de dados para posterior utilização em estatísticas e propagandas não teria lógica.

A lucratividade da venda desses dados pessoais fez com que surgisse a indústria dos *data brokers* (corretores de dados), segundo Bioni (2021), não é a única indústria que surgiu com essa finalidade, pois, não surgiu com essa finalidade, pois, existe a organização de uma rede colaborativa para a entrega desse tipo de informação que envolve diversas empresas. O autor comenta que em relação aos *data brokers*, o foco inicial dessa indústria era no setor financeiro, entretanto, com o surgimento do comércio de publicidade comportamental, a indústria expandiu-se para esse ramo no intuito de reunir pedaços de informações de várias fontes e revender os dados pessoais.

No Brasil, a Mosaic Brasil, uma plataforma do Serasa Experian[25], é um exemplo de data broker utilizado para classificar a população (CAMURÇA, 2021), tendo em vista que "classifica a população brasileira com base nas mais recentes variáveis sociodemográficas, econômicas, financeiras e comportamentais" (SERASA EXPERIAN, s.d.) e os dados extraídos dessa classificação são revendidos às empresas para que otimizem suas vendas.

## 3.4 MANIPULAÇÃO DOS DADOS PESSOAIS

Se a sociedade atual se baseia no uso de informações para a realização dos mais diversos serviços que possam existir – para tudo há armazenamento de dados – não foi à toa que o Estado entendeu necessário criar uma categoria de direitos previstos em legislações específicas para garantir que tais informações não sejam utilizadas indiscriminadamente.

Dada a importância da utilização dos dados pessoais em um mercado digital em que a informação tornou-se um dos produtos mais valiosos, não é novidade que sua utilização de forma indiscriminada eleva o risco de discriminação entre os consumidores, e a facilidade de manipulação da vontade de escolha dos usuários, como, por exemplo, vender aos usuários

[25] Serasa Experian é uma empresa que faz análises de créditos e capta informações para que outras empresas possam fornecer crédito aos seus consumidores.

propostas que lhe são agradáveis a fim de conseguir votos para uma eleição, gerando, dessa forma, uma série de problemas à democracia de um país e influenciando em diversas áreas da sociedade. Problemas à democracia, porque os eleitores são manipulados por máquinas que traçam o seu perfil e lhes apresentam ideias condizentes com aquilo que acreditam, isso através de propagandas e propostas eleitorais:

> Com este tipo de manipulação, os robôs criam a falsa sensação de amplo apoio político a certa proposta, ideia ou figura pública, modificam o rumo de políticas públicas, interferem no mercado de ações, disseminam rumores, notícias falsas e teorias conspiratórias, geram desinformação e poluição de conteúdo, além de atrair usuários para links maliciosos que roubam dados pessoais, entre outros riscos (MAGRANI, 2019, p.165).

A Cambridge Analytica, empresa que realiza consultoria política, foi denunciada por realizar a utilização indevida de dados de usuários do Facebook, a fim de orientar a posição política de seus usuários para a Campanha de Donald Trump (BARUFI *et al*, 2021). Para que essa orientação aconteça, a empresa utiliza um algoritmo capaz de manipular a opinião política dos eleitores pela análise de seus perfis, determinando traços de sua personalidade, isso para que possa direcionar conteúdo de manipulação política (MAGRANI, 2019).

Essa empresa é um grande exemplo de como o comportamento do consumidor/ usuário/eleitor, pode ser manipulado a ponto de afetar a escolha do indivíduo para direcionamento das mais variadas de propagandas no mercado de consumo e, até mesmo, para espionagem de chefes de Estado como a revelação de Edward Snowden de que a Agência de Segurança Americana estavam vigiando e coletando dados de líderes de Estado, tais como Angela Merkel (primeira-ministra alemã) e a presidente do Brasil Dilma Rousseff (VALENTE, 2019).

Um outro método de manipulação, é o caso da divulgação de notícias falsas na internet, conhecidas popularmente por seu termo em inglês “fake news”. Essas notícias falsas ou distorcidas sobre determinados acontecimentos ou sobre determinadas pessoas, ocasiona desinformação generalizada e faz as pessoas perderem a autonomia sobre suas decisões (MARTINS; TAKEONI, 2019). A consequência disso é que mesmo que tais notícias tenham sua falsidade confirmada, as pessoas acabam ficando desacreditadas e sem saber em quem confiar, o que a depender do viés da notícia, pode trazer graves consequências até mesmo para a própria pessoa – como é o caso da divulgação de fake news sobre a eficácia das vacinas contra

a Covid-19, que faz com que muitas pessoas no Brasil deixem de se imunizar[26] – e até mesmo para uma eleição, pois mesmo que comprovadas as fake news sobre determinado candidato, corre o risco população continuar com a confiança abalada e restar prejudicada a reputação do candidato.

Interligando o caso das fake news à manipulação de dados, é possível que os métodos de análise comportamental já utilizados para traçar o perfil dos eleitores a fim de saber suas preferências, sejam utilizados como base para criação e redirecionamento de notícias falsas contra o adversário político, causando uma série de desdobramentos à democracia e a liberdade de escolha de cada cidadão. A partir do que foi esclarecido nesse tópico, podemos constatar que a proteção dos dados pessoais de cada indivíduo, alcança muito mais que a sua individualidade, ela traz mecanismos que em larga escala auxiliam o processo democrático e a liberdade da coletividade de eleitores.

## 3.5 O CÓDIGO DE DEFESA DO CONSUMIDOR E A PROTEÇÃO DA RELAÇÃO DE CONSUMO

O CDC é aplicável a toda e qualquer relação de consumo, seja no ambiente virtual ou no ambiente físico – não trataremos sobre como a relação consumerista ocorre e a definição de consumidor e fornecedor, pois já definida no tópico 3 e sobre o princípio da vulnerabilidade do consumidor, pois explanado no tópico 2 –, carregando consigo princípios gerais a fim garantir equilíbrio nas relações de consumo e efetivar a proteção do consumidor como parte mais fraca da relação de consumo, pois o fornecedor é quem detém maior poder sobre os bens e produtos.

No intuito de amparar as relações de consumo, trouxe um rol de direitos básicos em seu art. 6º[27], dentre os quais estão a proteção contra a publicidade enganosa ( inciso IV) e o direito à informação adequada e clara sobre os produtos e serviços (inciso III) (BRASIL, 1990), mas que segundo Theodoro Júnior (2021), não trata-se de rol taxativo porque tais direitos não

[26] Várias são as notícias falsas, mas dentre elas, algumas têm sido objeto aceitação por uma boa parte da população, tais como: a modificação do DNA de quem toma a vacina; a existência de um chip líquido e inteligência artificial para controle da população e várias outras notícias absurdas (LORENZETTI; VERDUM, 2022).

[27] Art. 6º São direitos básicos do consumidor:
I - a proteção da vida, saúde e segurança contra os riscos provocados por práticas no fornecimento de produtos e serviços considerados perigosos ou nocivos;
II - a educação e divulgação sobre o consumo adequado dos produtos e serviços, asseguradas a liberdade de escolha e a igualdade nas contratações; (BRASIL, 1990).

excluem outros direitos advindo de outras legislações, regulamentos, tratados ou convenções, estando essa previsão expressa no art. 7º[28] do CDC.

Do rol previsto no art. 6º, destacamos alguns incisos que possuem influência na relação de consumo virtual. O inciso III – pincelamos algumas considerações a respeito da vulnerabilidade informacional no tópico 2.1 –, porque trata-se de direito do consumidor de ser informado de forma clara e adequada a respeito dos produtos e serviços, o que em tese deveria garantir ao consumidor no ambiente virtual o acesso a todas as informações do produto anunciado. Isso porque o consumidor na relação de consumo digital só visualiza a oferta por meio de imagens e textos e qualquer informação omissa pode acarretar na frustração do consumidor (SANTOS; SILVA, 2011).

O consumidor também é protegido contra a publicidade enganosa (art. 6º, IV), o que no ambiente virtual pode tornar-se uma prática muito comum, tendo em vista que a relação não permite um contato maior com o fornecedor e dessa forma o consumidor pode ser facilmente enganado e induzido ao erro. Theodoro Júnior (2021), enfatiza que o artigo 30[29] tratará da proteção do consumidor com relação a oferta e vinculá-la ao fornecedor que será responsabilizado sobre ela. Ainda em relação à publicidade, o art. 37[30] proíbe qualquer forma de publicidade enganosa, inclusive quando omitir alguma informação ou dado que seja essencial ao produto ou serviço.

O CDC teve sua previsão na Carta Magna, que garante a proteção do consumidor no rol de direitos fundamentais da CRFB/88 (art. 5º, XXXII) – já citado alhures no tópico 2.1–

---

[28] Art. 7° Os direitos previstos neste código não excluem outros decorrentes de tratados ou convenções internacionais de que o Brasil seja signatário, da legislação interna ordinária, de regulamentos expedidos pelas autoridades administrativas competentes, bem como dos que derivem dos princípios gerais do direito, analogia, costumes e equidade.
Parágrafo único. Tendo mais de um autor a ofensa, todos responderão solidariamente pela reparação dos danos previstos nas normas de consumo (BRASIL, 1990).

[29] Art. 30. Toda informação ou publicidade, suficientemente precisa, veiculada por qualquer forma ou meio de comunicação com relação a produtos e serviços oferecidos ou apresentados, obriga o fornecedor que a fizer veicular ou dela se utilizar e integra o contrato que vier a ser celebrado (BRASIL, 1990).

[30] Art. 37. É proibida toda publicidade enganosa ou abusiva.
§ 1° É enganosa qualquer modalidade de informação ou comunicação de caráter publicitário, inteira ou parcialmente falsa, ou, por qualquer outro modo, mesmo por omissão, capaz de induzir em erro o consumidor a respeito da natureza, características, qualidade, quantidade, propriedades, origem, preço e quaisquer outros dados sobre produtos e serviços.
§ 2° É abusiva, dentre outras a publicidade discriminatória de qualquer natureza, a que incite à violência, explore o medo ou a superstição, se aproveite da deficiência de julgamento e experiência da criança, desrespeita valores ambientais, ou que seja capaz de induzir o consumidor a se comportar de forma prejudicial ou perigosa à sua saúde ou segurança.
§ 3° Para os efeitos deste código, a publicidade é enganosa por omissão quando deixar de informar sobre dado essencial do produto ou serviço.
§ 4° (Vetado). (BRASIL, 1990).

devendo, portanto, ser analisado através dos princípios constitucionais que estão ligados à defesa do consumidor e que devem servir de norteadores à aplicação e interpretação da legislação consumerista Theodoro Júnior (2021).

Os princípios constitucionais de defesa do consumidor que devem ser observados para a aplicação do CDC, segundo o autor Humberto Theodoro Júnior (2021), são os seguintes princípios: Princípio da dignidade da pessoa humana, Princípio da Liberdade, Princípio da Isonomia e Princípio da Publicidade.

O autor fala do princípio da dignidade humana como princípio que ocupa a posição central de princípio "a que caberia, entre outras, a função estrutural de realizar a proporcionalidade entre todos os princípios presentes na ordem constitucional" (THEODORO JÚNIOR, 2021, p. 25).

Quanto ao Princípio da Liberdade, este, segundo o autor, assegura a livre iniciativa aos que querem empreender no mercado, estando previsto em vários dispositivos da CRFB/88 – dentre eles o art. 1º, IV como fundamento da livre iniciativa e o art. 3º, I, como objetivo fundamental a construção de uma sociedade justa, livre e solidária – e em relação ao consumidor, atribui a liberdade de aquisição de produtos e serviços, caso queira e de escolher quem será contratado.

O princípio da isonomia – previsto pelo caput do artigo 5º da CRFB/88 – trata-se, segundo Theodoro Júnior, da igualdade de todos perante a lei, pois o legislador, ao aplicar tratamento desigual ao consumidor, obtém igualdade entre as partes, isso porque na relação de consumo a desigualdade impõe a necessidade de tratamento diferenciado ao consumidor, ao passo que a proteção da vulnerabilidade do consumidor confere igualdade material na formação do vínculo contratual, respeitando o princípio da isonomia. Ou seja, o legislador a fim de conferir isonomia da igualdade de todos perante a lei, garante ao consumidor proteção hábil a fim de que se estabeleça na relação de consumo igualdade entre as partes proporcionalmente. Cunha (2011), afirma que o tratamento desigual conferido ao consumidor em decorrência de sua vulnerabilidade, possui a mesma medida do princípio da igualdade previsto pela Carta Magna, isso porque possui o intuito de conferir tratamento igual aos consumidores.

O Princípio da Publicidade, segundo Theodoro Júnior, protege o consumidor à medida que protege a verdade nas publicidades, pois a Constituição trata em seu art. 220, §3º, II, trata da comunicação social e garante meios legais à pessoa e à família para que possam defender-se de propagandas e serviços que lhes sejam nocivos.

O CDC também traz princípios gerais a fim de proteger o consumidor nas relações de consumo, que são: Princípio da vulnerabilidade do consumidor (já tratamos desse princípio no tópico 2 no que compete a relação virtual do consumidor), Princípio da intervenção estatal, Princípio da harmonia das relações de consumo, Princípio da boa-fé objetiva, Princípio do equilíbrio, Princípio da educação e da informação, Princípio da qualidade e segurança e a novidade introduzida pela Lei n. 13.486, de 2017, Princípio da coibição e repressão ao abuso, Princípio da racionalização e melhoria dos serviços públicos, Princípio da responsabilidade solidária, Princípio da continuidade do serviço público (ALMEIDA; LENZA, 2020).

Não adentraremos à explicação de cada princípio, nosso foco será com base nos ensinamentos de Almeida e Lenza (2020) e nos seguintes princípios: da harmonia das relações de consumo, da boa-fé objetiva e da educação e informação. Não que os outros sejam menos importantes, mas para o presente estudo se tornam mais relevantes à compreensão de como o CDC ampara a vulnerabilidade do consumidor no ambiente digital.

Segundo os autores, o princípio da harmonia das relações de consumo está disposto no artigo 4º, III[31], do CDC e possui como objetivo principal a garantia do equilíbrio nas relações de consumo, trazendo a proteção do consumidor de forma que não seja imposta como um diploma arbitrário, mas sim para privilegiar o consumidor que é a parte mais vulnerável e reequilibrar essa relação jurídica desigual.

O princípio da boa-fé objetiva, que se apresenta como um dos princípios mais importantes no direito privado, com relevância no direito contratual e com previsão expressa no CDC mais especificamente no artigo 4º, III e no 51, IV, e no Código Civil nos artigos 113, 187 e 222 (SANTOS; SILVA, 2011). No que se refere sua previsão no CDC, o princípio da boa-fé é tratado no mesmo inciso que prevê o princípio da harmonização das relações de consumo e apesar da falta de previsão expressa, a boa-fé é tratada como a objetiva, que trata das regras de conduta na relação de consumo e pode ser analisada com base nos deveres anexo, laterais e secundários, que são ligados aos deveres de informação, cooperação e informação (ALMEIDA, LENZA, 2020).

[31] Art. 4º A Política Nacional das Relações de Consumo tem por objetivo o atendimento das necessidades dos consumidores, o respeito à sua dignidade, saúde e segurança, a proteção de seus interesses econômicos, a melhoria da sua qualidade de vida, bem como a transparência e harmonia das relações de consumo, atendidos os seguintes princípios:
[…]III - harmonização dos interesses dos participantes das relações de consumo e compatibilização da proteção do consumidor com a necessidade de desenvolvimento econômico e tecnológico, de modo a viabilizar os princípios nos quais se funda a ordem econômica (art. 170, da Constituição Federal), sempre com base na boa-fé e equilíbrio nas relações entre consumidores e fornecedores; […] (BRASIL, 1990)

Os princípios da educação e da informação, estão previstos no art. 4º, IV[32] do CDC. E que segundo os autores Almeida e Lenza (2020), são princípios de extrema importância por causa da carência do sistema educacional na sociedade. A importância desse princípio para Theodoro Júnior (2021), ocorre porque ele conscientiza os consumidores e fornecedores sobre seus direitos e deveres na relação consumerista.

Há também um princípio trazido por Claudia Lima Marques (2016), denominado princípio básico da confiança, estabelecido pelo CDC a fim de assegurar ao consumidor um produto ou serviço adequado, evitar riscos e prejuízos, garantir o ressarcimento do consumidor caso o fornecedor não cumpra com seu dever, e que segundo a autora, são as leis imperativas do CDC que protegerão a confiança que é depositada pelo consumidor no vínculo contratual. No ambiente virtual, em que há inúmeras ofertas e milhares de fornecedores, o fornecedor precisará adquirir a confiança do consumidor, mantendo uma boa conduta a fim de manter sua credibilidade (SANTOS; SILVA, 2011). Theodoro Júnior (2021) enfatiza que através da confiança é que os consumidores geram expectativas, devendo ser respeitadas e garantidas como resultado do princípio da boa-fé objetiva.

Até mesmo porque, hoje em dia existem sites que os consumidores podem deixar suas reclamações a respeito da má conduta do fornecedor, valendo citar o site "reclameaqui.com.br" famoso nesse segmento e de fácil utilização pelos usuários.

## 3.6 LEI DO COMÉRCIO ELETRÔNICO – DECRETO Nº 7.962/2013

Anos após a promulgação do CDC e após a utilização em massa do meio eletrônico para a comunicação e relação de consumo, finalmente surgiu um aparato estatal para regulamentar o CDC e falar sobre a contratação no comércio eletrônico. Alguns artigos do Decreto serão analisados de forma breve, somente a fim de conhecimento sobre o diploma legal, que foi o primeiro a tratar especificamente da contratação no comércio eletrônico.

O artigo 1º do Decreto, traz alguns deveres por parte do fornecedor que precisam ser observados na relação de consumo, dentre eles: a prestação de informações claras sobre o

[32] Art. 4º A Política Nacional das Relações de Consumo tem por objetivo o atendimento das necessidades dos consumidores, o respeito à sua dignidade, saúde e segurança, a proteção de seus interesses econômicos, a melhoria da sua qualidade de vida, bem como a transparência e harmonia das relações de consumo, atendidos os seguintes princípios:
[...] IV - educação e informação de fornecedores e consumidores, quanto aos seus direitos e deveres, com vistas à melhoria do mercado de consumo; […] (BRASIL, 1990).

produto, serviço e sobre o fornecedor; que o atendimento do consumidor seja realizado de forma facilitada e o respeito ao direito de arrependimento do consumidor.

A respeito das informações claras, Theodoro Júnior (2021) fala da importância do direito à informação no comércio eletrônico não ser limitado às informações sobre características dos produtos ou serviços, pois é necessário que o fornecedor deixe informações acessíveis a respeito da sua identificação. O autor enfatiza que a situação que é realizada a relação de consumo coloca o consumidor em posição de vulnerabilidade dada a falta de contato direto com o consumidor.

Essa necessidade de identificação por parte do fornecedor é expressa nos artigos 2º, I e II, ao prever a disponibilização de informações em local de destaque e de fácil visualização da qualificação da empresa, acompanhado de número telefônico. Isso para que caso seja necessário o consumidor entrar em contato, seja mais fácil identificá-lo (THEODORO JÚNIOR, 2021).

Quanto ao atendimento facilitado do consumidor no comércio eletrônico – ressaltamos novamente que a condição virtual influencia a falta de informação e contato com o fornecedor, colocando o consumidor em posição desfavorável – o artigo 4º[33] traz uma série de deveres do fornecedor para que garanta essa facilitação, especialmente em relação a necessidade de manter um serviço de atendimento eletrônico para a retirada de dúvidas, reclamações, suspensão ou cancelamento do contrato por parte do consumidor (inciso V) e previsão de um prazo de 5 (cinco) dias para o dever de resposta do fornecedor.

Sem sombra de dúvidas a debilidade informacional nas relações de consumo virtuais se deve a distância entre fornecedor e consumidor, levando em conta que as únicas informações que o usuário possui acesso são justamente as escolhidas pelo fornecedor (LÊDO; MARQUESI; SABO, 2018).

---

[33] Art. 4º Para garantir o atendimento facilitado ao consumidor no comércio eletrônico, o fornecedor deverá:
I - apresentar sumário do contrato antes da contratação, com as informações necessárias ao pleno exercício do direito de escolha do consumidor, enfatizadas as cláusulas que limitem direitos;
II - fornecer ferramentas eficazes ao consumidor para identificação e correção imediata de erros ocorridos nas etapas ante riores à finalização da contratação;
III - confirmar imediatamente o recebimento da aceitação da oferta;
IV - disponibilizar o contrato ao consumidor em meio que permita sua conservação e reprodução, imediatamente após a contratação;
V - manter serviço adequado e eficaz de atendimento em meio eletrônico, que possibilite ao consumidor a resolução de demandas referentes a informação, dúvida, reclamação, suspensão ou cancelamento do contrato;
VI - confirmar imediatamente o recebimento das demandas do consumidor referidas no inciso, pelo mesmo meio empregado pelo consumidor ; e
VII - utilizar mecanismos de segurança eficazes para pagamento e para tratamento de dados do consumidor.
Parágrafo único. A manifestação do fornecedor às demandas previstas no inciso V do **caput** será encaminhada em até cinco dias ao consumidor (BRASIL, 2013).

As relações consumeristas no ambiente virtual também possuem amparo pelo direito de arrependimento por parte do consumidor. O artigo 5º[34] estabelece o dever do fornecedor oferecer informação clara e os meios adequados para que o consumidor possa exercer o seu direito de arrependimento e sem que tenha que cumprir qualquer dever imposto pelo fornecedor.

O decreto não prevê um prazo para o exercício do direito de arrependimento, mas como ele é utilizado para regulamentar o CDC e trata-se de uma relação de consumo, deverá ser aplicado o prazo previsto pelo art. 49[35] do Código de defesa do consumidor, que prevê prazo de 7(sete) dias a partir do recebimento do produto ( no caso de compra on-line), ou da assinatura do contrato (fora do estabelecimento comercial), além de ter o direito a receber os valores pagos pelo produto.

A única exigência para que o consumidor possa ter o direito de se arrepender pela aquisição do produto ou serviço, é que essa aquisição tenha ocorrido fora do estabelecimento comercial, não podendo a empresa, segundo decisão do STJ, exigir que o consumidor pague as despesas postais para a entrega do bem ou do produto (THEODORO JÚNIOR, 2021).

Uma preocupação necessária e que foi atendida pelo Decreto, foi a previsão de sanção em caso de descumprimento das condutas especificadas por ele, no artigo 7º[36], prevendo que a aplicação das sanções seja de acordo com as já reguladas no art. 56º[37] do CDC.

---

[34] Art. 5º O fornecedor deve informar, de forma clara e ostensiva, os meios adequados e eficazes para o exercício do direito de arrependimento pelo consumidor.
§ 1º O consumidor poderá exercer seu direito de arrependimento pela mesma ferramenta utilizada para a contratação, sem prejuízo de outros meios disponibilizados.
§ 2º O exercício do direito de arrependimento implica a rescisão dos contratos acessórios, sem qualquer ônus para o consumidor.
§ 3º O exercício do direito de arrependimento será comunicado imediatamente pelo fornecedor à instituição financeira ou à administradora do cartão de crédito ou similar, para que:
I - a transação não seja lançada na fatura do consumidor; ou
II - seja efetivado o estorno do valor, caso o lançamento na fatura já tenha sido realizado.
§ 4º O fornecedor deve enviar ao consumidor confirmação imediata do recebimento da manifestação de arrependimento (BRASIL, 2013).

[35] Art. 49. O consumidor pode desistir do contrato, no prazo de 7 dias a contar de sua assinatura ou do ato de recebimento do produto ou serviço, sempre que a contratação de fornecimento de produtos e serviços ocorrer fora do estabelecimento comercial, especialmente por telefone ou a domicílio.
Parágrafo único. Se o consumidor exercitar o direito de arrependimento previsto neste artigo, os valores eventualmente pagos, a qualquer título, durante o prazo de reflexão, serão devolvidos, de imediato, monetariamente atualizados (BRASIL, 1990).

[36] Art. 7º A inobservância das condutas descritas neste Decreto ensejará aplicação das sanções previstas no art. 56 da Lei nº 8.078, de 1990 (BRASIL, 2013).

[37] Art. 56. As infrações das normas de defesa do consumidor ficam sujeitas, conforme o caso, às seguintes sanções administrativas, sem prejuízo das de natureza civil, penal e das definidas em normas específicas:
I - multa;
II - apreensão do produto;
III - inutilização do produto;
IV - cassação do registro do produto junto ao órgão competente;
V - proibição de fabricação do produto;

## 3.7 O MARCO CIVIL DA INTERNET- LEI Nº 12.965/2014

Sem sombra de dúvidas a criação da lei nº 12.965/2014 denominada Marco Civil da Internet – MCI, trouxe um grande avanço para a legislação brasileira ao ser a primeira lei a tratar da garantia dos direitos dos cidadãos à utilização da internet no Brasil.

Bioni (2021) destaca que a criação dessa lei ocorreu por causa de uma movimentação legislativa que propunha a regulamentação da internet pela legislação penal, o que não agradou a sociedade civil que se movimentou contra tal proposta. Outro fator que serviu para impulsionar a aprovação da lei, foi a espionagem da Agência Nacional de Segurança dos Estados Unidos à presidente Dilma Rousseff (BEZERRA; WALTZ, 2014). Bioni (2021), diz que a repercussão da espionagem fez com que o texto do projeto de lei fosse mais rígido, ocasionando a criação de novos incisos que possibilitassem maior proteção de dados pessoais.

O MCI surge com o intuito de combater à censura, promover direito constitucionais para a utilização da internet, trazendo princípios como a neutralidade da rede, privacidade e inimputabilidade da rede a fim de garantir aos internautas direitos e liberdades contra ações abusivas por parte do governo e das empresas (BEZERRA, WALTZ, 2014), garantindo um rol de princípios que fundamentam a referida de lei em seu art. 3º[38], dentre eles a proteção da privacidade (inciso II) – Barreto (2015) chama a atenção para o fato de ser a privacidade um dos princípios mais importantes da lei, pois essa proteção interessa aos usuários a medida que

---

VI - suspensão de fornecimento de produtos ou serviço;
VII - suspensão temporária de atividade;
VIII - revogação de concessão ou permissão de uso;
IX - cassação de licença do estabelecimento ou de atividade;
X - interdição, total ou parcial, de estabelecimento, de obra ou de atividade;
XI - intervenção administrativa;
XII - imposição de contrapropaganda.
Parágrafo único. As sanções previstas neste artigo serão aplicadas pela autoridade administrativa, no âmbito de sua atribuição, podendo ser aplicadas cumulativamente, inclusive por medida cautelar, antecedente ou incidente de procedimento administrativo (BRASIL, 1990).

[38] Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
II - proteção da privacidade;
III - proteção dos dados pessoais, na forma da lei;
IV - preservação e garantia da neutralidade de rede;
V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
VII - preservação da natureza participativa da rede;
VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.
Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte (BRASIL, 2014).

não estão cientes da vigilância das empresas ao realizarem a mineração de seus dados pessoais – e a proteção dos dados pessoais (inciso III).

No artigo 5º, traz a definição de internet (inciso I), terminal (inciso II), endereço de protocolo de internet (IP) (inciso III), administrador de sistema autônomo (inciso IV), conexão à internet (inciso V), registro de conexão (inciso VI), aplicações de internet (inciso VII) e registros de acesso a aplicações de internet (inciso VIII)

A lei também assegura em sua Seção II um rol de direitos e garantias aos usuários no artigo 7º. Dentre eles a inviolabilidade da privacidade e da intimidade (inciso I); que o fluxo das comunicações na internet (inciso II) e das comunicações privadas armazenadas(inciso III) seja sigiloso e inviolável; o direito do usuário de ser informado de forma clara e completa sobre a coleta, uso, armazenamento e tratamento e proteção dos seus dados pessoais, observadas as finalidades que justifiquem sua coleta, não tenham vedação por lei e estejam especificadas nos contratos de serviços ou em termos de uso de internet (inciso VIII); consentimento expresso sobre uso, coleta, armazenamento e tratamento de dados pessoais (inciso IX); prevê o diálogo com o Código de Defesa do Consumidor ao enfatizar sua aplicação nas relações de consumo via internet (inciso XIII); além de prever o direito ao usuário em exigir a exclusão dos dados pessoais fornecidos a determinada aplicação de internet de forma definitiva, o que segundo Bioni (2021) serve para identificar o controle dos dados pessoais por seus usuários.

O Marco Civil da Internet, antes mesmo da entrada em vigor da LGPD, foi a legislação que inaugurou a proteção de dados pessoais, a necessidade de consentimento e a informação sobre a finalidade o uso, armazenamento e tratamento que os dados serão submetidos, além de prever a inviolabilidade da privacidade e intimidade do usuário

A legislação, muito embora tenha inovado ao tratar sobre o uso da internet no Brasil, acabou deixando alguns pontos abertos, por não prever normas expressas a fim de coibir a coleta e tratamento de dados pessoais, além de não conceituar expressamente o que seria considerado um dado pessoal e o que é o tratamento dos dados pessoais, além de não ter se mostrado eficaz quanto a necessidade de consentimento expresso sobre a utilização e tratamento dos dados pessoais (MAGRANI, 2019).

Em 2016, o Decreto nº 8.771/2016 veio para regulamentar conceitos, definições, requisitos e exigências que não foram normatizados no MCI. O decreto trouxe ao total 22 artigos. Destaque para o art. 18 que prevê a fiscalização e apuração das infrações resultantes das relações de consumo pela Secretaria Nacional do Consumidor com base no CDC.

O Decreto trouxe a definição de dado pessoal no art. 14, I: "dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa" (BRASIL, 2016), a definição de tratamento de dados pessoais em seu art. 14, inciso I:

> 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, 2016).

Importante destacar que a Seção II da referida lei, trata da proteção aos registros, dados pessoais e às comunicações privadas nos artigos 10[39], 11[40] . O artigo 12[41] trata especificamente

[39] Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
§ 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no **caput**, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º (BRASIL, 2014).
§ 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º
§ 3º O disposto no **caput** não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.
§ 4º As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais (BRASIL, 2014).

[40] Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.
§ 1º O disposto no **caput** aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.
§ 2º O disposto no **caput** aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.
§ 3º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações.
§ 4º Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo.

[41] Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa:
I - advertência, com indicação de prazo para adoção de medidas corretivas;
II - multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;
III - suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou
IV - proibição de exercício das atividades que envolvam os atos previstos no art. 11.

das sanções que podem ser aplicadas caso as normas dos artigos 10 e 11 sejam infringidas. O artigo 13, traz a necessidade de que os registros de conexão sejam guardados pelo prazo de 1 (um) ano, ao passo que a manutenção desses registros não pode ser transferida a terceiros e que os registros podem ser guardados por prazo superior, caso haja solicitação de autoridade policial, administrativa ou pelo Ministério Público um ano mais tempo pode ser estendido Ministério Público.

Analisando a Lei do Marco Civil da Internet, não pode ser utilizado o argumento de que esta lei não ganhou a mesma visibilidade que a LGPD, porque não previa sanções aplicáveis aos infratores, tendo em vista que o dispositivo traz a aplicabilidade de sanções de expressamente no referido art.12.

Barreto (2015) comenta que a proteção do usuário no MCI é contemplada apenas no plano principiológico, entendendo que embora as diretrizes gerais da lei sejam úteis, não são suficientes para a proteção e defesa dos dados pessoais do usuário.

Bioni (2021), verifica que o parâmetro adotado pela lei foi o da autodeterminação informacional para a proteção dos dados pessoais, pois todas as normas possuem a finalidade de chegar até o usuário, a fim de que tenha ciência e controle sobre o fluxo de seus dados pessoais. Ademais, o fato de o MCI não trazer regulamentação específica ao tratamento dos dados pessoais não deve ser interpretado negativamente, pois o objeto da referida lei é a ampla regulamentação do uso da internet (COTS; OLIVEIRA, 2021).

## 3.8 LEI GERAL DE PROTEÇÃO DE DADOS

Essa lei foi muito aguardada, pois até então não havia uma normativa que regulasse o tratamento dos dados pessoais no Brasil (em ambiente físico e no ambiente digital[42]). Segundo Camurça (2021), a lei não surgiu a fim de reestruturar a regulação trazida pelo MCI, o seu principal intuito foi trazer novos direitos e proteger de forma abrangente a utilização dos dados pessoais, regulamentando a utilização dos dados pessoais pelos setores que se beneficiam sobre eles. Ademais, a discussão sobre a entrada em vigor de uma legislação que trate sobre a proteção dos dados pessoais advém desde meados de 2010 (BIONI, 2021). Basan (2021) explica que

Parágrafo único. Tratando-se de empresa estrangeira, responde solidariamente pelo pagamento da multa de que trata o **caput** sua filial, sucursal, escritório ou estabelecimento situado no País (BRASIL, 2014).

[42] Art. 1º 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.
Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios (BRASIL, 2018).

mesmo que existam leis anteriores abordando a temática dos dados pessoais (MCI), nenhuma delas tratou especificamente sobre a tutela dos dados pessoais como a LGPD.

Essa lei traz em seu arcabouço a regulamentação sobre o modo que os dados pessoais serão armazenados e a forma que ocorrerá o seu tratamento, o que acaba conferindo atenção especial ao consumidor que agora tem o poder de determinar quem terá acesso aos seus dados pessoais e os limites da utilização por terceiros (FOLLONE; SIMÃO FILHO, 2020). A partir dessa finalidade, podemos compreender que se há pouco tempo o consumidor não tinha amparo na legislação para garantir seus direitos de navegação na internet e da proteção de seus dados pessoais, agora possui duas legislações que lhe tem como figura principal de proteção, ainda mais agora que sua proteção foi elevada ao rol de direitos fundamentais da Carta Magna.

A necessidade de consentimento para o tratamento dos dados pessoais é um dos elementos fundamentais da Legislação e, embora não seja o único, não deixa de ser o condutor da normativa, tendo em vista que os princípios trazidos pela legislação e a forma com que ela aborda o consentimento no decorrer do texto legal, demonstram uma enorme preocupação sobre a participação do indivíduo na utilização de suas informações pessoais (BIONI, 2021).

Tecidas algumas considerações sobre a importância da Lei Geral de Proteção de dados na proteção dos usuários e sobre o tratamento especial que ela confere à necessidade de consentimento sobre a utilização de dados pessoais, adentraremos agora à interpretação de alguns artigos importantes ao tema do texto normativo. O artigo 6º[43] da LGPD inaugura um rol

[43] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas (BRASIL, 2018).

de princípios e seus conceitos, para que a lei possa tornar-se referência a futuras legislações e auxiliar na interpretação de outras normas que possuam como foco o tratamento de dados pessoais (COTS; OLIVEIRA, 2021). Um total de 10 (dez) princípios os quais são: finalidade, adequação, necessidade, livre acesso, qualidade de dados, transparência, segurança, prevenção, não discriminação e a responsabilização e prestação de contas.

Em relação ao consentimento, este é previsto pelo art. 5º, XII e se resume a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada", este mesmo artigo conceitua dado pessoal (inciso I) como sendo a informação que seja relacionada a pessoa natural identificada ou identificável; deixa claro quem é o controlador (inciso VI) sendo quem toma decisão referente ao tratamento dos dados pessoais; chama de operador (inciso VII) aquele que em nome do controlador faz o tratamento dos dados pessoais; une controlador e operador e os denomina com agentes de tratamento (inciso IX); autoridade nacional como sendo o órgão responsável pelo cumprimento da referida lei (inciso XIX) e banco de dados como "conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico" (inciso IV); tratamento (inciso X) "toda operação realizada com dados pessoais". O referido artigo traz um total de 19 incisos.

O artigo 2º elenca os fundamentos da LGPD: o respeito à privacidade; à autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião; a 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; os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. A concretização dos fundamentos deste artigo ocorre no Capítulo III, que trata dos direitos do titular (TASSO, 2020).

### 3.8.1 Tratamento de Dados Pessoais

Para que o tratamento dos dados pessoais possa ocorrer, terá que estar previsto no rol taxativo do artigo 7º[44]. Somente serão consideradas para tratamento dos dados pessoais as bases

[44]Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
I - mediante o fornecimento de consentimento pelo titular;
II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

legais previstas no referido artigo, exceto aqueles tratamentos que autorizados pela legislação no artigo 4º, e que caso a base legal não seja observada pelo controlador ao realizar o tratamento dos dados, correrá o risco de ser punido através de processo judicial ou de forma administrativa (COTS; OLIVEIRA, 2020).

A necessidade de consentimento que consta no inciso I é somente a primeira das hipóteses de permissão para o tratamento de dados pessoais e, embora não seja a única, possui papel principal na estrutura da legislação ao ser citado várias no decorrer do texto normativo (BIONI, 2021).

Não adentraremos às particularidades de cada inciso, apenas voltaremos a nossa atenção no próximo tópico ao legítimo interesse previsto pelo inciso IX, tendo em vista o grau de subjetividade a que ficou submetido (COTS; OLIVEIRA, 2020).

### 3.8.2 O legítimo interesse

O legítimo interesse é previsto na LGPD nos artigos 7º, inciso IX, no artigo 10 e no artigo 37 e sua importância caracteriza-se por ter sido colocado como base legal de tratamento de dados pessoais (COTS; OLIVEIRA, 2020).

---

IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.
§ 1º (Revogado).
§ 2º (Revogado).
§ 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.
§ 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei.
§ 5º O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.
§ 6º A eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular.
§ 7º O tratamento posterior dos dados pessoais a que se referem os §§ 3º e 4º deste artigo poderá ser realizado para novas finalidades, desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos nesta Lei (BRASIL, 2018).

O artigo 7º, inciso IX da referida lei prevê que o legítimo interesse pode ser utilizado como hipótese de tratamento de dados pessoais: "quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais". Pode-se dizer que é uma espécie de abertura ao controlador, concedendo a ele o poder de realizar o tratamento dos dados pessoais para atender aos seus interesses (desde que sejam legítimos).

No artigo 10[45], inclui situações concretas (mas não se limita a elas) para que o legítimo interesse possa ser utilizado como fundamento de tratamento de dados pessoais. E no artigo 37[46] prevê a obrigação por parte de controlador e operador em garantir o registro das operações de tratamento de dados pessoais, principalmente quando ocorrerem com base no legítimo interesse.

Cots e Oliveira (2020) explicam que foi necessário estruturar o legítimo interesse como base legal para que os empreendedores e não sofressem tanto com o impacto da LGPD, tendo em vista que alguns bancos de dados já existentes poderiam tornar-se inutilizados pelo fato de não se encaixarem nas bases legais previstas pela lei. Por esse motivo, o legislador criou a possibilidade de tratamento de dados pessoais sem que precise estar previsto dentro do rol de hipóteses de tratamento de dados pessoais, dado a sua taxatividade.

Nesse caminho, segundo os autores, o legislador não trouxe a conceituação de legítimo interesse no artigo 5º – e em nenhuma outra parte da LGPD – devendo ser interpretado o legítimo interesse como aquilo que seja importante suficientemente para o controlador, a fim de que tenha que realizar o tratamento dos dados.

A sua finalidade, portanto, precisa ser fundamentada a partir da compreensão do conceito da boa-fé objetiva, pois é ela quem dará suporte para que o conteúdo do legítimo

---

[45] Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:
I - apoio e promoção de atividades do controlador; e
II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.
§1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.
§2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.
§3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial (BRASIL, 2018).

[46] Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse (BRASIL, 2018).

interesse do controlador seja definido corretamente e dentro do limites e deveres de sua atividade como agente de tratamento de dados (GROSSI, 2020).

### 3.8.3 Dados Sensíveis

Os dados pessoas sensíveis, conforme destacado anteriormente, foram conceituados pela própria lei no artigo 5º, II da LGPD: "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". A necessidade de restringir a utilização dos dados pessoais sensíveis advém da preocupação em relação a utilização desses dados para fins que ensejem a discriminação dos titulares (SALDANHA, 2020).

Um regime jurídico que garante proteção ao titular dos dados sensíveis, possibilita que ele se relacione diante da sociedade sem que seja frustrado através de atos discriminatórios, podendo assim desenvolver a sua personalidade de forma livre (BIONI,2021). O artigo 11[47] da LGPD traz um rol taxativo prevendo que somente nas hipóteses ali elencadas é que poderá ocorrer o tratamento dos dados pessoais sensíveis.

### 3.7.4 Dados Anonimizados

O dado anonimizado é conceituado no artigo 5º, inciso III da LGPD como: "dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos

[47] Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
a) cumprimento de obrigação legal ou regulatória pelo controlador;
b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
e) proteção da vida ou da incolumidade física do titular ou de terceiro;
f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou (Redação dada pela Lei nº 13.853, de 2019)
g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.[...] (BRASIL, 2018).

razoáveis e disponíveis na ocasião de seu tratamento", ou seja, os dados somente serão considerados anônimos caso o titular dos dados não possa ser identificado ou identificável (não pode ser identificado após tratamento para tornar-se anonimizado), não podendo ser associado ao titular de forma permanente e irreversível (DONEDA; MACHADO, 2018).

Segundo Bioni (2020, p. 197) "o processo de anonimização deve representar um conjunto de ações contínuo e logicamente ordenado que abrace toda a extensão do ciclo de vida de um dado – da coleta ao descarte". O autor também afirma que o legislador enfatiza aos agentes de tratamento de dados a necessidade de utilizar boas técnicas de anonimização, a fim de que os dados não possam ser reidentificados nem por quem realizou a anonimização.

O artigo 12[48] da referida lei destaca que os dados anonimizados não são considerados dados pessoais, mas que essa lógica poderá ser alterada caso o processo de anonimização possa ser revertido com esforços razoáveis ou por meios próprios, sendo que "o filtro de razoabilidade depende de uma "régua" que viabilize a imputação de responsabilidade civil em caso de reversão"(FALEIROS JÚNIOR; MARTINS, 2021, p. 387).

Faleiros Júnior e Martins (2021) explicam que a prioridade da proteção aos dados pessoais vai além da classificação do que seria considerado razoável, pois a necessidade é de que existam elementos mínimos para que a anonimização seja confiável e que a definição de anonimização leva em conta os meios que proporcionam a reidentificação com base na razoabilidade.

O artigo também inova ao considerar em seu §2º que os dados utilizados para formar perfis comportamentais podem tornar-se dados pessoais caso a pessoa possa ser identificada. Quanto a utilização das técnicas e padrões para que os processos de anonimização sejam confiáveis, o §3º confere à Agência nacional de proteção de dados (ANPD) poder para criar padrões e técnicas para a realização da anonimização e a verificação quanto à segurança do processo. Ainda há muitos debates acerca das técnicas que podem ser utilizadas para a

[48] Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.
§ 1º A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios.
§ 2º Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada.
§ 3º A autoridade nacional poderá dispor sobre padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de Proteção de Dados Pessoais (BRASIL, 2018).

anonimização e do procedimento que com o avanço das tecnologias pode ser revertido, no entanto, não vamos adentrar ao assunto.

## 4 A NECESSIDADE DE CONSENTIMENTO DO CONSUMIDOR SOBRE A UTILIZAÇÃO DE SEUS DADOS PESSOAIS NO MEIO DIGITAL

Durante muito tempo o usuário[49] da internet teve papel de mero espectador sobre o destino e a finalidade de tratamento a que eram submetidos os seus dados pessoais, até que o ordenamento jurídico passou a estruturar leis que previssem de forma expressa a tutela das suas informações pessoais.

A lei nº 12.527 de 2011 denominada como Lei de Acesso à Informação foi a primeira lei brasileira a tratar da conceituação de informação pessoal, mesmo que seja delimitada a atuação dos órgãos públicos, tendo em vista que trata apenas do acesso à informação de caráter público, sendo sua finalidade ditar as regras para o acesso dos cidadãos às informações públicas e subordinar os órgão públicos[50] ao dever em observar os procedimentos previstos na lei para o acesso à informação. A conceituação de informação pessoal dada pela lei, refere-se "aquela relacionada à pessoa natural identificada ou identificável" (BRASIL, 2011), além de ter destinado seu capítulo IV para tratar das "Restrições de Acesso à informação" e reservar a Seção V para tratar " Das Informações Pessoais", prevendo em seu artigo 31 que o tratamentos dos dados pessoais seja realizado de forma transparente, com respeito aos direitos da personalidade (caput) e que a divulgação de informações pessoais só poderá ser divulgada ou acessada por terceiros diante de previsão legal ou mediante o consentimento expresso de seu titular. Mesmo que essa lei delimite a utilização de informal pessoal mediante consentimento apenas aos órgãos públicos, ela inova ao trazer limites para a divulgação de informações pessoais.

---

[49] Neste trabalho os termos usuário e consumidor possuem o mesmo sentido, tendo em vista que a relação de consumo no ambiente digital atribui ao cidadão os dois papéis.

[50] Art. 1º Esta Lei dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal.
Parágrafo único. Subordinam-se ao regime desta Lei:
I - os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público;
II - as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios (BRASIL, 2011)

Importante mencionar que a LGPD não ficou alheia a regulamentação da utilização de dados pessoais pelos órgãos públicos, pois em seu Capítulo IV dispõe sobre o "tratamento de dados pessoais pelo poder público" e deixa claro em seu artigo 23 as regras que devem ser atendidas pela administração pública ao realizar o tratamento do dados pessoais referidos na Lei de acesso à informação (BRASIL, 2018). Sendo assim, o Poder Público está submetido a agir de acordo com as regras constantes na LGPD e só pode exigir informações e dados de seus cidadãos que estejam limitados essencialmente a seus propósitos, o que de certa o expõe a um risco maior de não conseguir cumprir com as obrigações previstas pela lei, tendo em vista que a sua atuação requer amplo acesso aos dados e informações de seus cidadãos (LOURENÇO; TAQUES, 2020).

Em relação às legislações que regulamentam o setor privado, a primeira a destacar a necessidade de consentimento para a coleta de dados pessoais foi a lei do Marco Civil da Internet, que traz a palavra consentimento em 3 ocasiões: a primeira no artigo 7º, inciso VII ao tratar que o fornecimento de dados a terceiros somente poderá ser realizado mediante consentimento expresso; a segunda ainda no artigo 7º, mas em seu inciso IX que assegura ao usuário o direito de consentimento expresso sobre o destino de seus dados; a terceira no artigo 16, inciso II quando veda a guarda de dados que excedam o propósito ao qual lhes foi dado consentimento.

Com a entrada em vigor da LGPD e conforme citado no capítulo anterior, a necessidade de consentimento passa a ser uma das bases legais para o tratamento de dados pessoais (art. 7º, I), mas o consentimento não deixa de ser protagonista na estruturação da lei (BIONI, 2021).

## 4.1 O DIREITO À PRIVACIDADE

A intimidade e a vida privada dos cidadãos brasileiros possui contorno específico na legislação brasileira, sendo tratadas pela Constituição Federal no art. 5º, X, como direito fundamental à privacidade e, por este motivo, a proteção que lhe é conferida precisa ser observada pelas legislações infraconstitucionais, de modo não existam mecanismos que limitem sua atuação como direito de cada cidadão em ter sua individualidade e intimidade preservadas. Na verdade, as legislações infraconstitucionais devem assegurar essa garantia através de mecanismos que garantam com que cada cidadão não tenha sua privacidade violada.

Quanto a sua conceituação, podemos dizer que se modifica com o passar dos anos em decorrência da evolução da sociedade, principalmente com a chegada de novas tecnologias, as

quais modificam os contornos da vida privada dos cidadãos (BRITO; CARNEIRO; TAVARES, 2020) e seu direito de escolha sobre quem terá acesso a sua intimidade. Atualmente, o direito à privacidade "pode ser compreendido como o direito de gerir e de como serão divulgadas as informações no cenário social e virtual" (CARDIN; TOBBIN, 2021, p.257).

Essas modificações são observadas a partir do amplo acesso ao uso da internet que se tornou um meio apto à troca de informações das mais variadas e amplamente acessíveis. Foi essa facilidade de troca de informações e adesão de um grande número de usuários, ocasionou o surgimento do mercado de compra e venda de informações pessoais, conforme explicado nos capítulos anteriores. Nesse contexto, a necessidade de aplicação da privacidade proporcionou a origem da regulação de proteção dos dados pessoais, ao passo que essa proteção pode ser considerada uma extensão da privacidade por outros caminhos, e que assume o dever de criar mecanismos que possibilitem amparar os interesses pessoais além da limitação de um direito à privacidade estruturado na esfera patrimonialista, como era conceituado antigamente (DONEDA, 2020).

O direito à privacidade em uma sociedade baseada no acesso às informações, precisou delimitar novos caminhos a fim de criar novas garantias de defesa à individualidade de cada pessoa. Por isso, que Doneda (2020) vai defender que a proteção de dados pessoais não deve ser compreendida como uma derivação do direito à privacidade, isso porque é uma disciplina que deve alçar caminhos além da esfera comunicativa e dessa forma consiga abranger a complexidade da informação.

Após a Emenda Constitucional nº 115/2022, ficou clara a intenção do legislador em colocar a proteção de dados como um direito fundamental autônomo, no entanto, é importante frisar que a LGPD conferiu papel de destaque ao direito de privacidade ao colocá-lo como um de seus fundamentos em seus artigos 1º (prevê que o tratamento de dados pessoais deve ser realizado com o objetivo de proteção à privacidade) com e 2º, I (prevê o respeito à privacidade como um de seus fundamentos (ROCHA, 2020).

Portanto, o direito à privacidade e o direito à proteção de dados pessoais não devem ser confundidos como um único direito, mas sim como direitos que se complementam com o intuito de alcançar os interesses pessoais de cada cidadão sobre a divulgação de suas informações pessoais.

## 4.2 A INEFETIVIDADE DO CONSENTIMENTO NA ESTRUTURAÇÃO DA PROTEÇÃO DE DADOS PESSOAIS

A estruturação da proteção de dados pessoais é realizada, conforme citado no tópico 3, com base no consentimento do titular dos dados pessoais. Segundo Fonseca e Mendes (2020), o consentimento é tido como núcleo estruturante para o tratamento dos dados pessoais e proteção, no entanto, tem se mostrado insuficiente para garantir o controle do titular sobre os seus dados pessoais. Os autores propõem três pontos para explicar essa deficiência regulatória.

a) as limitações cognitivas, que seriam o poder de decisão do titular após ser informado sobre o que será realizado com seus dados pessoais e analisar se isso possui alguma influência sobre ele e partindo desse entendimento consentir ou não sobre o tratamento de seus dados pessoais. Essa informação sobre a finalidade do tratamento então seria e pressuposição de que o titular está apto para tomar decisões, no entanto, em algumas situações o consentimento for dado pelo titular sem que o mesmo entenda o que está fazendo – isso diante da falta de compreensão e avaliação dos riscos que pode correr ao consentir sobre tratamento de seus dados pessoais;

b) as diversas situações em que o consentimento não é concedido livremente, pois o titular é induzido a consentir com o tratamento de seus dados pessoais para que possa usufruir de determinado serviço ou produto, sob pena de não poder acessá-los;

c) as técnicas de tratamento que no momento do consentimento não são informadas, mas que posteriormente podem estruturar os dados e transformá-los em uma representação do titular no ambiente virtual. Essas técnicas são realizadas com base no big data[51] e não são possíveis de serem previstas pelo titular no momento do consentimento.

Os autores propõem três caminhos para concretizar a proteção de dados pessoais, sejam eles: 1) por meio do auxílio de tecnologias que possam auxiliar o titular dos dados pessoais a controlá-los e de sistemas informacionais – citam o privacy by design[52] –; 2) através da prestação de contas pelos agentes de tratamento para a análise prévia de riscos, com a elaboração de relatórios de impacto feitos por eles mesmos e que já são previstos pela LGPD (art. 5º, inciso XVII); 3) controle contextual do consentimento, ou seja, contextualizar o

[51] O big data é um grande número de informações brutas armazenadas que facilita a utilização por parte das técnicas de comunicação a realizarem o processamento desse grande volume de informações e transformá-los em informações relevantes (DONEDA, 2010).

[52] Privacy by design é o desenvolvimento de softwares capazes de integrar o conceito de proteção de dados e implementar garantias de privacidade, segurança e proteção do titular de dados pessoais (FREITAS, 2020).

consentimento no intuito de adequá-lo à finalidade do tratamento e pelo contexto em que está inserido. Os autores ainda chamam a atenção para o fato de que a efetivação da proteção de dados pessoais precisa estar além da garantia formal do consentimento individualizado, necessitando de garantias materiais para a proteção de dados e construção de um espaço que garanta a liberdade do indivíduo em manejar as suas informações.

O consentimento atua como protagonista na estruturação da LGPD, no entanto, embora seja conferido expressamente ao titular dos dados pessoais o poder de decisão sobre o destino de seus dados, não existe previsão ou regulação de como ele poderá fazer valer esse direito, muito menos uma normativa que regule como o controlador deverá colher a manifestação do titular (BIONI, 2021), o legislador só define o que é consentimento no artigo 5º, XII de forma ampla: " manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada" (BRASIL, 2018).

É necessário entender a adjetivação do consentimento a partir de sua definição dada pelo legislador (livre, informado, inequívoco) para que possamos avaliar se elas levam a um destino que consiga estruturar o livre consentimento do titular.

Almeida e Lugatti (2020) interpretam o consentimento livre como o seguimento das necessidades trazidas pela LGPD, não contendo nenhum dos vícios elencados pelo Código Civil de 2002, sejam eles: erro, dolo, coação, estado de perigo, lesão, ressaltando a vedação de tratamento dos dados pessoais caso ocorra vício no consentimento (artigo 8º, §3º, LGPD), devendo ser analisado o contexto ao qual houve consentimento por parte do titular e se realmente ocorreu de forma livre. Quanto ao consentimento informado, os autores destacam que o titular deve ser cientificado de forma transparente e verdadeira sobre como será realizado o tratamento dos dados a fim de preservar sua autonomia informacional. Por último, o consentimento inequívoco, está relacionado a aceitação do titular com aceitação por escrito e em cláusula destacada (art. 8º, §1º LGPD), referindo-se à finalidade específica a que serão submetidos os dados para tratamento e prevendo que no caso de autorização genérica, esta será considerada nula (art. 8º, §1º LGPD). Bioni (2021) vai dizer que embora exista essa adjetivação, existe um "descaso normativo" (p. 166) com relação a forma com que deveria ocorrer essa operacionalização dessa adjetivação.

Com relação ao consentimento expresso e a forma com que muitos sites têm lidado com a necessidade de obtê-lo de seus usuários, essa prática acaba gerando algumas dúvidas

quanto a sua efetividade e se realmente nesses casos o titular dos dados pessoais exerce o consentimento de forma livre, ou se é mascarado pelas políticas adotadas pelas empresas.

Voltaremos, portanto, às políticas de privacidade já citadas no item 1.3.4 que são incluídas pelo mercado para a tomada de consentimento do usuário – inclui-se as novas políticas de cookies – através da análise de Bioni (2021) sobre a carência de efetividade do consentimento.

Ele esclarece que o surgimento dessas políticas ocorreu em meio a uma necessidade do mercado em seu autorregular, pois, embora haja a necessidade de recolhimento de consentimento por parte do titular de dados pessoais de forma expressa, não houve regulamentação que tratasse da forma com que deverá ocorrer sua operacionalização, carecendo então de uma normativa que pudesse concretizar o domínio do controle dos dados pessoais.

O autor enfatiza que essa lógica utilizada pelo mercado em colher o consentimento para a legitimação do tratamento dos dados pessoais continua reforçando o desequilíbrio informacional existente entre o mercado e o cidadão, isso pelo fato de não induzir o usuário ao efetivo exercício de controle sobre suas informações pessoais e o expor a aceitação de um contrato feito pelo próprio fornecedor, que determinará o caminho do fluxo informacional. Bioni também fala que pelo fato de ser um contrato de adesão[53], ao qual o consentimento do consumidor ocorre através da aceitação ou não do que for estabelecido pelo fornecedor, elimina qualquer tipo de controle que o usuário possa ter sobre seus dados pessoais.

Em palavras simplificadas: a tomada de consentimento dos usuários pelos sites a partir da aceitação dessas políticas de privacidade e de cookies, trata-se de mera formalidade, tendo em vista que o cidadão não exerce efetivamente o controle de seus dados pessoais. Na verdade, o consentimento de uma forma geral e para qualquer tipo de tratamento de dados pessoais, segundo Bioni (2021), diante da falta de regulamento não tem sido um instrumento eficaz.

Cardin e Tobbin (2021) também chamam a atenção à falta de eficácia do consentimento quando baseado na aceitação dos termos de uso que se restringem a aceitação instantânea do usuário ( aceito, autorizo, não autorizo), pois limitam o seu direito de escolha ao passo que ele pode sentir necessidade em acessá-lo apenas para que seu acesso não seja excluído.

Quanto a falta de acesso a bens e serviços por parte da liberalidade do titular em não consentir o tratamento de dados pelo utilizador, a lei também prevê (art. 18, inciso VIII) que

[53]O contrato de adesão possui um modelo uniforme com as cláusulas contratuais da relação de consumo definidas pelo contratado (empresa), cabendo ao consumidor conceder seu consentimento (ou não) sobre os termos e condições ali estabelecidos (MARQUES, 2016).

caso o titular dos dados não queira dar consentimento ao controlador para tratamento de seus dados, possui o direito de ser informado sobre as consequências dessa falta de autorização (BRASIL, 2018). Dessa forma, a lei para auxiliar o titular quanto ao seu direito de consentimento, prevê que caso o consentimento ao tratamento de dados seja condicionado para que o controlador forneça acesso de determinado bem ou serviço, o controlador possui o dever de informar os efeitos da negativa (TEFFÉ; TEPEDINO, 2020).

Segundo Bioni (2021), embora o direito do titular a consentir sobre o tratamento de suas informações pessoais seja previsto em vários artigos da LGPD, a lei não proporciona uma regulação efetiva à autodeterminação pois não oferece recursos para que isso aconteça e, por este motivo, seria necessário reavaliar o processo que conduz à autodeterminação informacional, além da criação de novos formatos para instrumentalizar o consentimento do titular de forma eficiente, a fim de que ele consiga ter controle sobre suas informações pessoais.

Há outro ponto que eleva a tecnologia para auxiliar o titular de dados pessoais, que é destacada por Bioni (2021), pela possibilidade ser aliada à proteção de dados pessoais, já existindo proposição neste sentido através da privacy by design (privacidade por concepção), já citada anteriormente, e pelas tecnologias que fazem parte dela, denominadas de tecnologias de facilitação da privacidade (privacy enhancing technologies/PETs) que são ferramentas tecnológicas capazes de auxiliar o indivíduo a controlar os seus dados pessoais, mas que devem ser desenvolvidas no intuito de serem utilizadas facilmente pelos usuário. O autor destaca que tais tecnologias atualmente não se mostram eficazes por não haver regulação sobre o seu uso, o que seria fundamental que houvesse, a fim de que pudesse proporcionar aos usuários a utilização de PETs que seriam " [...] o aparato para um controle genuíno dos dados pessoais [...]" (BIONI, 2021, p. 199).

Ademais, toda essa função atribuída ao consentimento na LGPD e a legislação em si, advém de regulamentação da União Europeia – Diretiva 95/46 item 2.1, ) e da implementação do regulamento 2016/679 denominado General Data Protection Regulation (GDPR) pela União Europeia, tendo a criação da GPDR estimulado ainda mais a criação da LGPD (ALMEIDA; LUGATI, 2020). Foi a GDPR que trouxe previsão expressa sobre o privacy by design (MORASSUTTI, 2019), que atualmente é defendido no Brasil por alguns autores citados neste trabalho, tais como: Fonseca e Mendes (2020), Bioni (2021), como um potencializador material da proteção de dados pessoais no que tange o consentimento do titular dos dados.

Ademais, entende-se que o desenvolvimento de tecnologias que possibilitem a proteção de dados pessoais pode ser um instrumento eficaz, tendo em vista as chamadas

privacidades por concepção (privacy by design), que como citado anteriormente é a ideia uma tecnologia que auxilie na segurança da proteção de dados.

Mas, enquanto não há um marco regulatório que proporcione o efetivo desenvolvimento das PETs, será importante observar que mecanismos a legislação deixou em evidência para que o titular dos dados pessoais possa fazer valer o seu poder de consentimento e quais medidas pode adotar sem que precise recorrer ao Poder Judiciário.

Algo relevante a ser analisado é que embora o Brasil tenha demorado a adotar uma legislação sobre o tratamento dos dados pessoais e assegurar o direito à proteção de dados pessoais como direito fundamental, o país tem crescido exponencialmente com o uso de novas tecnologias e a cada dia  a indústria tem implementado o uso de tecnologias de inteligência artificial, o que eleva a necessidade de regulamentação sobre o seu uso e que deixará mais evidente que em um futuro não tão distante a figura do consentimento deverá ser repensada pelo legislativo a fim de que propicie meios para que seja normatizada – conforme as propostas de implementação de tecnologias que auxiliem os usuários nesse processo de decisão. Vale mencionar que já há em curso o Projeto de Lei nº 5051/2019 proposto pelo Styvenson Valentim (PODEMOS/RN), para estabelecer princípios ao uso da Inteligência Artificial no Brasil, que prevê como um de seus fundamentos garantia à proteção dos dados pessoais e da privacidade (BRASIL, 2019d).

Magrani (2019) já falava que mesmo que o consentimento fosse empregado de forma eficaz na proteção de dados de acordo com a LGPD, seria mesmo assim um desafio empregá-lo na utilização da tecnologia da internet da coisas[54] e da inteligência artificial[55], pois, nesse tipo de tecnologia pelo fato da comunicação de dados ocorre de forma rápida entre os humanos e as máquinas, seria um desafio implementar o consentimento expresso e válido sobre  o tratamento de dados de pessoais na utilização dessas tecnologias.

Desta forma, com base nos autores apresentados, conclui-se que os contornos dados ao consentimento são insuficientes para que ele garanta proteção ao direito de decisão do titular sobre suas informações pessoais, porque não traz uma regulamentação que garanta o efetivo

[54]Internet das coisas ou seu termo em inglês internet of things (IOT), trata-se de uma tecnologia que permite a integração de bens e serviços de forma física ou virtual e através de redes de comunicação que permitem conexão com a internet, o Brasil já possui o Decreto nº 9.854/2019  que institui o Plano Nacional de Internet das coisas a fim de desenvolvê-la no país (art. 1º)  e  que traz a definição de Internet das coisa em seu Art. 2º, inciso I, como sendo "a infraestrutura que integra a prestação de serviços de valor adicionado com capacidades de conexão física ou virtual de coisas com dispositivos baseados em tecnologias da informação e comunicação existentes e nas suas evoluções, com interoperabilidade" (MIRAGEM, 2019).

[55]Inteligência artificial (IA) ou seu termo em inglês artificial intelligence (AI) é a capacidade através de um sistema informatizado de execução de comandos pré-programados e de interpretar dados sem que necessitem ser pré-definidos (MIRAGEM, 2019).

controle do titular sobre as suas informações. E, tendo em vista o cenário tecnológico atual, se faz necessário pensar numa forma que possa proporcionar ao cidadão que o consentimento sobre seus dados pessoais seja válido e não manipulável e que alcance o uso de novas tecnologias, tais como a Internet das Coisas e das Inteligências Artificiais.

Enquanto não existe uso de tecnologias no Brasil que auxiliem o processo de consentimento, vamos propor no próximo tópico quais os mecanismos podem ser utilizados para que o titular dos dados pessoais possa fazer valer o seu direito ao consentimento livre, informado e inequívoco.

## 4.3 OS MECANISMOS QUE PODEM AUXILIAR O TITULAR DOS DADOS PESSOAIS A FAZER VALER O SEU DIREITO AO CONSENTIMENTO

Conforme mencionado no tópico anterior, a forma com que o consentimento é recolhido pelos agentes de tratamento e consentido pelo titular de dados pessoais não vem sendo delineada da forma que realmente deveria ser – as medidas adotadas não tornaram-se eficazes à autodeterminação do titular de dados –, isso tendo em vista que as medidas de autorregulação adotas pelo mercado a fim de tomar o consentimento do titular de dados de forma expressa e por escrito (art. 7º e 8º LGPD), foram adotadas através da utilização de contratos de adesão que de forma unilateral tratam das políticas de privacidade, que de forma algum induzem o usuário a exercer controle efetivo sobre os destinos de seus dados pessoais (BIONI, 2021).

O que acaba acontecendo com a utilização dos contratos de adesão para a finalidade de tomada de consentimento, é que o usuário continua exposto as regras estabelecidas pelo próprio agente de tratamento e não consegue ter informações completas sobre todas as finalidades a que seus dados serão submetidos, o que de certa forma continua abrindo margem ao uso indiscriminado dos dados pessoais.

Importante destacar que embora a legislação não tenha regulamentado um procedimento que deveria ser adotado pelos sites para que o consentimento tivesse realmente o desdobramento daquilo que o seu usuário efetivamente quer e sem ser ludibriado pelas falta ou omissão de informação, há meios que os cidadãos podem utilizar que não necessariamente a necessidade de que tenham de dispor do Sistema Judiciário. Os próximos tópicos irão tratar da possibilidade que cada cidadão poderá utilizar para que faça valer o efetivo cumprimento do seu direito ao consentimento voluntário, sem que precise judicializar sua reclamação.

### 4.3.1 AS OUVIDORIAS PÚBLICAS

A Constituição Federal previu em seu art. 37, §3º a criação de leis a fim de que o usuário dos serviços públicos possa participar da administração pública, seja para prestar reclamações referentes aos serviços públicos (inciso I), seja para obter acesso a informações e registros administrativos (inciso II), seja para representar exercício de serviço negligente ou abusivo de cargo na administração pública (III) (BRASIL, 1988).

As ouvidorias públicas antes mesmo da entrada em vigor da CRFB/88 já existiam no Brasil, tendo como marco a primeira ouvidoria pública criada pelo Município de Curitiba/PR no ano de 1986, são órgãos públicos que possuem independência para desempenhar a função de ouvidor (NASSIF, 2007). O papel do ouvidor adotado pelo Brasil tem como base uma legislação criada na Suécia que previa o cargo de "agente parlamentar de justiça" no ano de 1809, e que trazia ressignificação a um termo de origem escandinava que já existia denominado "*ombudsman"* e que significa representante do povo perante o Estado (NASSIF, 2007).

No Brasil, a legitimação para a criação das ouvidorias ocorreu a partir da previsão constitucional de participação dos usuários trazidas pelo artigo 37 (NASSIF, 2007), tendo como objetivo mediar a comunicação e participação entre Estado e sociedade (BARREIRO; PASSONE; PEREZ, 2018). Para Cardoso (2010), a ouvidoria pública assume importante papel de ampliação e inclusão social, além de fomentar a igualdade de direitos formais e colaborar para a construção de garantias de cidadania e ser fundamental ao processo de desenvolvimento da democracia.

Segundo Nassif (2007), as ouvidorias públicas possuem principalmente a função de ouvir a sociedade e a partir daí garantir que a prestação dos serviços públicos seja realizada de forma eficiente e, portanto, constitui-se um instrumento hábil ao aperfeiçoamento da democracia.

A partir da atribuição às ouvidorias do papel de mediadora sobre os assuntos existentes entre os usuários e serviço público é que ela poderá atuar a fim de estabelecer controle social entre ambas as partes e assumir posição de destaque no que tange a proteção dos dados pessoais do usuário de serviços públicos (LOURENÇO; TAQUES, 2020).

Lourenço e Taques (2020) que trazem a visão de que o papel desenvolvido pelas ouvidorias pode auxiliar o diálogo entre o titular dos dados pessoais que é usuário da administração pública e os próprios órgão públicos, caso haja alguma violação com relação ao tratamento de dados pessoais por parte dos órgãos.

Os autores enfatizam que em decorrência da grande abrangência dos órgãos públicos e da necessidade que eles possuem em ter acesso a uma gama de dados pessoais de seus usuários, os órgãos tornam-se mais suscetíveis a cometerem infrações no tratamento de dados pessoais. E, por este motivo, "na condição de facilitadoras do diálogo, as ouvidorias podem e devem assumir papel de destaque na implementação e efetivação da LGPD" (LOURENÇO; TAQUES, 2020, p. 24).

Segundo os autores, é a partir do artigo 41[56] da LGPD que há possibilidade das ouvidorias públicas tomarem o papel de encarregado previsto pelo artigo. Isto porque, segundo eles, o artigo 40 da Lei de Acesso à Informação possui previsão similar, e porque já havia entendimento por parte da CGU de que as ouvidorias poderiam de fato assumir o papel previsto pelo próprio artigo 40 da Lei de Acesso à Informação, tendo em vista a autoridade prevista no referido artigo e as ouvidorias possuem função similar. Em suma, esse entendimento por parte da CGU foi concluído através da realização de uma pesquisa, e que segundo os autores, a competência das ouvidorias públicas analisada naquele momento para a realização do papel da autoridade previsto pela lei de acesso à informação, pode por analogia encaminhar ao próprio órgão o papel de encarregado previsto pelo art. 41 da LGPD. Desta forma, as duas leis estariam interligadas e as ouvidorias teriam competência para atuar de acordo com os ditames de cada legislação, ademais, a lei de acesso à informação trata da transparência do acesso à informação aos cidadãos, mas também traz regras em que será necessário restringir esse acesso quando tratar-se de informação pessoal, enquanto a LGPD traz as regras para o tratamento de dados pessoais previstos pela lei de acesso à informação. Ou seja, há um diálogo entre as legislações e dessa forma as ouvidorias públicas podem exercer o papel de encarregado, pois, conforme definição trazida pela própria LGPD em seu artigo 4º, inciso VIII, o encarregado seria " "pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)" (BRASIL,

[56]Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.
§ 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.
§ 2º As atividades do encarregado consistem em:
I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
II - receber comunicações da autoridade nacional e adotar providências;
III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.
§ 3º A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados. (BRASIL, 2018).

2018), o que para Lourenço e Taques (2020, p. 25), deixa em evidência que ambos possuem semelhança e isso abre margem para que sejam centralizados em uma única figura.

No caso, o controlador seria o órgão público e o papel de encarregado seria atribuído à ouvidoria pública. Isso porque, conforme citado no item 3, o Poder Público também está submetido ao cumprimento das normas impostas pela Lei Geral de Proteção e, por realizar o tratamento de dados pessoais de seus usuários, a ele é atribuído o papel de controlador. A lei lhe confere essa atribuição quando define no artigo 5º, inciso VI que o controlador pode ser a pessoa jurídica de direito público a quem compete decidir sobre o tratamento de dados pessoais (BRASIL, 2018).

Desta forma, as ouvidorias poderiam ter papel de auxiliadoras de ambas as partes (titular dos dados e controlador), de modo que através do recebimento de reclamações, críticas e elogios, poderiam auxiliar a administração pública, de modo a facilitar a participação e o diálogo entre o usuário do serviço público que tenha seus dados pessoais violados e a administração pública, sem que tenha que recorrer a qualquer outro método e dessa forma garantir os seus direitos (LOURENÇO; TAQUES, 2020).

Como a LGPD prevê a participação do titular sobre a decisão da finalidade de seus dados pessoais, este poderia interagir com órgão público através das ouvidorias que por serem representantes dos usuários de serviços públicos, teriam maior capacidade em resolver as demandas advindas do tratamento de dados pessoais realizado pela administração pública.

Ademais, cabe ressaltar que a LGPD atribui à Autoridade Nacional de Proteção de Dados (ANPD) a possibilidade de emitir parecer técnico a fim de que garanta o cumprimento da lei pelos órgãos públicos (art. 29 LGPD ) e que caso o órgão público cometa alguma infração com relação ao tratamento de dados pessoais previsto na lei, a ANPD poderá apresentar medidas que sejam cabíveis à cessação da violação cometida (art. 31 LGPD). Note-se que a legislação não obriga que medidas de cessação sejam apresentadas pela Autoridade Nacional, apenas prevê que ela possui capacidade, ou seja, isto será liberalidade da própria ANPD.

### 4.3.2 AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD)

A Lei geral de Proteção de dados, por intermédio da Lei nº 13.853/2019 (que incluiu a Autoridade Nacional de Proteção de Dados na LGPD), trouxe um capítulo específico para tratar da ANPD e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (Capítulo IX).

Hoeren e Pinelli (2020) esclarecem que a tarefa da ANPD é monitorar a aplicação da LGPD, criar regulamentos para implementação e aplicação das normas previstas pela lei, além de impor sanções nos casos em que haja violação por parte do agente de tratamento dos dados pessoais.

Como citado várias vezes no decorrer deste trabalho, a Lei Geral de Proteção de dados conferiu direitos ao titular dos dados pessoais, dentre eles a necessidade de consentimento e o seu direito de a qualquer momento requerer informações ao controlador sobre o tratamento de seus dados. O artigo 18 da lei prevê expressamente esses direitos e dá autonomia para que o próprio titular resolva com o controlador qualquer problema existente que se encaixe nas hipóteses previstas pelo referido.

A autonomia conferida ao titular lhe confere os seguintes poderes: requisitar a efetivação deste direito através de requerimento expresso ao agente de tratamento (§ 3º), peticionar sobre os seus dados contra o controlador perante a autoridade nacional para que analise a violação cometida (§1º ), além de prever no mesmo artigo que o seu direito de peticionar contra o controlador também poderá ser exercido perante os organismos de defesa do consumidor (§8º).

Portanto, para além da esfera judiciária, a lei traz previsão de três possíveis formas que o titular dos dados pessoais poderá fazer valer o seu direito quanto a sua autonomia sobre seus dados pessoais. A primeira, na tentativa de resolver o problema diretamente com o controlador e caso isso não funcione – a lei prevê uma ordem, tendo em vista que o artigo 55-J prevê em seu inciso V, que o titular ao peticionar à ANPD deverá comprovar que apresentou reclamação ao controlador e que não foi solucionada – o titular de dados pessoais que também é consumidor, pode peticionar à ANPD, ou a organismos de defesa do consumidor.

A lei também prevê que as sanções previstas na LGPD deverão ser aplicadas pela própria autoridade e que será o órgão central responsável pela interpretação da Lei e do estabelecimento de normas e diretrizes para a sua implementação (art. 55-K).

Com relação ao direito do titular em peticionar à Autoridade Nacional, compete ao próprio órgão "implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta Lei" (art. 55-J, inciso XXIV). A lei não traz maiores especificações quanto a possibilidade de peticionamento de forma física, porém, em seu site explica como deve ocorrer o peticionamento por parte do titular.

No site, há uma aba denominada “canais de atendimento” que dentre as opções disponibiliza atendimento ao cidadão titular dos dados pessoais, explicando que é fundamentalmente necessário que antes de apresentar petição à ANPD é necessário tentar resolver com o controlador o exercício do direito e que caso isso não seja possível, o peticionamento deverá ser realizado através do Sistema Eletrônico de Peticionamento do Sistema Eletrônico de Informações (SEI) e disponibiliza um manual[57] para auxiliar o usuário a cadastrar-se no sistema SEI. Ainda após esse cadastramento, será necessário obter aprovação do cadastro e para isso, o usuário deverá apresentar no Protocolo Central da Presidência da República, o termo de “declaração de concordância e veracidade”[58] preenchido, juntamente com cópias de RG e CPF. Após a aprovação, o usuário poderá protocolar sua reclamação no sistema SEI e aguardar o processo administrativo para apurar as irregularidades (

Cabe ressaltar que o art. 55-J, prevê em seu inciso que compete à ANPD “fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso”, portanto, depreende- se que o processo para apurar as regularidades apresentadas pelo titular ao realizar o peticionamento, ocorrerá conferindo oportunidade de defesa ao controlador.

O procedimento acima referido é um pouco burocrático e requer atenção por parte do titular para que compreenda todos os passos que deve realizar até poder peticionar à ANPD, o que nos leva a conclusão de que pode não ser de fácil acesso aos consumidores, tendo em vista que impõe um procedimento que não será facilmente compreendido por usuários que possuam pouca escolaridade ou que não tenham tanta afinidade com este tipo de burocracia.

### 4.3.3 SITE DO CONSUMIDOR.GOV

Um outro meio hábil a resolver os problemas existentes entre consumidor e fornecedor – abrange também os problemas entre titular de dados pessoais e controlador, tendo em vista que se equipara uma relação de consumo e que a LGPD prevê essa possibilidade (art. 18, §8º).

A política nacional das relações de consumo desenvolveu como um de seus instrumentos o Sistema Nacional de Defesa do Consumidor (SNDC), que está regulamentado pelo decreto nº 2181/1997, é coordenado pela Secretaria Nacional do Consumidor (Senacon) e

[57] Manual disponibilizado para o cadastramento no sistema SEI está disponível em: https://www.gov.br/secretariageral/pt-br/centrais-de-conteudo/manual_usuario_externo_sei_atualizado.pdf

[58] Termo de declaração de concordância e veracidade disponível em: https://www.gov.br/secretariageral/pt-br/sei-peticionamento-eletronico/TermodeDeclaraodeConcordnciaeVeracidadeSEIUsurioExterno.pdf

é composto pelos seguintes órgãos: Procons, Ministério Público, Defensoria Pública, Delegacias de Defesa do Consumidor, Juizados Especiais Cíveis e Organizações Civis de defesa do consumidor (MAIOLINO; TIMM, 2020, p. 86). Ao Senacon, de acordo com o Decreto nº 2181/97, compete fiscalizar e aplicar as sanções previstas pelo CDC, e em outras normas pertinentes à defesa do consumidor (art. 3º, inciso X) (BRASIL, 1997).

O site do consumidor.gov foi criado pelo Decreto nº 8573/2015 no intuito de ser um sistema alternativo para a resolução de conflitos consumeristas e possui como finalidade estimular a autocomposição entre consumidores e fornecedores para a solução de conflitos de consumo (art. 1º). Seus objetivos, de acordo com o art. 2º, são: ampliar o atendimento ao consumidor (inciso I), prevenir violação aos direitos do consumidor (inciso II), promover transparência nas relações consumeristas (inciso III), contribuir para a elaboração e implementação de políticas de defesa do consumidor (inciso IV), estimular a harmonização entre fornecedor e consumidor (inciso V) e incentivo a competitividade através da melhoria da qualidade do atendimento ao consumidor (inciso VI) ( BRASIL, 2015).

As empresas que aderem ao site (a adesão é voluntária) preenchem um termo e se comprometem a analisar e investir esforços a fim de solucionar os problemas apresentados pelos consumidores (CONSUMIDOR.GOV.BR, 2022).

Segundo Maiolino e Timm (2020, p. 88), após a adesão da empresa, ela recebe acesso para responder às reclamações registradas, acompanhar as reclamações em nome da empresa e interagir com o consumidor pela plataforma.

Para que o consumidor tenha acesso a plataforma, basta realizar o cadastro no site, verificar se a empresa está cadastrada no site, registrar sua reclamação e aguardar o prazo de 10(dez) dias para que a empresa responda a sua reclamação e, caso sua reclamação não seja atendida pela empresa, o site recomenda que que o consumidor busque os órgãos do Sistema Nacional de defesa do consumidor (CONSUMIDOR.GOV.BR, 2022).

É um site de fácil acesso e manipulação e está habilitado para atender demandas referentes aos dados pessoais e Privacidade, portanto, mais uma mecanismo que pode ser utilizado caso o titular de dados pessoais necessite abrir reclamação contra o controlador, no entanto, para que sua demanda possa ser respondida pela empresa, será necessário que ela esteja cadastrada no site. Ademais, uma outra possibilidade para o titular de dados pessoais é deslocar-se até uma agência do Procon para registrar sua reclamação, ou procurar outros órgãos, tais como: Defensorias Públicas, Juizados Especiais Cíveis e Ministério Público.

Cabe ressaltar, que a ANPD e o Senacon firmaram acordo de cooperação técnica em 22 de março de 2021, a fim de realizar ações conjuntas na área de proteção de dados pessoais e de defesa do consumidor, uniformização de entendimentos e outras disposições (ANPD, 2021).

## 5 CONCLUSÃO

Tendo em vista os aspectos tratados no presente trabalho, observou-se que a posição do consumidor no ambiente virtual é agravada em decorrência da falta de contato direto com o fornecedor e da falta de informações sobre os produtos e serviços disponibilizados, isto porque a divulgação da informação ocorre de acordo com a liberalidade do fornecedor.

É o fornecedor quem escolhe quais informações quer deixar em evidência e, por este motivo, a relação de consumo no ambiente virtual eleva o grau de vulnerabilidade do consumidor, que já é considerado a parte mais fraca da relação de consumo e que por isso o CDC lhe confere proteção especial.

A realização dessas compras no ambiente virtual, também acabam proporcionando o surgimento de um mercado focado nas informações deixadas pelos próprios consumidores, quando navegam pelos sites e fazem cadastros para a compra de produtos e serviços. Os dados do consumidor tornam-se produtos que podem ser utilizados como moeda de troca por uma grande indústria focada na coleta, armazenamento e tratamento desses dados.

O tratamento desses dados torna-se uma prática comum pelas empresas, no entanto, uma prática que fere direitos constitucionais e faz com que o consumidor pague duas vezes pelo produto: a primeira quando paga efetivamente pelo produto (seja por boleto, cartão de crédito, cartão de débito, pix) e a segunda vez quando o fornecedor recebe os dados pessoais cedidos pelo consumidor  e os torna um produto a ser explorado pela própria empresa ou vende a outros fornecedores, o que escancara sua vulnerabilidade e deixa mais evidente o quanto podem ser manipulados e enganados no ambiente virtual.

Os dados deixados pelos consumidores quando visitam sites e fazem compras pela internet, podem ser facilmente vigiados e armazenados hoje em dia, isso em decorrência do avanço da tecnologia., que possibilita através de softwares e técnicas de coleta de informações a possibilidade de traçar o perfil do usuário a fim de disponibilizar publicidades fundadas no seu gosto, diferenciar consumidores de acordo com o que compram e até mesmo para fins estatísticos. Por isso tais informações são tão úteis aos vários setores do mercado e em especial o Marketing.

Por serem informações pessoais, cabe ao indivíduo consentir quais informações sobre a sua vida podem ser acessadas por terceiros ou não, ainda mais tendo em vista que essas informações podem ocasionar algum tipo de discriminação. É por esse motivo que a proteção de dados pessoais é tão importante e passa a ser delineada no ordenamento jurídico brasileiro com a entrada em vigor da Lei Geral de Proteção de dados, do Marco Civil da internet e passa a ser resguardada pela CRFB/88 expressamente como um direito fundamental (art. 5º, LXXIX).

É com a entrada em vigor da LGPD que o titular ganha a garantia de que terá que consentir (exceto o tratamento de dados previsto no art. 4º da lei), para que eles possam ser utilizados pelos controladores. O consentimento então passa a ser umas das bases legais para o tratamento dos dados pessoais, ao passo que a lei também passa a exigir que seja necessário que o titular dos dados pessoais disponibilize seu consentimento de forma expressa e escrita.

A partir dessa necessidade de consentimento trazida pela LGPD é que este trabalho analisa se ele tem sido efetivamente cumprido e quais os meios extrajudiciais que o consumidor poderá utilizar caso tenha seus dados utilizados sem consentimento. A resposta para o problema é que o consentimento do usuário para o tratamento de seus dados pessoais é extremamente necessário, mas que, no entanto, a legislação não trouxe um suporte para instrumentalizá-lo e garantir que ele seja realizado de forma efetiva e de acordo com a verdadeira vontade do titular de dados pessoais.

Dessa forma, essa falta de regulação faz com que o próprio mercado tome medidas a fim de cumprir essa tomada de consentimento, dentre as quais está a tomada de consentimento do consumidor através de termos de adesão, que nada mais são que contratos feitos unilateralmente e sem a possibilidade de participação do consumidor. O que evidencia que o consentimento fornecido pelo titular de dados pessoais pode ser manipulado em decorrência da falta de informação que pode constar nestes contratos – já que são especificadas pelo próprio controlador e é ele mesmo que escolher quais informações quer disponibilizar – e da falta de entendimento por parte do consumidor, que não tem meios para saber se as informações não estão sendo utilizadas para outras finalidades as quais ele concedeu a autorização.

Ademais, uma alternativa que pode ser adotada pelo consumidor, caso este entenda que o tratamento de seus dados pessoais está sendo feito em discordância com o que foi autorizado por ele, ou até mesmo esteja sendo realizado sem a sua autorização, é recorrer a órgãos que a própria LGPD deixou em evidência que podem ser utilizados por eles.

O consumidor pode recorrer à Agência Nacional de Proteção de dados pessoais (ANPD), caso não consiga elucidar o problema diretamente com o controlador, como também

pode recorrer aos órgãos de defesa do consumidor, dentre eles os procons e o próprio site do consumidor.gov, que já está adequado às demandas sobre proteção de dados pessoais, isso na relação privada. Quanto a relação do usuário de serviço público, uma opção é entrar em contato com as ouvidorias públicas, a fim de que tente solucionar o problema.

**REFERÊNCIAS**

ALMEIDA, Fabricio Bolzan de; LENZA, Pedro. **Direito do Consumidor Esquematizado**. 8. ed. São Paulo: Saraiva Educação, 2020. 920 p.

ALVES, Fabrício Germano. Análise da Possibilidade de Regulação da Publicidade Comportamental (Behavioral Advertising) pelo Microssistema Consumerista. **Revista de Direito, Globalização e Responsabilidade nas Relações de Consumo**, [S.L.], v. 2, n. 1, p. 208-223, 1 jun. 2016. Conselho Nacional de Pesquisa e Pós-graduação em Direito - CONPEDI. http://dx.doi.org/10.26668/indexlawjournals/2526-0030/2016.v2i1.696. Disponível em: https://www.indexlaw.org/index.php/revistadgrc/article/view/696/689. Acesso em: 01 fev. 2022.

ANDRADE, Marta Cleia Ferreira de; SILVA, Naiara Taiz Gonçalves da. O comércio eletrônico (e-commerce): um estudo com consumidores. **Perspectivas em Gestão & Conhecimento**, v. 7, n. 1, p. 98-111, 30 jun. 2017.Disponível em: https://periodicos3.ufpb.br/index.php/pgc/article/view/26895/17910. Acesso em: em 07 fev. 2022.

AVELINO, Rodolfo da Silva. A evolução dos mecanismos de rastreamento e vigilância intrusivos em clientes web. In: SIMPÓSIO INTERNACIONAL LAVITS, 6., 2019, Salvador. **Anais [...] .** Salvador: Lavits - Rede Latino-Americana de Estudos Sobre Vigilância Tecnologia e Sociedade, 2019. p. 1-16. Disponível em: https://www.rodolfoavelino.com.br/a-evolucao-dos-mecanismos-de-rastreamento-e-vigilancia-intrusivos-em-clientes-web/. Acesso em: 16 fev. 2022.

BARRETO, Ricardo de Macedo Menna. Privacidade e redes sociais na internet: notas à luz da lei n. 12.965/2014 (marco civil da internet). **Faculdade de Direito do Sul de Minas**, Pouso Alegre, v. 31, n. 1, p. 261-280, jan./jun. 2015. Semestral. Disponível em: https://www.fdsm.edu.br/adm/artigos/217e4f2765dc938165eff96223c3fa1c.pdf. Acesso em: 15 fev. 2022.

BARUFI, Renato Britto *et al*. A (hiper)vulnerabilidade do consumidor no ciberespaço e as perspectivas da LGPD. **Revista Eletrônica Pesquiseduca**, Santos, v. 13, n. 29, p. 236-255, 21 jan./abr. 2021. Mensal. Disponível em: https://periodicos.unisantos.br/pesquiseduca/article/view/1029. Acesso em: 27 fev. 2022.

BASAN, Arthur Pinheiro. **Publicidade digital e proteção de dados pessoais**: o direito ao sossego - Indaiatuba, SP: Editora Foco, 2021. 264 p.

BENJAMIN, Antonio Herman V.; BESSA, Leonardo Roscoe; MARQUES, Claudia Lima. **Manual de direito do consumidor**. 9. ed. São Paulo: Revista dos Tribunais, 2021. 608 p.

BEZERRA, Arthur Coelho; WALTZ, Igor. Privacidade, neutralidade e inimputabilidade da internet no brasil: avanços e deficiências no projeto do marco civil. **Eptic Online**, [S. L.], v. 16, n. 2, p. 161-175, mai./ago. 2014. Quadrimestral. Disponível em: https://ridi.ibict.br/bitstream/123456789/858/2/Arthur.pdf. Acesso em: 20 fev. 2022.

BIONI, Bruno Ricardo. Compreendendo o conceito de anonimização e dado anonimizado. **Cadernos Jurídicos**, São Paulo, v. 53, n. 21, p. 191-201, 2020. Trimestral. Disponível em:

https://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/ii_9_anonimiza%C3%A7%C3%A3o_e_dado.pdf?d=637250349860810398. Acesso em: 06 mar. 2022.

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021. 311 p.

BORGES, Gabriel Oliveira de Aguiar; VASCONCELOS, Sthéfane Alves. Data mining versus privacidade do consumidor na internet. In: FALEIROS JUNIOR, José Luiz de Moura; LONGHI, João Victor Rozatti (org.). **Estudos essenciais de direito digital**. Uberlândia: Laecc - Laboratório Americano de Estudos Constitucionais Comparados, 2019. Cap. 4. p. 113-130.

BRASIL. **Câmara dos Deputados**. Proposta de Emenda à Constituição - PEC 17/2019, de 03 de julho de 2019. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília: Câmara dos Deputados, 2019b. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2210757. Acesso em: 26 fev. 2022.

BRASIL. **Câmara dos Deputados**. Proposta de Emenda à Constituição - PEC 17/2019, de 03 de julho de 2019. Parecer do Relator, Dep. Orlando Silva (PCdoB-SP), pela aprovação da Proposta de Emenda Constitucional nº 17, de 2019, na forma do Substitutivo de 04 dez. 2019. Brasília: Câmara dos Deputados, 2019c. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1841176&filename=Tramitacao-PEC+17/2019. Acesso em 26 fev. 2022.

BRASIL. **Senado Federal**. Proposta de emenda à constituição N° 17, DE 2019. Diário do Senado Federal. Brasília, 13 mar. 2019a. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=7925004&ts=1640110351856&disposition=inline. Acesso em: 23 fev. 2022.

BRASIL. **Senado Federal**. Projeto de Lei nº N° 5051, DE 2019. Estabelece os princípios para o uso da Inteligência Artificial no Brasil. Brasília, DF: Senado Federal, 2019d. Disponível em:https://legis.senado.leg.br/sdleg-getter/documento?dm=8009064&ts=1646420511147&disposition=inlineAcesso em: 06 mar. de. 2022.

CANTO, Rodrigo Eidelvein do. **A vulnerabilidade dos consumidores no comércio eletrônico e a reconstrução da confiança na atualização do código de defesa do consumidor**. 2014. 224 f. Dissertação (Mestrado) - Curso de Direito, Faculdade de Ciências Jurídicas e Sociais, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2014. Disponível em: https://www.lume.ufrgs.br/handle/10183/211758. Acesso em: 29 jan. 2022.

CARMUÇA, Lia Carolina Vasconcelos. **Sociedade de vigilância, direito à privacidade e proteção de dados pessoais**: uma análise sobre a influência de técnicas de publicidade comportamental na internet no consumidor-usuário. 2021. 279 f. Monografia (Especialização) - Curso de Direito, Centro de Estudos Judiciários, Conselho da Justiça Federal, Brasília, 2021. Disponível em: https://www.cjf.jus.br/cjf/corregedoria-da-justica-federal/centro-de-estudos-judiciarios-1/publicacoes-1/monografias-do-cej2. Acesso em: 27 fev. 2022.

CARVALHO, Marcelo Sávio Revoredo Menezes de. **A trajetória da internet no brasil**: do surgimento das redes de computadores à instituição dos mecanismos de governança. 2006. 240 f. Dissertação (Mestrado) - Curso de Engenharia de Sistemas e Computação, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2006. Disponível em: https://www.cos.ufrj.br/uploadfile/1430748034.pdf. Acesso em: 06 fev. 2022.

CHAGAS, Genira Correia; FERNANDES, Carla Montuori. 21 anos de privatização da Telebras: políticas públicas para o setor de telecomunicações. **Revista Epitic**, [*s. l*], v. 21, n. 3, p. 62-73, 2019. Set.-Dez. Disponível em: https://seer.ufs.br/index.php/eptic/article/view/12469. Acesso em: 15 fev. 2022.

CORTAZIO, Renan Soares. Bancos de dados no Brasil: uma análise do sistema credit scoring à luz da lei n. 13.709/2018 (LGPD). **Revista Eletrônica da Pge-Rj**, [S.L.], v. 2, n. 3, p. 1-28, 16 jun. 2019. Centro de Estudos Jurídicos da Procuradoria Geral do Estado do Rio de Janeiro. http://dx.doi.org/10.46818/pge.v2i3.99. Disponível em: https://revistaeletronica.pge.rj.gov.br/index.php/pge/article/view/99. Acesso em: 12 fev. 2022.

CUNHA, Belinda Pereira da. **Direito do Consumidor**. 4. ed. São Paulo: Saraiva, 2011. 130 p.

DONEDA, Danilo Cesar Maganhoto. **A proteção de dados pessoais nas relações de consumo**: para além da informação creditícia. Brasília: Escola Nacional de Defesa do Consumidor, 2010. 122 p. Disponível em: https://www.defesadoconsumidor.gov.br/images/manuais/vol_2_protecao_de_dados_pessoais.pdf. Acesso em: 02 mar. 2022.

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./ago. 2011. Semestral. Disponível em: https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em: 16 fev. 2022.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais fundamentos da lei geral de proteção de dados pessoais**. 2. ed. São Paulo: Revista dos Tribunais, 2020. 352 p.

DONEDA, Danilo; MACHADO, Diego. Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados. **Revista dos Tribunais**: Caderno Especial, São Paulo, v. 998, n. 1, p. 99-128, dez. 2018. Disponível em: https://www.researchgate.net/publication/330401277_Protecao_de_dados_pessoais_e_criptografia_tecnologias_criptograficas_entre_anonimizacao_e_pseudonimizacao_de_dados. Acesso em: 23 fev. 2022.

FALEIROS JÚNIOR, José Luiz de Moura; MARTINS, Guilherme Magalhães. PROTEÇÃO DE DADOS E ANONIMIZAÇÃO: perspectivas à luz da lei nº 13.709/2018. **Rei - Revista Estudos Institucionais**, [S.L.], v. 7, n. 1, p. 376-397, 30 abr. 2021. Revista Estudos Institucionais. http://dx.doi.org/10.21783/rei.v7i1.476. Disponível em: https://www.estudosinstitucionais.com/REI/article/view/476/681. Acesso em: 02 mar. 2022.

FERNEDA, Ariê Scherreier; FERRAZ, Miriam Olivia Knopik; GUIMARÃES FILHO, Pedro Andrade. A proteção de dados e a defesa do consumidor: autonomia privada frente à privacidade. **Revista Meritum**, Belo Horizonte, v. 15, n. 2, p. 38-52, 2020. Mai./ago. Disponível em: https://doi.org/ 10.46560/meritum.v15i2.7749. Acesso em: 29 jan. 2022.

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: 5 mar. 2022.

FONSECA, Gabriel C. Soares da; MENDES, Laura Schertel. Proteção de dados para além do consentimento: tendências contemporâneas de materialização. **Revista Estudos Institucionais**, Rio de Janeiro, v. 6, n. 2, p. 507-533, 2020. Quadrimestral. Disponível em: https://estudosinstitucionais.com/REI/article/view/521/510. Acesso em: 05 mar. 2022.

FONSECA, Maurício Leopoldino da; NOGUEIRA, Fernanda Araújo Couto e Melo. O consentimento na Lei Geral de Proteção de Dados: autonomia privada e o consentimento livre, informado, específico e expresso. In: GROSSI, Bernardo Menicucci (org.). **Lei Geral de Proteção de Dados**: uma análise preliminar da lei 13.709/2018 e da experiência de sua implantação no contexto empresarial. Porto Alegre: Fi, 2020. p. 15-44.

FONTES, Daniele Kleiner. **Universalização da internet banda larga no Brasil**: o plano nacional de banda larga sob a perspectiva da Análise Jurídica da Política Econômica - AJPE. 2014. 162 f., il. Dissertação (Mestrado em Direito) — Universidade de Brasília, Brasília, 2014. Disponível em: https://repositorio.unb.br/handle/10482/16750. Acesso em: 15 fev. 2022

FREITAS, Michele Siqueira Braga. **O SDLC e a proteção de Dados desde a Conceção e por Defeito**. 2020. 188 f. Dissertação (Mestrado) - Curso de Engenharia Informática, Escola Superior de Tecnologia e Gestão Politécnico do Porto, Margaride, 2020. Disponível em: http://hdl.handle.net/10400.22/17438. Acesso em: 05 mar. 2022.

GROSSI, Bernardo Menicucci. O legítimo interesse como base legal para o tratamento de dados pessoais. In: GROSSI, Bernardo Menicucci (org.). **Lei Geral de Proteção de Dados**: uma análise preliminar da lei 13.709/2018 e da experiência de sua implantação no contexto empresarial. Porto Alegre: Fi, 2020. p. 64-81.

GUIMARÃES, Marcelo Cesar. Geoblocking and geopricing: uma análise à luz da teoria do interesse público de Mike Feintuck. **Law, State And Telecommunications Review**, [S.L.], v. 11, n. 2, p. 87-106, 3 set. 2019. Biblioteca Central da UNB. http://dx.doi.org/10.26512/lstr.v11i2.27025. Disponível em: https://periodicos.unb.br/index.php/RDET/article/view/27025. Acesso em: 16 fev. 2022.

LANZILLO, Anderson Souza da Silva; OLIVEIRA, Fabiane Araújo de. Estado, novas tecnologias e proteção de dados pessoais como direito fundamental. **Revista de Direito, Governança e Novas Tecnologias**, [S. L], v. 7, n. 1, p. 92-107, jan./jul. 2021. Semestral. Disponível em: https://scholar.google.com.br/scholar?hl=pt-BR&as_sdt=0%2C5&q=ESTADO%2C+NOVAS+TECNOLOGIAS+E+PROTE%C3%87%C3%83O+DE+DADOS+PESSOAIS+COMO+DIREITO+FUNDAMENTAL&btnG=. Acesso em: 24 fev. 2022.

LÊDO, Ana Paula Ruiz Silveira; MARQUESI, Roberto Wagner; SABO, Isabela Cristina. A necessidade do diálogo das fontes nas relações de consumo SUSCETÍVEIS AO COMÉRCIO ELETRÔNICO. **Revista Quaestio Iuris**, [S.L.], v. 11, n. 2, p. 757-775, 20 abr. 2018. Universidade de Estado do Rio de Janeiro. http://dx.doi.org/10.12957/rqi.2018.30346. Disponível em: https://www.e-

publicacoes.uerj.br/index.php/quaestioiuris/article/view/30346/24688. Acesso em: 05 mar. 2022.

LEONARDI, Marcel. **Tutela e privacidade na internet**. São Paulo: Saraiva, 2011. 402 p.

LOURENÇO, Ana Lucia; TAQUES, João Daniel Vilas Boas. O papel das ouvidorias públicas na implementação da lei geral de proteção de dados (LGPD). **Revista do Ministério Público de Contas do Estado do Paraná**, Curitiba, v. 7, n. 13, p. 12-28, 2020. Semestral. Disponível em: https://revista.mpc.pr.gov.br/index.php/RMPCPR/issue/view/2/1. Acesso em: 24 fev. 2022.

LUGATI, Lys Nunes; ALMEIDA, Juliana Evangelista de. Da evolução das legislações sobre proteção de dados: a necessidade de reavaliação do papel do consentimento como garantidor da autodeterminação informativa. **Revista de Direito**, [S.L.], v. 12, n. 02, p. 01-33, 27 ago. 2020. Revista de Direito. http://dx.doi.org/10.32361/2020120210597. Disponível em: https://doi.org/10.32361/2020120210597. Acesso em: 05 mar. 2022.

MAGRANI, Eduardo. **Entre dados e robôs**: ética e privacidade na era da hiperconectividade. 2. ed. Porto Alegre: Arquipélago Editorial, 2019. 304 p.

MARQUES, Claudia Lima. **Contratos no Código de Defesa do Consumidor**: o novo regime das relações contratuais. 8. ed. São Paulo: Revista dos Tribunais, 2016. 1596 p.

MENDES, Laura Schertel. **Transparência e privacidade**: violação e proteção da informação pessoal na sociedade de consumo. 2008. 156 f. Dissertação (Mestrado) - Curso de Direito, Departamento de Pós-Graduação, Universidade de Brasília - UnB, Brasília, 2008. Disponível em: https://repositorio.unb.br/handle/10482/4782. Acesso em: 30 jan. 2022.

MIRAGEM, Bruno. Novo paradigma tecnológico, mercado de consumo digital e o direito do consumidor. **Revista de Direito do Consumidor**, São Paulo, v. 125, n. 25, p. 17-62, set-out/2019. Bimestral. Disponível em: https://revistadedireitodoconsumidor.emnuvens.com.br/rdc/article/view/1243. Acesso em: 06 mar. 2022.

MORASSUTTI, Bruno Schimitt. **Regulação de tecnologias e arquitetura de sistemas**: um estudo sobre o privacy by design e a transparência aplicada a algoritmos computacionais. 2019. 182 f. Dissertação (Mestrado) - Curso de Direito, Escola de Direito, Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2019. Disponível em: http://tede2.pucrs.br/tede2/handle/tede/8794. Acesso em: 05 mar. 2022.

NASPOLINI, Samyra Haydêe dal Farra; ROSSINI, Valéria. Obsolescência programada e meio ambiente: a geração de resíduos de equipamentos eletroeletrônicos. **Revista de Direito e Sustentabilidade**, Brasília, v. 3, n. 1, p. 51-71, jan./jun. 2017. Semestral. Disponível em: https://pdfs.semanticscholar.org/b618/a00eda1752b552862ff1fffc17b28e69bb72.pdf. Acesso em: 10 fev. 2022.

NEVES, Thiago Ferreira Cardoso. O comércio eletrônico e o direito do consumidor. **R. Emerj**, Rio de Janeiro, v. 17, n. 64, p. 154-163, 2014. Jan.- Abr. Disponível em: https://www.emerj.tjrj.jus.br/revistaemerj_online/edicoes/revista64/revista64_154.pdf.. Acesso em: 02 fev. 2022.

OLIVA, Milena Donato; VIÉGAS, Francisco de Assis. Tratamento de dados para a concessão de crédito. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito brasileiro**. 2019. ed. São Paulo: Revista dos Tribunais, 2019. Cap. 6. p. 561-599.

OLIVEIRA, Deymes Cachoeira de; SOBHIE, Amir Ayoub. Proteção do consumidor no comércio eletrônico: inovações relevantes para as vendas on-line no brasil a partir do decreto federal nº 7.962/2013. **Revista Eletrônica de Iniciação Científica.**, Itajaí, v. 4, n. 4, p. 84-107, 2013. 4º Trimestre. Disponível em: https://www.univali.br/graduacao/direito-itajai/publicacoes/revista-de-iniciacao-cientifica-ricc/edicoes/Lists/Artigos/Attachments/934/Arquivo%2006.pdf. Acesso em: 10 fev. 2022.

OLIVEIRA, Ricardo; COTS, Márcio (coord.). **O legítimo interesse e a LGPDP: Lei Geral de Proteção de Dados Pessoais**. 1 ed. São Paulo: Revista dos Tribunais, 2020. 312 p.

PERILLI, Paulo Roberto Godoy. Proteção de dados, privacidade e o Marco Civil da Internet. In: GROSSI, Bernardo Menicucci (org.). **Lei Geral de Proteção de Dados**: uma análise preliminar da lei 13.709/2018 e da experiência de sua implantação no contexto empresarial. Porto Alegre: Fi, 2020. p. 192-213.

RAMOS, Pedro Henrique. **A regulação de proteção de dados e seu impacto para a publicidade online**: um guia para a LGPD. um guia para a LGPD. 2019. Disponível em: https://baptistaluz.com.br/a-regulacao-de-protecao-de-dados-e-seu-impacto-para-a-publicidade-online-um-guia-para-a-lgpd/. Acesso em: 22 fev. 2022.

ROCHA, Sidney Cassio Alves. O direito à privacidade e o direito à proteção de dados na Lei Geral de Proteção de Dados. In: GROSSI, Bernardo Menicucci (org.). **Lei Geral de Proteção de Dados**: uma análise preliminar da lei 13.709/2018 e da experiência de sua implantação no contexto empresarial. Porto Alegre: Fi, 2020. p. 133-150.

SALDANHA, João Lucas Vieira. A concepção de privacidade através dos tempos: do rupestre à lei geral de proteção de dados pessoais. In: GROSSI, Bernardo Menicucci (org.). **Lei Geral de Proteção de Dados**: uma análise preliminar da lei 13.709/2018 e da experiência de sua implantação no contexto empresarial. Porto Alegre: Fi, 2020. p. 232-267.

SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais**: uma teoria geral dos direitos fundamentais na perspectiva constitucional. 13. ed. Porto Alegre: Livraria do Advogado, 2018. 515 p.

SILVA, Rodrigo Fernandes da. **A qualidade do serviço de acesso à internet para os consumidores brasileiros: um estudo sobre os elementos mais relevantes para a qualidade percebida pelos clientes.** 2020. Dissertação (Mestrado em Administração). Escola de administração de empresas de São Paulo, Fundação Getúlio Vargas, São Paulo. Disponível em: https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/29008/Operacao-Tecnologia-SilvaRodrigo-Disserta%c3%a7aoMPA_Final_ok.pdf?sequence=3&isAllowed=y. Acesso em: 19 fev. 2022.

SILVA, Rosane Leal da. Contratos Eletrônicos e a Proteção de dados Pessoais do Consumidor: diálogo de fontes entre o código de defesa do consumidor e o marco civil da internet. **Revista de Direito, Governança e Novas Tecnologias**, [S.L.], v. 2, n. 1, p. 74-91, 21 out. 2016. Conselho Nacional de Pesquisa e Pós-graduação em Direito - CONPEDI.

http://dx.doi.org/10.26668/indexlawjournals/2526-0049/2016.v2i1.805. Disponível em: https://indexlaw.org/index.php/revistadgnt/article/view/805/pdf. Acesso em: 01 fev. 2022.

TASSO, Fernando Antonio. A responsabilidade civil na Lei Geral de Proteção de Dados e sua interface com o Código Civil e o Código de Defesa do Consumidor. Direito Digital e proteção de dados pessoais. **Cadernos Jurídicos**, São Paulo, v. 21, n. 53, p. 97-115, jan./mar. 2020.Trimestral.

TEFFÉ, Chiara Spadaccini de; TEPEDINO, Gustavo. CONSENTIMENTO NA CIRCULAÇÃO DE DADOS PESSOAIS. **Revista Brasileira de Direito Civil – Rbdcivil**, Belo Horizonte, v. 25, n. 03, p. 83-116, 2020. Trimestral. Disponível em: https://rbdcivil.emnuvens.com.br/rbdc/article/view/521/389. Acesso em: 04 mar. 2022.

THEODORO JÚNIOR, Humberto. **Direitos do consumidor**. 10. ed. Rio de Janeiro: Forense, 2021. 606 p.

TOMÉ, Luciana Mota. Comércio eletrônico. **Caderno Setorial Etene**, Fortaleza, v. 3, n. 43, p. 1-9, set. 2018. Disponível em: https://www.bnb.gov.br/s482-dspace/handle/123456789/358. Acesso em: 01 fev. 2022.

VALENTE, Jonas. A atuação de organizações ativistas na regulação da proteção de dados pessoais no Brasil: o caso da lei geral de proteção de dados (nº 13.709 de 2018). In: CZYMMECK, Anja (ed.). **Proteção de dados pessoais**: privacidade versus avanço tecnológico. Rio de Janeiro: Konrad Adenauer Stiftung, 2019. p. 49-70. (Cadernos Adenauer xx (2019), nº3). Disponível em: https://www.kas.de/documents/265553/265602/Caderno+Adenauer+3+Schutz+von+pers%C3%B6nlichen+Daten.pdf. Acesso em: 19 fev. 2022.

WATFE, Clarice Garcia de Campos. **A internet e a violação da intimidade e privacidade**. 2006. 119 f. Dissertação (Mestrado) - Curso de Mestrado em Ciências Jurídicas, Cesumar - Centro Universitário de Maringá, Maringá, 2006. Disponível em: https://www.sapili.org/portugues/a-internet-e-a-violacao-da-intimidade-e-privacidade-clarice-garcia-de-campos-watfe. Acesso em: 16 fev. 2022.

BRASIL. Lei nº 12527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Brasília, 18 nov. 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 10 fev. 2022.

BRASIL. Lei nº 9742, de 16 de julho de 1997. Dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais, nos termos da Emenda Constitucional nº 8, de 1995. Brasília, 17 jul. 1997.Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9472.htm. Acesso em: 11 fev. 2022.

BRASIL. Decreto nº 3294, de 15 de dezembro de 1999. Institui o Programa Sociedade da Informação e dá outras providências. Brasília, 16 dez. 1999. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/d3294.htm. Acesso em: 12 fev. 2022.

BRASIL. Lei nº 10052, de 28 de novembro de 2000. Institui o Fundo para o Desenvolvimento Tecnológico das Telecomunicações – Funttel, e dá outras providências. Brasília, 29 nov. 2000. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l10052.htm. Acesso em: 12 fev. 2022.

BRASIL. Decreto nº 9612, de 17 de dezembro de 2018. Dispõe sobre políticas públicas de telecomunicações. Brasília, 18 dez. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9612.htm. Acesso em: 12 fev. 2022.

BRASIL. Decreto nº 7962, de 15 de março de 2013. Regulamenta a Lei nº 8.078, de 11 de setembro de 1990, para dispor sobre a contratação no comércio eletrônico. Brasília, 15 mar. 2013. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/decreto/d7962.htm. Acesso em: 12 fev. 2022.

BRASIL. Lei nº 12414, de 09 de junho de 2011. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Brasília, 10 jun. 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 13 fev. 2022.

BRASIL. Lei nº 13709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 06 fev. 2022.

BRASIL. Lei nº 12965, de 23 de abril de 2014. Regulamento estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, 24 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 06 fev. 2022.

BRASIL. Lei nº 8078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, 12 set. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 25 jan. 2022.

BRASIL. Emenda Constitucional nº 115, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília, 11 fev. 2022. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 01 mar. 2022.

BRASIL. Decreto nº 9854, de 25 de junho de 2019. Institui o Plano Nacional de Internet das Coisas e dispõe sobre a Câmara de Gestão e Acompanhamento do Desenvolvimento de Sistemas de Comunicação Máquina a Máquina e Internet das Coisas. Brasília, 26 jun. 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D9854.htm. Acesso em: 06 mar. 2022.

GENERA (São Paulo). **Teste de ancestralidade**. Disponível em: https://www.genera.com.br/. Acesso em: 06 mar. 2022.

BRASIL. Constituição (**1988**). Constituição da República Federativa do Brasil. Brasília, DF. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 06 mar. 2022.

ANATEL, Agência nacional de Telecomunicações; NORMA 004/1995. Uso de meios da rede pública de telecomunicações para acesso à internet. Disponível em:https://www.anatel.gov.br/hotsites/Direito_Telecomunicacoes/TextoIntegral/ANE/prt/minicom_19950531_148.pdf. Acesso em 15 fev. 2022.

DELOITTE. **O valor da publicidade no brasil: O impacto do setor nos negócios, na economia e na sociedade**. 2021. Disponível em: <https://www.abap.com.br/wp-content/uploads/2021/09/deloittevalorpublicidadeptdigital.pdf>. Acesso em: 20 fev. 2022.

SÃO LUCAS CLÍNICA E HOSPITAL. Política de privacidade e cookies. 2021. Disponível em: https://policlinicasaolucas.com.br/lgpd.pdf. Acesso em: 06 mar. 2022.

SERASA EXPERIAN. Conheça o seu público-alvo com a mais completa solução de segmentação de consumidores. Disponível em: https://www.serasaexperian.com.br/solucoes/mosaic/. Acesso em 27 fev. 2022.

PAESANI, Liliana Minardi. **Direito e Internet**: liberdade de informação, privacidade e responsabilidade civil. 6. ed. São Paulo: Atlas, 2013. 128 p.

LINS, Bernardo Felipe Estellita. A evolução da Internet: uma perspectiva histórica. **Cadernos Aslegis**, Brasília, n. 48, p. 11-45, jan./abr. 2013. Trimestral. Disponível em: https://aslegis.org.br/files/cadernos/2013/caderno-48/Aslegis48_baixa.pdf. Acesso em: 06 mar. 2022.

CARDOSO, Antonio Semeraro Rito. **Ouvidoria pública como instrumento de mudança**.2010. Disponível em: https://www.ipea.gov.br/portal/index.php?option=com_content&view=article&id=5034. Acesso em: 07 mar. 2022.

BARREIRO, Adriana Eugênia Alvim; PASSONE, Eric Ferdinando Kanai; PEREZ, José Roberto Rus. ESTADO, CIDADANIA E OUVIDORIAS PÚBLICAS NO BRASIL. **Revista Científica da Associação Brasileira de Ouvidores/Ombudsman**, [*s. l*], v. 1, n. 1, p. 13-28, 2017/2018. Disponível em: http://revista.abonacional.org.br/files/edicoes/artigos/1_1.pdf. Acesso em: 07 mar. 2022.

LORENZETTI, Caroline Schneider; VERDUM, Kelvin. Top 5 Fake News mais absurdas sobre a vacina. UFSM, 2021. Disponível em: https://www.ufsm.br/midias/experimental/agencia-da-hora/2021/11/11/top-5-fake-news-mais-absurdas-sobre-a-vacina/. Acesso em 27 fev. 2022

MARTINS, Marcelo Guerra; TAKEONI, Victor Augusto. Proteção de dados pessoais e democracia: fake news, manipulação do eleitor e o caso da Cambridge Analytica. **Redes**: Revista Eletrônica Direito e Sociedade, Canoas, v. 7, n. 3, p. 135-148, out. 2019. Disponível em: http://dx.doi.org/10.18316/redes.v7i3.5610. Acesso em: 01 mar. 2022.

CARDIN, Valéria Silva Galdino; TOBBIN, Raissa Arantes. Política de cookies e a "crise do consentimento": lei geral de proteção de dados e a autodeterminação informativa. **Revista da**

**Faculdade de Direito da UFRGS**, Porto Alegre, n. 7, p. 241-262, dez. 2021. Disponível em: https://doi.org/10.22456/0104-6594.113663. Acesso em: 01 mar. 2022.

SANTOS, Wellington Fonseca dos; SILVA, Michael César. O DIREITO DO CONSUMIDOR NAS RELAÇÕES DE CONSUMO VIRTUAIS. **Revista da Faculdade Mineira de Direito - PUC Minas,** [*s. l*], v. 15, n. 30, p. 119-147, jan./jun.2012. Semestral. Disponível em: Revista da Faculdade Mineira de Direito. Acesso em: 01 mar. 2022.

BRITO, Lucimeire Zago de; CARNEIRO, Aline Ferreira Costa; TAVARES, Viviane Ramoni. Compliance Digital: novas perspectivas sobre ética na sociedade da informação. In: LONGHI, João Victor Rozatti *et al* (org.). **Fundamentos do Direito Digital**. Uberlândia: Laecc - Laboratório Americano de Estudos Constitucionais Comparados, 2020. Cap. 9. p. 207-229.

PAPA, Uriel de Almeida. **A regulação brasileira do registro de nomes de domínios em perspectiva comparada**. 2011. Disponível em: https://portal.tcu.gov.br/biblioteca-digital/a-regulacao-brasileira-do-registro-de-nomes-de-dominios-em-perspectiva-comparada.htm. Acesso em: 04 mar. 2022.

NASSIF, Gustavo Costa. **Ouvidorias públicas instrumento de aprimoramento da democracia**. 2007. 242 f. Dissertação (Mestrado) - Curso de Direito, Faculdade Mineira de Direito, Pontifícia Universidade Católica de Minas Gerais, Belo Horizonte, 2007. Disponível em: http://www.biblioteca.pucminas.br/teses/Direito_NassifGC_1.pdf. Acesso em: 08 mar. 2022.

CONSUMIDOR.GOV.BR. **Conheça o consumidor.gov.br**. Disponível em: https://www.consumidor.gov.br/pages/principal/empresas-participantes. Acesso em: 08 mar. 2022.

ANPD. **ANPD e Senacon assinam acordo de cooperação técnica**. 2021. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-e-senacon-assinam-acordo-de-cooperacao-tecnica. Acesso em: 08 mar. 2022

Autoridade Nacional de Proteção de Dados. **Petição de Titular**. 2021. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/cidadao-titular-de-dados/peticao-de-titular-contra-controlador-de-dados. Acesso em: 08 mar. 2022.

BRASIL. Lei nº 13853, de 08 de julho de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Brasília, 20 dez. 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Acesso em: 08 mar. 2022.

BRASIL. Decreto nº 2181, de 20 de março de 1997. Dispõe sobre a organização do Sistema Nacional de Defesa do Consumidor - SNDC, estabelece as normas gerais de aplicação das sanções administrativas previstas na Lei nº 8.078, de 11 de setembro de 1990, revoga o Decreto Nº 861, de 9 julho de 1993, e dá outras providências. Brasília, 21 mar. 1997. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/d2181.htm. Acesso em: 08 mar. 2022.

BRASIL. Decreto nº 7738, de 28 de maio de 2012. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão do Conselho Administrativo de Defesa Econômica – CADE; remaneja cargos em comissão e funções de confiança; altera os Decretos nº 6.061, de 15 de março de 2007, nº 2.181, de 20 de março de 1997, e nº 1.306, de 9 de novembro de 1994. Brasília, 29 maio 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/decreto/d7738.htm. Acesso em: 08 mar. 2022.

BRASIL. Decreto nº 8573, de 19 de novembro de 2015. Dispõe sobre o Consumidor.gov.br, sistema alternativo de solução de conflitos de consumo, e dá outras providências. Brasília, 20 nov. 2015. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/decreto/D8573.htm. Acesso em: 08 mar. 2022.

HOEREN, Thomas; PINELLI, Stefan. A NOVA LEI BRASILEIRA DE PROTEÇÃO DE DADOS - UMA VISÃO CRÍTICA. In: WACHOWICZ, Marcos (org.). **Proteção de dados pessoais em perspectiva**: LGPD e RGPD na ótica do direito comparado. 22. ed. Curitiba: Gedai/UFPR, 2020. p. 25-38.

MAIOLINO, Isabela; TIMM, Luciano Benetti. Como as plataformas digitais podem promover a desjudicialização. Direito Digital e proteção de dados pessoais. **Cadernos Jurídicos**, São Paulo, v. 21, n. 53, p.81-93, jan./mar. 2020.Trimestral.