

**UNIVERSIDADE DE CAXIAS DO SUL  
CAMPUS UNIVERSITÁRIO DA REGIÃO DAS HORTÊNSIAS  
ÁREA DO CONHECIMENTO DE CIÊNCIAS JURÍDICAS  
BACHARELADO EM DIREITO**

**ALINE GIL**

**LEI GERAL DE PROTEÇÃO DE DADOS E A VULNERABILIDADE DO  
CONSUMIDOR NA ERA DIGITAL**

**CANELA  
2022**

**ALINE GIL**

**LEI GERAL DE PROTEÇÃO DE DADOS E A VULNERABILIDADE DO  
CONSUMIDOR NA ERA DIGITAL**

Trabalho de Conclusão de Curso apresentado no Curso de Bacharelado em Direito da Universidade de Caxias do Sul, Campus Universitário da Região das Hortênsias, como requisito parcial à obtenção do título de Bacharel em Direito. Área de Concentração: Direito Civil e Direito do Consumidor.

Orientador Prof. Me. Luiz Fernando Castilhos Silveira

**CANELA  
2022**

**ALINE GIL**

**LEI GERAL DE PROTEÇÃO DE DADOS E A VULNERABILIDADE DO  
CONSUMIDOR NA ERA DIGITAL**

Trabalho de Conclusão de Curso apresentado no Curso de Bacharelado em Direito da Universidade de Caxias do Sul, Campus Universitário da Região das Hortênsias, como requisito parcial à obtenção do título de Bacharel em Direito. Área de Concentração: Direito Civil e Direito do Consumidor.

**Aprovada em 12 de agosto de 2022.**

**Banca Examinadora**

---

Prof. Me. Luiz Fernando Castilhos Silveira Orientador  
Universidade de Caxias do Sul – UCS

---

Convidado (a): Me. Fernanda Martinotto  
Universidade de Caxias do Sul – UCS

---

Convidado(a): Me. Moisés João Rech  
Universidade de Caxias do Sul – UCS

## AGRADECIMENTOS

Agradeço aos meus pais Loiva e Luciano, por me ensinarem a querer mais, a estudar e a não colocar limites nos meus sonhos. Deles, desde muito cedo eu tive as palavras mais doces de incentivo, os melhores exemplos de resiliência e coragem, sem o amor deles a realização deste sonho não seria possível.

A minha amada irmã Carol, tão doce e inocente que me fez ter vontade de dar voz e direitos para aqueles que não os têm.

Ao Matheus, que me apoiou desde o início da trajetória acadêmica e passou comigo os piores e melhores momentos da construção deste trabalho, acreditando em mim quando nem eu mesmo acreditava, certamente a presença dele fez essa caminhada mais leve.

Aos meus avós Teresinha e Waldomiro, que acompanharam cada passo da graduação torcendo com afincos para verem a neta deles formada numa profissão que eles tanto admiram.

Aos meus avós Lauro e Iria (*in memoriam*).

Aos tantos amigos que fiz durante o curso, nestes anos dividimos conhecimento, angústias e perrengues. Aos mestres e professores que acrescentaram e dividiram tanto conhecimento, em especial ao Prof. Luiz, sem a orientação dele, este trabalho não seria possível.

A Edy, que nestes anos se mostrou mais que uma amiga, estando presente em todos os momentos, me encorajando, apoiando, sobretudo entendendo meus momentos de ausência.

Aos queridos colegas de trabalho, em especial ao Arthur, Nath, Rachel, Ju e Michele com quem divido meus anseios e dúvidas, neles enxergo o tipo de profissional que um dia quero ser.

Por último, dirijo meu agradecimento ao Mauro, “A felicidade existe para aqueles que acreditam na beleza dos seus sonhos”. Obrigada, mil vezes obrigada, por ter acreditado e tornado a realização do meu sonho possível.

## RESUMO

O presente trabalho analisa a Lei Geral de Proteção de Dados, que colocou o Brasil na lista de mais de 100 países que possuem legislação destinada a proteger a privacidade e uso de dados pessoais, além de verificar o impacto de sua publicação para as transações e relações geradas no meio digital, bem como os desafios encontrados pelos consumidores e empresas de se adequarem a mesma. Considerando a evolução do comércio eletrônico, a Lei Geral de Proteção de Dados é tida como um grande avanço para a sociedade, que doutrinou o conceito de dado pessoal e trouxe meios para protegê-lo de uso indiscriminado, aplicando sanções, que vão desde uma advertência até a aplicação de multa. Através do presente trabalho, entenderemos que para a real efetivação da Lei, além do conhecimento desta, é necessário o desenvolvimento de uma cultura de proteção de dados, por todas as pessoas que utilizam serviços, realizam compras ou se comunicam em meio digital, procurando seguir os princípios da lei e atender aos direitos dos titulares dos seus dados. Analisaremos também o impacto e as ferramentas existentes hoje tanto para as empresas que utilizam do meio digital para fomentar o consumo por meio de anúncios e demais formas de abordagens e a problemática do acesso ilimitado aos dados dos usuários e terceiros, quanto dos consumidores que devem ter conhecimento de como seu direito é preservado.

Palavras-chave: Lei Geral de Proteção de Dados; direito do consumidor; comércio eletrônico.

## **ABSTRACT**

This work was written with the intention of analysing the General Law of Data Protection, that put Brazil on the list of the over a 100 countries that have a legislation destined to protect the privacy and use of personal data, besides verifying the impact of its publication for transactions and relations generated in the digital medium, as well as the challenges found by consumers and companies to suit themselves to it. Considering the evolution of e-commerce, the General Law of Data Protection is seen as a great breakthrough for society, that edified the concept of personal data and brought the means to protect it from indiscriminate use, applying sanctions, that goes from warnings to fines. Through this work, we shall understand that to the actual realization of the law, in addition to knowledge of it, is necessary the development of a culture of data protection by everyone that uses these services, makes purchases or otherwise communicates through the digital medium, looking to follow the principles of the law and meet the rights of the data owners. We will also analyze the impact and the tools that exists today to companies that utilizes the digital medium to promote consumption through ads and other forms of approach and the problems of unlimited access to users and third parties data and the consumers need to know how their rights are preserved.

Keywords: General Law of Data Protection; consumer rights; e-commerce.

## LISTA DE ABREVIATURAS E SIGLAS

ANPD	Autoridade Nacional de Proteção de Dados Pessoais
CDC	Código de Defesa do Consumidor
CPF	Cadastro de Pessoa Física
GDPR	General Data Protection Regulation
LGPD	Lei Geral de Proteção de Dados
MP	Ministério Público
PROCON	Programa de Proteção e Defesa do Consumidor
RG	Registro Geral
SENACON	Secretária Nacional do Consumidor

## SUMÁRIO

<b>1</b>	<b>INTRODUÇÃO .....</b>	<b>8</b>
<b>2</b>	<b>INTERNET COMO MEIO DE CONSUMO.....</b>	<b>10</b>
2.1	DADOS DE USO DA INTERNET NO BRASIL NOS ÚLTIMOS ANOS .....	10
2.2	COMÉRCIO ELETRÔNICO.....	12
2.3	MARCO CIVIL DA INTERNET .....	15
2.4	DIREITO E DEFESA DO CONSUMIDOR .....	19
<b>3</b>	<b>LEI GERAL DE PROTEÇÃO DE DADOS E A VULNERABILIDADE DO CONSUMIDOR NA ERA DIGITAL.....</b>	<b>24</b>
3.1	LEI GERAL DE PROTEÇÃO DE DADOS .....	24
3.2	PRINCÍPIOS DA LEI GERAL DE PROTEÇÃO DE DADOS.....	27
3.3	PRINCIPAIS CONCEITOS .....	32
3.4	AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD).....	37
3.5	RESPONSABILIDADE CIVIL .....	39
3.6	A VULNERABILIDADE DO CONSUMIDOR.....	42
<b>4</b>	<b>ANÁLISE DE CASOS ENVOLVENDO O VAZAMENTO DE DADOS NO BRASIL À LUZ DA LGPD.....</b>	<b>47</b>
4.1	DROGARIA RAIA .....	47
4.2	MEGAVAZAMENTO DE DADOS DE 223 MILHÕES DE BRASILEIROS .....	48
4.3	CAMBRIDGE ANALYTICA – DADOS DE BRASILEIROS.....	49
4.4	BANCOS .....	50
4.5	APPLE – APLICATIVO DE ENVELHECIMENTO FACIAL .....	51
<b>5</b>	<b>CONCLUSÃO .....</b>	<b>53</b>
	<b>REFERÊNCIAS.....</b>	<b>55</b>

## 1 INTRODUÇÃO

Com a popularização do acesso a internet, iniciando sua maior difusão nos últimos anos, houve uma profunda mudança na forma em que as pessoas enxergam o mundo, se comunicam e interagem uns com os outros. A distância antes existente entre culturas e países passou a ser explorada em um único clique, de forma que o distanciamento físico deixou de representar um obstáculo real para as relações e transações em geral.

Desta forma, para muitas empresas os dados pessoais de seus clientes, hábitos de consumo e interações com seus produtos, permanecem sendo seus principais ativos. Assim, no meio digital não poderia ser diferente, sendo inclusive mais evidente, já que não é exagero mencionar que existem mecanismos que monitoram cada clique e armazenam todos os dados de quem os acessa, suas preferências, históricos de busca e comportamento de consumo.

Com relação à legislação, o Brasil possui apenas uma Lei Civil sobre o tema, o Marco Civil da Internet, que está próximo de completar uma década, surgiu num contexto de necessidade de proteção e segurança aos usuários das redes.

Mesmo com uma legislação específica, a facilidade com que os dados dos consumidores são obtidos na esfera virtual representa cada vez mais a necessidade de proteção dos direitos dos usuários, refletindo num problema cada vez mais preocupante: o que possíveis vazamentos ou o uso indiscriminado destes dados podem trazer como consequência ao consumidor?

É natural que não somente as relações interpessoais, mas o consumo e demais transações comerciais ocorram no ambiente online que vive em constante crescimento.

Neste contexto, a Lei Geral de Proteção de Dados surge a fim de trazer maior segurança aos usuários, afetando diretamente na maneira em que os dados dos consumidores são coletados e tratados, sendo reconhecida como o maior avanço legislativo sobre o assunto desde o Marco Civil da Internet.

A LGPD trouxe à tona a necessidade de bom senso de quem lida com os dados dos usuários, procurando penalizar severamente os excessos e abusos cometidos, por meio da definição concreta da responsabilidade e dever de indenizar.

Nesta senda, um dos objetivos deste trabalho é adentrar na vulnerabilidade do consumidor final no comércio digital, sendo considerado o contexto em que essa

problemática é envolvida. Como já referido, com o passar dos dias, a Internet, que permanece em constante evolução, se torna mais acessível e atrativa, utiliza de estratégias e propagandas com o objetivo claro de cativar seu público-alvo, que muitas das vezes não tem noção do risco que a disponibilização dos dados sem critério pode trazer.

Por isso, além de analisar o comportamento das empresas que utilizam o comércio eletrônico como meio para estimular e aumentar o consumo, deve-se observar como estas empresas lidam e armazenam os dados do consumidor final.

A abordagem a ser feita no presente trabalho se dará através do método dedutivo, a forma de pesquisa será a básica, visto que a análise a ser estruturada no presente trabalho se dará com a finalidade de obtenção de respostas, isto posto, as conclusões serão obtidas através da análise de dados objetivos, leis e doutrinas.

Desta forma, no primeiro capítulo, abordaremos como o avanço da internet contribuiu para mudar o modo em que as pessoas realizam compras e se relacionam no meio digital, além das peculiaridades e informações referentes ao comércio eletrônico. Ainda, serão expostos os aspectos gerais sobre o Marco Civil da Internet, a primeira legislação que regula o tema no país.

No segundo capítulo, falaremos sobre o impacto da Lei Geral de Proteção de Dados na era da informação, seus conceitos, princípios e diretrizes. Além disso, analisaremos a figura do consumidor como a parte mais vulnerável de todas as relações comerciais, mas especialmente das realizadas no meio eletrônico.

No terceiro e último capítulo será exposto casos de vazamentos de dados no país e como os órgãos fiscalizadores estão atuando frente ao descumprimento da Lei Geral de Proteção de Dados.

## 2 INTERNET COMO MEIO DE CONSUMO

No presente capítulo, abordaremos o avanço da internet e tecnologias nos últimos anos no país, além de destacar como essas mudanças influenciaram o surgimento e consolidação do comércio eletrônico. Nesta senda, iremos analisar o comportamento das empresas que utilizam diariamente desta modalidade de comércio como meio de venda e divulgação de produtos.

Ainda, no presente capítulo, iremos falar sobre o Marco Civil da Internet, a primeira legislação que regulamentou o tema no país, seus princípios e como ela contribui com a proteção dos consumidores que usam a internet como ferramenta de compra e consumo.

### 2.1 DADOS DE USO DA INTERNET NO BRASIL NOS ÚLTIMOS ANOS

Conforme pesquisa realizada pelo Comitê Gestor da Internet do Brasil, em 2020 o país chegou à marca de 152 milhões de usuários, o que demonstra o porquê cada vez mais as pessoas dependem da Internet para realizarem suas funções mais básicas do dia a dia. Hoje é possível realizar qualquer tarefa do cotidiano de forma on-line. Acompanhando esta curva de crescimento, as empresas se adequaram para prestarem e disponibilizarem todo e qualquer serviço de maneira digital (LEÓN, 2021).

A possibilidade de fazer tudo online ficou ainda mais evidente com a pandemia de Covid-19, em razão do confinamento e com a impossibilidade de sair de casa, tudo era resolvido através de um computador ou smartphone. Milhares de pessoas, até as que não tinham qualquer intimidade com a vida on-line, viram no espaço virtual o único meio possível para manter as relações na ativa, sendo elas de consumo, pessoais ou profissionais.

Neste contexto, Miragem (2022, não paginado):

O que parecia uma consequência inafastável do avanço da tecnologia da informação acelerou-se com a pandemia: o consumo pela internet — o comércio eletrônico — passou a contemplar uma série de produtos e serviços tradicionalmente oferecidos no mundo físico. O distanciamento social fez com que a aquisição de produto mais diversos, consultas médicas e com uma série de outros profissionais, serviços de educação, encontros e congressos profissionais, entre outros, passassem a se realizar pela internet. Há tele-entrega de quase tudo, embora não acessível a todos. A

agilidade do fornecimento e o conforto de adquirir e receber em casa rivaliza com as dificuldades no caso de desacertos negociais, a crescente automatização das contratações, a reclamação de vícios de produtos e serviços, ou ainda problemas de conexão (em especial para quem não contratar planos com melhor velocidade e dados). A equação de vantagens e desvantagens permite perceber a tendência de que muitas dessas atividades que passaram a se realizar pelo meio digital prossigam assim no pós-pandemia.

De acordo com uma pesquisa realizada pelo Instituto Brasileiro de Geografia e Estatística, o uso da internet entre brasileiros com dez anos ou mais, subiu de 74,7% em 2018 para 78,3% em 2019, ainda, de acordo com a referida pesquisa, a internet chega a oito em cada dez domicílios do país (BARROS, 2021).

Este número segue crescendo mesmo após o ápice da pandemia. Uma pesquisa divulgada em setembro de 2022 no site do Governo Federal, demonstra que a internet é uma realidade em 90% dos lares das famílias brasileiras, o número já expressivo em 2019 aumentou em 5,8 milhões de usuários (GOV.BR, 2022a).

O mundo globalizado é uma realidade e a sociedade vem acompanhando essa transformação e a curva de ascensão da internet demonstra isso com clareza.

O fato é que para se manterem em destaque e fomentarem o consumo, os sites e plataformas necessitam dos dados dos usuários para mantê-los conectados, interessados, e sobretudo fiéis aos conteúdos disponibilizados e comercializados pelas empresas nas redes.

Neste ponto, esclarecem Teffé e Moraes (2017, p. 121):

O oferecimento de dados pessoais vem se tornando rotina no ambiente virtual, de forma que muitas vezes, o indivíduo perde o controle sobre as próprias informações logo após fornecê-las, pouco sabendo sobre sua utilização e se serão repassadas, por meio de trocas comerciais, a terceiros. Uma vez munidas de tais informações, entidades privadas e governamentais tornam-se capazes de “rotular” e relacionar cada pessoa a um determinado padrão de hábitos e de comportamentos, situação que pode favorecer inclusive graves discriminações, principalmente se analisados dados sensíveis.

Importante observar que com o advento da Internet, a facilidade de obter os dados dos consumidores não se restringe apenas as lojas que utilizam de sites como ponto central de relacionamento com o consumidor, mas também aos estabelecimentos físicos que conseguem armazenar os dados dos consumidores em sistemas, softwares, e até mesmo aplicativos, algo que só foi possível com a evolução da internet e do meio digital.

## 2.2 COMÉRCIO ELETRÔNICO

Em que pese a Lei Geral de Proteção de Dados tenha abrangência em qualquer ambiente, o foco do trabalho é falar sobre sua aplicabilidade no meio digital e nas transações realizadas em ambiente on-line, por meio da internet.

O termo e-commerce teve sua origem na década de 60, quando nos Estados Unidos, redes privadas eram utilizadas para a realização de transações comerciais, através de sistemas, que se destacavam pela inovação no comércio da época (NADIA, 2022).

No Brasil, o acesso aos computadores se deu no início dos anos 90, conforme bem pontua Nadia (2022), na época a Internet era um artigo de luxo, não sendo acessível para a maioria da população, desta forma, o comércio eletrônico iniciou suas atividades de maneira tímida em 1995. Já nos anos 2000, o serviço de internet começou a melhorar no país, e as grandes empresas passaram a enxergar a internet como um meio de aumentar as vendas e consolidar o que conhecemos hoje como comércio eletrônico.

A partir daí, o comércio eletrônico está em crescente expansão, a Associação Brasileira de Comércio Eletrônico (ABCOMM) estima que só em 2021, o comércio eletrônico alcançou a marca de 150 bilhões de reais em faturamento (ABCOMM, 2021).

Não poderia ser diferente, considerando que temos a possibilidade de estarmos conectados o tempo todo, sem limitação territorial ou de tempo, podendo realizar qualquer compra, em qualquer lugar, independente do horário ou localização.

Neste sentido, é natural que não somente as relações interpessoais, mas o consumo e demais transações comerciais, também ocorram no ambiente online.

Com base no que o comércio eletrônico representa, Teixeira (2020, p. 21) conceitua:

O comércio eletrônico ou e-commerce representa parte do presente e do futuro do comércio. Existem várias oportunidades de negócios espalhadas pela internet, além de muitas que são criadas em todo momento. É bem provável que uma pesquisa de preços na internet traga não só o menor preço, como também melhores opções de bens. E, apesar do gargalo representado pelo “analfabetismo digital” de uma grande parcela da

população, o e-commerce já desponta junto a uma geração que nasceu com o computador “no colo” ou “nas mãos”. O crescimento do número de internautas na última década é espantoso.

A narrativa do autor corrobora com o exposto anteriormente, a facilidade de acesso à internet trouxe mudanças significativas no modo em que as pessoas compram e fazem negócios. Tarcísio tem o comércio eletrônico como sendo uma extensão ao comércio convencional, tratando-se de meio digital por onde os usuários realizam operações de compra com o suporte de aparelhos tecnológicos.

Premebida (2021, p. 3) conceitua:

O comércio eletrônico é em suma o processo de compra e venda de produtos por meios eletrônicos, como aplicativos móveis e Internet, tanto para o setor de varejo e compras online, bem como transações eletrônicas. Com o advento da globalização, o comércio não se limita mais a ir à loja física de minha preferência escolher um produto, ocorreu o fácil acesso a produtos antes que não acontecia; com um clique podemos conferir ofertas de concorrentes, escolher marcas, ver o que outros compradores falam sobre o produto que estou analisando, tudo em tempo real. Estamos em uma nova era.

Com o distanciamento social ocasionado pela pandemia, a utilização deste meio ganhou intensidade, isto porque até mesmo as empresas que não utilizavam o meio eletrônico como meio de venda, tiveram que adequar a modalidade de comércio para conseguirem se manter abertas durante a pandemia de COVID - 19. Ainda, é possível observar que o perfil do consumidor tem mudado com uma certa frequência, com o passar dos anos, o comércio eletrônico tem ganhado um público cada vez maior (PREMEBIDA, 2021).

O desenvolvimento da tecnologia da internet e toda a melhoria na capacidade de processamento e armazenamento de volume de dados (*Big Data*), permite o refinamento das informações, possibilitando uma série de utilidades e funcionalidades, como a segmentação dos consumidores que irão receber a oferta de um produto específico, agregando maior precisão na análise dos riscos de operações e contratações, em suma, possibilitando a exatidão e eficiência do uso das informações coletadas (MIRAGEM, 2019).

Com a precisão de coleta de dados é possível traçar padrões utilizando o comportamento de compra dos consumidores, acessando suas preferências, acesso às redes sociais, localização geográfica, etc.

Notadamente nas relações de consumo, o tratamento de dados pessoais pode trazer para os fornecedores vantagens capazes de potencializar a vulnerabilidade dos consumidores e criar um grande desequilíbrio contratual. Com efeito, o avanço tecnológico transformou os dados pessoais dos consumidores em um dos principais ativos empresariais, como nos explica Bruno Miragem em seu artigo intitulado “Discriminação injusta e o Direito do Consumidor” (SOUZA *apud* MIRAGEM, 2019, não paginado).

Conforme entendimento de Rodotà (2008, p. 62 *apud* TEFFÉ; MORAES, (2017, p. 121-122):

Dessa forma torna-se possível não só um controle mais direto do comportamento dos usuários, como também a identificação precisa e atualizada de certos hábitos, inclinações, interesses, preferências. Daí decorre a possibilidade de uma série de usos secundários dos dados, na forma de ‘perfis’ relacionados aos indivíduos, família, grupos. Trata-se de uma nova ‘mercadoria’ cujo comércio pode determinar os tradicionais riscos para privacidade: mas pode, sobretudo, modificar as relações entre fornecedores e consumidores de bens e serviços, reduzindo a autonomia destes últimos de tal forma que pode chegar a incidir sobre o modelo global de organização social e econômica.

Aqui o cerne da questão central do comércio eletrônico, a proteção legal do usuário que utiliza deste modelo de consumo diariamente, e que como em qualquer relação de consumo, segue sendo a parte mais vulnerável desta relação.

Como traz, Teixeira (2020, p. 80):

A par da discussão sobre a necessidade ou não de uma norma específica para o e-commerce, entrou em vigor o Decreto n. 7.962, de 15 de março de 2013, que regulamenta o Código de Defesa do Consumidor para dispor sobre a contratação no comércio eletrônico. Ele dispõe acerca da necessidade de informações claras sobre o produto, o serviço, o fornecedor, o atendimento facilitado ao consumidor e o respeito ao exercício do direito de arrependimento (art. 1º).

Em que pese não exista uma lei específica que fale sobre o “e-commerce” ou comércio digital, em 2013 entrou em vigor o Decreto 7962 de 2013, regulamentando o Código de Defesa do Consumidor, para dispor sobre a contratação no comércio eletrônico (BRASIL, 2013).

O decreto acompanha o CDC, tem nos pilares o direito de arrependimento, fala sobre o suporte imediato ao cliente, além de clareza nas informações disponibilizadas. Desta forma, a empresa que utiliza do e-commerce deve ter visível

e com fácil acesso seu nome empresarial, CNPJ, além dos dados para contato (BRASIL, 2013). Essa prática facilita a vida do consumidor, pois consegue dificultar a aplicação de golpes, já que com estes dados, é possível realizar pesquisas relacionadas as informações das empresas, se ela de fato existe, qual a sede, índice de reclamações, etc.

Cristalino que o Código de Defesa do Consumidor é eficaz no cuidado com o direito dos consumidores, no entanto, é notável o avanço das novas tecnologias, inclusive no que diz respeito ao comércio digital, se ele evolui diariamente certamente um decreto que está prestes a completar dez anos não acompanha esta evolução, por isso, cada vez mais é necessário, os consumidores estarem mais atentos aos seus direitos.

### 2.3 MARCO CIVIL DA INTERNET

Embora esteja numa crescente, a proximidade da população mundial com a internet não é recente, mesmo que como referido anteriormente, a quantidade de usuários e adeptos a internet tenha tido um aumento significativo nos últimos anos. Em 2014, o Brasil sancionou o Marco Civil da Internet (Lei nº 12.965/2014), uma Lei para controlar o acesso e disponibilidade de dados da internet no país (BRASIL, 2014).

Nesta senda, é importante que se considere como acontecimentos fora do território nacional, influenciaram a aprovação de uma Lei que estabelecesse limites no âmbito da internet.

O caso do funcionário da Cia, Edward Snowden, ficou conhecido em 2013, quando o então ex técnico da companhia foi acusado de ser o responsável pelo vazamento de dados e informações sigilosas relacionadas a segurança dos Estados Unidos. A notícia do vazamento chocou a população internacional, estendendo esta preocupação até o Brasil, já que na época ficou comprovada a espionagem de cidadãos, empresas e até mesmo do governo brasileiro (G1, 2014).

Conforme esclarecem Leite e Lemos (2014, p. 4):

Dentre todas as propostas consideradas como reação ao caso Snowden, a mais completa, séria, viável e necessária foi, sem margem para dúvidas, a retomada do debate sobre a aprovação do Marco Civil da Internet. O mais curioso é que o Marco Civil não foi uma proposta de governo, mas sim uma proposta da sociedade. Sua concepção surgiu muitos anos antes do

escândalo Snowden, quando se debatia na esfera pública como seria feita a regulação da internet em nosso país.

Destaca-se na fala dos autores o fato do Marco Civil da Internet ter surgido através do anseio da sociedade, que já buscava um meio de ter garantida alguma segurança no que diz respeito ao uso da internet, e foi a partir deste episódio de espionagem que, para o governo brasileiro, a aprovação da lei que até o momento estava em segundo plano, se tornou urgente (LEITE; LEMOS, 2014).

O então Projeto de Lei, encaminhado a Câmara em agosto de 2011, foi aprovado em 2014, a fim de trazer mais segurança para a população brasileira, já que até o momento o país não tinha qualquer lei que regulamentasse a Internet.

Embora o Marco Civil da Internet tenha surgido antes da LGPD, a Lei introduziu em seus artigos o conceito básico de consentimento, coleta e registro de dados.

Ainda no campo dos direitos dos usuários da internet no Brasil, o Marco Civil trata das questões que envolvem a captação de dados (normalmente via uso de cookie) e a formação de banco de dados (mailing list) e sua cessão ou comercialização para terceiros. Conforme o art. 7º, o usuário tem direito: (i) a informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que justifiquem sua coleta, não sejam vedadas pela legislação e estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet; (ii) a necessidade de consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais deverá constar de forma destacada das demais cláusulas contratuais (TEIXEIRA, 2020, p. 42).

Importa falar que, embora o objetivo principal do Marco Civil da Internet seja o de regulamentar o uso da Internet, o legislador se preocupou em manter a liberdade dos usuários como um dos focos centrais da Lei.

De acordo com Teixeira (2020, p. 39), “É possível abstrair da Lei n. 12.965/2014 três grandes pilares: a garantia à liberdade de expressão, a inviolabilidade da privacidade e a neutralidade no uso da internet.”

Com base na lição do autor, importante frisar que a Lei garante a liberdade de expressão de quem usa a internet, ou seja, os usuários podem utilizar e se manifestar na rede com total liberdade, tendo garantida a privacidade dos seus dados, não havendo diferenciação na aplicabilidade da Lei, independentemente da finalidade do uso.

Teixeira (2021, p. 33) ainda acrescenta:

Quanto à liberdade de expressão (cujo direito está assegurado na Constituição Federal, art. 5º, IX, consistindo na liberdade de manifestação intelectual, artística, científica e de comunicação, sem censura ou necessidade de licença), o usuário da internet pode se expressar escrevendo e postando o que bem entender, sendo que o conteúdo somente pode ser removido pelo provedor mediante ordem judicial. Nos casos de imagens (fotos e vídeos) com conteúdo pornográfico, os interessados envolvidos nas cenas podem exigir a retirada do conteúdo junto ao provedor mediante notificação própria ou de seu procurador, não sendo neste caso necessária ordem judicial. Obviamente, que o exercício da liberdade de expressão não impede de o prejudicado pleitear indenização junto ao internauta ofensor se a manifestação deste causar dano de ordem moral e/ou patrimonial (ficando o provedor livre de responsabilidade, via de regra). No que diz respeito à proteção da privacidade (direito inerente à inviolabilidade da intimidade, da vida privada, da honra e da imagem da pessoa, nos termos da Constituição Federal, art. 5º, X), a lei garante o sigilo dos dados pessoais do usuário, do que ele acessa na rede e do conteúdo de suas comunicações. Assim, não é permitido monitorar ou fiscalizar os pacotes de dados (conteúdos) transmitidos pelos usuários na internet, sendo que o acesso a esses dados necessita de ordem judicial.

O direito a privacidade dos usuários é levado a sério por algumas empresas que usam a internet como meio de negócio. A exemplo do *Whatsapp*, o aplicativo de mensagens instantâneas foi bloqueado em 04 oportunidades, por não acatar decisões judiciais que determinaram o compartilhamento de conversas trocadas entre os usuários (G1, 2021).

O aplicativo utiliza de criptografia de ponta a ponta, modalidade onde as mensagens só podem ser acessadas pelas partes envolvidas na conversa.

O compromisso em manter os dados dos usuários em sigilo foi tamanho, que em 2020, a impossibilidade de multa cominatória para aplicativo criptografado, foi parar no Superior Tribunal de Justiça, nas palavras do Ministro Dantas (*apud* STJ, 2021, não paginado):

[...] ao buscar mecanismos que protegem a intimidade da comunicação privada e a liberdade de expressão, por meio da criptografia de ponta a ponta, as empresas estão assegurando direitos fundamentais reconhecidos expressamente na Constituição Federal. Diante disso, ele entende que a aplicação da multa não deve ser admitida, pois a realização do impossível, sob pena de sanção, não encontra guarida na ordem jurídica.

Nesse sentido, existem duas ações no STF em que o objeto é a discussão acerca da inconstitucionalidade do bloqueio do aplicativo, em ambas os ministros

mostram compartilharem da mesma opinião, que tal medida seria inconstitucional, levando em consideração os princípios de liberdade e inviolabilidade da vida privada.

Sobre o princípio da neutralidade, Del Masso, Abrusio e Florêncio Filho (2014) dizem que todos os dados que trafegam na rede devem ser tratados da mesma forma e com a mesma velocidade. Este princípio representa uma garantia de que os pacotes de dados que circulam a internet sejam tratados de forma igualitária, sem distinção sobre o conteúdo, origem ou destino, em regra, o provedor de conexão não pode escolher o que você acessa, dando preferência para alguns sites com os quais possua um acordo comercial, por exemplo.

“De modo enfático, sem a neutralidade garantida, os provedores poderiam analisar e discriminar o conteúdo acessado pelo consumidor, podendo até mesmo restringir e comprometer o conteúdo que o internauta gostaria de acessar.” (DEL MASSO; ABRUSIO; FLORÊNCIO FILHO, 2014, não paginado).

Neste ponto Teixeira (2021, p. 33) acrescenta:

A neutralidade (ou princípio da neutralidade) no uso da internet consiste no fato de que o acesso à internet pelo usuário pode dar-se de forma livre para quaisquer fins: realizar pesquisas ou compras, estabelecer comunicações como por e-mail, utilizar redes sociais em geral, visualizar e postar textos, fotos e vídeos etc. Dessa forma, o tratamento deve ser neutro, não podendo haver diferenciação em razão do uso realizado pelo internauta, sendo possível apenas serem oferecidos pacotes com valores diversos para fins da velocidade na navegação. Dessa forma, o usuário pode usar a conexão à internet para o fim que desejar (e-mails, blogs etc.) sem precisar pagar valores distintos para tanto e sem estar sujeito à fiscalização do provedor.

Importante falar que os princípios do Marco Civil da Internet estão em sintonia com a Constituição Federal. Outro paralelo possível de ser realizado é com relação a Lei Geral de Proteção de Dados, já que ambas as leis possuem alguns termos e conceitos em comum.

O Art. 7º do Marco Civil da Internet fala sobre os direitos e garantias dos usuários, referindo sobre inviolabilidade da intimidade e vida privada; inviolabilidade e sigilo do fluxo de suas comunicações; informações claras e completas sobre os contratos de prestação de serviços; não fornecimento a terceiros de seus dados pessoais, salvo mediante consentimento livre, expresso e informado; informações claras sobre coleta, uso, armazenamento, tratamento e proteção de dados pessoais,

que só podem ser utilizados para finalidades que justifiquem sua coleta de forma específica não for vedada pela legislação (BRASIL, 2014).

Notável que diante da falta de uma lei que falasse especificamente sobre a proteção de dados, estabeleceu-se no Marco Civil da Internet direitos essenciais sobre este tema aos usuários da rede, levando em consideração o controle e a autodeterminação normativa (TEFFÉ; MORAES, 2017).

Neste ponto, cabe salientar que o Marco Civil da Internet não é uma lei geral de proteção de dados, então não aborda questões como transferência internacional de dados, vazamentos, dados anonimizados, entre outros tópicos (SOUZA *et al.*, 2018).

Em que pese a Lei tenha sua importância reconhecida, trazendo certa segurança jurídica aos usuários da internet, e sua sanção tenha sido bastante comemorada, a aplicabilidade da lei abriu discussões sobre a sua eficácia no tocante a proteção de dados de quem usa o ambiente on-line frequentemente.

## 2.4 DIREITO E DEFESA DO CONSUMIDOR

Com base no tema proposto, dado o avanço e crescimento diário da tecnologia, o consumidor se torna o protagonista das relações comerciais digitais, fato este evidenciado pelo faturamento bilionário do comércio digital nos últimos anos (ABCOMM, 2021).

Atualmente, existem serviços, inclusive de Órgãos Públicos, que só funcionam de forma on-line. Utilizando aqui mais uma vez o exemplo da pandemia, onde diversas pessoas que fizeram jus ao auxílio emergencial tiveram que usar do meio eletrônico para movimentar e utilizar os valores. Embora o acesso à internet esteja à disposição da maioria, ainda não está ao alcance de todos, razão pela qual se torna imprescindível que o Estado garanta a tutela do direito destes usuários.

A internet proporciona o aumento do mercado de consumo, possibilitando o surgimento de novas lojas, sites, meios de divulgação de produtos e oportunidades. Além de ser uma facilitadora de relacionamentos comerciais, ela também é uma importante ferramenta para fazer valer os direitos do consumidor. Hoje existem plataformas totalmente digitais especializadas em registrar reclamações de consumidores insatisfeitos.

A exemplo do Reclame Aqui, o site é conhecido por ser o canal oficial do consumidor brasileiro, atuando como um importante meio de comunicação entre consumidores e empresas. A plataforma funciona também como meio de estudo, estimando-se que 92% dos consumidores utilizam do site como meio de pesquisa com relação à reputação de empresas (RECLAME AQUI, [202-?]).

Nesta senda, é importante conhecer como a legislação consumerista protege o consumidor.

Na Constituição Federal, a defesa do consumidor é um dos princípios da atividade econômica, sendo reconhecido como um direito e garantia fundamental do cidadão (BRASIL, 1988).

Assim esclarece Peres Filho (2022, p. 24):

O fato de o legislador constituinte haver colocado a defesa do consumidor dentre esses princípios dá mostras de que sem um consumidor protegido não se pode falar em desenvolvimento, em prosperidade econômica do país. A economia precisa dos consumidores para crescer. E estes precisam da proteção estatal para poderem usar de forma justa e equilibrada os seus recursos econômicos, que muitas vezes são bastante reduzidos.

O CDC é aplicado sobre as relações de consumo, outras relações não relacionadas devem observar seus próprios ordenamentos. Cumpre esclarecer que as relações de consumo são os vínculos estabelecidos entre consumidores e fornecedores, cujo objeto seja a oferta ou aquisição de produtos ou serviços no mercado de consumo (PERES FILHO, 2022).

Neste sentido, conforme definições do CDC (BRASIL, 1990):

- a) consumidor é toda pessoa física ou jurídica que adquire ou utiliza produto ou serviço como destinatário final;
- b) fornecedor é toda pessoa física ou jurídica que desenvolve atividade de produção, montagem, criação, construção, transformação, importação, exportação, distribuição ou comercialização de produtos ou prestação de serviços;
- c) produto é qualquer bem móvel ou imóvel, material ou imaterial.

O Código de Defesa do Consumidor versa sobre a proteção da parte mais frágil das relações de consumo, diante do fornecedor que possui uma posição de superioridade, seja por razões de natureza técnica, econômica ou psicológica. O mercado de consumo é passível de manipulações com o objetivo de aumento de

vendas, usando das mais diferentes estratégias que vão de mudança de preços até dominação de setores (PERES FILHO, 2022).

Neste sentido, o CDC busca a proteção dos interesses dos consumidores, se baseando numa série de princípios norteadores, sendo fundamental falarmos sobre os principais deles.

O princípio da transparência diz que as relações de consumo devem ser transparentes. Sem subterfúgios por parte do fornecedor que possam vir a prejudicar o consumidor (PERES FILHO, 2022).

O princípio da vulnerabilidade é amplamente conhecido e é uma das bases legais do CDC, sendo reconhecido na legislação consumerista, este princípio será melhor abordado no próximo capítulo.

De acordo com reportagem divulgada pelo Extra (2022), em relação a golpes na Internet onde as vítimas são consumidores, em seis de dez casos empresas são responsabilizadas na Justiça por prejuízos financeiros. A vulnerabilidade do consumidor e responsabilidade das empresas fica ainda mais evidente, a doutrina e as decisões judiciais demonstram isso em seus textos e decisões, o consumidor precisa ser protegido.

Nesta senda, Theodoro Júnior (2020, p. 11) diz:

É certo que a vulnerabilidade do consumidor constitui uma presunção legal absoluta, que impõe o tratamento diferenciado que lhe é dispensado, em face do fornecedor. Isto porque, 'não se pode pensar em proteção e defesa ao consumidor sem colocá-lo nesta posição de inferioridade perante os fornecedores de modo geral, principalmente diante das intensas transformações pelas quais passaram as relações jurídicas e empresariais nos últimos tempos'. Assim, todo consumidor é vulnerável perante a lei, sendo essa característica de ordem material. A vulnerabilidade, destarte, "é elemento posto da relação de consumo e não um elemento pressuposto, em regra".

O princípio da intervenção estatal acompanha o texto do Art. 5 XXXII da CF, que diz que o Estado promoverá a defesa do consumidor nos termos da lei, ou seja, cabe ao Estado proteger o consumidor contra qualquer meio fraudulento ou ilegal por parte do fornecedor. Assim esclarece Peres Filho (2022, p. 69):

Esse protecionismo fica patente desde a ementa da Lei nº 8.078/1990 – “dispõe sobre a proteção do consumidor e dá outras providências” – e do seu art. 1º – “o presente código estabelece normas de proteção e defesa do consumidor [...]”.

O imperativo de ordem pública e interesse social, que vem também no art. 1º do Código de Defesa do Consumidor, significa que as normas estabelecidas por essa lei devem prevalecer sobre os acordos privados, sobre interesses particulares, ainda que manifestados contratualmente, quando constatado que as cláusulas contratuais estão maculadas por ofensas à legislação protetiva do consumidor.

Necessário também falar do princípio da boa-fé objetiva, se espera que as empresas e fornecedores mantenham uma conduta baseada na ética e transparência. Neste sentido, Peres lembra que esta postura é exigível das duas partes da relação de consumo.

Além disso, é importante lembrar que é direito do consumidor receber informações adequadas e claras sobre os produtos e serviços, o que acompanha o princípio de segurança abordado em diversos artigos da legislação consumerista, o Art. 8 da referida lei diz que:

Os produtos e serviços colocados no mercado de consumo não acarretarão riscos à saúde ou segurança dos consumidores, exceto os considerados normais e previsíveis em decorrência de sua natureza e fruição, obrigando-se os fornecedores, em qualquer hipótese, a dar as informações necessárias e adequadas a seu respeito (BRASIL, 1990, não paginado).

Ainda, o Art. 6º do CDC, são direitos básicos do consumidor: a proteção da vida, saúde e segurança; a educação e divulgação sobre os produtos e serviços, resguardados os direitos de liberdade de escolha; a informação adequada, proteção contra publicidade enganosa e abusiva; a modificação e revisão de cláusulas contratuais; a prevenção e reparação de eventual dano; acesso aos órgãos de proteção com vistas à prevenção e reparação; o acesso facilitado da defesa dos seus direitos; a adequada e eficaz prestação dos serviços públicos em geral (BRASIL, 1990).

Neste sentido, mais do que nunca, é importante informar de forma clara tudo que é relevante para o consumidor. Já se identificou que muitas vezes o consumidor perderia horas para ler termos de usos disponíveis na internet, razão pela qual muitas vezes ele opta por não ler. Por outro lado, mesmo os anúncios mais simples acabam por não atender o exposto na legislação. As empresas defendem a falta de informação como uma alternativa para simplificar as páginas virtuais, a fim de não confundir o consumidor, além disso, colocam em foco o comportamento do

consumidor na busca de informações que lhe dizem respeito quando o assunto é sua segurança e proteção (MIRAGEM, 2022).

O Código de Defesa do Consumidor completou 32 anos em setembro deste ano. A lei consumerista é de uma época onde a sociedade iniciava sua caminhada para o mundo virtual que conhecemos hoje. A internet que atualmente é presente na vida da maioria da população não tinha nem chegado ao Brasil, evidente que a lei consumerista está um pouco defasada com relação aos avanços tecnológicos do comércio eletrônico.

No entanto, os princípios sólidos trazidos pela legislação fazem diferença na proteção dos direitos dos consumidores, isto porque ele permanece sendo a figura mais vulnerável da relação independentemente de onde ela aconteça.

Neste sentido, a LGPD se apresenta como uma nova ferramenta de proteção ao consumidor, já que a Lei se baseia no consentimento e informações claras, conceitos semelhantes com os encontrados no CDC. Assim, juntos os ordenamentos devem trazer mais segurança jurídica aos titulares de dados.

### 3 LEI GERAL DE PROTEÇÃO DE DADOS E A VULNERABILIDADE DO CONSUMIDOR NA ERA DIGITAL

Neste capítulo, abordaremos o surgimento da LGPD, analisaremos seus princípios, conceitos e a base legal do consentimento para a correta aplicabilidade da Lei no meio digital. Além disso, entenderemos as sanções aplicáveis em caso de descumprimento da Lei, a função da ANPD, a responsabilidade e importância dos agentes para a adequação do tratamento de dados perante a legislação.

Por fim, analisaremos a relação do Código de Defesa do Consumidor com a LGPD, a fim de destacar a vulnerabilidade do consumidor diante da disponibilização massiva de dados no meio digital.

#### 3.1 LEI GERAL DE PROTEÇÃO DE DADOS

Na era da informação digital, nunca se falou tanto na proteção de Dados. A facilidade de transferência de informações traz uma nova fase de interação entre as pessoas no meio eletrônico.

Como referido anteriormente, o Marco Civil da Internet se preocupou em regular o uso e tráfego da Internet, além de trazer a primeira base legal sobre tratamento pessoal e tratamento de dados no nosso ordenamento jurídico.

Em que pese o conceito de respeito à privacidade não tenha surgido com a LGPD, já que ambos são direitos fundamentais garantidos na Constituição Federal, a Lei Geral de Proteção de Dados é a primeira legislação específica sobre o tema, sendo considerada um avanço legislativo no que diz respeito ao armazenamento e tratamento de dados.

Miragem (2019, p. 2) define que:

A proteção de dados pessoais é projeção de direitos fundamentais consagrados. Relaciona-se com a proteção da vida privada e da intimidade (art. 5º, X, da CF (LGL\1988\3)), da dignidade da pessoa humana (art. 1º, III, da CF (LGL\1988\3)) e contra a discriminação (art. 3º, IV), como expressões da liberdade e da igualdade da pessoa. A Constituição Federal, igualmente, assegura como direito fundamental a inviolabilidade do sigilo de dados (art. 5º, XII). Por tais razões sustenta-se a autonomia.

de Proteção de Dados, nesta linha, define em seu art. 1º, seu objetivo de proteção dos “direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.”

Inicialmente, a lei teria o tempo de 18 meses para entrar em vigor, mas com as alterações realizadas pela Lei 13.853/2019, o prazo foi estendido para 02 anos, sendo que o primeiro dia de vigência da legislação foi em 16 de agosto de 2021 (TEIXEIRA, 2021).

O matemático londrino Clive Humby criou a expressão “Dados são o novo petróleo” (VERÍSSIMO, 2021, não paginado), não é à toa que as maiores empresas do mundo trabalham com a tecnologia da informação, utilizando dados a todo momento, quando este dado é bem tratado, ele é capaz de revolucionar empresas, ajudar no desenvolvimento de serviços especializados e soluções específicas.

Segundo Frazão, Tepedino e Oliva (2020, p. RB-1.2):

Do ponto de vista econômico, dados importam na medida em que podem ser convertidos em informações necessárias ou úteis para a atividade econômica. Conseqüentemente, os dados precisam ser processados para que possam gerar valor.

As empresas disponibilizam aplicativos, sites e serviços gratuitos, mas para o resultado deste investimento implicar em ganhos financeiros, o dado disponibilizado pelos usuários precisa necessariamente ser tratado.

Quando falamos em proteção de dados, a primeira legislação relacionada ao tema surgiu na Europa. No contexto internacional, a União Europeia já havia percebido a necessidade de uma tutela jurídica para os dados e privacidade da população. A General Data Protection Regulation, conhecida como GDPR, começou a ser idealizada em 2012, entrou em vigor em maio de 2016, e começou a ser aplicada em maio de 2018.

No site da União Europeia, a GDPR tem a seguinte definição:

Este regulamento é uma medida essencial para reforçar os direitos fundamentais das pessoas na era digital e facilitar a atividade comercial mediante a clarificação das normas aplicáveis às empresas e aos organismos públicos no mercado único digital. A adoção de um ato legislativo único visa também acabar com a fragmentação resultante da coexistência de sistemas nacionais diferentes e com encargos administrativos desnecessários (COMISSÃO EUROPEIA, [201-?], não paginado).

A norma Europeia passou a ter forte influência na aprovação de leis sobre o mesmo tema ao redor do mundo, especialmente no Brasil. Assim sendo, em 2018, o Brasil incorporou em seu ordenamento jurídico, a Lei Geral de Proteção de Dados.

De acordo com Teixeira (2020, p. 8):

A Lei n. 13.709/2018, Lei Geral de Proteção de Dados Pessoais é indiscutivelmente um grande marco no cenário nacional quanto à proteção de dados de pessoas físicas. Essa tutela é fruto do amadurecimento da questão pelo mundo, tanto é que 28 de janeiro é o Dia Internacional da Proteção de Dados.

A Lei nº 13.709/2018 é dividida em 10 capítulos e 65 artigos, que dispõem sobre o tratamento de dados pessoais em meios físicos e digitais, com a finalidade de proteger os direitos fundamentais de liberdade e privacidade, dentre eles: assegurar maior controle de titulares sobre seus dados pessoais, mitigar riscos relacionados a coleta massiva de dados bem como impacto nos titulares, além de assegurar maior transparência perante os titulares dos dados (BRASIL, 2018).

A LGPD cuida dos tratamentos de dados tanto no meio físico quanto no digital, mas é evidente que é no meio digital que o acesso, transferência e disponibilização dos dados acontecem com maior facilidade.

Frazão, Tepedino e Oliva (2020, p. RB1.3) dizem que:

É inequívoco que a proteção de dados, tal como inclusive deixa claro a LGPD, não se restringe ao meio virtual, mas a todos os meios pelos quais os dados podem ser coletados e utilizados. Entretanto, também não há dúvida de que é no meio virtual que se concentram as maiores preocupações e os maiores desafios da proteção de dados.

Teixeira (2021, p. 78) ainda acrescenta: “E, mesmo a LGPD tendo um alcance que vai além do e-commerce, sem sombra de dúvidas, é nesse ambiente de compras digital que a lei nacional tem um terreno muito fértil quanto à sua aplicação.”

Vivemos na era da informação, o Big Data permite um rápido acesso há um volume significativo de informações, ficando os dados disponíveis para serem utilizados de formas que nem sempre são legítimas ou lícitas (MIRAGEM, 2019).

As afirmações dos autores demonstram que a empresa que não se adequar a Lei Geral de Proteção de Dados, ou que não encontrar um meio que evidencie a

segurança dos usuários no meio digital, acabará perdendo seu espaço no mercado (MIRAGEM, 2019).

Diante das afirmações é possível verificar que para o devido cumprimento da Lei, há a necessidade de um trabalho conjunto entre as pessoas naturais e empresas. O fato de disponibilizar o dado indiscriminadamente se configura como algo cultural. É comum deixar a disposição o número de documento para comprar um remédio na farmácia, ou para conseguir um desconto no supermercado. Fornecemos informações diariamente sem notar, isto, porque de certa forma, o consumidor dá o consentimento para as empresas utilizarem deste dado.

E se à luz do Marco Civil da Internet o consentimento era suficiente, a LGPD deixa claro que é necessário informar detalhadamente o motivo que estes dados são tratados (BRASIL, 2018).

De acordo com Lima (2020, p. 47):

No entanto, a proteção dos dados pessoais não pode ser estruturada tão somente com base no consentimento livre e informado do titular dos dados, em razão de sua vulnerabilidade. Em outras palavras, o indivíduo, que necessita de serviços essenciais na sociedade informacional, quando solicitadas informações que lhe digam respeito para poder usufruir do serviço, não poderá resistir à anuência exigida pelos prestadores de serviços ao tratamento de seus dados pessoais.

Aqui fica caracterizada a vulnerabilidade do consumidor, como cobrar consentimento de alguém que não sabe para qual fim a empresa utiliza estes dados, ou pior, precisa de determinado serviço, e se vê obrigado a dar o consentimento, não podendo dizer não.

Diante das análises feitas, principalmente no que diz respeito aos dados que o consumidor disponibiliza ao acessar sites na internet, é imperioso observar como a lei trata e protege os usuários, e qual a punição de quem não respeita o consumidor como deveria.

### 3.2 PRINCÍPIOS DA LEI GERAL DE PROTEÇÃO DE DADOS

A LGPD em seu artigo 6º, além de elencar os princípios da lei, definiu que toda atividade de tratamento de dados deve observar a boa-fé.

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, não paginado).

De acordo com Miragem (2019), a boa-fé é o princípio que disciplina amplamente as relações jurídicas de direito público e privado. Tem por conteúdo essencial, a eficácia criadora de deveres anexos àqueles que decorrem da lei ou do conteúdo expresso da relação jurídica. É comum que a ela se associem os deveres de cooperação e lealdade, assim como o respeito às legítimas expectativas das partes. No caso do tratamento de dados pessoais, o Art. 10 deixa isto claro, fala sobre a boa-fé fundamentada na tutela das legítimas expectativas do titular dos dados frente ao controlador, o que deve se delinear, sempre a partir das circunstâncias concretas em que se deu o consentimento, a finalidade de uso e tratamento dos dados que foi indicada na ocasião e o modo como foram compreendidas as informações prévias oferecidas.

No princípio da finalidade, a empresa que utiliza os dados do consumidor, deve utilizar e tratar este dado nos termos específicos da autorização que lhe foi

dada, não havendo a possibilidade de tratamento posterior de forma incompatível com esta finalidade, é o foco central na proteção de dados.

A finalidade é a forma de se justificar a utilização do dado pessoal de terceiro, sendo requisito o consentimento do titular. O titular do dado pessoal ao prestar o seu consentimento, o faz para que seus dados sejam utilizados para certa e determinada finalidade apenas, finalidade esta que deve ser expressa no processo de tratamento de dados.

De acordo com Miragem (2019, p. 6):

A primeira hipótese de finalidade legítima permitida para tratamento dos dados pela legislação, é a do consentimento do titular dos dados (art. 7º, I, da LGPD). Porém também se admite o tratamento de dados para “o cumprimento de obrigação legal ou regulatória pelo controlador” (art. 7º, II, da LGPD). Pode o fornecedor ter de utilizar os dados dos seus consumidores inclusive em seu próprio benefício, quando por exemplo, conforme certas informações se lhe ofereçam preços ou tarifas mais vantajosas segundo regras definidas pelo regulador (p.ex. tarifa dos serviços de energia elétrica de consumidores de baixa renda).

Enquanto o princípio da finalidade se preocupa com a regularidade do tratamento, o princípio da adequação aborda o procedimento realizado para chegar na finalidade pretendida, ou seja, a compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

Conforme esclarece Miragem (2019, p. 9):

O atendimento ao princípio da adequação no tratamento de dados pessoais é definido pela “compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento” (art. 6º, II, da LGPD). Neste sentido, visa preservar a vinculação necessária entre a finalidade de utilização dos dados informada ao titular e seu efetivo atendimento na realização concreta do tratamento de dados. Neste sentido, a adequação vincula-se diretamente ao consentimento dado pelo titular para o tratamento dos dados ou as demais finalidades legais admitidas que deverão ser informadas, e a situação de confiança que se cria do estrito atendimento dos termos da informação prévia ao consentimento ou do uso informado.

O princípio do livre acesso, deixa claro que a partir do momento em que o usuário consente na utilização dos dados por terceiro, o usuário deve ter acesso facilitado e ilimitado a estes dados para consulta, além de saber o tempo em que seus dados ficarão disponibilizados. Neste sentido, visa preservar a vinculação

necessária entre a finalidade de utilização dos dados informada ao titular e seu efetivo atendimento na realização do tratamento de dados (MIRAGEM, 2019).

Miragem (2019, p. 10) fala sobre as sanções de quem não disponibilizar o acesso aos dados dos usuários:

A violação do direito de acesso aos dados, que se pode caracterizar pela simples recusa, mas, sobretudo na dinâmica atual do mercado de consumo, pela imposição de obstáculos ao acesso, exigindo que o consumidor reporte-se a diferentes pessoas ou setores distintos para acesso a estas informações, retardando-o injustificadamente<sup>26</sup> e deixando de facilitar o exercício do direito, configura infração aos direitos do consumidor passível de sanção, em comum, pela LGPD e pelo CDC (LGL\1990\40), sem prejuízo de eventual responsabilização por danos.

O princípio da transparência afirma que o titular dos dados deve tratar o dado de forma transparente, deixando claro a todo momento para que e até quando os dados serão utilizados. A transparência sobre o procedimento de tratamento de dados e os sujeitos envolvidos na atividade é uma marca da legislação sobre proteção de dados em diversos sistemas jurídicos.

De acordo com Lima (2020, p. 83):

Em uma relação de consumo, esse princípio é imperativo, posto que está previsto no artigo 4º, caput, do CDC, pelo qual a política nacional das relações de consumo tem como objetivo alcançar a transparência, influenciando, a partir daí todas as normas deste microsistema para concretizá-lo.[...]

Quem está tratando o dado, deve garantir a segurança do titular, usando de medidas para proteger os dados de eventual vazamento, uso indevido, acesso não autorizado, entre outros.

Sobre o princípio da segurança, Lima (2020, p. 84) “O princípio da segurança está consagrado em todas as regulações sobre proteção de dados, até porque é inerente à proteção à própria segurança.” Ou seja, a empresa que está tratando os dados deve garantir a segurança destes, utilizando todas as medidas que forem necessárias para evitar o vazamento ou uso indiscriminado de dados.

Miragem (2019, p. 12) acrescenta:

Um dos principais objetivos da legislação de proteção de dados é assegurar um arcabouço normativo que assegure o tratamento dos dados pessoais de modo compatível aos direitos dos titulares dos dados, evitando seu

tratamento sem observância das exigências legais, assim como a prevenção de riscos inerentes à atividade. Neste cenário, o princípio da segurança é definido pela “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” (art. 6º, VII, da LGPD).

Nesta senda, o princípio da prevenção diz que todas as medidas para evitar danos, ou utilização indevida dos dados deve ser tomada e utilizada por quem é responsável pelo tratamento de dados.

De acordo com Miragem (2019, p. 13):

O princípio da prevenção é comum às legislações de proteção de dados pessoais e de defesa do consumidor (art. 6º, VI, do CDC (LGL\1990\40)). O modo como se opera a prevenção de riscos de dano tanto abrangem providências materiais a serem exigidas, com o incremento técnico da atividade, quanto a possibilidade de delimitar, nos termos da lei, o tratamento de dados pessoais sensíveis, assim considerados também em razão da maior gravidade dos danos que podem decorrer de sua utilização indevida.

O princípio da não discriminação traz os dados de todos devem ser tratados e respeitados da mesma forma, independentemente da natureza destes dados, do sexo, raça, cor e crença destes usuários.

Miragem (2019, p. 13) diz:

Afinal, a grande vantagem do processamento dos dados pessoais para maior precisão da segmentação e personalização dos consumidores no mercado de consumo não pode servir para prejudicar, restringir ou excluir qualquer consumidor da possibilidade de acesso ao consumo.

Já o princípio da prestação de contas fala que o agente precisa demonstrar que adotou medidas eficazes e capazes de comprovar a observância e cumprimento das normas de proteção de dados.

Miragem (2019, p. 15) acrescenta:

[...] Relaciona-se diretamente com o princípio da transparência e da prevenção, impelindo aqueles que se ocupam do tratamento de dados pessoais não apenas de observar o cumprimento das normas jurídicas aplicáveis, mas terem a capacidade de demonstrar esta conformidade legal e sua eficácia. A enunciação do princípio se inspira no Regulamento europeu, no qual consta ainda a explicitação do conteúdo do comportamento exigido na demonstração de atendimento às normas, ao referir que “essas medidas deverão ter em conta a natureza, o âmbito, o

contexto e as finalidades do tratamento dos dados” (n. 74 do Regulamento 2016/679). Esta obrigação compreende inclusive a adoção de programas de conformidade (n. 78 do Regulamento 2016/679), bem como um detalhado procedimento de avaliação de impacto sobre proteção de dados (art. 35 do Regulamento 2016/679).

### 3.3 PRINCIPAIS CONCEITOS

Para falar na Lei Geral de Proteção de Dados, é importante considerar o que a Lei define como dado.

O legislador se preocupou em esclarecer de forma taxativa, para que não restassem dúvidas acerca das definições descritas na lei, classificando dado como a informação relacionada à pessoa natural identificada ou identificável, o tipo deste dado como pessoal ou pessoal sensível, conceitos descritos no Art. 5º incisos I, II, III, da Lei Lei Geral de Proteção de Dados (BRASIL, 2018).

Quando falamos em dado, logo pensamos no número de algum documento de identificação, como CPF, RG ou até mesmo o número de telefone, no entanto, é importante dizer que deve ser reconhecido como dado qualquer informação pela qual a pessoa possa ser reconhecida e identificada.

Montemezzo (2020, p. 564) diz que:

Considera-se dado pessoal, conforme art. 5º da LGPD, toda a informação relacionada à pessoa natural identificada ou identificável. Há, também, a definição de dados sensíveis, que são aqueles relacionados à origem racial e étnica; à religião, ideologia política; os referentes à saúde e à vida sexual; dados biométricos e genéticos e de filiação a sindicatos e partidos políticos, bem como, a organizações de caráter filosófico e religioso. Como se verifica, a lei tratou de diferenciar os dados cadastrais dos dados sensíveis, os quais podem gerar algum tipo de discriminação do titular.

Teixeira (2020, p. 79) resume desta forma: “A título distintivo e ilustrativo, enquanto o dado pessoal está relacionado à privacidade do titular, o dado pessoal sensível diz respeito à intimidade dele.”

Nesta senda, vale ressaltar que:

- a) dado pessoal: considera qualquer dado, que isoladamente ou agregado a outro possa permitir a identificação de uma pessoa natural, ou que consegue sujeitá-la a um determinado comportamento.

Soler (2022, p. 12) exemplifica:

Dessa maneira, a proteção de dados pessoais versa exatamente sobre esse fragmento de informação referente à pessoa natural, identificada ou identificável, considerando que a inclusão do identificável é exatamente oriunda da possibilidade de cumulação de dados que identifica uma pessoa. Por exemplo, se tivermos os seguintes dados: (i) cantor internacionalmente famoso; (ii) dançarino internacionalmente conhecido; e (iii) apelido “Rei do Pop”, muitas pessoas já identificariam que estamos falando do Michael Jackson. Em alguns casos, somente pelo conhecimento do apelido já seria possível saber quem é o artista;

- b) dado sensível por sua vez, é aquele que pela sua própria natureza pode sujeitar o seu titular a práticas discriminatórias, tais como dados sobre a origem racial ou étnica, a convicção religiosa, a opinião política, dado referente à saúde ou à vida sexual do indivíduo;
- c) dado anonimizado é classificado como o dado pessoal que foi submetido a um procedimento para torna-lo não identificável.

No que diz respeito a LGPD e o tratamento deste dado pessoal protegido, é importante ressaltar alguns agentes envolvidos no tratamento destes dados. Ressaltando o conceito da legislação, que tratamento é toda operação realizada com dados pessoais, tais como a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (BRASIL, 2018).

- a) Considera-se titular de dados pessoais a pessoa natural quem se referem os dados pessoais objeto do tratamento;
- b) considera-se controlador, a pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais. No âmbito público, figura-se como controlador os órgãos públicos, entidades públicas, empresas públicas ou sociedades de economia mista que decidem sobre o tratamento de dados pessoais;
- c) considera-se operador quem realiza o tratamento de dados pessoais em nome do controlador;
- d) considera-se encarregado, a pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados.

De acordo com Soler (2022, p. 30, grifos do autor): “Ao controlador, atribui-se a tarefa de *tomar as decisões* sobre o tratamento de dados (‘controlar’) e, ao

operador, por sua vez, executar o tratamento de dados em nome do controlador ('efetivamente *operacionalizar* o tratamento de dados')".

Soler (2022) esclarece que o controlador é crucial no contexto da LGPD, já que boa parte das obrigações descritas na Lei Geral de Proteção de Dados serão realizadas por ele, além de ter a responsabilidade de comunicar a ANPD incidentes de segurança, trabalhar com as bases legais, sendo o principal responsável pela gestão dos dados.

Ainda, conforme Rodrigues e Ferreira (*apud* MONTEMEZZO, 2020, p. 569):

Melhor explicitando, os sujeitos, Rodrigues e Ferreira<sup>6</sup> ensinam que o controlador é o agente que procede com a coleta e a gestão dos dados pessoais, enquanto o operador, por sua vez, seria a pessoa, também jurídica ou física, que procede com o tratamento dos dados pessoais sob as ordens do primeiro (controlador). Já o encarregado é a pessoa indicada pelo controlador, que possui como responsabilidade fazer as conexões entre controlador, titulares e a autoridade nacional da proteção de dados.

Com relação aos princípios da Lei Geral de Proteção de Dados, os agentes de tratamento devem se atentar ao princípio da boa-fé, esperando deles o cumprimento das regras da legislação.

Ainda, relacionado aos conceitos da legislação, é impossível falar sobre Lei Geral de Proteção de Dados sem falar de consentimento. No texto da lei, no Art. 5º XII se fala que o consentimento é "a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada." (BRASIL, 2018, não paginado).

Esclarece Montemezzo (2020, p. 569):

Assim, como referido, um dos principais pilares que estrutura o texto da LGPD é a ideia do consentimento do titular dos dados para que eles sejam tratados. O consentimento deve ser dado de forma inequívoca, sugerindo-se que seja de forma escrita, ou por outro meio que comprove sua manifestação de vontade.

O consentimento é tido como um dos pilares da Lei, e é uma dificuldade a mais para quem faz o tratamento de dados pessoais, já que o titular destes dados pode retirar o consentimento em qualquer momento. Aqui mais um desafio para as empresas que realizam o tratamento de dados, isto porque este consentimento não é presumido, ele deve ser por escrito, ou por outro meio que demonstre a

manifestação de vontade do titular, conforme garante o Art. 8º da referida Lei (BRASIL, 2018).

Considerando o teor do texto legal, somado a uma rápida navegação na internet, verifica-se que muitas empresas não realizam este procedimento, já que na maioria das vezes o consentimento é de fato presumido.

Por este ângulo, Soler (2022, p. 17, grifo nosso) leciona:

Cumprido destacar que o consentimento pode estar presente em termos de uso, políticas de privacidade, contratos, etc. sendo usualmente utilizado quando existe uma relação direta entre a empresa e o consumidor. Cabendo nestas previsões as recomendações da LGPD, observamos que poderão ser aceitas pelo usuário com uma opção revestida por um “sim” em um formulário (*opt-in*), por exemplo.

Quando se trata de dados sensíveis, o Art. 11 da LGPD fala que o tratamento precisa ser específico e destacado (BRASIL, 2018).

Neste sentido, na construção de um documento que preveja o consentimento para tratamento de dados pessoais sensíveis, será necessário incluir: (i) quais dados serão tratados com essa base legal; (ii) que sua redação seja destacada das demais, podendo ser expressa por uma cláusula diferente, sob a forma de um subitem no documento, uma seção diferente, com a inclusão de outros elementos gráficos, enfim, apresentando destaque desta previsão em específico; (iii) que não seja genérico, se for possível, detalhando a finalidade específica, ou ao menos informando a finalidade de seu tratamento; (iv) por escrito ou outro instrumento que demonstre a manifestação da vontade do titular (SOLER, 2020, p. 23).

Pode-se concluir que o consentimento do titular dos dados se torna prejudicado, pois na maioria das vezes o que era pra ser claro e de fácil acesso é disfarçado por quem tem como objetivo o tratamento destes dados, não sendo as informações suficientes para preservar o direito do titular.

Evidenciada mais uma vez a importância do controlador, pois a Lei determina que em qualquer discussão cujo objeto seja o consentimento, é do controlador o ônus da prova de que o consentimento foi obtido nos termos definidos na legislação (BRASIL, 2018).

Outro problema evidente no tratamento de dados é relacionado ao próprio titular, conforme vimos, é através do consentimento que o titular dos dados define se estes dados podem ou não serem tratados. Então, cabe ao proprietário dos dados criar juntamente com a Legislação uma cultura de proteção de dados.

A LGPD é aplicada no meio físico e digital, sendo direcionada a qualquer entidade, empresa, pessoa física e jurídica que faça tratamento de dados pessoais, mas é fundamental entender onde a Lei não é aplicável. Conforme relembra Teixeira (2020, p. 51):

De outra forma, conforme o seu próprio art. 4º, a Lei n. 13.709/2018 não se aplica ao tratamento de dados pessoais quando: (i) praticado por pessoa natural para fins exclusivamente particulares e não econômicos; (ii) praticado para fins exclusivamente jornalísticos, artísticos ou acadêmicos; (iii) operacionalizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais; ou (iv) resultantes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto na Lei n. 13.709/2018.

A própria Lei Geral de Proteção de Dados refere que quando os dados não são usados para fins econômicos, não há a aplicação da Lei. Quando falamos em fins econômicos, automaticamente relacionamos a expressão com venda, comercialização e circulação de dinheiro, caracterizando mais uma vez a relação comercial ou de consumo carente de regulamentação em relação aos dados.

Ainda, importante mencionar como funciona a exclusão de dados no âmbito da Lei Geral de Proteção de Dados. O Art. 18 IV da legislação refere que a exclusão de dados pode ser solicitada a qualquer tempo pelo titular do dado (BRASIL, 2018).

Esta solicitação de eliminação encerra qualquer operação de dados que esteja sendo realizada com os dados fornecidos pelo titular, insta salientar que quando o dado tiver cumprido a finalidade pela qual foi tratado, o tratamento deste deverá ser encerrado independentemente de solicitação.

A exceção está no Art. 16 do ordenamento jurídico, a conservação dos dados pode ser realizada com a finalidade de cumprimento de obrigação legal ou regulatória pelo controlador; nos estudos por órgãos de pesquisa; no caso em que haja transferências para terceiros, desde que respeitada a Lei, ou para uso exclusivo do controlador, vedado seu acesso por terceiro (BRASIL, 2018).

Nos casos em que o dado seja conservado, a Lei orienta que o dado passe pelo processo de anonimização.

Gize-se por oportuno que o titular de dados precisa ter bom senso, caso ele tenha uma relação jurídica ou qualquer outra obrigação contratual e legal com a

empresa que possui seus dados, a empresa pode mantê-los, a fim de garantir seus direitos, inclusive os de contraditório e ampla defesa.

### 3.4 AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD)

De acordo com o próprio site do Governo Federal (GOV.BR, 2022b, não disponível): “A ANPD é o órgão da administração pública federal responsável por zelar pela proteção de dados pessoais e por implementar e fiscalizar o cumprimento da LGPD no Brasil.”

A instauração da Autoridade no Brasil, mesmo sendo um órgão independente, gerou bastante polêmica, visto que, faltando alguns meses para que a lei entrasse em vigor, o Governo Federal ainda não tinha indicado os membros, ou instituído a autoridade no país.

Conforme acrescenta Lima (2020, p. 109):

Um dos entraves para a criação de um órgão independente e autônomo para a proteção dos dados pessoais seria o contexto político e econômico do país o qual inviabilizava a criação de uma entidade que representaria mais gastos ao Governo.

Ainda, de acordo com o Governo Federal, as principais funções da ANPD são:

- Elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade;
- Fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;
- Promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança;
- Estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis;
- Promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional;
- Editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos na LGPD;
- Ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento;
- Editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de

pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se à Lei;  
Deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação da LGPD, as suas competências e os casos omissos;  
Articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação; e  
Implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com a LGPD (GOV.BR, 2022b, não paginado).

A criação da autoridade traz mais peso para as empresas que utilizam os dados e possuem acesso as informações dos titulares. De forma simples, a Autoridade Nacional de Proteção de Dados, serve principalmente para fiscalizar o cumprimento da LGPD.

Neste sentido, a própria Lei Geral de Proteção de Dados permite a ANPD de buscar relatórios e acompanhar o processo de empresas ou órgãos que recolhem e tratam dados, a fim de assegurar que estes estejam em sintonia com a LGPD.

As sanções administrativas da LGPD vigoram desde agosto de 2021, mas até o momento não foi aplicada nenhuma multa em valores, o que deve mudar em breve. Em agosto deste ano, foi aberta a consulta pública para a elaboração da norma de dosimetria e aplicação de sanções pela ANPD.

Rego e Campos (2022, não paginado) esclarecem que:

Inicialmente, é importante destacar que, apesar de ainda não terem sido publicadas objetivamente as formas e dosimetrias para o cálculo do valor-base das sanções de multa, as penalidades terão efeito retroativo e as empresas poderão ser multadas por situações ocorridas desde 01 de agosto de 2021, data do início da vigência das sanções. Logo, possivelmente as primeiras sanções em pecúnia da ANPD serão referentes a eventos já ocorridos e que estão sob investigação.

Destaca-se que embora tenha demorado para ser realizada, a norma de dosimetria promete aplicar sanções retroativas, neste sentido, as empresas que não se adequaram a lei não estão impunes de aplicação de multas.

No cenário internacional, em 2021, a Amazon, uma das gigantes do comércio eletrônico, recebeu uma multa no valor de US\$ 887 milhões por desrespeitar a GDPR, o valor representa 0,2% da receita total da empresa (PANCINI, 2021).

Já no Brasil, o Art. 52 da Lei Geral de Proteção de Dados, traz as sanções impostas aos agentes que desrespeitarem a Lei. As sanções vão desde advertência com prazo determinado para a adoção de medidas corretivas, até multa simples, limitada a 2% do faturamento da pessoa jurídica no seu último exercício, excluídos os tributos, limitados a R\$ 50.000.000 por infração (BRASIL, 2018).

Além da multa em valores, há as sanções que suspendem o funcionamento do banco de dados da empresa, ainda que parcialmente, pelo período prorrogável de 06 meses, podendo, dependendo do caso, ter a suspensão total do exercício de atividades relacionadas ao tratamento de dados (BRASIL, 2018).

Recentemente, através da Lei 14.460/2022, a ANPD foi transformada em Autarquia, a mudança foi realizada com o pretexto de trazer uma maior confiabilidade ao sistema regulatório, além de oferecer mais autonomia administrativa e financeira (CÂMARA DOS DEPUTADOS, 2022a).

Com esta recente mudança, acredita-se que a ANPD está cada vez mais próxima de cumprir o seu papel de fiscalização, com a aplicação de multas e demais sanções previstas em lei em razão do descumprimento da LGPD.

### 3.5 RESPONSABILIDADE CIVIL

Com a necessidade de trazer mais segurança jurídica aos titulares dos dados, a Lei Geral de Proteção de Dados trouxe uma seção que fala especificamente sobre a responsabilidade e necessidade de ressarcimento de eventuais danos. No artigo 42 da referida lei, há uma cláusula geral de reparação, em caso de danos causados devido a falha do tratamento de dados (BRASIL, 2018).

De acordo com Miragem (2022, p. 42) “[...] a responsabilidade civil leva à reparação do dano aquele que o causa a partir de um ato ilícito, com o escopo de restabelecer o equilíbrio violado, bem como de prevenir os outros atos lícitos causadores de novos prejuízos.”

Conforme esclarece Medeiros (2021, não paginado):

Inicialmente, importante mencionar que a responsabilidade civil pode ser subjetiva, ou seja, quando há necessidade de se provar o dano, nexos causal entre a conduta e a lesão, e a culpa do agente causador do dano (se houve culpa ou dolo). Por outro lado, há a responsabilidade objetiva (essa é a regra nas relações de consumo, por exemplo), onde basta a prova do dano e do nexos causal, ou seja, nesta haverá a obrigação de reparar o dano

independentemente da avaliação de culpa quando sua atividade implicar, por sua natureza e risco para os direitos de outrem.

A responsabilidade civil no âmbito da LGPD nada mais é do que obrigar a pessoa civilmente responsável a indenizar em caso de dano.

Art. 42 da LGPD diz que: O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo (BRASIL, 2018, não paginado).

Importante frisar que nos princípios da Lei, já se fala em prevenção, no sentido de que todas as medidas para evitar danos, ou utilização indevida dos dados deve ser tomada e utilizada por quem é responsável pelo tratamento de dados. Ou seja, caso haja eventual uso indevido os responsáveis pelo tratamento deverão ser responsabilizados.

Na visão de Miragem (2022), a responsabilidade civil possui 3 funções: Reparatória, Punitiva e Preventiva.

A função reparatória é apresentada como a mais clássica e consiste na reparação do dano. O causador do referido dano deverá levar a vítima as condições anteriores da violação, não conseguindo, deverá indenizá-la pelos prejuízos causados.

A função punitiva é bastante criticada na literatura sendo admitida como exceção. Se a vítima já teve seu dano reparado não há sentido em punir o causador do dano.

Quanto a função preventiva, Miragem (2022, p. 49) esclarece que:

Além de estar presente no artigo 12 do Código Civil, a função preventiva está constitucionalmente assegurada como direito fundamental, uma vez que o artigo 5º, inciso XXXV da Constituição Federal estabelece que “a lei não excluirá da apreciação do Poder Judiciário lesão ou ameaça a direito.

O autor ainda esclarece que a função preventiva está presente em todo sistema jurídico brasileiro, tanto nas relações de consumo, quanto nas que incide a Lei Geral de Proteção de Dados (MIRAGEM, 2022).

A LGPD em seu artigo 45, diz que:

Art. 45. As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente (BRASIL, 2018, não paginado).

Fazendo um paralelo com o Código de Defesa do Consumidor, Teixeira (2020, p. 57):

É possível assemelhar a responsabilização do controlador pelos atos de seus operadores à responsabilidade solidária – atribuída aos fornecedores de serviço pelos atos de seus prepostos e representantes autônomos – prevista no art. 34 do Código de Defesa do Consumidor (CDC). Isso para o âmbito das relações de consumo.

Teixeira (2021) ainda acrescenta que o direito a reparação de danos por utilização indevida já estava previsto no próprio Código de Defesa do Consumidor.

Na visão de Novakoski e Naspolini (2020, p. 162):

De forma similar ao regime implantado pelo Código de Defesa do Consumidor - CDC (Lei 8.078/90), a LGPD estabeleceu a solidariedade dos agentes que causaram a lesão (art. 42, § 1º, I e II) e, para mitigar a assimetria na relação entre controladores, operadores e titulares de dados pessoais, permitiu a inversão do ônus da prova por critério judicial (art. 42, § 2º), o que, a rigor científico, implica um sistema de presunção legal do dano sofrido pela vítima lesada.

Devido a relação com o CDC, há uma discussão se a responsabilidade civil no âmbito da Lei Geral de Proteção de Dados seria objetiva ou subjetiva, nestes termos, esclarecem Bioni e Dias (2020, não paginado):

Deve-se, assim, avançar para além da análise binária do regime jurídico de responsabilidade civil da LGPD, julgando-o de natureza objetiva ou subjetiva. Isto porque não deve haver dúvidas de que a política legislativa adotada exige a investigação em torno de um juízo de culpa dos agentes de tratamento de dados, mas, ao mesmo tempo, prescreve uma série de elementos com alto potencial de erosão dos filtros para que os agentes de tratamentos de dados sejam responsabilizados. O resultado parece ir no sentido de um regime jurídico de responsabilidade civil subjetiva com alto grau de objetividade.

Importante o destaque e a relação com o Código de Defesa do Consumidor, já que a própria Lei Geral de Proteção de Dados, traz em seu Art. 45 que as normas previstas na seção de responsabilidade não serão aplicadas em todos os casos, podendo depender da relação jurídica (BRASIL, 2018).

No caso de violação das normas jurídicas ou técnicas relacionadas a Lei Geral de Proteção de Dados, insta salientar que a responsabilidade civil só é caracterizada quando a violação de tais normas ocasionarem efetivamente dano ao titular de dados (BRASIL, 2018).

Frisa-se que a responsabilidade do controlador e operador é solidária, semelhante com os termos da responsabilidade civil utilizados no CDC.

A Lei traz ainda a hipótese de exclusão de responsabilidade, tal hipótese está prevista no Art. 43, podendo a responsabilidade civil do controlador e/ou operador ser afastada (BRASIL, 2018).

Nestes termos esclarece Teixeira (2021, p. 88):

Especificamente na LGPD, os agentes de tratamento não são responsabilizáveis quando provarem que: não realizaram o tratamento de dados pessoais que lhes é atribuído; não houve violação à legislação de proteção de dados; ou o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro (art. 43). Essas são hipóteses de excludentes de responsabilidade.

O instituto da responsabilidade civil deixa claro que as empresas precisam se atentar as regras da legislação, e mais do que cumprir a lei, precisam comprovar o cumprimento e adequação, sempre observando a postura do operador e controlador frente ao tratamento de dados.

### 3.6 A VULNERABILIDADE DO CONSUMIDOR

Após conhecermos um pouco sobre a LGPD, é importante comentarmos os impactos e correlações existentes com as regras previstas no Código de Defesa do Consumidor que conforme entendimento jurisprudencial, estabelece a responsabilidade objetiva, ou seja, independentemente da existência de culpa, dos fornecedores e prestadores de serviço na relação com os consumidores, que presumidamente são vulneráveis (SOUZA, 2022).

Como referido anteriormente, o Código de Defesa do Consumidor não apresenta atualizações que acompanhem o avanço crescente do comércio eletrônico, isso somado ao fato de que muitas vezes, o consumidor, parte mais vulnerável da relação, não possui o conhecimento técnico necessário para garantir a sua própria segurança.

Ainda, por muitas vezes, o consumidor precisa utilizar do serviço disponibilizado e não possui tempo hábil para ler uma política de privacidade extensa por exemplo, ou para entender o que os aplicativos, Órgãos e empresas vão fazer com os dados que ele disponibiliza nestas plataformas digitais.

Neste contexto, Ottobelli (*apud* BIONI; DIAS, 2020, não paginado), salienta:

O consumidor passou a ter uma participação ativa na economia informacional, pois sua opinião tornou-se o vetor que vai filtrar o que deve ou não ser produzido. Nas políticas de privacidade, as empresas especificam como usarão os dados pessoais e o usuário “decide” se concorda ou não – sendo que a discordância implica numa prejudicialidade até à própria participação social da pessoa. Dessa forma, as políticas de privacidade podem ser interpretadas como um contrato de adesão, onde a parte fornecedora decide as cláusulas, unilateralmente, solapando a ideia de autodeterminação informacional.

Neste sentido, Miragem, Marques e Magalhães (2020, p. 243) complementam:

A ordem jurídica defende o consumidor porque reconhece a necessidade de fazê-lo, identificando sua situação desigual em relação aos demais agentes do mercado (os fornecedores). Seu propósito fundamental é promover o equilíbrio das partes na relação de consumo, mitigando os efeitos de uma relação de subordinação estrutural do consumidor ao fornecedor (igualdade) de modo a assegurar sua regular ação na realização de seus interesses legítimos no mercado (liberdade). [...] Não restam dúvidas no sentido de que o consumidor é a parte mais vulnerável de qualquer relação comercial, não é a toa que existe uma lei inteira cujo objetivo principal é a tutela de seus direitos. Gize-se por oportuno que o CDC existe há mais de 30 anos, evidente que a Lei não conseguiu acompanhar os avanços tecnológicos da atualidade.

Quando falamos em vulnerabilidade do consumidor, importante relacionar o que a doutrina denomina como a classificação tríplex de vulnerabilidade. A vulnerabilidade técnica é aquela por onde o consumidor não possui o conhecimento especializado sobre o produto ou serviço da relação de consumo, evidente a desigualdade perante o fornecedor, que ao participar da oferta do produto, possui mais informações sobre ele. A vulnerabilidade jurídica é relacionada a falta de conhecimento que o consumidor possui com relação a seus direitos e deveres, já a vulnerabilidade fática é oriunda da relação desproporcional do consumidor com o fornecedor, essa desproporcionalidade pode ser relacionada a diferença de porte econômico, por exemplo (MIRAGEM; MARQUES; MAGALHÃES, 2020).

É possível verificar que um dos maiores desafios do Código de Defesa do Consumidor é a velocidade das transformações do mercado de consumo, especialmente com o fluxo da internet como reforçam Miragem, Marques e Magalhães (2020).

Este avanço tecnológico acaba criando uma pressão pela atualização do CDC, mas a própria velocidade destas transformações demonstra a dificuldade em seguir com qualquer alteração legislativa que se mantenha atualizada na medida em que a tecnologia avança.

Neste sentido:

Quanto aos novos modelos de oferta, o comércio eletrônico – inclusive por plataformas digitais – assim como o tratamento de dados pessoais dos consumidores para a definição de perfis de consumo, alteram o *modo* de consumir. Por outro lado, o surgimento de bens digitais, a aplicação crescente de inteligência artificial e o desenvolvimento da internet das coisas, acrescentando automação dos produtos e serviços, modificam substancialmente o *objeto* do consumo (MIRAGEM; MARQUES; MAGALHÃES, 2022, p. 249, grifos dos autores).

Miragem, Marques e Magalhães (2022) defendem uma nova forma de vulnerabilidade informacional, que não se restringe à falha na falta de informação prestada, mas a falta de intimidade com o ambiente virtual somada aos estímulos causados pelo meio digital, essa junção pode identificar uma vulnerabilidade própria do consumidor na internet, o que o autor chama de vulnerabilidade digital.

Quando falamos em vulnerabilidade digital, Lehfeld *et al.* (2021, p. 245):

Diante da falta de informação e despreparo técnico acerca dos contratos de consumo realizados, os consumidores virtuais passaram a ser vulneráveis não somente diante da relação material que é promovida por meio de compra de produtos ou serviços tradicionais, mas principalmente diante das empresas virtuais e pessoas dispostas a utilizarem a plataforma digital para aplicar golpes e utilizarem-se de dados não protegidos pelo fornecedor. A exacerbação da vulnerabilidade tornou-se tão notória diante dos mais diversos contratos de adesão pelos quais são obrigados a aceitar, informando seus dados pessoais e demais informações, que diversos mecanismos de proteção, para além do código do consumidor têm sido criados. A Lei Geral de Proteção de Dados demonstra a necessidade de reafirmação do Princípio da Vulnerabilidade no ciberespaço e a tutela dos indivíduos enquanto consumidores virtuais.

O Código parou no tempo, mas as empresas não, neste contexto, Miragem, Marques e Magalhães (2020, p. 3) esclarecem:

[...] para a formação de perfis e segmentação de consumidores, interessam dados relativos as suas transações comerciais (tais como o histórico de transações, frequência e valores envolvidos), estilo de vida e preferências pessoais, interesses e hábitos, obtidos por questionários diretos (como os que envolvem há décadas, a participação em prêmios e sorteios comerciais), ou análise de comportamento, mediante pesquisas ou coleta de informações específicas, como é o caso do itinerário de navegação na internet, utilização de dispositivos associados à internet das coisas,<sup>18</sup> ou as diferentes manifestações e reações em redes sociais e outros espaços virtuais de interação.

Ainda, de acordo com Tomasevicius Filho (2021, p. 177):

No Brasil, a tutela de tais dados foi objeto da legislação consumerista durante muito tempo, como consequência de o Código de Defesa do Consumidor (“CDC”) ter reconhecido o consumidor como parte hipossuficiente da relação, mas não em toda a sua complexidade. Afinal, na elaboração do CDC a sociedade ainda não tinha tão nítida a exploração dos dados como ativo principal das relações de consumo.

Exemplificando o comportamento das empresas em relação aos dados dos consumidores. De acordo com uma notícia publicada pelo Terraço Econômico (2019), nos Estados Unidos, em 2012, quando a Internet não havia alcançado a dimensão que possui atualmente, uma das maiores loja de varejo dos Estados Unidos, a Target, usou da análise de dados para concluir que uma cliente estava grávida antes mesmo dela saber.

Na época, a empresa já mantinha os registros de compras, além de outros dados dos usuários, acompanhando o padrão de consumo dos clientes. Falando especificamente deste caso, a equipe da loja definiu uma cesta com 25 produtos que mulheres grávidas costumam comprar.

Com base nestes dados, a empresa encaminhava cupons de desconto e ofertas personalizadas, tudo baseado no modelo de negócio construído pela loja. Em determinado momento, um consumidor questionou o envio de ofertas relacionadas à gravidez para a sua filha adolescente. A loja explicou não entender o motivo da adolescente fazer parte do algoritmo, quando meses depois, o consumidor volta a loja informando que o nascimento do neto estava previsto para o próximo mês.

Ottobelli (2021, não paginado, grifo do autor) diz que:

Todos os dias utilizamos a internet sem perceber o rastro que deixamos ao acessar, buscar e compartilhar informações, que relevam nossos interesses e preferências. Com esse material, os *cookies* de navegador são utilizados reunindo informações dos usuários que, posteriormente, irão direcionar publicidade, de acordo com o comportamento traçado a partir desses dados.

Mesmo que as compras sejam realizadas no meio eletrônico, o consumidor segue sendo amparado pelo CDC, a doutrina e a jurisprudência reconhecem o consumidor como a parte mais frágil e vulnerável da relação. Com o advento do comércio eletrônico, certamente este entendimento consolidado continuará presente nas decisões judiciais, agora também com base legal na Lei Geral de Proteção de Dados.

## 4 ANÁLISE DE CASOS ENVOLVENDO O VAZAMENTO DE DADOS NO BRASIL À LUZ DA LGPD

Conforme vimos anteriormente, a ANPD ainda não começou a aplicar as multas relacionadas ao descumprimento da Lei Geral de Proteção de Dados, no entanto, não é o único Órgão responsável por aplicar as sanções.

Neste capítulo, iremos observar como o Poder Judiciário, Ministério Público, Procons e Órgãos de Defesa do Consumidor estão atuando para que as empresas que descumpram a LGPD não saiam impunes.

### 4.1 DROGARIA RAIA

A Droga Raia é conhecida como uma das maiores redes de farmácia do país. Ao realizarmos uma pesquisa rápida, a empresa tem inúmeras reclamações registradas na plataforma Reclame Aqui, por onde consumidores registram seu descontentamento com relação ao descumprimento da LGPD.

Em suma, a empresa utiliza de estratégias para dar desconto vinculado ao CPF ou algum outro dado do cliente, os relatos são de clientes que pedem a exclusão e continuam recebendo e-mails e ligações da farmácia.

A conduta chamou a atenção do Ministério Público do Mato Grosso e do Procon, devido a quantidade extensa de reclamações sobre o mesmo tema. De acordo com o site do Procon do Mato Grosso:

Há indícios de que empresas estariam coletando dados pessoais e obtendo de forma irregular a autorização dos clientes para o tratamento e uso de seus dados pessoais sem passar as informações de forma clara e adequada, o que viola o Código de Defesa do Consumidor.

É uma prática regular a concessão de descontos em farmácias mediante o cadastro na base de dados das empresas, condicionando o fornecimento do CPF no momento da compra. Mas, com a entrada em vigor da Lei Geral de Proteção de Dados (LGPD), a regulamentação dada à coleta, uso, processamento e armazenamento de dados ganhou novas proporções, com o objetivo de garantir maior proteção para o consumidor.

Então, quando a empresa condiciona descontos e promoções ao cadastro de clientes, ela está comprando os dados do consumidor sem avisá-lo, o que viola a LGPD. Para obter os dados e o consentimento para o uso, o cidadão deve ser informado previamente, de forma clara e transparente, sobre quem terá acesso, para que seus dados serão utilizados, por quanto tempo, com quem serão compartilhados, entre outras informações. O consentimento é considerado nulo se for obtido de forma enganosa ou abusiva (PROCON-MT, 2021, não paginado).

Após a conclusão da investigação, foi aplicada multa no valor de R\$ 572.680,71 à Rede de Farmácias. De acordo com informações do site do Procon-MT (2021), durante as fiscalizações restou comprovado que a empresa estava obtendo o consentimento dos consumidores para tratar os dados deles, sem que eles entendessem o que de fato estava acontecendo com estes dados.

Ainda, de acordo com o site do Procon-MT (2021, não paginado):

Entre as irregularidades constatadas pelos fiscais do Procon estão a ausência de informações sobre o recadastramento (em dois estabelecimentos) e a falta/inadequação de informações sobre o recadastramento e autorização para o tratamento de dados pessoais em todas as unidades vistoriadas.

“Ficou comprovado que o principal objetivo da atualização cadastral é conseguir a autorização para o tratamento de dados, prevalecendo-se da ignorância do consumidor, e não apenas garantir a participação em programas de descontos e benefícios, como era informado aos clientes durante o recadastramento”, explica o coordenador de Fiscalização, Controle e Monitoramento de Mercado, Ivo Vinícius Firmo.

Para fixar o valor da multa foi considerada a condição econômica das unidades da empresa em Mato Grosso e o atenuante de o fornecedor atuado ser primário (Dec. Fed. Nº. 2.181/97, art. 25, II). Foram vistoriadas as unidades da Drogasil localizadas nos bairros Jardim Cuiabá, Cidade Alta (duas farmácias), Baú, Bosque da Saúde e Santa Rosa, todos na Capital.

No que diz respeito ao termo de consentimento assinado pelo consumidor, o Procon-MT (2021, não paginado) ainda acrescenta:

Ao analisar a íntegra do ‘Termo de Consentimento de Uso de Dados Pessoais’ do fornecedor, o Procon verificou que a autorização permitia ao grupo Raia/Drogasil coletar e utilizar os dados pessoais e de comportamento de compra de produtos obtidos em seus canais de atendimento, como sites, aplicativos, televendas, SAC e lojas.

Esses dados poderiam ser usados para pesquisas, participação de programas de fidelidade/descontos/participação em Programas de Benefícios em Medicamento e Produtos de Uso Contínuo e compartilhados com empresas do grupo, fornecedores e parceiros. Entretanto, a empresa não identificava o nome de quem teria acesso aos dados dos clientes.

## 4.2 MEGAVAZAMENTO DE DADOS DE 223 MILHÕES DE BRASILEIROS

Em 2021, o Brasil registrou o maior vazamento de dados da história do país. O número de dados vazados supera o da população total brasileira, estimando-se que neste caso, foram compartilhados inclusive dados de pessoas falecidas (G1, 2021).

De acordo com o site de notícias G1 (2021), foi realizado o vazamento de 223 milhões de números de CPFs, acompanhados de nome, sexo, dados de veículos, além de informações como renda, benefícios, programas sociais, fotos de rosto, entre outros. As informações estavam sendo vendidas por criminosos. Os CPFs eram ofertados de forma gratuita, e as demais informações eram vendidas em um fórum online destinado exclusivamente para a comercialização de base de dados.

Algumas pessoas foram presas pelo crime, mas ainda não se sabe de onde estes dados foram roubados. Há referência à algumas empresas e serviços, mas até o momento nenhuma hipótese restou comprovada (G1, 2021).

Na época a ANPD foi cobrada acerca do vazamento, mas demorou alguns dias para se pronunciar, o que resultou em severas críticas a instituição que seria a responsável por garantir o cumprimento da Lei Geral de Proteção de Dados.

A pedido da ANPD, foi aberta uma investigação pela Polícia Federal, importante frisar que na época vazaram dados de ministros do STF e do atual presidente da República. Considerando a quantidade de dados vazados estima-se que pelo menos um dado de cada brasileiro foi disponibilizado na plataforma utilizada pelos Hackers. (G1, 2021).

De acordo com reportagem do Tecnoblog (KNOTH, 2022), os dados vazados seguem disponibilizados na rede. Uma das grandes constatações no que diz respeito ao vazamento de dados no mundo virtual, é que uma vez que os dados são divulgados na internet, é praticamente impossível apagá-los 100%, sem que fique algo em alguma base de dados.

Certamente essa quantidade massiva de dados saiu do banco de dados de alguma empresa com vasto armazenamento de informações, já que foram vazados dados de praticamente toda a população brasileira, a desconfiança foi direcionada para o Serasa, que negou a possibilidade de vazamento.

Até o momento, os autores do vazamento foram presos, mas não se sabe de onde estes dados partiram, portanto, nenhuma empresa teve qualquer sanção aplicada em decorrência deste vazamento.

#### 4.3 CAMBRIDGE ANALYTICA – DADOS DE BRASILEIROS

Em 2018, milhares de dados de usuários da plataforma Facebook foram repassados a Cambridge Analytica, uma consultoria de marketing especializada em política, contratada para a campanha eleitoral de Donald Trump. Estima-se que aproximadamente 87 milhões de pessoas tiveram seus dados vazados, entre eles, 443 mil brasileiros (RIBEIRO, 2022).

De acordo com Ribeiro (2022), ainda em 2018, a investigação concluiu que o vazamento foi realizado através de um aplicativo de teste de personalidade.

Na época, a Senacon entendeu que o Facebook cometia prática abusiva com os usuários, e aplicou uma multa no valor de 6,6 milhões de reais (RIBEIRO, 2022).

Ainda este ano, com base no princípio da ampla defesa, o Órgão anulou a multa. Em sua defesa, o Facebook continuou negando que os dados dos brasileiros foram vazados e compartilhados com a Cambridge Analytica, com a afirmação de que não haviam provas deste possível vazamento. O Senacon não aceitou a justificativa, e a multa foi mantida no valor original de 6,6 milhões (RIBEIRO, 2022).

#### 4.4 BANCOS

O Banco Safra foi multado na importância de 2,4 milhões de reais pelo Senacon, em razão de uso indevido e compartilhamento de dados de aposentados e pensionistas do INSS, adquiridos através de listas de dados pessoais comercializadas (GOV.BR, 2022d).

De acordo com a denúncia de entidades de defesa do consumidor, o Safra era responsável por fazer o vazamento de dados de aposentados e pensionistas do INSS aos correspondentes bancários, que ofereciam empréstimos consignados por meio de ligações telefônicas consideradas insistente e abusivas (GOV.BR, 2022c, não paginado).

De acordo com o Ministério da Justiça (GOV.BR, 2022c), o banco apresentou recurso, o qual foi negado, sendo mantida a condenação administrativa para o pagamento da multa. No processo administrativo, foi entendido que o banco não fiscalizou as atividades feitas pelos correspondentes bancários, o que violou a LGPD e o Marco Civil da Internet. Não é mais possível recorrer da decisão.

Mais uma multa referente ao uso indevido de dados de aposentados e Pensionistas do INSS. O Banco BMG foi multado em 5,1 milhões de reais por

infrações de oferta de créditos envolvendo correspondentes bancários, semelhante ao que ocorreu com o Banco Pan.

De acordo com o Ministério da Justiça:

Ficou comprovado nos autos que a instituição financeira não impediu que terceiros, por ela contratada, agissem de forma abusiva. Os consumidores cujos dados foram utilizados para os contatos não eram informados da abertura de banco de dados e de cadastro, o que ocasionou exploração da hipervulnerabilidade de idosos aposentados e pensionistas do INSS (GOV.BR, 2022c, não paginado).

#### 4.5 APPLE – APLICATIVO DE ENVELHECIMENTO FACIAL

A APPLE foi multada pelo Procon de São Paulo, por desrespeitar o CDC ao disponibilizar um aplicativo que envelhece o rosto dos usuários, isto porque a política de privacidade e os termos de uso foram escritos totalmente em inglês, o que dificulta o acesso e entendimento do usuário (ARCOVERDE, 2019).

Uma das cláusulas prevê a possibilidade de compartilhamento dos dados do consumidor com as empresas que fazem parte do mesmo grupo, prestadoras de serviços e organizações terceirizadas, o que é ilegal, segundo a Fundação Procon-SP (ARCOVERDE, 2019, não paginado).

Na época da aplicação da multa, a Lei Geral de Proteção de Dados ainda não havia sido sancionada, mas o descumprimento da LGPD está claro, já que as informações de privacidade e termos de uso do aplicativo estavam em outro idioma, o que impossibilita o consentimento do titular, uma das bases da Lei.

De acordo com o Procon de São Paulo, a Justiça manteve a aplicação da multa no valor aproximado de 7 milhões de reais (PROCON SP, 2021).

Ainda, de acordo com o Procon SP (2021, não paginado):

Uma das cláusulas previa a possibilidade de compartilhamento dos dados do consumidor com outras empresas; outra estabelecia que os dados poderiam ser transferidos para países sem as mesmas leis de proteção de dados que as do país de origem. Também havia previsão de que conflitos entre usuários e as empresas seriam resolvidos não por meio judicial, mas por um serviço realizado no condado de Santa Clara, na Califórnia. A Apple estabelecia ainda cláusula que isentava suas responsabilidades por vício (problema) de qualquer natureza do produto ou serviço disponibilizado.

Isto posto, é possível concluir que as empresas que realizam tratamento de dados não devem se preocupar apenas com a fiscalização da ANPD. O Ministério da Justiça, em conjunto com o Procon, Ministério Público e demais Órgãos de fiscalização, têm realizado um trabalho minucioso no que diz respeito a proteção de dados.

Podemos falar que os órgãos possuem competência comum à ANPD, isto reforça quanto o atraso da atuação da Autoridade Nacional de Dados Pessoais impacta nas sanções das empresas que não respeitam a LGPD como deveriam.

Se não fosse a atuação dos Órgãos fiscalizadores acima citados, muitas empresas ainda não teriam sido multadas. Ora, se empresas gigantes do mercado, famosas e amplamente conhecidas, não fossem multadas, por que todas as outras empresas deveriam se adequar aos termos da legislação.

Importante referir que infelizmente, a aplicação de multas que resultam em perdas financeiras nem sempre são eficazes, especialmente quando usamos o parâmetro estabelecido na legislação brasileira. Conforme já referido no presente trabalho, a maior multa aplicada pela GDPR alcançou o valor de 887 milhões de dólares, muito além dos valores permitidos na LGPD.

Evidente que, quanto maior a empresa, maior a quantidade de dados que se trata, talvez as sanções financeiras não sejam suficientes para mudar a conduta das companhias, razão pela qual a atuação da ANPD se torna cada vez mais esperada, já que as sanções vão além de valores monetários.

## 5 CONCLUSÃO

O presente trabalho fala sobre a vulnerabilidade do consumidor á luz da Lei Geral de Proteção de Dados.

Primeiramente, a fim de demonstrar o advento da Internet, discorreu-se sobre os números e avanço da era digital no Brasil nos últimos anos, o que proporcionou o surgimento e consolidação do comércio eletrônico. O comércio eletrônico trouxe benefícios ao consumidor, aproximou pessoas, diminuiu o limite territorial e mudou o jeito das empresas e pessoas se relacionarem no âmbito comercial.

O comércio eletrônico também evidenciou a fragilidade do consumidor diante do meio eletrônico, isto porque este tipo de comércio alcança um maior número de consumidores, aumentando consideravelmente os riscos de fraudes, golpes e vazamento de dados.

Se nas lojas físicas o consumidor não possui total conhecimento de como seus dados são tratados, ou o motivo pelo qual necessariamente algum documento precisa ser vinculado ao clube de vantagens que o estabelecimento oferece, no meio eletrônico isso é ainda mais preocupante dada a quantidade de pessoas que acessam esse meio.

Verificou-se que o Marco Civil da Internet surgiu justamente para regularizar a navegação on-line, apresentando o conceito de dado e consentimento, trazendo um aspecto introdutório de alguns termos bem familiares de quem tem contato com a Lei Geral de Proteção de Dados. Utilizando de alguns princípios similares, as duas legislações surgiram para garantir o direito dos usuários, uma especificamente na Internet, outra em qualquer meio em que exista tratamento de dados.

Enquanto no Marco Civil o consentimento não passa de uma formalidade, na LGPD ele precisa ser fornecido com meios que demonstrem a manifestação absoluta de vontade do titular, sem textos genéricos ou abusivos.

O conceito de privacidade e transparência acompanham as legislações desde a Constituição Federal, e com a Lei Geral de Proteção de Dados não foi diferente, a Lei vem em sintonia com estes princípios, a fim de garantir o respeito, cuidado com os dados, informações e segurança da pessoa natural.

Não há dúvidas que a LGPD é um avanço legal que buscou trazer segurança jurídica especialmente quando falamos em meio digital, ponto focal da presente pesquisa.

Considerando que os dados são amplamente utilizados pelas empresas com a finalidade de fomentar o consumo, a necessidade de uma cultura de proteção de dados se demonstra mais que essencial, é quase uma urgência.

Não é improvável que as empresas considerem as possíveis multas aplicadas em caso de descumprimento da legislação como algo que não vai interferir no orçamento tanto quanto o valor despendido a título de programas de segurança, atualização de sites, especialistas, políticas internas e outros métodos que as tornem inteiramente adequadas a Lei.

Dito isso, pode-se concluir que não só as empresas devem investir na segurança de dados para evitar as multas e sanções do texto legal, mas os consumidores precisam entender e fazer valer o seu Direito, não há dúvidas que a figura do consumidor permanece sendo a parte mais vulnerável da relação comercial, isto está claro em todas as doutrinas e decisões judiciais que versam sobre o tema, mas ele precisa entender a importância do dado que lhe pertence.

## REFERÊNCIAS

ABCOMM. **Principais indicadores do e-commerce 2021**. 2021. Disponível em: <https://dados.abcomm.org/numeros-do-ecommerce-brasileiro>. Acesso em: 12 ago. 2022.

ARCOVERDE, Léo. Procon-SP aplica multas milionárias em Google e Apple por aplicativo que envelhece rostos. **G1**, São Paulo, 30 ago. 2019. Disponível em: <https://g1.globo.com/sp/sao-paulo/noticia/2019/08/30/procon-sp-aplica-multas-milionarias-em-google-a-apple-por-aplicativo-que-envelhece-rostos.ghtml>. Acesso em: 5 nov. 2022.

BARROS, Alexandre. **Internet chega a 88,1% dos estudantes, mas 4,1 milhões da rede pública não tinham acesso em 2019**. 2021. Disponível em: Acesso em: 12 ago. 2022.

BIONI, Bruno; DIAS, Daniel. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. **Civilistica.com**, Rio de Janeiro, a. 9, n. 3, 2020. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/662>. Acesso em: 10 nov. 2022.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/constituicao/constituicao.htm](https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm). Acesso em: 15 nov. 2022.

BRASIL. **Decreto nº 7.962, 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. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2013/decreto/d7962.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/decreto/d7962.htm). Acesso em: 25 nov. 2022.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/leis/l8078compilado.htm](https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm). Acesso em: 5 nov. 2022.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2014/lei/l12965.htm](https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm). Acesso em: 12 ago. 2022.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei geral de proteção de dados. Diário Oficial da União, Brasília, 14 ago. 2018. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/L13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm). Acesso em: 12 ago. 2022.

**CÂMARA DOS DEPUTADOS. Lei nº 14.460, de 25 de outubro de 2022.**

Transforma a Autoridade Nacional de Proteção de Dados (ANPD) em autarquia de natureza especial e transforma cargos comissionados; altera as Leis nºs 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), e 13.844, de 18 de junho de 2019; e revoga dispositivos da Lei nº 13.853, de 8 de julho de 2019. 2022a. Disponível em: <https://www2.camara.leg.br/legin/fed/lei/2022/lei-14460-25-outubro-2022-793355-norma-pl.html>. Acesso em: 5 nov. 2022.

**CÂMARA DOS DEPUTADOS. Promulgada lei que transforma Autoridade Nacional de Proteção de Dados em autarquia.** 2022b. Disponível em:

<https://www.camara.leg.br/noticias/915858-promulgada-lei-que-transforma-autoridade-nacional-de-protecao-de-dados-em-autarquia>. Acesso em: 5 nov. 2022.

**CGI.BR. Cresce o uso de internet durante a pandemia e número de usuários no Brasil chega a 152 milhões, é o que aponta pesquisa do Cetic.br.** 2021.

Disponível em: <https://www.cgi.br/noticia/releases/cresce-o-uso-de-internet-durante-a-pandemia-e-numero-de-usuarios-no-brasil-chega-a-152-milhoes-e-o-que-aponta-pesquisa-do-cetic-br>. Acesso em: 12 ago.2022.

**COMISSÃO EUROPEIA. A proteção de dados na EU.** [201-?]. Disponível em:

[https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu\\_pt](https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_pt). Acesso em: 26 ago. 2022.

DEL MASSO, Fabiano; ABRUSIO, Juliana; FLORÊNCIO FILHO, Marco Aurélio (coords.). **Marco civil da internet:** lei 12.965/2014. São Paulo: Revista dos Tribunais, 2014. Disponível em: <https://proview.thomsonreuters.com/launchapp/title/rt/monografias/99378514/v1/document/99512327/anchor/a-99512327>. Acesso em: 27 nov. 2022.

EXTRA. Golpes na internet: em 6 de 10 casos, empresas são responsabilizadas na justiça por prejuízos financeiros. **Extra**, 19 jan. 2022. Disponível em:

<https://extra.globo.com/economia-e-financas/golpes-na-internet-em-6-de-10-casos-empresas-sao-responsabilizadas-na-justica-por-prejuizos-financeiros-25359089.html>. Acesso em: 12 ago. 2022.

FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões do direito brasileiro.** 2020. Disponível em:

<https://next-proview.thomsonreuters.com/launchapp/title/rt/monografias/195107452/v2/page/1>. Acesso em: 26 ago. 2022.

G1. Entenda o caso de Edward Snowden, que revelou espionagem dos EUA. **G1**, São Paulo, 14 fev. 2014. Disponível em: <https://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html>.

Acesso em: 17 ago. 2022.

G1. Megavazamento de dados de 223 milhões de brasileiros: o que se sabe e o que falta saber. **G1**, 28 jan. 2021. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2021/01/28/vazamento-de-dados-de-223-milhoes-de-brasileiros-o-que-se-sabe-e-o-que-falta-saber.ghtml>. Acesso em: 8 nov. 2022.

GOV.BR. **90% dos lares brasileiros já tem acesso à internet no Brasil, aponta pesquisa.** 2022a. Disponível em: <https://www.gov.br/casacivil/pt-br/assuntos/noticias/2022/setembro/90-dos-lares-brasileiros-ja-tem-acesso-a-internet-no-brasil-aponta-pesquisa>. Acesso em: 23 set. 2022.

GOV.BR. **Autoridade Nacional de Proteção de Dados: perguntas frequentes.** 2022b. Disponível em: [https://www.gov.br/anpd/pt-br/acesso-a-informacao/perguntas-frequentes-2013-anpd#:~:text=de%20Dados%20\(ANPD\)-,3.1%20%2D%20O%20que%20%C3%A9%20a%20Autoridade%20Nacional%20de%20Prote%C3%A7%C3%A3o%20de,cumprimento%20da%20LGPD%20no%20Brasil.https://www.stj.jus.br/sites/portalp/Leis-e-normas/lei-geral-de-protecao-de-dados-pessoais-igpd#:~:text=A%20ANPD%20%C3%A9%20respons%C3%A1vel%2C%20entre,e%20das%20pol%C3%ADticas%20p%C3%BAblicas%20sobre](https://www.gov.br/anpd/pt-br/acesso-a-informacao/perguntas-frequentes-2013-anpd#:~:text=de%20Dados%20(ANPD)-,3.1%20%2D%20O%20que%20%C3%A9%20a%20Autoridade%20Nacional%20de%20Prote%C3%A7%C3%A3o%20de,cumprimento%20da%20LGPD%20no%20Brasil.https://www.stj.jus.br/sites/portalp/Leis-e-normas/lei-geral-de-protecao-de-dados-pessoais-igpd#:~:text=A%20ANPD%20%C3%A9%20respons%C3%A1vel%2C%20entre,e%20das%20pol%C3%ADticas%20p%C3%BAblicas%20sobre). Acesso em: 1 nov. 2022.

GOV.BR. **Ministério da Justiça e Segurança Pública multa banco por utilizar dados sem consentimento de consumidores idosos.** 2022c. Disponível em: <https://www.gov.br/mj/pt-br/assuntos/noticias/ministerio-da-justica-e-seguranca-publica-multa-banco-por-utilizar-dados-sem-consentimento-de-consumidores-idosos>. Acesso em: 10 nov. 2022.

GOV.BR. **Senacon mantém multa de R\$2,4 milhões ao Banco Safra por abuso em oferta de empréstimo.** 3 nov. 2022d. Disponível em: <https://www.gov.br/mj/pt-br/assuntos/noticias/senacon-mantem-multa-de-r-2-4-milhoes-ao-banco-safra-por-abuso-em-oferta-de-emprestimo>. Acesso em: 5 nov. 2022.

HACKEROTT, Nadia Andreotti Tüchumantel. **Aspectos jurídicos do e-commerce.** São Paulo: Thomsom Reuters Revista dos Tribunais, 2020. *E-book*. Disponível em: <https://next-proview.thomsonreuters.com/launchapp/title/rt/monografias/257723059/v2/page/RB-1.1%20>. Acesso em: 20 out. 2022.

IBGE EDUCA. **Uso de internet, televisão e celular no Brasil.** c2022. Disponível em: <https://educa.ibge.gov.br/jovens/materias-especiais/20787-uso-de-internet-televisao-e-celular>. Acesso em: 12 ago. 2022.

KNOTH, Pedro. **Megavazamento de 223 milhões de CPFs: um ano se passou e ainda há perguntas sem resposta.** 2022. Disponível em: <https://tecnoblog.net/especiais/megavazamento-de-223-milhoes-de-cpfs-um-ano-se-passou-e-ainda-ha-perguntas-sem-resposta/#h-especialistas-avaliam-postura-da-anpd>. Acesso em: 8 nov. 2022.

LEHFELD, Lucas de Souza *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, jan./abr. 2021. Disponível em: <https://webcache.googleusercontent.com/search?q=cache:SYtcqd2qCsoJ:https://periodicos.unisantos.br/pesquiseduca/article/download/1029/902/2789&cd=18&hl=pt-BR&ct=clnk&gl=br>. Acesso em: 25 nov. 2022.

LEITE, George Salomão; LEMOS, Ronaldo (coord.). **Marco civil da internet.** São Paulo: Atlas, 2014. *E book*.

LEÓN, Lucas Pordeus. **Brasil tem 152 milhões de pessoas com acesso à internet**. 2021. Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2021-08/brasil-tem-152-milhoes-de-pessoas-com-acesso-internet>. Acesso em: 12 ago. 2022.

LIMA, Cíntia Rosa Pereira de. **Autoridade nacional de proteção de dados e a efetividade da Lei Geral de Proteção de Dados**: de acordo com a Lei Geral de Proteção de Dados (Lei n. 13.709/2018 e as alterações da Lei n. 13.853/2019), o Marco civil da Internet (Lei n. 12.965/2014) e as sugestões de alteração do CDC (PL 3.514/2015). São Paulo: Grupo Almedina Brasil, 2020. *E-book*.

MEDERIDOS, Erick Felipe. **Responsabilidade civil segundo e LGPD**. 2021. Disponível em: <https://www.migalhas.com.br/depeso/348113/responsabilidade-civil-segundo-a-lgpd>. Acesso em: 13 nov. 2022.

MIRAGEM, Bruno. A lei geral de proteção de dados (Lei 13.709/2018) e o direito do consumidor. **Revista dos Tribunais**, [S. l.], v. 1009/2019, nov. 2019. Disponível em: <https://www.brunomiragem.com.br/wp-content/uploads/2020/06/002-LGPD-e-o-direito-do-consumidor.pdf>. Acesso em: 12 out. 2022.

MIRAGEM, Bruno. **O direito do consumidor pós-pandemia**. 2021. Disponível em: <https://brunomiragem.com.br/2021/03/19/o-direito-do-consumidor-pos-pandemia>. Acesso em: 25 nov. 2022.

MIRAGEM, Bruno. **Responsabilidade civil na LGPD**. [S. l.]: Foco Jurídico, 2022.

MIRAGEM, Bruno; MARQUES, Claudia Lima; MAGALHÃES, Lucia Ancona Lopez de (org.). **Direito do consumidor 30 anos de CDC**: da consolidação como direito fundamental aos atuais desafios da sociedade. Rio de Janeiro: Forense, 2020. *E-book*.

MONTEMEZZO, Patrícia. Privacidade de dados em tempos de pandemia. *In*: DRAGO, Guilherme Dettmer; MIRANDA, Daniela de Oliveira; SILVEIRA, Luiz Fernando Castilhos (orgs.). **Coletânea de artigos científicos alusiva aos 20 anos do Bacharelado em Direito do Campus Universitário da Região das Hortênsias**. Caxias do Sul, RS: Educs, 2020. *E-book*. p. 590-614. Disponível em: <https://www.ucs.br/educs/arquivo/ebook/coletanea-alusiva-aos-20-anos-do-bacharelado-em-direito-do-campus-universitario-da-regiao-das-hortensias>. Acesso em: 7 nov. 2022.

MP MT. **Redes de drogarias são notificadas pelo Ministério da Justiça e Segurança Pública por possível infração à Lei de Proteção de Dados**. 2021. Disponível em: <https://www.mpmt.mp.br/portalcdo/news/725/107906/redes-de-drogarias-sao-notificadas-pelo-ministerio-da-justica-e-seguranca-publica-por-possivel-infracao-a-lei-de-protecao-de-dados/137>. Acesso em: 1 nov. 2022.

NADIA, Andreotii Tuchumante Hackerott (coord.). **Aspectos jurídicos do e-commerce**. 2. ed. [S. l.]: Revista dos Tribunais, 2022. Disponível em: <https://next-proview.thomsonreuters.com/launchapp/title/rt/monografias/257723059/v2/page/V>. Acesso em: 10 nov. 2022.

NOVAKOSKI, André Luis Mota; NASPOLINI, Samyra Haydêe Dal Farra. Responsabilidade civil na LGPD: problemas e soluções. **Conpedi Law Review** Evento Virtual, v. 6, n. 1, p. 158-174, jan./dez. 2020. Disponível em: <https://indexlaw.org/index.php/conpedireview/article/view/7024>. Acesso em: 1 nov. 2022.

OTTOBELLI, Gisele Fernanda. A (hiper)vulnerabilidade do consumidor no mercado informacional: LGPD e o Consentimento. **Revista Consultor Jurídico**, 5 nov. 2021. Disponível em: <https://www.conjur.com.br/2021-nov-05/ottobelli-hipervulnerabilidade-consumidor-mercado-informacional>. Acesso em: 5 nov. 2022.

PANCINI, Laura. Amazon recebe multa recorde de US\$ 887 milhões da União Europeia. **Exame**, 30 jul. 2021. Disponível em: <https://exame.com/tecnologia/amazon-multa-recorde-da-uniao-europeia>. Acesso em: 20 out. 2022.

PERES FILHO, José Augusto. **Direito do consumidor**. 2. ed. Rio de Janeiro: Método, 2022. *E-book*.

PREMEBIDA, Eduardo Antero. E-commerce em 2020, um cenário de oportunidades em meio a pandemia. **Research, Society and Development**, [S. l.], v. 10, n. 2, 2021. Disponível em: <https://rsdjournal.org/index.php/rsd/article/view/12984/11640>. Acesso em: 25 nov. 2022.

PROCON-MT. Procon **Estadual multa rede de farmácias por infração à Lei de Proteção de Dados Pessoais**. 2021. Disponível em: <http://www.procon.mt.gov.br/-/17501890-procon-estadual-multa-rede-de-farmacias-por-infracao-a-lei-de-protecao-de-dados-pessoais>. Acesso em: 15 nov. 2022.

PROCON SP. **Justiça mantém multa do Procon-SP à Apple**. 2021. Disponível em: <https://www.procon.sp.gov.br/justica-mantem-multa-do-procon-sp-a-apple>. Acesso em: 5 nov. 2022.

RECLAME AQUI. **Sobre o Reclame Aqui**. [202-?]. Disponível em: <https://www.reclameaqui.com.br/como-funciona>. Acesso em: 15 nov. 2022.

REGO, Maria Beatriz Torquato; CAMPOS, Lucas Cruz. O que esperar das primeiras multas da LGPD aplicadas pela ANPD. **Revista Consultor Jurídico**, 17 ago. 2022. Disponível em: [https://www.conjur.com.br/2022-ago-17/rego-campos-primeiras-multas-anpd#\\_edn1](https://www.conjur.com.br/2022-ago-17/rego-campos-primeiras-multas-anpd#_edn1). Acesso em: 19 ago. 2022.

RIBEIRO, Luci. Facebook é multado em R\$ 6,6 milhões no Brasil por vazar dados de usuários. **CNN Brasil**, 23 ago. 2022. Disponível em: <https://www.cnnbrasil.com.br/business/facebook-e-multado-em-r-66-milhoes-no-brasil-por-vazar-dados-de-usuarios>. Acesso em: 5 nov. 2022.

SOLER, Fernanda G. **Proteção de dados**: reflexões práticas e rápidas sobre a LGPD. São Paulo: Saraiva, 2022. *E-book*.

SOUZA, Carlos Affonso et al. **Marco civil da internet**. [S. l.]: Revista dos Tribunais, 2018. Disponível em: <https://proview.thomsonreuters.com/launchapp/title/rt/monografias/133433160/v1/document/145690847/anchor/a-145690847>. Acesso em: 27 nov. 2022.

SOUZA, Nara. **A LGPD no âmbito das relações de consumo**: os benefícios da conformidade legal para consumidores e fornecedores. 2022. Disponível em: <https://www.nextlawacademy.com.br/blog/a-lgpd-no-ambito-das-relacoes-de-consumo-os-beneficios-da-conformidade-legal-para-consumidores-e-fornecedores>. Acesso em: 12 out. 2022.

SUPERIOR TRIBUNAL DE JUSTIÇA – STJ. **Criptografia em aplicativo de mensagem não permite multa cominatória, decide Quinta Turma**. 2021. Disponível em: <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/24062021-Criptografia-em-aplicativo-de-mensagem-nao-permite-multa-cominatoria--decide-Quinta-Turma.aspx>. Acesso em: 1 nov. 2022.

SUPERIOR TRIBUNAL DE JUSTIÇA – STJ. **Um marco na regulamentação sobre dados pessoais no Brasil**. [2022?]. Disponível em: <https://www.stj.jus.br/sites/portalp/Leis-e-normas/lei-geral-de-protexao-de-dados-pessoais-lgpd#:~:text=A%20ANPD%20%C3%A9%20respons%C3%A1vel%2C%20entre,e%20das%20pol%C3%ADticas%20p%C3%ABlicas%20sobre>. Acesso em: 2 nov. 2022.

TEFFÉ, Chiara Spadaccini de; MORAES, Maria Celina Bodin de. Redes sociais virtuais: privacidade e responsabilidade civil análise a partir do marco civil da internet. **Pensar**, Fortaleza, v. 22, n. 1, p. 108-146, jan./abr. 2017. Disponível em: <https://ojs.unifor.br/rpen/article/view/6272/pdf>. Acesso em: 25 nov. 2022.

TEIXEIRA, Tarcísio. **Direito digital e processo eletrônico**. 5. ed. São Paulo: Saraiva, 2020. *E-book*.

TEIXEIRA, Tarcísio. **LGPD e o e-commerce**. 2. ed. São Paulo: Saraiva, 2021. *E-book*.

TERRAÇO ECONÔMICO. **Big Data**: como a Target descobriu uma gravidez antes da família? 2019. Disponível em: <https://www.oguiafinanceiro.com.br/textos/big-data-como-a-target-descobriu-uma-gravidez-antes-da-propria-familia>. Acesso em: 5 nov. 2022.

THEODORO JÚNIOR, Humberto. **Direitos do consumidor**. 10. ed. Rio de Janeiro: Forense, 2020. *E-book*.

TOMASEVICIUS FILHO, Eduardo. **A lei geral de proteção de dados brasileira**: análise setorial. São Paulo: Almedina Brasil, 2021. 2 v. *E-book*.

VERÍSSIMO, Érico. **Os dados não são o novo petróleo.** 2021. Disponível em: [https://www.linkedin.com/pulse/os-dados-n%C3%A3o-s%C3%A3o-o-novo-petr%C3%B3leo-erico-verissimo/?trk=pulse-article\\_more-articles\\_related-content-card&originalSubdomain=pt](https://www.linkedin.com/pulse/os-dados-n%C3%A3o-s%C3%A3o-o-novo-petr%C3%B3leo-erico-verissimo/?trk=pulse-article_more-articles_related-content-card&originalSubdomain=pt). Acesso em: 1 nov. 2022.

WHATSAPP. **Sobre a criptografia de ponta a ponta.** c2022. Disponível em: [https://faq.whatsapp.com/791574747982248/?locale=pt\\_BR](https://faq.whatsapp.com/791574747982248/?locale=pt_BR). Acesso em: 1 nov. 2022.