



UNIVERSIDADE DO SUL DE SANTA CATARINA
ADOLFO CHÁVEZ WILLRICH

**COMÉRCIO ELETRÔNICO E A REGULAMENTAÇÃO DA LEI GERAL DE
PROTEÇÃO DE DADOS**

Florianópolis
2020

ADOLFO CHÁVEZ WILLRICH

**COMÉRCIO ELETRÔNICO E A REGULAMENTAÇÃO DA LEI GERAL DE
PROTEÇÃO DE DADOS PESSOAIS**

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Direito, da Universidade do Sul de Santa Catarina, como requisito parcial para obtenção do título de Bacharel em Direito.

Orientador: Prof. Hernani Luiz Sobierajski, Msc.

Florianópolis

2020

ADOLFO CHÁVEZ WILLRICH

**COMÉRCIO ELETRÔNICO E A REGULAMENTAÇÃO DA LEI GERAL DE
PROTEÇÃO DE DADOS**

Este Trabalho de Conclusão de Curso foi julgado adequado à obtenção do título de Bacharel em Direito e aprovado em sua forma final pelo Curso de Graduação em Direito, da Universidade do Sul de Santa Catarina.

Florianópolis, (dia) de (mês) de (ano da defesa).

Professor e orientador Nome do Professor, titulação
Universidade do Sul de Santa Catarina

Prof. Nome do Professor, titulação
Universidade do Sul de Santa Catarina

Prof. Nome do Professor, titulação
Universidade do Sul de Santa Catarina

TERMO DE ISENÇÃO DE RESPONSABILIDADE

COMÉRCIO ELETRÔNICO E A REGULAMENTAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS

Declaro, para todos os fins de direito, que assumo total responsabilidade pelo aporte ideológico e referencial conferido ao presente trabalho, isentando a Universidade do Sul de Santa Catarina, a Coordenação do Curso de Direito, a Banca Examinadora e o Orientador de todo e qualquer reflexo acerca deste Trabalho de Conclusão de Curso.

Estou ciente de que poderei responder administrativa, civil e criminalmente em caso de plágio comprovado do trabalho monográfico.

Florianópolis, 06 de julho de 2020.

ADOLFO CHÁVEZ WILLRICH

Dedico esta monografia às minhas filhas,
Raíssa e Luisa, que são minha fonte de alegria.

AGRADECIMENTOS

Agradeço primeiramente ao meu Professor Hernani, por ter acolhido a proposta de me orientar neste trabalho, pela instrução, conselhos seguros, suporte e sempre me incentivar, de que estava no caminho certo, estas, sem dúvidas, foram peças chaves para a elaboração deste trabalho monográfico, ainda mais em tempos de pandemia, no qual nos encontramos.

Agradeço aos meus colegas de curso que me auxiliaram durante toda a faculdade e tornaram o meu período na instituição acadêmica um dos mais felizes.

Agradeço a Deus, pela minha vida e pela família que me deu. Por fim, agradeço aos meus pais, que são meus exemplos, e que sem eles eu não chegaria até aqui.

“Quando observares a corrupção a ser recompensada e a honestidade se converter em autossacrifício; então poderás constatar que a tua sociedade está condenada” (Ayn Rand).

RESUMO

O presente estudo foi elaborado com o propósito de apresentar o contexto evolutivo da Internet, inicialmente, discorrendo sobre a origem do comércio eletrônico e suas características, principalmente no tocante ao advento da Lei Geral de Proteção de Dados e como esta impactará as empresas, já que a proteção de dados é tema muito discutido na atualidade. Utiliza-se como método de abordagem o de pensamento dedutivo e de natureza qualitativa, posto o caráter interpretativo da LGPD no domínio do comércio eletrônico. A técnica de pesquisa adotada é a bibliográfica, com base em doutrinas, artigos científicos, notícias e legislação. Quanto ao objetivo é justamente debater o tema e proporcionar uma maior familiaridade, possibilitado por meio do procedimento monográfico. O trabalho desenvolve, num primeiro capítulo acerca do surgimento da Internet, e como isso ajudou a impulsionar o comércio, por conseguinte, descreve-se o conceito de comércio eletrônico, apresentando os contratos celebrados eletronicamente, as lojas virtuais, e a legislação aplicada à estas. O segundo capítulo busca examinar Lei Geral de Proteção de Dados, demonstrando-se o cuidado em manter um dado preservado, seja ele pessoal ou sensível, bem como o consentimento do titular. Por fim, no terceiro capítulo são examinadas as disposições acerca da regulação da lei no âmbito do comércio eletrônico. Conclui-se que até que a ANPD esteja devidamente constituída e atuando nos casos concretos e a LGPD esteja em vigor, não há como garantir o quanto a privacidade estará preservada, nessa senda, o usuário brasileiro titular de dados precisará saber o que é proteção de dados pessoais e quais são seus direitos.

Palavras-chave: Comércio Eletrônico. Internet. Lei Geral de Proteção de Dados. Regulamentação.

LISTA DE SIGLAS

ANPD – Autoridade Nacional de Proteção de Dados

ARPA – Advanced Research Projects Agency

ARPANET – Advanced Research Projects Agency Network

CE – Conselho Europeu

CEDH – Convenção Europeia dos Direitos do Homem e das Liberdades Fundamentais

CF – Constituição Federal

DPO – Data Protection Officer

DUDH – Declaração Universal de Direitos Humanos

IP – Internet Protocol

LAN – Local Area Networks

LGPD – Lei Geral de Proteção de Dados

GDPR – General Data Protection Regulation

MCI – Marco Civil da Internet

TCP – Transmission Control Protocol

UCLA – Universidade da Califórnia em Los Angeles

WWW – World Wide Web

SUMÁRIO

| | | |
|--------------|---|-----------|
| 1 | INTRODUÇÃO..... | 11 |
| 2 | COMÉRCIO ELETRÔNICO | 14 |
| 2.1 | EVOLUÇÃO DO COMÉRCIO COM A INTERNET | 16 |
| 2.2 | CONCEITO..... | 18 |
| 2.3 | CONTRATOS ELETRÔNICOS..... | 20 |
| 2.4 | LOJAS VIRTUAIS | 24 |
| 2.5 | LEGISLAÇÃO APLICÁVEL AS EMPRESAS DE COMÉRCIO ELETRÔNICO | 26 |
| 3 | LEI GERAL DE PROTEÇÃO DE DADOS | 29 |
| 3.1 | ORIGEM DA LEI GERAL DE PROTEÇÃO DE DADOS..... | 30 |
| 3.2 | TERMOS E CONCEITOS ESTABELECIDOS PELA LEI | 33 |
| 3.3 | ÂMBITO DE APLICAÇÃO | 36 |
| 3.4 | PRINCÍPIOS DA LEI GERAL DE PROTEÇÃO DE DADOS | 38 |
| 3.5 | CONSIDERAÇÕES SOBRE O MARCO CIVIL DA INTERNET | 41 |
| 4 | REGULAMENTAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS..... | 44 |
| 4.1 | AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD) | 45 |
| 4.2 | AGENTES DE TRATAMENTO | 47 |
| 4.2.1 | Responsabilidade e Ressarcimento de Danos | 51 |
| 4.3 | CONSENTIMENTO PELO TITULAR | 53 |
| 4.4 | PENALIDADES | 54 |
| 4.5 | COMÉRCIO ELETRÔNICO EM CONFORMIDADE COM A LEI GERAL DE PROTEÇÃO DE DADOS..... | 58 |
| 5 | CONCLUSÃO..... | 60 |
| | REFERÊNCIAS | 62 |

1 INTRODUÇÃO

Com o advento da Lei Geral de Proteção de Dados (LGPD), será fundamental existir uma coleta e tratamento adequado dos dados pessoais por parte das empresas de comércio eletrônico, já que a lei encontra-se em *vacatio legis* até 3 de maio de 2021. A LGPD define o que são dados pessoais e sensíveis, posto a necessidade de novas disposições no ordenamento jurídico brasileiro relacionadas à proteção de dados, vez que o comércio eletrônico está em constante evolução e é preciso acompanhá-lo, as empresas corporativas estão sempre em busca de inovações e novos negócios, de modo que há uma mudança de cultura, de pensamento, e de consumo que interfere em direitos profundamente ligados a nós, especialmente no que se refere à privacidade, direito fundamental consagrado pela Constituição Federal e a proteção de dados no Brasil que vem ganhando espaço.

No meio digital, os dados pessoais são extremamente valiosos, já que fornecem informações sobre nossa vida, gostos pessoais, endereço de residência ou eletrônico, e quem os possuir deverá cumprir com a legislação, sendo que as empresas terão que se adequar para que a lei não se torne um regramento que limite as atividades empresariais, menos ainda que as sanções sejam maiores do que os cuidados que esta propõe. Ademais, não é exagero dizer que quando entramos em qualquer site da Internet, existe a captura de suas preferências de compras, interesses, vontades de consumo, à vista disso, se faz pertinente uma lei que regule como se dará esse tratamento de dados.

Especificamente na última década, viu-se que diversos aspectos da vida cotidiana poderiam ser resolvidos em pouco tempo, a título de exemplo, a compra de livros, contratação de algum serviço, a ida ao mercado pode ser feita através de uma compra on-line, aquisição de remédios que podem ser entregues em sua residência, assistir a filmes na televisão como o Netflix. Hoje, apenas um clique de um celular pode resolver a vida de milhares de pessoas.

É verdade que nunca se falou tanto em temas como a privacidade, dados pessoais, consentimento, vazamento de dados, lei para fake news, sigilo, criptografias, redes sociais, evolução tecnológica, isso são só alguns exemplos da magnitude que tem este assunto, e a LGPD vem para reiterar essa mudança de comportamento da sociedade.

A partir dessas considerações, foi elaborado o seguinte problema de pesquisa: como se dará a funcionalização da Lei Geral de Proteção de Dados no âmbito do comércio eletrônico?

O objetivo geral desta monografia é discutir como se dará a atuação da lei nas empresas de e-commerce, para tanto, este trabalho está estruturado em três capítulos de desenvolvimento, permeado pelos seguintes objetivos específicos: no primeiro capítulo fornece-se informações relacionadas à evolução do comércio com o advento da Internet; descrevendo-se o conceito do comércio eletrônico e apresentando os contratos celebrados eletronicamente, cada vez mais presente na atualidade, as lojas virtuais e a legislação aplicada à estas; no segundo capítulo evidencia-se a importância dos dados pessoais com a chegada da LGPD, destacando-se sua origem, termos e definições estabelecidos pela lei, seu campo de aplicação, princípios que o regem e reafirmar a importância que tem o Marco Civil da Internet para o direito brasileiro; o terceiro capítulo se busca examinar a normatização da LGPD, que possivelmente entrará em vigor em maio de 2021, para isto, aborda-se a Autoridade Nacional de Proteção de Dados, agentes de tratamento e o encarregado de dados, as responsabilidades inerentes à função, o consentimento pelo titular dos dados e as penalidades aplicadas pela Autoridade Nacional, bem como ponderar a respeito de como as empresas poderão estar em conformidade com a Lei Geral de Proteção de Dados.

A motivação do pesquisador está em trabalhar numa empresa de e-commerce, compreender os meios legais que possa regularizar as atividades, obrigações e limites das empresas, ao armazenarem, agregarem, utilizarem e modificarem dados dos usuários sem seu consentimento, além de verificar quais as possíveis sanções e penalidades que podem ser atribuídas, como também aprender sobre o direito digital, comércio eletrônico e a LGPD.

O método de abordagem utilizado é o de pensamento dedutivo, em virtude do tratamento das situações gerais relacionadas a regulação da LGPD. O método de abordagem quanto à sua natureza é qualitativo, utilizando-se das informações e dos dados recolhidos. O método de procedimento utilizado é o monográfico com técnica de pesquisa bibliográfica, uma vez que efetua coleta de informações em doutrinas, leis, artigos científicos, dissertações e conteúdo de notícias dispostos em mídias virtuais.

A presente pesquisa tem como propósito colaborar com a exposição e familiarização do tema, demonstrando o cuidado que as empresas devem ter em preservar os dados, mantendo-os em segurança, seja no meio digital ou físico e também o alerta sobre a importância dos dados pessoais e a privacidade tem na contemporaneidade. No trabalho desenvolvido apresenta-se a regulação da LGPD no meio digital pelas empresas de comércio eletrônico, e diante da

magnitude e do debate existente, se faz relevante o conhecimento desse direito essencial para reivindicá-lo da maneira correta, como também para a construção digna que a privacidade tem para o ser humano.

2 COMÉRCIO ELETRÔNICO

Quem imaginou há poucos anos que o comércio fosse sofrer uma tamanha revolução e que hoje tantas empresas investissem tanto tempo e dinheiro neste novo meio de comunicação? O chamado e-commerce como também é conhecido, consiste em “toda atividade que tenha por objeto a troca de bens físicos e/ou digitais por meios eletrônicos”, conforme afirma Lorenzetti (2004, p. 219). Cumpre esclarecer que o termo “Internet” será utilizado no decorrer do trabalho com a letra “i” em maiúsculo, visto que se refere à rede global de computadores conectados entre si, enquanto que internet com “i” minúsculo é a contração de interconnected network (rede interconectada) conforme entendimento de Marcel Leonardi (2011, p. 23).

O comércio eletrônico é a venda de produtos ou prestações de serviços realizadas por meio de transmissão eletrônica de informações, conforme Coelho (2012, p. 54, apud GLANZ, 1998).

No comércio eletrônico podemos ter contratos oriundos de relações de direito público, quando celebrados entre empresas ou cidadãos e o Estado; ou de direito privado, por meio de relações civis, empresariais e de consumo (LORENZETTI, 2004). Sendo assim, faz-se necessário a compreensão dessa expressão “comércio eletrônico”. Conforme Rocco (2003, p. 4), “comércio é aquele ramo da produção econômica que faz aumentar o valor dos produtos pela interposição entre produtores e consumidores, a fim de facilitar a troca das mercadorias”. Desse modo, o comércio pode ser visto como o conjunto de trocas e compras e vendas tendo como objetivo ganhos e/ou satisfações.

Quanto à palavra “eletrônico”, afirma Barbagalo (2001), essa terminologia é derivada de “eletrônica”, que é a parte da física que trata de circuitos elétricos, em que a comunicação de dados via computador se faz por meio de impulsos elétricos, o que a marca como comunicação eletrônica, portanto, justifica-se o adjetivo eletrônico para o comércio firmado por comunicação gerada por impulsos elétricos.

Fábio Ulhoa Coelho salienta que o comércio eletrônico significa a circulação de bens, seja a prestação ou intermediação de serviço, em que as tratativas pré-contratuais e o contrato firmado se fazem por transmissão e recebimento de dados via eletrônica, usualmente em ambiente digital (2011).

Finkelstein acentua que o comércio eletrônico parece se dividir em duas vertentes principais, quais sejam, o B2B e o B2C. O B2B (business-to-business) significa as contratações eletrônicas efetuadas entre empresas nas transações envolvendo insumos. Já o B2C (business-to-consumer) são as transações efetuadas com consumidores ou utilitários finais de produtos e/ou serviços adquiridos pela Rede (2011, p. 39).

Na visão de Coelho, são três os tipos de estabelecimentos virtuais:

B2B (que deriva da expressão business to business), em que os internautas compradores são também empresários, e se destinam a negociar insumos; B2C (denominação derivada de business to consumer), em que os internautas são consumidores, na acepção legal do termo (CDC, art. 2º); e C2C (consumer to consumer), em que os negócios são feitos entre internautas consumidores, cumprindo o empresário titular do site apenas funções de intermediação (é o caso dos leilões virtuais). Os contratos celebrados via página B2B regem-se pelas normas do direito comercial. Os celebrados via página B2C, pelo direito do consumidor. No caso da página C2C, as relações entre o empresário titular do estabelecimento virtual e os internautas regem-se também pelo direito do consumidor, mas o contrato celebrado entre esses últimos está sujeito ao regime contratual de direito civil (2011, p. 117).

Assim, o referido autor entende que existe ainda o panorama do consumidor para consumidor, de usuários da Internet consumidores cumprindo o requisito de empresário titular do site apenas fazendo a intermediação.

Ademais, Tarcisio Teixeira (2015) exemplifica que o comércio eletrônico possibilita a diminuição da cadeia de distribuição dos bens, visto que os fabricantes e prestadores de serviços podem vender diretamente aos consumidores os seus produtos ou serviços, não precisando obrigatoriamente de intermediários, por exemplo, hotéis e companhias aéreas que vendem hospedagens e passagens sem a intermediação de agentes de viagens.

Acrescenta ainda o aludido autor (2015, p. 37) que a conhecida criatividade dos empresários tem se manifestado cada vez mais rápida a partir do e-commerce, que se transformou em um campo fértil para o exercício da arte de criar e inovar, de modo mais intenso, consequência da dinamicidade com que a Internet se apresenta.

A fim de assimilar esse ritmo acelerado da mudança tecnológica do comércio no meio eletrônico e que influência diretamente em nosso cotidiano, este capítulo tratará de seus primeiros passos como comércio eletrônico, seu conceito e os contratos eletrônicos tão usados neste ambiente digital para depois adentrar na era das lojas virtuais e a legislação aplicada a elas.

2.1 EVOLUÇÃO DO COMÉRCIO COM A INTERNET

A globalização e a criação da Internet, a partir do desenvolvimento do computador, originário de uma preocupação militar em obter um mecanismo capaz de codificar e decodificar as mensagens durante a Segunda Guerra Mundial, na primeira metade do século XX, foi um episódio extremamente importante para o surgimento da Internet e conseqüentemente o comércio eletrônico como conhecemos (TEIXEIRA, 2015).

Conforme o mencionado autor, (2015, p. 27) “mais tarde percebeu-se a necessidade de uma comunicação mais eficiente entre as bases militares em território norte americano, desenvolvendo-se assim, a partir de 1969, a interligação entre computadores, então denominada Arpanet, embrião da Internet”.

Assim, as primeiras comunicações ocorreram quando a Arpanet conectou em quatro centros de pesquisa dos Estados Unidos (Universidade de Utah, Universidade da Califórnia em Los Angeles - UCLA, Universidade da Califórnia em Santa Barbara e Instituto de Pesquisa de Stanford) com uma mensagem simples, formando assim uma rede de informações em comum (RIBEIRO, 2019).

A Arpanet foi financiada pelo Governo Federal dos Estados Unidos, com o intuito de construir uma comunicação resistente a falhas ou ataques locais, por meio da criação de uma rede de computadores interconectados utilizando o protocolo TCP/IP para se comunicarem entre si (MAGRANI, 2018). No dizer de Manuel Castells, “a Arpanet, como projeto bélico, serviu no início para a interconexão de redes militares regionais” (2005, p. 82).

De acordo com Teixeira (2015), em 1972 foi criado um software permitindo o envio de e-mails (mensagens eletrônicas); no ano seguinte foi feita a primeira comunicação internacional, entre Inglaterra e Noruega. Não obstante, somente em 1987 é que a rede mundial dos computadores foi liberada pelo governo norte-americano para uso comercial.

No começo da década de 1980, com a consolidação do protocolo TCP/IP como meio de comunicação entres as redes de computadores e com o início da comercialização dos primeiros computadores pessoais, acelerou o crescimento de utilização da internet como ambiente digital, permitindo a difusão de LANs, PCs e workstations nos anos que seguiram (RIBEIRO, 2019).

Por volta de 1985, a Internet já estava estabilizada como uma comunidade de pesquisadores e desenvolvedores ao redor do mundo. O próximo avanço significativo veio

através de Tim Berners-Lee, Robert Cailliau e demais pesquisadores. Em 1989, criou-se a World Wide Web, que ficou conhecida pela sigla WWW ou mais facilmente por web. Nascida no Laboratório Europeu de Física, em Genebra, instrumento de grande valia para o tráfego de documentos, imagens e sons pela rede, sendo um protocolo eficiente para distribuir a informação e transformando a Internet num fenômeno de comunicação de massa e componente de globalização que predomina em todo o mundo de acordo com Barreto de Araújo (2017).

Nesse âmbito precisa-se observar o crescimento nos Estados Unidos com a Internet, realizando as primeiras ofertas de venda de produtos e serviços no ambiente eletrônico, conforme destaca Luiz Claudio Pinho Almeida (1999 apud ARAÚJO, 2017, p. 8):

Nessa fase, as empresas apresentavam sites onde predominava a divulgação institucional e, no máximo, a promoção comercial. Mas, logo após, já em fins de 1994, surgiam as primeiras ofertas de vendas de produtos e serviços através da Internet que, a partir de então, vêm crescendo de forma surpreendente, especialmente nos Estados Unidos. Isto ocorreu e continua ocorrendo, principalmente, face à tradição norte-americana de comercialização por catálogo que remonta à época da colonização e ao costume de usar cartão de crédito de forma intensiva, além de todas as outras facilidades que o meio oferece a uma sociedade.

Os autores corroboram que o comércio eletrônico só passou na realidade a existir a partir de 1993, principalmente com a exploração comercial da Internet, possuindo forte influência norte-americana, pois foi nos Estados Unidos que primeiro se desenvolveu e é onde ainda conta com o maior número de usuários, assim como empresas dedicadas à criação de aplicativos (FINKELSTEIN, 2004).

Nesse contexto, Coelho afirma:

A expansão da internet deve muito ao extraordinário potencial para o incremento de negócios e atendimento aos consumidores revelado pelo comércio eletrônico (comércio-e). Na segunda metade dos anos 1990, a rede popularizou-se e ultrapassou os circuitos universitários (onde já gozava de inegável prestígio), em razão das comodidades oferecidas ao ato de consumo. A evolução tem sido vertiginosa: ilustrativa, a propósito, é a trajetória do leilão eletrônico Ebay (www.ebay.com), que intermediava, em 1999, a venda de mais de dois milhões de objetos e antiguidades por dia. Quando surgiu, 4 anos antes, era apenas uma página de encontro de colecionadores, criada por Pierre Omidyar para impressionar a namorada, ao custo de 30 dólares (2012, p. 54).

Em 1998, o Google foi criado e como bem analisa Eduardo Magrini (2018, p. 64) “Essa popularização e profusão de produtores de conteúdo e consumidores de informações deu início à revolução digital, modificando profundamente a sociedade”.

Getting (2007) relata que, os primeiros sites de e-commerce encaixam-se na definição de web 1.0, pois apenas disponibilizavam os catálogos em formato virtual, para que mais pessoas pudessem saber sobre seus produtos e serviços, de modo mais cômodo para o consumidor.

Já na web 2.0, os sites de e-commerce passaram a criar ferramentas de classificação dos produtos e abriram espaço para comentários dos usuários, fazendo com que a experiência da compra pudesse ser compartilhada com futuros consumidores conforme afirma Magrini (2018).

Marcelo Barreto de Araújo interpreta o grande desenvolvimento da Internet como funcionamento de uma rede global de comunicação que passou a afetar o cotidiano das pessoas de tal maneira, que a forma de relacionamento social, os modos de produção e até a forma de pensar mudaram (2017).

A seguir contextualiza-se a respeito do conceito de comércio eletrônico.

2.2 CONCEITO

Comércio eletrônico seria o comércio “clássico”, hoje realizado por meio de contratação à distância. Alcança os contratos celebrados pela Internet, por telefones fixos e celulares, pela televisão a cabo, etc. De forma estrita, e-commerce é uma forma de contratação não presencial para a aquisição de produtos e serviços por meio eletrônico. Já de forma ampla, este envolveria qualquer tratativa ou troca de informação objetivando negócios, aí incluídos os dados transmitidos prévia e posteriormente à venda ou à contratação, bem como o envio de bens materiais e imateriais, os serviços de busca e link’s, a publicidade, os meios de pagamento (MARQUES, 2004. p. 35-39).

Newton De Lucca, argumenta que o comércio eletrônico contempla as trocas de produtos e serviços pela rede mundial de computadores, bem como aquelas cuja utilização de uma ferramenta eletrônica é empregada para a concretização do negócio, não abrangendo somente aos computadores, mas também de outros equipamentos que permitem comunicação recíproca, como, por exemplo, o telefone fixo e celular, o rádio, telegrama e outros (2009).

Já Carlos Vattier Fuenzalida alerta que comércio eletrônico pode ser classificado em: *stricto sensu*, quando o contrato é realizado mediante um diálogo instrumentalizado pelos computadores do emissor e receptor, ou seja, estar em rede; e *lato sensu*, que se dá quando realizado por qualquer meio eletrônico (2001, p. 51-52).

Nos ensinamentos de Zuliani, comércio eletrônico não se refere tão somente à venda e compra de produtos e prestação de serviços com fins lucrativos em ambiente digital, mas envolve também as relações entre órgãos do Poder Público, negócios entre particulares e entre empresas e consumidores (2012, p. 370).

Na procura de um conceito para o e-commerce, Patricia Peck Pinheiro chama atenção pelo fato de que o comércio eletrônico não é algo tão recente, isso porque o comércio eletrônico não se restringe às operações realizadas pela Internet, mas contempla as transmissões de fax, transferências bancárias, a compensação de cheques, o uso do cartão de crédito. Atualmente o comércio eletrônico permite que não apenas a concretização do negócio seja eletrônica, mas a apresentação dos contratantes aconteça eletronicamente, bem como a formação da documentação comprobatória (2016, p. 66-72).

No dizer de Castro, “comércio eletrônico” consiste no conjunto de operações de compra e venda de mercadorias ou prestações de serviços por meio eletrônico; ou as operações com conteúdo econômico, realizadas por intermédio de meios digitais. Assim, como os autores citados anteriormente, ele expõe que o comércio eletrônico pode ser classificado em duas espécies: próprio/direto e impróprio/indireto. A primeira espécie trata da comercialização de bens intangíveis, como o software; a segunda, de bens tangíveis, como equipamentos eletrônicos. No primeiro caso a operação começa, desenvolve-se e termina nos meios eletrônicos. Na segunda espécie, tem-se um desdobramento físico da operação, um bem corpóreo sairá do estabelecimento do vendedor e será entregue no domicílio do comprador (2002, p. 254).

Nesse sentido, Fábio Ulhoa Coelho, pondera que a venda de produtos, virtuais ou físicos, ou a prestação de serviços realizada em ambiente virtual é o comércio eletrônico em si. Dessa maneira, externa-se que tanto a oferta quanto a celebração do contrato é realizada por transmissão e recepção eletrônica de dados, podendo ocorrer por meio da internet ou fora dela (2012, p. 47).

Gilberto Marques Bruno ressalta que o comércio eletrônico se constitui em uma modalidade de compra a distância, cuja aquisição de bens e/ou serviços ocorre por meio de equipamentos eletrônicos de tratamento e armazenamento de dados, nos quais são transmitidas e recebidas informações. Trata-se de umas das possíveis formas de comércio não presencial, como por exemplo, os casos de vendas por catálogo, por telefone, pela televisão e tantas outras (2001). Maria Eugênia Reis Finkelstein também adota este conceito (2004, p. 53).

Em vista disso, entende-se o comércio eletrônico como uma expansão e sofisticação na forma de se divulgar e comercializar produtos e serviços, sendo assim, é o comércio convencional realizado por meio de contratação à distância utilizando-se da informática.

Feito essas reflexões, o próximo tópico aborda-se os contratos eletrônicos.

2.3 CONTRATOS ELETRÔNICOS

O que seriam os contratos eletrônicos? Na opinião de Orlando Gomes (1998, p. 10), contrato é concebido como “o negócio jurídico bilateral, ou plurilateral, que sujeita as partes à observância de conduta idônea à satisfação dos interesses que regularam”. Primeiramente podemos dizer que o nascedouro da aceitação jurídica dos contratos celebrados por via eletrônica ocorreu com a Lei Modelo da Uncitral (Comissão das Nações Unidas para o Direito Comercial Internacional) de 1996, que no seu art. 5º disse o seguinte: “não se negarão efeitos jurídicos, validade ou eficácia à informação apenas porque esteja na forma de mensagem eletrônica” (PINHEIRO, 2016).

A mesma lei tratou ainda em seu art. 11 sobre a formação e validade dos contratos, onde diz “salvo disposição em contrário das partes, na formação de um contrato, a oferta e sua aceitação podem ser expressas por mensagens eletrônicas. Não se negará validade ou eficácia a um contrato pela simples razão de que se utilizaram mensagens eletrônicas para sua formação” (UNCITRAL, 1996).

O crescimento do e-commerce está intimamente ligado ao contrato eletrônico, que se integra ao rol dos documentos eletrônicos. Exemplifica, Marcelo Barreto de Araújo, ao dizer que “ontologicamente, ele possui todas as características de um contrato físico, que se constitui num pacto, um acordo de vontade celebrado por duas ou mais pessoas voltadas para criar, preservar, alterar e extinguir direitos (2017).

Na visão de Santos e Rossi, os contratos eletrônicos são “os negócios jurídicos bilaterais que utilizam o computador como mecanismo responsável pela formação e instrumentalização do vínculo contratual” (2000, p. 108).

No mercado de capitais, as operações de subscrição ou alienação de valores mobiliários, já há algum tempo, realizam-se eletronicamente, na sua quase totalidade (COELHO, 2012).

Outro ensinamento de Lorenzetti (1998), o contrato eletrônico traduz uma transação eletrônica em que as declarações de vontade se manifestam por meios eletrônicos, ou mediante a oferta pública em um site e a aceitação pelo consumidor através de um click.

No dizer de Tarcisio Teixeira (2015, p. 43), o campo do comércio eletrônico é possível ocorrer vários tipos de contratos. Existem aqueles negócios cujas fases contratuais ocorrem totalmente na Internet, ou seja, as tratativas preliminares, a conclusão e a execução do contrato se dão eletronicamente. Por exemplo, a compra de software pela Internet, dado que o pagamento seja realizado por débito em conta bancária e a entrega do bem por meio de download.

As assinaturas digitais já são meio seguros de celebrar contratos eletrônicos, como afirma Fábio Ulhoa Coelho:

Atualmente, as assinaturas digitais, autenticadas por certificado digital concedido no âmbito da Infraestrutura de Chaves Públicas Brasileira (ICP Brasil) é um meio seguro de identificar os sujeitos de direito no contrato eletrônico. Em termos sucintos, cada pessoa recebe um par de chaves, sendo uma de “conhecimento público”, isto é, processável por qualquer máquina ligada à rede mundial de computadores; e outra de “conhecimento privado”, quer dizer, processável apenas pela máquina do titular, mediante a sua leitura num token, cartão com chip ou outra mídia. As chaves públicas e a privada estão relacionadas por um algoritmo que apenas os computadores podem processar. Uma mensagem criptografada pela chave pública de um certo sujeito somente pode ser descryptografada pela chave privada dele e vice-versa. As tecnologias de informação associadas à criptografia assimétrica permitem que o suporte eletrônico cumpra rigorosamente as mesmas funções do suporte papel (2012, p. 64).

O contrato eletrônico, como afirma Finkelstein (2004), é caracterizado por empregar meio eletrônico para sua celebração, ou ainda, “o negócio jurídico bilateral que resulta do encontro de duas declarações de vontade e é celebrado por meio da transmissão de dados”.

A evolução tecnológica dos contratos é nítida, com o advento da Internet passou-se a ter uma dimensão maior, alçando novas características e alterando definitivamente os padrões culturais e econômicos da sociedade contemporânea. Nos dias de hoje, vivemos a era digital, ou também entendida como Sociedade da Informação, fortemente marcada pelas tecnologias

digitais, naturalmente a contratação por meio digital se tornará a forma mais comum de se transacionar (OPICE BLUM, 2017, p. 25).

Sabe-se que o princípio da liberdade de forma de contratação para validade jurídica da declaração de vontade encontra seu respaldo no art. 107 do Código Civil, in verbis:

Art. 107. A validade da declaração de vontade não dependerá de forma especial, senão quando a lei expressamente a exigir.

Já a validade do negócio jurídico, são necessários agentes capazes, objeto lícito, possível, determinado ou determinável e forma prescrita ou não defesa em lei, nos termos do art. 104 do mesmo diploma legal:

Art. 104. A validade do negócio jurídico requer:

- I - agente capaz;
- II - objeto lícito, possível, determinado ou determinável;
- III - forma prescrita ou não defesa em lei.

Maria Helena Diniz ensina sobre a forma livre:

Nosso Código Civil inspira-se no princípio da forma livre, o que quer dizer que a validade da declaração da vontade só dependerá de forma determinada quando a norma jurídica explicitamente o exigir. A forma livre é qualquer meio de exteriorização da vontade nos negócios jurídicos, desde que não previsto em norma jurídica como obrigatório: palavra escrita ou falada, mímica, gestos e até mesmo o silêncio (2017, p. 132).

Ronaldo Alves de Andrade afirma que:

O contrato eletrônico não tem um perfil ou natureza jurídica distinta da dos contratos em geral. Não se trata de nova espécie não tipificada de contrato, como são os contratos de leasing, de franquia, de cartão de crédito, etc. Em verdade, é tão somente um novo e atual meio de se efetivar um contrato, cuja instrumentação pode ser aportada em mídia eletrônica (2004, p. 31).

O princípio da equivalência funcional consiste na garantia de que os contratos celebrados por meio digital tenham reconhecido os mesmos efeitos aos contratos em papel. Nesse sentido Fábio Ulhôa Coelho (2008, p. 56), “pelo princípio da equivalência funcional, afirma-se que o suporte eletrônico cumpre as mesmas funções que o cartáceo”. Aceita essa

premissa, não há razões para se considerar inválido ou ineficaz o contrato tão só pela circunstância de ter sido registrado em meio magnético.

Esses conceitos foram formulados e amadurecidos pela Comissão de Direito Comercial Internacional da ONU, na elaboração da Lei Modelo sobre Comércio Eletrônico, aprovada em 1996 pela Assembleia Geral daquele organismo e cuja adoção é recomendada a todos os países-membros (UNCITRAL, 1996, p. 38-45).

Para Coelho (2012), o princípio da equivalência funcional é o argumento mais genérico e básico da tecnologia jurídica dos contratos virtuais. Afirma que o registro em meio magnético cumpre as mesmas funções do papel. Assim, as desconfianças que podem exsurgir do contrato eletrônico não são diferentes das do contrato em papel.

Nesse sentido Jorge José Lawand leciona sobre o direito fundamental dos contratos eletrônicos:

[...] princípio fundamental que rege a disciplina dos contratos eletrônicos é o que veda qualquer espécie de diferenciação entre os contratos clássicos, produzidos em papel e reconhecida a sua legitimidade através de um tabelionato de notas, e os contratos efetivados através dos meios eletrônicos, em especial pela Internet. Visa-se impedir qualquer espécie de preconceito com relação ao que consta da rede mundial de computadores (2003, p. 44).

Consequentemente, não pode ser negada a existência, validade e eficácia jurídica dos contratos pactuados por meios eletrônicos e a sua tendência nos próximos anos. Em outras palavras “o contrato forma-se precisamente quando essa proposta e essa aceitação se encontram, dando lugar aquilo que se chama o consenso contratual” (ROPPO, 2009, p. 73).

Na definição de Santos e Rossi (2000, p. 109) a diferença do contrato eletrônico dos demais documentos eletrônicos, é que na medida em que o contrato eletrônico pode ser também um documento eletrônico, a recíproca não é necessariamente verdadeira. “No conceito amplo de documento eletrônico se incluem todos os documentos gerados, transmitidos ou armazenados no ambiente digital”.

E documento, por sua vez, é “toda representação material destinada a reproduzir determinada manifestação do pensamento” (CHIOVENDA, 2009, p. 1091).

Conceitua Finkelstein (2004) que o contrato eletrônico, seria uma nova tecnologia de formação contratual, podendo ter como objeto, o contrato tradicional, uma locação, um

comodato, uma doação, uma compra e venda, uma prestação de serviços e tantas outras matérias.

Exemplifica Newton de Lucca que o contrato telemático, é o negócio jurídico bilateral que tem, o computador e uma rede de comunicação como suportes essencial para sua celebração (2009).

Desta maneira, todos os tipos contratuais podem se formar em meio telemático, não se admitindo apenas os contratos que a lei prescreve forma especial (contratos solenes), como salienta Maria Eugênia Finkelstein (2004).

Para Pinheiro (2016), há nos contratos eletrônicos um consenso em torno dos princípios que norteiam a sua tutela, quais sejam: a boa-fé, a vedação ao enriquecimento sem causa, o da proteção pela aparência, e alguns mais que possamos identificar como essenciais à tutela de relações éticas e sustentáveis.

Em síntese a evolução tecnológica está trazendo mais força jurídica para os contratos, por exemplo a geração de provas que incluem até a geolocalização das partes (local da celebração), autoria e integridade e que o acontecido foi devidamente testemunhado, faz com que aumente sua executividade e não o contrário, conforme supradito autor (2016).

Em seguida serão efetuadas observações a respeito das lojas virtuais.

2.4 LOJAS VIRTUAIS

Na atualidade, o Brasil conta com diversas opções de lojas virtuais. Uma das mais famosas atualmente é a Submarino, que vem crescendo substancialmente. A “Americanas.com e a Submarino fundiram-se em 2006, criando, de forma inquestionável a maior loja virtual do país. Outras empresas da economia tradicional vêm sendo atraídas pelo mercado eletrônico”, conforme destaca Finkelstein (2016, p. 60). Outra das grandes é a Peixe Urbano, que no início, fazia o modelo de negócio de compras coletivas, após, se tornou um shopping de ofertas, para hoje em dia ser uma plataforma de ofertas. Já no final de 2017 se fundiu com a maior plataforma de ofertas dos Estados Unidos, a Groupon Latam, que já existia também no Brasil, sendo inclusive concorrente da Peixe Urbano antes da fusão.

Verçosa (2000, p. 90), descreve que o modo extremamente dinâmico como as atividades negociais têm se desenvolvido nos últimos anos, especificamente na área do comércio

eletrônico, produz a criação de novas operações e a conseqüente necessidade de estabelecimento de novos mecanismos técnico-jurídicos para regê-las.

Coelho (2012), entende que com o aparecimento do comércio eletrônico, a loja virtual também denominadas como estabelecimento virtual eram sempre estabelecimentos empresariais físicos, ou seja, a empresa encontrava-se instalada em um imóvel fisicamente acessível ao consumidor/adquirente.

Em vista da criação desse novo canal de vendas, que metaforicamente, é equiparado a um ambiente para o consumidor fisicamente inacessível, o adquirente do produto ou serviço deve manifestar a sua aceitação por meio da transmissão eletrônica de dados. São as chamadas lojas virtuais. Ao ver de Barreto de Araújo (2017, p. 118), o símbolo do comércio eletrônico é a loja virtual, que se origina da democratização do acesso à Internet e da construção paulatina de uma série de vantagens atrativas, típicas do universo virtual.

O autor mencionado argumenta ainda que importante é a atratividade e a informação adequada do site, com bons textos, imagens, vídeos, apresentações interessantes, atualização com frequência, isso sim se tornam bons instrumentos de vendas.

Alerta Finkelstein que a prioridade para os clientes é que a encomenda chegue no prazo, sendo assim, analisa que:

As lojas virtuais devem estar preparadas para o volume de devoluções feitas pelos consumidores, sendo este um real desafio para a área de logística do comércio eletrônico. Por esse motivo, as empresas devem maximizar o valor dos produtos devolvidos, aprimorando todos os seus sistemas de logística reversa, inclusive coleta e análise de dados de consumo (2016, p. 61).

Marcelo Araújo (2017, p. 118) observa que em grande parte, os conceitos mercantis do comerciante tradicional e do comerciante virtual são os mesmos, a começar pelo perfil empreendedor, capacidade de planejamento e enfrentamento de riscos. O símbolo do comércio eletrônico é a loja virtual, que se origina da democratização do acesso à Internet e da construção paulatina de uma série de vantagens atrativas, típicas do universo virtual.

A questão de grande praticidade para o supradito autor (2017) é o estilo “self-service”, onde o comprador não se sente constrangido por um eventual assédio indevido do vendedor, permitindo-se a tranquilidade na pesquisa do produto desejado e redução de tempo gasto. Outra facilidade é que a loja não tem filas, não tem melhor ou pior horário para comprar e existe

enorme comodidade na escolha do produto desejado, na efetivação do pagamento e na entrega da mercadoria.

Ele ainda afirma que, em regra geral, a loja virtual representa para o empresário eletrônico o barateamento dos gastos com investimento comercial (2017, p. 119).

Na concepção de Teixeira (2015, p. 32) a loja virtual é uma extensão do comércio convencional, o comércio eletrônico vem apresentando um crescimento vertiginoso em razão de suas características que são bem interessantes: rapidez na negociação, eliminação das distâncias geográficas, o barateamento do acesso para a venda e a compra por meio eletrônico, preços mais atraentes ao consumidor, entre outros.

O mencionado autor argumenta sobre o auxílio do Direito nesse sentido:

O Direito pode auxiliar a estabelecer este novo paradigma se conseguir firmar a devida proteção ao usuário leigo, por meio: da exigência de transparência; da redução da assimetria informacional; do respeito ao direito de o comprador se arrepender da compra; de mais segurança com os meios de pagamento no ambiente virtual; e de mais diligência com os dados coletados (2015, p. 34).

Para Marques (2004, p. 32), “a confiança seria o paradigma necessário para adaptar o direito do consumidor ao comércio eletrônico”.

Seguidamente verifica-se a legislação aplicável as empresas de comércio eletrônico na contemporaneidade.

2.5 LEGISLAÇÃO APLICÁVEL AS EMPRESAS DE COMÉRCIO ELETRÔNICO

Nas palavras de Teixeira (2015, p. 59), o comércio eletrônico sendo como base o conjunto de operações contratuais de trocas, vendas e compras e prestações de serviços não encontra limites geográficos, uma vez que a rede mundial de computadores pode ser acessada de qualquer lugar do globo terrestre onde haja sinal e inexistam controles governamentais restritivos.

Carlos Roberto Gonçalves (2018, p. 103), cita que em âmbito nacional (quando as pastes estão sediadas no Brasil), os contratos celebrados pela Internet estão sujeitos as mesmas regras e princípios aplicáveis aos demais contratos firmados fisicamente no território brasileiro.

Destaca-se que, sem prejuízo da aplicação de outras normas especiais, aplicam-se as regras do Código Civil e do Código de Defesa do Consumidor (neste caso, quando configurada uma relação de consumo) aos negócios concretizados eletronicamente (CARVALHO, 2001, p. 60).

Destarte, são aplicáveis as regras locais sobre contrato de adesão, publicidade enganosa e abusiva, cláusulas leoninas, responsabilidade por não cumprimento contratual e por ato ilícito (TEIXEIRA, 2014, p. 131).

Patricia Peck Pinheiro (2016) analisa que não há necessidade de uma norma específica para o comércio eletrônico, na medida em que se tornaria obsoleta rapidamente diante da dinâmica da tecnologia da informação.

Por outro lado, o professor Ênio Santarelli Zuliani (2012, p. 403), entende ser necessária uma regulamentação específica tendo em vista o grande crescimento do setor e a vulnerabilidade dos usuários.

Haroldo Malheiros Duclerc Verçosa em passagem sobre os contratos celebrados via Internet, questiona se do ponto de vista jurídico houve mudança abrupta em razão da rede mundial de computadores:

O que teria acontecido corresponderia a uma sofisticação técnica quanto aos mecanismos utilizados para a contratação em razão do advento da Internet. É claro que há problemas sobre a formação e a caracterização do acordo, o momento da conclusão, do conteúdo e da prova das obrigações contratadas, sendo preciso verificar se as categorias jurídicas clássicas podem albergar esses negócios ou se será preciso construir novos institutos jurídicos para reger a matéria (2010, p. 292-293).

Tendo como preceito que o e-commerce é o conjunto de operações contratuais de trocas, vendas, compras e prestações de serviços não encontra limites geográficos, haja vista que a Internet pode ser acessada de qualquer lugar do mundo onde tenha sinal e inexista controle governamental restritivo, como caracteriza Teixeira (2015).

Sendo assim, caso seja celebrado um contrato eletronicamente entre partes sediadas em países distintos faz-se necessário entender que envolve o direito internacional privado. Deste modo, indispensável observar o que dispõe o Decreto-lei n. 4.657/1942, conhecido como LINDB – Lei de Introdução às Normas do Direito Brasileiro, cujo art. 9º, caput e § 2º, prevê que se aplica a lei do país onde se constituírem as obrigações. Nesse aspecto, é considerado o

local se constituiu as obrigações, o lugar onde residir o proponente, melhor dizendo, aquele que estiver ofertando o produto ou o serviço na Internet.

Também pode ser aplicável a Convenção de Viena, em vigor no Brasil por força do Decreto Legislativo n. 538/2012, que aprovou o texto do Tratado sobre Contratos de Compra e Venda Internacional de Mercadorias, no âmbito da Comissão das Nações Unidas para o Direito Mercantil Internacional (TEIXEIRA, 2014, p. 476).

No que tange a aplicação da legislação brasileira aos contratos eletrônicos, considera-se que a maior parte desses negócios é suscetível de aplicação do Código de Defesa do Consumidor, sendo que na maioria das vezes uma das partes seria o consumidor, ainda que nada impeça que empresas também os realizem, conforme explana Tarcisio Teixeira (2015).

Não se pode falar em comércio eletrônico sem citar o Decreto n. 7.962/2013, que trata da regulamentação do e-commerce, estando em vigor desde o dia 15 de março de 2013, disciplinando o Código de Defesa do Consumidor (CDC) para dispor sobre a contratação em ambiente digital.

Teixeira pontua que em seus 9º artigos o Decreto busca trazer mais segurança aos internautas que comprem pela Internet, bem como estabelecer um comportamento mais adequado de vendedores, prestadores de serviço e intermediários, facilitando assim as relações jurídicas mais seguras e transparentes como também ampliando o acesso às informações sobre fornecedores, produtos e serviços (2015, p. 83).

Sublinha-se que o decreto não cuida com precisão da extensão da responsabilidade civil nas compras pela Internet, cujo tema está pautado fundamentalmente pelo Código Civil, artigos 927 e 931, e pelo CDC, nos artigos 12 e 13. A doutrina é uniforme quanto à admissibilidade da aplicação do ordenamento jurídico brasileiro às relações estabelecidas no comércio eletrônico (DE LUCCA, 2003, p. 109).

Nesse contexto, Maciel (2019) entende que o Decreto do Comércio Eletrônico foi na realidade uma transposição de parte do texto do Projeto de Lei do Senado 281/2012, que visava atualizar o código consumerista, e, como não foi possível inovar, o decreto regulamentou alguns pontos da lei, dentre eles determinou ao fornecedor a utilização de mecanismos de segurança eficazes para o pagamento e para o tratamento de dados do consumidor. Com isto trouxe à tona a obrigatoriedade de implementação de medidas técnicas adequadas para a sua consecução.

De qualquer forma, o Marco Civil da Internet (MCI) mantém o sistema da responsabilidade subjetiva (em que é necessária a demonstração de culpa do causador do dano), permitindo a livre manifestação de pensamento e de conteúdo sem prévio controle de provedores e/ou intermediários (TEIXEIRA, 2015, p. 101).

Este capítulo apresentou conceitos sobre o comércio eletrônico, os principais elementos que estão associados a compra/venda eletronicamente, tratando a evolução da Internet como uma nova forma de fazer negócios em um ambiente virtual do ponto de vista jurídico, os contratos celebrados no meio digital, bem como a legislação aplicada a estas empresas de comércio eletrônico. Denota-se pelo exposto que existem formas para celebração dos contratos via eletrônica, as lojas virtuais são o caminho para se chegar ao consumidor, mesmo que distante.

O capítulo seguinte examina-se a Lei Geral de Proteção de Dados, desde o seu surgimento na União Europeia até a contemporaneidade, serão destacados os conceitos que envolvem esta temática, os termos e definições estabelecidos pela Lei, seu campo de aplicação, princípios que o regem, por conseguinte, são feitas considerações sobre o Marco Civil da Internet.

3 LEI GERAL DE PROTEÇÃO DE DADOS

Acompanhando a evolução sobre a privacidade dos dados, bem como o incentivo dado pelo Marco Civil da Internet, em conjunto com o Regulamento Geral de Proteção de Dados (GDPR), definida em inglês como *General Data Protection Regulation*, em vigor na União Europeia desde maio de 2018, vislumbrou-se a necessidade de uma regulamentação específica sobre a proteção de dados e a privacidade destes. Assim nasceu a LGPD (publicada em 14 de agosto de 2018), Lei n. 13.709.

Florenço destaca a evolução dos meios tecnológicos, gerando riscos a defesa do consumidor, diante da descontrolada propagação de seus dados, e como a LGPD será responsável por guarnecer proteção contra a utilização excessiva dessas informações por meio de instrumentos garantidores, limitadores e transparentes quantos à divulgação dos dados pessoais de consumidores (2016, p. 166).

Em sua especialização, Coêlho (2019, p. 36) aclara ser perceptível o enfoque da LGPD, tendo em vista que seu maior objetivo é tutelar os direitos de privacidade de informações pessoais que circulam por meios online e off-line, partindo da grande demanda tecnológica no mercado de consumo.

Em 2018, o Brasil passou a entrar no rol de países com uma legislação voltada à proteção de dados pessoais, nitidamente inspirada no regulamento europeu, o GDPR. Com vigência inicialmente prevista para o dia 16 de fevereiro de 2020, com a edição da Medida Provisória nº 869/18, tal prazo foi estendido por seis meses, passando para agosto do mesmo ano.

Nesse ínterim, diante do contexto pandêmico do Coronavírus que assolou todos os países, o Governo Brasileiro adotou a Medida Provisória 959, publicada em edição extra do Diário Oficial da União (DOU), prorrogando a entrada da LGPD, passando está a vigorar possivelmente em maio de 2021, assim como as sanções que passam a valer também possivelmente em agosto de 2021.

Valoriza-se a importância da entrada da LGPD que marcará o início de um processo de adaptação, tanto para as empresas, como para o poder público em relação as práticas de privacidade, afetando drasticamente a coleta de dados e o modelo de negócio das empresas, para os usuários é um grande ganho, posto que a privacidade é fundamental em um mundo onde tudo acontece de maneira tão rápida.

No tópico seguinte contextualiza-se acerca da origem e influência da GDPR na lei brasileira de proteção de dados pessoais.

3.1 ORIGEM DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

A privacidade sempre foi uma preocupação constante dos europeus, o que é visto pelas leis que antecederam o regulamento geral de proteção de dados, sendo que tem quase total influência na legislação brasileira, como demonstra Cinthya Ribeiro em sua dissertação (2019, p. 69).

Para compreendermos a LGPD, é prudente voltarmos no passado e visualizarmos como a privacidade tornou-se um direito fundamental, passível da proteção pelo estado jurisdicional e como tornou-se mais valioso com o avanço das tecnologias (MACIEL, 2019).

Rafael Fernandes Maciel, resgata o emblemático artigo “The Right to Privacy”, publicado na *Harvard Law Review*, por dois advogados americanos, Samuel Warren e Louis Brandeis, sendo considerado como um dos que mais influenciou o direito à privacidade:

[...] O interesse em divulgar fatos da vida privada de forma sensacionalista e fofocas cada vez mais sendo estampadas nos jornais (Yellow Journalism) - que ganhavam ainda mais circulação (1000% entre 1850 e 1890) –, somados ao avanço tecnológico com o uso de câmeras fotográficas portáteis, motivou os advogados a levantar a necessidade de se pensar em um direito à privacidade mais amplo e não apenas sobre meios físicos, como o sigilo da carta ou a violação de domicílio (2019, p. 7).

Na Declaração Universal dos Direitos Humanos (DUDH), o mundo teve garantido o direito de inviolabilidade à vida privada ser alçado a um direito fundamental do homem. O artigo 12 da Declaração dispõe que:

Ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques (Organização das Nações Unidas, 1948).

Em 1970, a Alemanha dispôs de uma das primeiras leis publicadas, a Lei de Proteção de Dados do Estado de Hesse, e, posteriormente, foi publicada a Lei de Dados da Suécia em 1973, o Estatuto de Proteção de Dados do Estado Alemão de *Rheinland-Pfalz* de 1974 e em 1981 o Conselho Europeu aprovou a *Data Protection Convention (Convention 108)*, que foi o primeiro marco europeu a proteger o usuário contra abuso na coleta e processamento de dados pessoais (MACIEL, 2019, p. 48).

Em sua parte inicial, a Convenção n. 108, também conhecida como Convenção de Strasbourg, deixa claro que a proteção de dados pessoais está diretamente ligada à proteção dos direitos humanos e liberdades fundamentais, tendo como pressuposto o estado democrático de direito, e evidenciando a sua preocupação com o artigo 8º da Convenção Europeia para os Direitos do Homem, em sintonia com o respeito pela vida privada e familiar:

1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência.

2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança

pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infracções penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros.

Gasiola (2019), afirma que em 1983 o Tribunal Constitucional da Alemanha deu início a discussão da Constitucionalidade da Lei do Censo, que permitia a coleta de dados e o seu tratamento para fins estatísticos, como a transmissão anônima desses dados para a execução de atividades públicas, sendo julgada parcialmente constitucional por ser possível a coleta de dados desde que houvesse a permissão do usuário, independentemente do seu consentimento, no entanto, no que toca aos dados públicos, foi considerada inconstitucional por violar o princípio da autodeterminação informativa, que é basicamente como uma extensão das liberdades presentes nas leis de segunda geração, e são várias as mudanças especificadas, nesse sentido, que podem ser identificadas na estrutura dessas novas leis.

A Alemanha passou a se preocupar com a transparência dos dados de seus cidadãos, acarretando a alteração da sua Constituição, bem como fomentando a discussão sobre o tema na comunidade europeia. Em 1995, entrou em vigor a Diretiva 95/46/CE tratando especificamente da proteção de dados (RIBEIRO, 2019).

Danilo Doneda (2006, p. 239), sobreleva a evolução que culminou, em 24 de outubro de 1995, sobre a Diretiva 95/46/CE do Parlamento Europeu, no que diz respeito à proteção e tratamento de dados pessoais e à livre circulação desses dados. O referenciado autor também avulta a importância da existência da Diretiva 2002/58/CE, promulgada em 12 de julho de 2002, que “procura regulamentar a proteção de dados pessoais especificamente nos serviços de comunicação eletrônica”, e fornecendo “instrumentos que permitem a adequação de suas finalidades à realidade tecnológica constituída pela comunicação em rede (2006).

O Regulamento 2016/679 do Parlamento e do Conselho Europeu, aprovado em 27 de abril de 2016, relativo à proteção das pessoas singulares no que concerne ao tratamento de dados pessoais e à livre circulação destes dados, revogando a Diretiva 95/46/CE, e por fim passando então a vigência da GDPR – *General Data Protection Regulation*, na União Europeia desde 25 de maio de 2018 (RIBEIRO, 2019).

Maciel (2019) destaca que com a entrada em vigor da GDPR, os legisladores brasileiros se viram pressionados a agilizar a votação de um projeto de lei de dados pessoais, caso contrário as empresas brasileiras teriam dificuldade em realizar negócios com europeus, em razão de o

país ser considerado não adequado para tratar dados de cidadãos que estiverem localizados na Europa.

O escândalo do caso Cambridge Analytica, foi um fator de suma importância para a apreciação do projeto de lei de Dados dos Pessoais, conforme descreve o Rafael Fernandes Maciel:

Pouco antes, estourou o caso Cambridge Analytica, em que foram escancaradas operações irregulares com dados coletados de usuários do Facebook, pela empresa, para utilização política, tendo inclusive sido ventilada a possibilidade de uso para influenciar o Brexit, as eleições presidenciais dos Estados Unidos e também seria utilizado nas eleições de 2018 no Brasil. Com o uso irregular de dados pessoais, o Facebook foi escrutinado por diversos órgãos na Europa, nos Estados Unidos e até mesmo no Brasil, sendo obrigado a arcar com pesadas multas e a rever sua prática comercial. Esse episódio, sem dúvida, acelerou a apreciação do projeto de lei de Dados Pessoais, levando à sua sanção e publicação no dia 14 de agosto de 2018, sob o número 13.709/18, bem como fez com que os Estados Unidos passasse a discutir seriamente uma legislação federal sobre o tema, algo até então pouco debatido, havendo uma clara preferência pelo modelo de proteção setorial lá existente (MACIEL, 2019, p. 17).

Há outras questões que influenciaram a produção da LGPD, ou o Brasil se tornava um país confiável, do ponto de vista da segurança jurídica, ou ficaria marginalizado por mais este motivo, além daqueles já conhecidos e contra os quais se combate há décadas, como a corrupção, burocracia, sistema tributário intragável, entre outras barreiras (COTS; OLIVEIRA, 2019).

Desse modo, é inevitável observar a forte influência que a GDPR tem na LGPD, Ribeiro (2019, p. 70), destaca inclusive a “utilização na legislação brasileira de termos europeus, de forma que ao entender aquela lei, é possível entender a nossa”. Se faz muito bem-vinda a LGPD na legislação brasileira, visto a necessidade de se regulamentar a proteção dos dados dos usuários em âmbito nacional.

No próximo tópico trata-se acerca dos termos e conceitos estabelecidos pela lei.

3.2 TERMOS E CONCEITOS ESTABELECIDOS PELA LEI

A Lei Geral de Proteção de Dados utiliza-se de diversas expressões não usuais, podendo levar à confusão, sendo pertinente uma breve explicação dos mais relevantes termos e conceitos definidos pela Lei. No entendimento de Maciel (2019), a LGPD adotou o modelo de

regulamento europeu, embora mais sintetizada, seus alicerces são praticamente os mesmos. Para isso, o legislador também adotou boa parte da PL 4060/12, que regulamenta o tratamento de dados pessoais no Brasil, tanto pelo poder público quanto pela iniciativa privada, aprovado pela Câmara dos Deputados em 29 de maio de 2018.

Ademais, o aludido autor explana que a lei busca um equilíbrio entre os novos modelos de negócio baseados no uso de dados pessoais e a proteção à privacidade, valor cada vez mais na pauta dos cidadãos a partir da divulgação cada vez maior de casos de uso indevido de tais informações.

O termo mais utilizado pela LGPD é dado, sendo este toda informação que se refere a um usuário e é dividido em pessoal, sensível e anonimizado (RIBEIRO, 2019, grifo do autor). O titular é a pessoa a quem se referem os dados pessoais que são objeto de algum tratamento. E tratamento dos dados seria toda operação realizada com algum tipo de manuseio de dados pessoais, quais seja, coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, edição, eliminação, avaliação ou controle da informação, modificação comunicação, transferência, difusão ou extração, assim clarifica Pinheiro (2020, p. 35).

O artigo 5º da Lei considera os seguintes dado:

Dado pessoal não é somente aquele que identifica uma pessoa física ou jurídica, com nome completo, Cadastro de Pessoa Física (CPF) ou número de registro de empresa (CNPJ), endereço de correio eletrônico, mas sim uma informação mais abrangente que se refere à forma como essa pessoa pode ser identificável de forma direta ou não imediata, exemplifica Cinthya Ribeiro (2019).

Na opinião de Patricia Peck Pinheiro (2020, p. 34-36), dado pessoal seria toda informação relacionada a uma pessoa identificada ou identificável, não se limitando, somente a nome, sobrenome, apelido, idade, endereço, podendo incluir dados de localização, placas de automóvel, perfis de compras, número do *Internet Protocol* (IP), dados acadêmicos, histórico de compras, entre outros. Sempre relacionados a pessoa natural viva.

Já os dados sensíveis são aqueles que remetem à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de cunho religioso, filosófico ou político, dado pertinente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural, nos termos do artigo 5º, inciso II.

Na visão de Pinheiro (2020), os dados sensíveis estão relacionados a características da personalidade do indivíduo e suas escolhas pessoais, tais como origem racial ou étnica, religião, opinião política, filiação a sindicatos, dado referente a saúde ou a vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Cumpra informar que a LGPD não fez menção aos dados bancários como sendo dado sensível, ainda assim, eles são de extrema relevância, já que em caso de vazamento, permitirá o uso indiscriminado por terceiros que estejam de má-fé, conforme resolve Ribeiro (2019).

Já o dado anonimizado relaciona-se com aquele dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento, ou seja que foi trabalhado para não ser identificado, assim sendo, perde-se a possibilidade de associação, direta ou indireta, a um indivíduo. Existem duas formas de anonimizar um dado: a primeira é a irreversível, de forma que o usuário não mais poderá ser identificado através dessa informação e a segunda, através da pseudoanonimização, em que o usuário também não será identificável, mas não pela exclusão do dado e sim pela possibilidade de criptografar os dados, método que pode ser utilizado com a tecnologia do *blockchain* (RIBEIRO, 2019, p. 80).

Na visão de Rafael Fernandes Maciel (2019, p. 83):

A tecnologia blockchain pode ser uma grande aliada no processo de pseudoanonimização. As características de descentralização, transparência, consenso e segurança, são muito pertinentes ao processo de pseudoanonimização, uma vez que insere uma camada de segurança adicional sem que tenham dados pessoais vinculados, já que as transações são identificadas por hashes. No entanto, é importante estar atento que blockchain pode não ser uma tecnologia apropriada para conformidade à LGPD, uma vez que impede a exclusão de dados, direito que deve ser assegurado pelo controlador ao titular.

O consentimento, seria a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada. É apenas uma das hipóteses que autoriza o tratamento de dados (PINHEIRO, 2020).

As figuras dos agentes de tratamento são o controlador que recebe os dados pessoais dos titulares de dados por meio do consentimento ou por hipóteses de exceção, e o operador que realiza algum tratamento de dados pessoais motivado por contrato ou obrigação legal. O termo encarregado é a pessoa natural, indicada pelo controlador, que atua como canal de comunicação entre o controlador e os titulares e a ANPD (PINHEIRO, 2020).

Continuamente trata-se sobre o seu campo de incidência.

3.3 ÂMBITO DE APLICAÇÃO

Em primeiro lugar, a lei se aplica a todos aqueles que realizam o tratamento de dados pessoais, sejam organizações públicas ou privadas, pessoas físicas ou jurídicas, que realizam qualquer operação de tratamento de dados pessoais, independentemente do meio, que possa envolver pelo menos um dos seguintes elementos: ocorrer em território nacional; que tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; e em que os dados tenham sido coletados no território nacional, como descrito por Pinheiro (2020, p. 39).

Verifica-se que a LGPD não está relacionada à cidadania ou à nacionalidade dos dados pessoais, tampouco à residência do indivíduo titular.

Nos termos do artigo 1º, é aplicável à pessoa natural ou pessoa jurídica de direito público ou privado, para proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural a todas as operações.

A LGPD aplica-se a todas as operações de tratamento realizadas no Brasil, com o objetivo de ofertar bens, serviços ou tratar dados de indivíduos localizados no país ou ainda, que tenham sido coletados no território nacional, como dispõe o artigo 3º.

Cintha Ribeiro desenvolve que o objetivo desta lei é combater o tratamento ilegal de dados pessoais realizado por qualquer pessoa, independentemente de ser pessoa física ou jurídica e que estejam em solo nacional. Por isso, a lei não faz distinção se a pessoa jurídica é, na verdade, estrangeira, pois estando em solo nacional, colhendo dados de brasileiros e ofertando a estes os serviços, estará sujeita a LGPD (2019, p. 77).

Consoante entendimento (VAINZOF; MALDONADO; BLUM, 2019, p. 19):

A Lei Geral de Proteção de Dados (LGPD) se preocupa e versa apenas e tão somente sobre o tratamento de dados pessoais. Ou seja, não atinge diretamente dados de pessoa jurídica, documentos sigilosos ou confidenciais, segredos de negócios, planos estratégicos, algoritmos, fórmulas, softwares, patentes, entre outros documentos ou informações que não sejam relacionadas a pessoa natural identificada ou identificável. Toda essa miríade de outros tipos de informações ou documentos encontram tutela em distintos diplomas legais, como a Lei de Propriedade Industrial (Lei 9.279/1996), a Lei de Direitos Autorais (Lei 9.610/1998) e a Lei de Software (Lei 9.609/1998), apenas para citar alguns exemplos. Não obstante, sempre quando tais documentos e

informações não tocados diretamente pela lei em estudo contiverem dados pessoais, estes, e tão somente estes, estarão protegidos por ela, motivo pela qual a análise da aplicabilidade da LGPD, sob esse enfoque, deverá se aprofundar no mapeamento e inventário de dados pessoais estruturados e não estruturados.

De outro modo, cabe mencionar os casos em que não existe aplicação da LGPD, hipóteses estas que estão disciplinadas no artigo 4º, tratando-se de rol taxativo:

Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:

I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;

II - realizado para fins exclusivamente:

a) jornalístico e artísticos; ou

b) acadêmicos;

III - realizado para fins exclusivos de:

a) segurança pública;

b) defesa nacional;

c) segurança do Estado; ou

d) atividades de investigação e repressão de infrações penais; ou

IV - provenientes 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 nesta Lei (BRASIL, 2018).

Como se trata de uma lei sem precedentes, necessário exemplificar as hipóteses de exclusão individualmente. No tocante ao inciso I, sobre uso particular e sem fim econômico, essa hipótese foi pensada para direcionar os recursos para o que realmente coloca a privacidade em risco, por isso, casos particulares ficam excluídos da lei, como afirma Ribeiro (2019).

Com relação aos fins jornalísticos, a LGPD não tem aplicação por conflitar com o direito de liberdade de expressão e pela verdade do jornalismo ter o intuito de informar as pessoas, exercendo função social de interesse público, como também não se aplica aos fins artísticos que visam propagar a arte, cultura e folclore. Entretanto, é necessário verificar “se a empresa tem como objeto social ou atividade preponderante o jornalismo, se a notícia possui interesse público ou relevância social, se há indicação de fontes confiáveis, etc.” (COTS; OLIVEIRA, 2019, p. 64).

Para os fins acadêmicos, Maciel (2019), explana que estes também são excluídos, já que os dados coletados servem de base para pesquisas, por exemplo, para desenvolvimento no meio acadêmico, porquanto os pesquisadores precisam ter conhecimento de dados como origem racial, sexo, opção sexual, entre outros.

No que diz respeito à segurança pública, defesa nacional e segurança do Estado ou atividades de investigação e repressão de infrações penais, tal medida se faz necessário pelos dados tratados nessa seara são de competência do Poder Público e a LGPD determina que haverá uma lei específica para o tratamento de dados por parte do interesse público, devendo prever medidas rigorosas ao atendimento do interesse público, observando o devido processo legal, os princípios gerais de proteção e os direitos do titular previsto em lei (RIBEIRO, 2019).

Enfim, ficam também excluídos da LGPD os dados provenientes de outro país e que não são tratados no Brasil. O supracitado autor, relembra que a empresa, ainda que seja estrangeira, estará sujeita à LGPD caso exerça atividades no Brasil ou se tratar dados aqui no país. Para atingir essa exceção, a LGPD dispõe de requisitos que devem ser cumulados. São os dados oriundos de país estrangeiro e não coletados em território nacional; não comunicação ou uso compartilhado de dados com agentes brasileiros; não pode haver transferência internacional de dados com outro país que não o de proveniência e o país de proveniência deve ter grau de proteção de dados pessoais adequados ao previsto na LGPD (VAINZOF; MALDONADO; BLUM, 2019, p. 83).

Pinheiro (2020, p. 40), esclarece o alcance extraterritorial da LGPD, os efeitos internacionais, na medida em que se aplica também aos dados que sejam tratados fora do Brasil, desde que a coleta tenha ocorrido em território nacional, ou por oferta de produto ou serviço para indivíduos no território nacional ou que estivessem no Brasil. Sendo assim, o dado pessoal tratado por uma empresa de serviço que armazene o dado fora do país terá que cumprir as exigências da LGPD.

O tópico seguinte apresenta-se os princípios que norteiam a lei.

3.4 PRINCÍPIOS DA LEI GERAL DE PROTEÇÃO DE DADOS

Os princípios da Lei Geral de Proteção de Dados visam fortalecer a proteção da privacidade do titular dos dados, a liberdade de expressão, de informação, de opinião e de comunicação, a inviolabilidade da intimidade, da honra e da imagem e o desenvolvimento econômico e tecnológico (PINHEIRO, 2020).

Para que uma empresa coletora de dados cumpra com seu papel, tratando efetivamente os dados e protegendo seu usuário, é requisito conhecer os princípios que regem a LGPD. Estes princípios estão inseridos no artigo 6º da legislação (BRASIL, 2018). São eles:

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.

Para um melhor entendimento, cabe explicitar cada um deles e constatar que todos estão interligados entre si. O princípio da finalidade significa que o tratamento dos dados pessoais deve ser realizado com um propósito bem definido, legítimo, específico e informado ao titular. Maciel (2019, p. 26), indica que “o quanto mais específica a descrição dos usos for, melhor protegido os segredos do negócio”. E modificando a finalidade o tratamento posterior deve

obter o novo consentimento ou expressar, se a base legal for outra, a mudança de finalidades para os titulares.

Quanto ao princípio da adequação se encontra relacionado com o da finalidade, pois os dados devem ser tratados de forma adequada, correta e que atenda a finalidade proposta, como assevera Ribeiro (2019).

Com relação ao princípio da necessidade cabe enfatizar que os dados devem ser tratados no limite necessário para atingir a finalidade informada. Maciel (2019), cogita que a finalidade, a adequação e a necessidade caminham bastante juntas. Sendo assim, os dados têm que ser pertinentes, proporcionais e não excessivos.

Os princípios do livre acesso, da qualidade dos dados e da transparência se completam, visto que o livre acesso abrange também a transparência e garante ao usuário a consulta de seus dados de forma completa e gratuita, saber como estão sendo tratados seus dados e conforme a finalidade da empresa. Ribeiro (2019, p. 86), argumenta que se a empresa se recusar a prestar tais informações aos usuários violará frontalmente a lei, o que poderá ensejar em denúncia à Autoridade Nacional de Proteção de Dados. Já a qualidade dos dados significa dizer que os dados devem ter qualidades, ou seja, serem claros, exatos, relevantes e atualizados junto a empresa em complemento com o livre acesso.

No tocante ao princípio da segurança e da prevenção, é obrigação legal dos agentes de tratamento em adotar medidas técnicas e administrativas de segurança protegendo os dados de acessos não autorizados, seja por imprudência, negligência ou imperícia dos funcionários ou também situações ilícitas que possam ocasionar alguma forma de tratamento inadequado de dados, sob pena de sanções administrativas e da responsabilidade civil. Já a prevenção, é no sentido de que se atue em conscientizar os funcionários e mudar a cultura das empresas, minimizando o risco de incidentes.

Ao falar do princípio da não discriminação, expressa ser que nenhum dado coletado, independentemente de sua base legal ou finalidade exposta com consentimento válido, poderá ser tratado para fins discriminatórios ou abusivos, conforme determina Rafael Fernandes Maciel (2019).

No entanto, o princípio da responsabilização e da prestação de contas, é o dever de não só cumprir com as normas, mas ter capacidade de comprovar sua conformidade. É o dever de

prestar contas, não apenas à ANPD, mas também aos clientes, público em geral, e a todos os quais seus dados estejam sendo coletados.

O espírito da lei foi proteger os direitos fundamentais de liberdade e da privacidade e o livre desenvolvimento da personalidade da pessoa natural, trazendo a premissa da boa-fé para todo o tipo de tratamento de dados pessoais (PINHEIRO, 2020).

No tópico seguinte aborda-se com relação ao Marco Civil da Internet.

3.5 CONSIDERAÇÕES SOBRE O MARCO CIVIL DA INTERNET

O Marco Civil da Internet (MCI) foi promulgado sob a Lei n. 12.965, em 23 de abril de 2014, foi desenhado a partir de uma consulta pública feita pela Internet, iniciada em 2009, e tramitou no Congresso Nacional entre 2011 e 2014. O projeto de lei passou pelo controle e revisão de diferentes áreas da sociedade, passando por empresas, organizações da sociedade civil, ativistas e comunidade técnica. Desde a sua concepção em 2007, até a efetiva aprovação da lei, em 2014, foram sete anos de desenvolvimento de um debate aberto com a sociedade. (SOUZA; LEMOS, 2016, p. 15-16).

A Lei do Marco Civil da Internet estabelece princípios, garantias, deveres e direitos para o uso da rede mundial de computadores no Brasil, determinando igualmente, as diretrizes que poderão ser adotadas pelo Poder Público nesse contexto, sobretudo para garantir o direito ao acesso desta rede a todas as pessoas físicas e jurídicas, conforme artigo 4º, inciso I, do MCI (ARAÚJO, 2017).

Nesse sentido, o supramencionado autor destaca que este novo diploma normativo, ofereceu uma base legal para o Poder Judiciário, sempre que este se depare com deveres de provedores de conexão e de acesso a aplicações da Internet, com o direito dos usuários, questões anteriormente que eram apreciadas com decisões contraditórias, oriundas de interpretação do Código Civil brasileiro, Código de Defesa do Consumidor e outras legislações existentes (2017, p. 85)

A motivação para que o MCI foi concebido, como uma lei que pudesse preservar as bases para a promoção das liberdades e dos direitos na Internet para a sociedade brasileira. Então, o Brasil ofereceu um dos mais simbólicos exemplos de debates globais sobre uma regulação da rede que tenha os direitos humanos como o seu fio condutor e que mantém o

caráter principiológico para evitar uma caducidade precoce de seus dispositivos, quando afirma Souza e Lemos (2016, p. 18).

Tarcisio Teixeira faz uma preliminar análise sobre o MCI:

Poderia se imaginar que a referida norma não trata claramente sobre comércio eletrônico em sentido estrito (quanto à compra e venda de produtos e prestação de serviços), mas apenas acerca de outras operações realizadas no comércio eletrônico em sentido amplo (como questões envolvendo a proteção à privacidade e a vedação da captação indevida de dados e da sua comercialização). Entretanto, suas regras e princípios têm implicação direta em tudo o que ocorre na Internet em âmbito brasileiro, inclusive o e-commerce, enquanto operações envolvendo a produção e a circulação de bens e serviços (2015, p. 91).

O artigo 5º, I, da Lei n. 12.965/2014, estabelece “internet” como “o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes”. Marcelo Barreto de Araújo (2017, p. 92) entender ser possível abstrair da referida lei três grandes pilares: a garantia à liberdade de expressão, a inviolabilidade da privacidade e a neutralidade da rede.

A proteção à privacidade, como direito inerente à inviolabilidade da intimidade, da vida privada, da honra e da imagem da pessoa, nos termos da Constituição Federal, em seu artigo 5º, X, garante a o sigilo dos dados pessoais do usuário, do que ele acessa na rede e do conteúdo das comunicações. Logo, não é permitido monitorar ou fiscalizar os pacotes de dados transmitidos pelos usuários na Internet, sendo que o acesso a esses dados necessita de ordem judicial.

Dados relacionados ao IP, que ficam armazenados em cada uma das vezes em que o e-mail é acessado, devem obrigatoriamente ser guardados pela empresa de correio eletrônico pelo prazo de seis meses, em cumprimento ao Marco Civil da Internet.

Para efeitos do comércio eletrônico, o artigo 6º da Lei n. 12.965/2014, prevê que na interpretação desta norma serão levados em consideração os seus fundamentos, princípios e objetivos, bem como a natureza da Internet, seus usos e costumes particulares, e sua importância para a promoção do desenvolvimento humano, econômico, social e cultural (TEIXEIRA, 2014, p. 93).

Conforme o artigo 7º do MCI, o usuário tem direito: 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. Quanto a necessidade de consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, deverá ocorrer de forma destacada das demais cláusulas contratuais, no entendimento de Tarcisio Teixeira (2015, p. 95).

Danilo Doneda, comenta sobre o Marco Civil da Internet:

O desenvolvimento de leis que procuram proteger a privacidade na Sociedade da Informação não se exaure com o Marco Civil da Internet. Ao contrário, cresce a demanda por uma abordagem geral das garantias do cidadão a respeito de seus próprios dados pessoais, dentro e fora da rede. Leis a esse respeito existem há mais de quatro décadas em vários outros países e, hoje, justifica-se mais do que nunca a incorporação desse gênero de normativa em nosso direito como forma de potencializar as liberdades pessoais do brasileiro diante da utilização cada vez maior de seus dados pessoais (2014, p. 137).

O MCI estabeleceu, na Seção II do Capítulo III, regramento para guarda e disponibilização dos dados pessoais, demandando ordem judicial para acesso ao conteúdo e ainda trouxe os princípios da finalidade e adequação, vedando a guarda, por provedores de aplicações, conforme art. 16:

I - dos registros de acesso a outras aplicações de internet sem que o titular dos dados tenha consentido previamente, respeitado o disposto no art. 7º; ou
II - de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular (BRASIL, 2014).

Para Finkelstein (2012, p. 82), o MCI deve complementar e respeitar as leis em vigor, visando garantir a privacidade de dados dos consumidores e ter a guarda segura dos mesmos, igualando aos demais países do exterior. Nesse contexto, Tarcisio Teixeira (2015), ressalta a grande importância da promulgação do Marco Civil da Internet na medida em que se trata de uma lei principiológica, porém com a capacidade necessária de promover uma maior transparência e confiança no uso da Internet, tornando ela não mais uma terra sem leis, mas sim ampliando a segurança jurídica no Brasil, essencialmente a evitar discrepâncias de decisões judiciais no campo da responsabilidade civil de provedores e intermediários e o exercício da

cidadania, da liberdade de expressão e a proteção da privacidade dos usuários, produzindo consequentemente bons efeitos para o comércio eletrônico brasileiro.

No último capítulo discute-se sobre a regulação da LGPD no comércio eletrônico, de forma que se explana sobre a Autoridade Nacional de Proteção de Dados, os agentes de tratamento e encarregado de dados, as responsabilidades e ressarcimento de danos causados por estes, bem como às sanções administrativas.

Por fim, pondera-se em relação de como a empresa de comércio eletrônico pode estar em concordância com a entrada da Lei.

4 REGULAMENTAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS

Tendo como base que a regulamentação de proteção de dados pessoais é uma legislação principiológica, e a melhor forma de analisar a lei é pela verificação da conformidade dos itens de controle, ou seja, se o controle não está presente, aplicado e implementado, logo a regulação não está atendida.

Pinheiro (2020, p. 41), expressa que “apesar de se referir a direitos fundamentais, como a proteção da privacidade, necessita-se de uma aplicação procedimental dentro dos modelos de negócios das estruturas empresariais”.

A referida autora sustenta que a necessidade de uma lei específica sobre proteção dos dados pessoais decorre da forma como está sustentado o modelo atual de negócios da sociedade digital, na qual a informação passou a ser a principal moeda de troca utilizada pelos usuários para ter acesso a bens, serviços ou conveniências.

Dessa forma, repara-se uma demanda significativa para a regulamentação das questões relativas aos dados pessoais, visto a grande proporção que estes tomaram, permitindo o surgimento de formas de monetizar os dados, ou seja, criou-se uma economia dos dados pessoais (RAPOSO E SILVA, 2018).

Ao longo do presente trabalho foram expostas as definições de comércio eletrônico e suas peculiaridades como os contratos, lojas virtuais, legislação específica e a LGPD. Neste capítulo, serão abordados o conceito e a funcionalização da ANPD, apresentando as legislações que normatizam as matérias relacionadas à competência, a figura do agente de tratamento e o encarregado de dados, o consentimento pelo titular e as penalidades.

4.1 AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD)

A regulamentação da Autoridade Nacional de Proteção de Dados, encontra-se disposta no Capítulo IX, artigos 55-A a 55-K. Enfatiza-se que a ANPD será responsável pela orientação geral no que tange à adequação e aplicação da LGPD, impondo as diretrizes do tratamento de dados no Brasil, além de poder alterar a Lei n. 13.709/2018 (LGPD). Também será responsável pela fiscalização dos tratamentos e aplicação das sanções e multas previstas. Já a composição da Autoridade é prevista no artigo 55-C da Medida Provisória n. 869, e prevê a formação de seis elementos, são eles: Conselho Diretor; Conselho Nacional de Proteção de Dados (CNPD); Corregedoria; Ouvidoria; Órgão de Assessoramento Jurídico Próprio; Unidades Administrativas e Unidades Especializadas que garantam a aplicação da lei (BRASIL, 2018).

Pode-se afirmar que a ANPD foi criada para trazer mais segurança e estabilidade para a aplicação da LGPD. No Brasil há uma previsão ampla de artigos da lei que dependem de futura regulamentação por parte da Autoridade, logo caberá a ela executar as adequações necessárias para que a legislação tenha uma ligação com a realidade social e econômica. Por tal razão é de grande responsabilidade de quem vier a assumir a ANPD, notadamente no primeiro mandato, que será muito mais estruturante, visto o marco legal da proteção de dados pessoais no país (PINHEIRO, 2020, p. 49).

O professor Danilo Doneda (2019, p. 320), escreve que:

[...] a atuação de uma autoridade de garantia nos moldes da maioria das autoridades de proteção de dados hoje existentes merece atenção, em primeiro lugar, porque nesse caso a simples atuação do indivíduo para a proteção de seus interesses – o controle individual, como em alguma das concepções de proteção de dados pessoais – não é capaz de projetar uma situação na qual o direito fundamental em questão receba tutela adequada. A impossibilidade de concretizar a autodeterminação informativa baseada meramente na ação singular de seu interessado é patente em vista da desproporção entre sua vontade e uma estrutura dirigida à coleta de seus dados e preparada a excluí-lo de certas vantagens caso decida não fornecê-los.

A ação de uma autoridade para a proteção de dados pessoais representa, nesse diapasão, a realização de uma garantia institucional nos ensinamentos de Fabio Konder Comparato (2001).

Entende-se que o processo de formulação da LGPD, se remonta ao ano de 2010, compreendendo duas fases de debate público em torno de versões de um Anteprojeto de Lei de

Proteção de Dados, a primeira em 2010-11 e a última em 2015. Em ambas ocasiões, as propostas colocadas discutiam a acerca da existência de uma autoridade competente para a aplicação da legislação de proteção de dados (DONEDA, 2019).

Ademais, o supracitado autor evidencia que com a sanção da LGPD, a Presidência da República, reconhecendo a necessidade do estabelecimento de um ente público para a efetividade da LGPD, anunciou sua intenção de elaborar ela própria a autoridade. Assim, em 27 de dezembro de 2018, o Poder Executivo publicou a Medida Provisória n. 869/2018, criando a Autoridade Nacional de Proteção de Dados. Após ter sofrido uma série de modificações pela Comissão Mista que a avaliou no Congresso Nacional, a MP 869/2019 foi finalmente convertida na Lei n. 13.853 no dia 8 de julho de 2019, registra-se que foi promulgada com vetos pela Presidência da República.

Danilo Doneda exemplifica acerca das modificações:

Imperioso dizer que em virtude das modificações introduzidas pela Lei 13.853/2019, a LGPD apresenta disposições específicas em relação à natureza da ANPD, visto que em seu artigo 55-A, parágrafos 1º e 2º, atesta uma natureza “transitória” para a ANPD estabelecendo um tipo de “gatilho” ao condicionar que se procederá, em até 2 anos da entrada em vigor da sua estrutura regimental, a uma avaliação acerca da sua possível conversão em uma “entidade da administração pública federal e indireta, submetida a regime autárquico e especial e vinculada à Presidência da República” (2019, p. 324-325).

Pinheiro é assertivo sobre o papel fundamental da ANPD como elo entre diversas partes interessadas que vão do titular ao ente privado e ao ente público, passando pela necessidade de alinhamento com demais autoridades reguladoras e fiscalizadoras, bem como os três poderes, Executivo, Legislativo e Judiciário que devem compreender a temática do dinamismo dos dados pessoais em contexto não apenas nacional, mas internacional (2020).

A referida autora delinea que a etapa após a entrada em vigor da lei é a mais importante, já que devem ser estabelecidas políticas públicas de adequação, e aplicações de Códigos de Conduta e Certificações será vital. Ela ainda observa que o trabalho de Proteção de Dados pelo mundo desde o advento do GDPR foi uma mudança de comportamento por parte das empresas de comércio eletrônico.

No que se refere à competência da ANPD – artigo 55-J –, é possível destacar: zelar pela proteção dos dados pessoais; elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade; Fiscalizar e aplicar sanções, mediante processo administrativo;

apreciar petições de titular contra controlador após comprovada pelo titular a apresentação de reclamação; promover na população o conhecimento das normas e das políticas sobre proteção de dados e das medidas de segurança; solicitar, às entidades do poder público e empresas privadas que realizam operações de tratamento de dados pessoais informe os detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico; realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização; editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais, como *startups*; garantir que o tratamento de dados de idosos seja efetuado de maneira clara, acessível e adequada ao seu entendimento, nos termos desta Lei e da Lei n. 10.741, de 1º de outubro de 2003 (Estatuto do Idoso).

Marcio Cots e Ricardo Oliveira (2019), articulam que a ANPD será incumbida de tornar a LGPD mais cristalina, acessível e palatável, tanto para os titulares de dados quanto para os agentes de tratamento, garantindo uma maior segurança jurídica nas questões que envolvem o tratamento de informações pessoais.

O tópico seguinte aborda-se a matéria relativa aos agentes de tratamento, apresentando a função do controlador, operador e o encarregado de dados.

4.2 AGENTES DE TRATAMENTO

A Lei Geral de Proteção de Dados traz grande impacto social e econômico, de todas as empresas de comércio eletrônico, posto que o usuário brasileiro titular de dados pessoais precisará saber o que é proteção de dados, assim como haverá necessidade de se disponibilizar recursos financeiros para que o sistema da pequena empresa e de *startups* possam estar em conformidade (PINHEIRO, 2020, p. 63).

A lei prevê e exige que existam encarregados da proteção dos dados pessoais nas empresas de comércio eletrônico. Ribeiro afirma que os agentes de tratamento fazem menção à figura do controlador e operador, figuras que nenhuma outra lei descreve, e que passarão a ser conhecidas quando da vigência da LGPD. Assim como também a representação de um terceiro denominado encarregado de dados, sendo os três responsáveis por adequar a cultura da empresa de e-commerce à cultura da lei, bem como de fazer o intermédio com a ANPD (2019). De uma

maneira mais simples o controlador é todo aquele que trata dados e decide sobre seu destino, enquanto o operador é responsável por agir conforme as diretrizes estabelecidas pelo controlador.

Conforme entendimento de Patricia Peck Pinheiro, o controlador e o operador devem pensar em regras e meios técnicos para proteger os dados pessoais e comprovar sua efetividade nas empresas, seja por aplicação de recursos de anonimização, controle de acesso, procedimentos, políticas de gestão e treinamentos para equipes (2020).

Os artigos 37 a 40 da LGPD versam sobre controlador e operador:

Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.

Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.

Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

Art. 39. O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria.

Art. 40. A autoridade nacional poderá dispor sobre padrões de interoperabilidade para fins de portabilidade, livre acesso aos dados e segurança, assim como sobre o tempo de guarda dos registros, tendo em vista especialmente a necessidade e a transparência (BRASIL, 2018).

Consoante entendimento de Pinheiro, o artigo 37 dá conta sobre o controle e a transparência das ações e do cumprimento dos propósitos do tratamento de dados, cabendo ao controlador e operador documentar todas as operações realizadas durante o processo de tratamento de dados (2020).

O artigo 38, dispõe que a proteção de dados deve ser realizada desde a sua entrada no banco de dados e que as certificações e o cumprimento dos códigos de conduta são medidas de verificação de que o controlador está cumprindo com suas obrigações.

O artigo 39 traz a vinculação entre controlador e operador, visto a responsabilidade solidária do controlador para com o operador, contudo, quem detém o consentimento do titular

é o controlador, dessa forma, é ele quem continua a ser responsável pelo que ocorre no ciclo de vida dos dados pessoais na gestão e governança do negócio (PINHEIRO, 2020, p. 119).

Rafael Fernandes Maciel (2019, p. 98), expõe a diferença entre controlador e operador conforme “a análise de dados coletados e a partir desses perquirir sobre quem define os propósitos de utilização e tratamento de dados e quem atua apenas em nome de quem definiu”.

Por outro lado, a LGPD não regulamenta como será a relação entre controlador e operador ou se estes serão agentes internos da empresa, todavia, é circunstância que deverá haver ao menos um contrato de prestação de serviços entre eles discriminando as obrigações de cada um (RIBEIRO, 2019, p. 83).

Quanto ao artigo 40, a supradita autora pondera que devido ao poder de fiscalização da ANPD, é relevante pontuar que a instituição de padrões de ação por esses órgãos facilita o cumprimento das normas.

Por fim, o encarregado pelo tratamento de dados, no GDPR, conhecido também como *Data Protection Officer* (DPO). Nos termos do inciso VIII do artigo 5º da LGPD, encarregado é uma pessoa, indicada pelo controlador e pelo operador, que atua como canal de comunicação entre o agente de tratamento os titulares e a autoridade nacional, cabendo manifestar que o encarregado não é considerado agente de tratamento, por força do inciso VIII do artigo 5º, respondendo de maneira diferenciada por seus próprios atos (COTS; OLIVEIRA, 2019, p. 175). As atribuições e especificidades da função do encarregado encontra-se no artigo 41 da LGPD (BRASIL, 2018), *in verbis*:

Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.

§ 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.

§ 2º As atividades do encarregado consistem em:

I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

II - receber comunicações da autoridade nacional e adotar providências;

III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

§ 3º A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.

§ 4º (VETADO). (Incluído pela Lei nº 13.853, de 2019)

Observa-se que a obrigatoriedade de indicar um encarregado passou a ser do controlador e do operador. Indicado o encarregado, o agente de tratamento deverá divulgar, preferencialmente em seu site, os dados de sua identificação, bem como dados para contato, como e-mail e telefone.

As atribuições pertinentes ao encarregado estão citadas no § 2º. A primeira e a segunda atribuições são as mais básicas, já que o encarregado é um meio de comunicação entre o agente de tratamento e terceiros. Compreende-se como terceiros possíveis, os titulares de dados e a autoridade nacional que mais demandarão atenção e trabalho por parte do encarregado.

A terceira atribuição demonstra que o encarregado deve ter certas habilidades necessárias para sua execução, exigindo-se conhecimento da própria legislação como também sobre atendimento e relacionamento com titulares. Além disso conhecer especialmente sobre ciber segurança e se possível de governança de dados (PINHEIRO, 2020).

Por fim, a quarta atribuição do encarregado é ser responsável por executar outras atribuições determinadas pelo controlador ou estabelecidas em normas complementares, sendo que estas últimas poderão ser estabelecidas pela ANPD.

Maciel faz uma análise com relação ao perfil do encarregado:

O encarregado deve possuir liberdade, não podendo ser penalizado por estar exercendo suas funções e, por isso, ainda que não seja vedado pela lei, é prudente não utilizar funcionário celetista, haja vista que esse, por não possuir estabilidade expressa na lei ao exercer tal mister, poderia sentir-se coagido em determinadas situações. Ainda, o encarregado deve agir sem conflito de interesse, devendo, por exemplo, evitar determinadas medidas por receio de perder o contrato. Em termos de capacidade técnica e conhecimento sugere-se que o encarregado tenha conhecimentos jurídicos e do ambiente regulatório relacionado a dados pessoais e habilidades para realizar as atividades previstas (2019, p. 77).

Com essas contemplações acerca dos agentes de tratamento e o encarregado de dados, em seguida, versa-se quanto às suas responsabilidades e quando necessário ressarcir os danos causados.

4.2.1 Responsabilidade e Ressarcimento de Danos

Os artigos que tratam sobre a responsabilidade dos agentes de tratamento e o encarregado de dados, estão elencadas nos artigos 42, 43, 44 e 45:

Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

§ 1º A fim de assegurar a efetiva indenização ao titular dos dados:

I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;

II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.

§ 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.

§ 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente.

§ 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.

Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:

I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;

II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou

III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:

I - o modo pelo qual é realizado;

II - o resultado e os riscos que razoavelmente dele se esperam;

III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.

Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano.

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).

Assim como no GDPR, nos artigos 24, 25 e 26, a lei brasileira também traz em sua previsão o caráter solidário da responsabilização do controlador e operador na essência do artigo 42, portanto, o controlador como o operador estão obrigados a reparar os danos causados em violação à legislação da LGPD, sejam morais, patrimoniais, individuais ou coletivos. A responsabilidade civil dos agentes de tratamento segue a regra geral estabelecida pelos artigos 186, 187 e 927 do Código Civil. Sendo assim, todos os controladores que estiverem envolvidos no tratamento do qual decorreram danos ao titular respondem solidariamente.

O objetivo da lei é dar maior efetividade nas indenizações aos titulares e, portanto, caberá aos agentes um cuidado redobrado na celebração dos contratos e definição das obrigações de cada parte, como mecanismos de controle e gerenciamento de forma a reduzir potenciais danos, agindo de forma preventiva (MACIEL, 2019).

O supradito autor (2019, p, 78), cita que o encarregado não responde pelos danos provocados pelos controladores ou operadores aos titulares, porém responderá em eventual ação de regresso por vício na prestação do serviço. Direito de regresso que também é assegurado àquele que reparar o dano ao titular contra os demais responsáveis (art. 42, §4º).

Ribeiro (2019, p. 84-85), elucida que a LGPD não apontou qual é a responsabilidade do encarregado, de que forma que resta subentendido que essa figura não responderá civilmente perante a ANPD no que diz respeito aos atos praticados pelo controlador. Não obstante, responderá penalmente e em casos que gere riscos para o controlador em caso de má execução de suas atividades, por exemplo, comunicar informações imprecisas ou abusivas aos funcionários e à ANPD.

Os agentes de tratamento, controlador e operador, somente não serão responsabilizados quando comprovarem (art. 43): (i) que não realizaram o tratamento de dados pessoais que lhes é atribuído; (ii) que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; (iii) que o dano é decorrente

de culpa exclusiva do titular dos dados ou de terceiro, desta forma, verifica-se o rol taxativo deste artigo.

O operador responderá solidariamente ao controlador quando descumprir as obrigações da legislação de proteção de dados ou descumprir as instruções lícitas do controlador (art. 42, §1º, I). E, todos os controladores que estiverem envolvidos no tratamento do qual decorreram danos ao titular respondem solidariamente. Mesmo em casos mais simples, caberá sempre ao agente demonstrar a licitude de suas operações, ainda que não haja essa inversão do ônus, sobretudo quando necessário provar o consentimento, por força do §2º do art. 8º da lei.

Em síntese, o controlador responde pelos danos patrimoniais, morais, individuais ou coletivos (dever de reparação), além de responder solidariamente pelos danos causados pelo operador, se diretamente envolvido no tratamento que resultar em danos aos titulares. Por outro lado, o operador responde pelos mesmos danos que o controlador, além da responsabilidade solidária com este em caso de descumprimento da legislação, caso não tenha seguido suas instruções (RIBEIRO, 2019, p. 83).

Com essas observações relativas a responsabilidade e o ressarcimento de danos pelos agentes de tratamento e o encarregado de dados, em seguida desenvolve-se acerca da importância do consentimento pelo titular de dados.

4.3 CONSENTIMENTO PELO TITULAR

A definição de consentimento é a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada, sendo apenas uma das bases legais para validar o tratamento de dados pessoais, assim conceitua Rafael Fernandes Maciel (2019).

O dito autor explana acerca do consentimento:

O consentimento, para ser válido, deve ser livre, informado e inequívoco, fornecido por escrito ou outro meio que demonstre a manifestação da vontade do titular, em cláusula destacada, sem vício de consentimento e referir-se a finalidades determinadas. Autorizações genéricas são consideradas nulas. Caixas de seleção pré-marcadas também são consideradas não legítimas, invalidando o consentimento. O controlador deve adotar mecanismos eficazes para poder provar o consentimento obtido, uma vez que o ônus da prova é seu, conforme teor do disposto no §2º do art. 8º (2019, p. 35).

O consentimento deve ser dado pessoa capaz, envolvendo um objeto lícito, possível, determinado e que seja obediente às formas descritas em lei, sendo um consentimento livre, informado e cristalino. A manifestação de vontade do usuário para que sejam tratados os dados, e do outro lado a pessoa que deverá tratá-lo, faz o consentimento ter natureza contratual (RIBEIRO, 2019).

Patricia Peck (2020, p. 43), deslinda que a linha mestra para o tratamento de dados pessoais é o consentimento pelo titular, que deve ser aplicado aos tratamentos de dados informados e estar vinculado às finalidades apresentadas.

A LGPD prevê que o consentimento faça com que a empresa possa capturar realmente a intenção do usuário, devendo ser por meio escrito ou outros meios, podendo ser estes “outros meios” como, via SMS, registro de áudio, de vídeo ou e-mail, além de apresentar um contrato e pedir assinatura, sendo possível identificar claramente que o usuário acorda em deixar que seus dados sejam tratados, cabendo ao controlador provar que o usuário consentiu nos termos da lei (RIBEIRO, 2019, p. 87).

Nesse sentido, garantir que as pessoas tenham ciência de que devem consentir o uso de dados, assim como tenham direito de saber a finalidade da coleta e acesso ao seu conteúdo em qualquer momento, é primordial para assegurar a liberdade e a privacidade (PINHEIRO, 2020).

Segundo Danilo Doneda, a disciplina do consentimento para o tratamento de dados pessoais não deve ser tratada sob um perfil negocial e deve ter como orientação a atuação do poder de autodeterminação informativa da pessoa e da consideração dos direitos fundamentais em questão (2019, p. 329).

Cintha Ribeiro destaca que a qualquer momento o consentimento pode ser revogado pelo usuário mediante pedido, não precisando ser escrito, mas deve ser gratuito, de modo fácil de ser feito e, principalmente, pela mesma forma como se deu o consentimento (2019).

No tópico seguinte serão abordadas as penalidades aplicadas pela Autoridade Nacional de Proteção de Dados.

4.4 PENALIDADES

No que diz respeito às penalidades previstas pela LGPD, estas encontram-se no artigo 52 a 54, tem-se que algumas das sanções sofreram veto presidencial, se tornando menores do

que as previstas pelo GDPR, tendo em vista a necessidade de adaptação para a realidade e a conjuntura do cenário econômico brasileiro (PINHEIRO, 2020, p. 45)

Por mais que as sanções sejam as mais difundidas como fator para obrigar as empresas a entrarem em consonância com a LGPD, é preciso dizer que a cultura de proteção de dados pessoais e a efetivação das medidas previstas na lei, garante ao controlador a confiança de seus consumidores, consequentemente, gerando oportunidade de mercado (MACIEL, 2019). Desta forma, a adequação não deve ser tão somente para evitar sanções ou responsabilidade civil, vez que são as empresas que devem se adequar e regularizar-se para valorizarem ante o consumidor.

Rafael Fernandes Maciel, leciona sobre o cuidado com os dados:

A LGPD, embora possua sanções pesadas, sopesa as punições àquelas empresas que possuem os cuidados mínimos com os dados pessoais dos titulares a elas confiados. E é essa balança e compreensão de que incidentes de segurança são impossíveis de serem evitados completamente, que faz com que a regulamentação seja protetiva à privacidade sem impedir a inovação e os negócios forjados em informações pessoais (2019, p. 88).

No artigo 52 (BRASIL, 2018) estão previstas as seguintes sanções:

I - advertência, com indicação de prazo para adoção de medidas corretivas;

II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R\$ 50.000.000,00 (cinquenta milhões de reais) por infração;

III - multa diária, observado o limite total a que se refere o inciso II;

IV - publicitação da infração após devidamente apurada e confirmada a sua ocorrência;

V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;

VI - eliminação dos dados pessoais a que se refere a infração.

VII - (VETADO);

VIII - (VETADO);

IX - (VETADO).

X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; (Incluído pela Lei nº 13.853, de 2019)

XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; (Incluído pela Lei nº 13.853, de 2019)

XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. (Incluído pela Lei nº 13.853, de 2019)

Para Pinheiro, um programa de gestão de dados pessoais bem implementado pode ajudar na redução das penas, na hipótese de ocorrência de um tipo de infração que enseje a aplicação de alguma penalidade (2020).

Nas lições de Rafael Fernandes Maciel:

Interessante notar que o teto máximo de valor pecuniário para aplicação da multa prevista no inciso II é por infração e, em um mesmo procedimento administrativo, poderão ser encontradas várias infrações a partir de uma mesma denúncia. Por exemplo, um incidente de vazamento de dados em que, no decorrer do procedimento, seja apurado que também havia um tratamento de dados pessoais excessivo ou desproporcional. Poderá haver uma infração pelo incidente e outra pela ilicitude do tratamento (2019, p. 89).

Outrossim, as sanções previstas pelos incisos X, XI e XII só podem ser aplicadas após já ter sido imposta ao menos uma das sanções de que tratam os incisos II, III, IV, V e VI do *caput* deste artigo para o mesmo caso concreto.

Verifica-se que a lei prevê que as sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso, observando-se alguns requisitos, em particular o da proporcionalidade. Entre os itens que podem ser considerados na minimização de uma punição pela Autoridade Nacional de Proteção de Dados, fiscalizadora e responsável, conforme previsto pelo próprio artigo 52, § 1º, estão: (i) a gravidade da infração; (ii) a boa-fé do infrator; (iii) a vantagem auferida; (iv) a condição econômica do infrator; (v) a reincidência; (vi) o grau de dano causado; (vii) a cooperação do infrator; (viii) a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano; (ix) a pronta adoção de política de boas práticas e governança; (x) a pronta adoção de medidas corretivas; e (xi) a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

Logo, a Autoridade Nacional de Proteção de Dados deve determinar a aplicação das sanções administrativas previstas na LGPD, observando os princípios da razoabilidade e proporcionalidade (COTS; OLIVEIRA, 2020, p. 214).

O parâmetro para fixação da multa diária deve observar a gravidade da falta e a extensão do dano ou prejuízo causado, e a intimação para cumprimento deverá descrever a obrigação imposta bem descrita, a fim de não haver dúvidas quanto à sua obrigação de fazer ou de não fazer, pois é sobre esse tipo de obrigação que a multa diária faz sentido, como também com prazo razoável para cumprimento.

Quanto a destinação do valor das multas, inscritas ou não em dívida ativa, o § 5º do artigo 52, dispõe que o valor será destinado ao Fundo de Defesa de Direitos Difusos de que tratam o art. 13 da Lei nº 7.347, de 24 de julho de 1985, e a Lei nº 9.008, de 21 de março de 1995.

Destarte, a empresa corporativa precisará focar nos princípios que foram elencados na LGPD para que o negócio seja sustentável (PINHEIRO, 2020).

As sanções administrativas descritas na LGPD dependem de regulamento próprio da autoridade nacional para serem aplicadas. A ANPD deverá submeter o regulamento à consulta pública, incluindo as metodologias que orientarão o cálculo do valor-base das multas (artigo 53). Após a aprovação do regulamento, deverá haver publicação para ciência geral, notadamente aos controladores, apresentando as formas de dosimetria das sanções, valor base, fundamentação detalhada, em que hipóteses serão aplicadas multas simples e diárias, entre outras informações descritas nos parágrafos do artigo 53.

Marcio Cots e Ricardo Oliveira entendem que a previsão é propícia:

[...] A previsão é benéfica por aumentar a segurança jurídica dos agentes de tratamento, mas não se pode perder de vista que as sanções administrativas são retributivas e pretendem desestimular condutas lesivas aos titulares. Em outras palavras, se as sanções não forem relevantes, o desestímulo não ocorrerá e a LGPD correrá grande risco de ser uma “lei que não pegou” (2019, p. 222).

Cinthyá Ribeiro destaca que essas questões são discutidas no âmbito teórico e somente poderão ser melhor examinadas quando da operação por parte da Autoridade Nacional e da vigência da lei frente aos fatos concretos (2019).

Feito estas alegações com relação às penalidades aplicadas pela ANPD, no tópico seguinte serão feitas considerações acerca de como a empresa de comércio eletrônico possa estar em consonância com a LGPD.

4.5 COMÉRCIO ELETRÔNICO EM CONFORMIDADE COM A LEI GERAL DE PROTEÇÃO DE DADOS

Em vista da empresa de comércio eletrônico estar em conformidade com a nova lei, é imprescindível realizar o tratamento de forma correta, protegendo o seu usuário, a empresa coleta deve conhecer os princípios que regem a LGPD, já expostos neste trabalho, e estabelecidos no artigo 6º: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança e prevenção, não discriminação e responsabilização e prestação de contas, sendo que todos os princípios devem sempre observar a boa-fé.

Patricia Peck Pinheiro, analisa que para atender aos requisitos da LGPD exige-se adequação dos processos de governança corporativa, com elaboração de um programa consistente de *compliance* digital, o que demanda investimentos, atualização de ferramentas de segurança de dados, revisão documental, melhoria de procedimentos e fluxos internos e externos de dados pessoais, com aplicação de mecanismos de controle e trilhas de auditoria e, sobretudo, mudança de cultura.

A lei prevê e determina que existam encarregado da proteção dos dados pessoais nas organizações. O controlador e operador devem pensar em regras e meios técnicos para proteger os dados pessoais e comprovar sua efetividade nas empresas de e-commerce, seja por aplicação de recursos de anonimização, controle de acesso, procedimentos, política de gestão e treinamentos para equipes. Pinheiro (2020, p. 63), pondera que ainda não se tem definido a questão de quem deve ser essa pessoa e como fazer o treinamento e a seleção deste profissional, podendo ser interno ou terceirizado.

O autor mencionado demonstra como iniciar a implementação dos requisitos de conformidade:

O primeiro passo é a realização de um levantamento. Ou seja, deve-se fazer uma análise de diagnóstico para identificar como a instituição está no tocante aos indicadores de conformidade e o que falta para atender aos controles exigidos. Para

tanto, a primeira atividade é fazer o inventário dos dados pessoais (quais são e onde estão). Depois, deve-se montar a matriz de tratamento dos dados pessoais (quais os tipos de tratamento e para que finalidades). Em seguida, como está sendo feito o controle de gestão de consentimentos. Com esse panorama, é desenvolvido o mapa de risco e elaborado o plano de ação, que permite fazer a cotação dos investimentos necessários às conformidades, implementadas, em geral, em quatro níveis: no nível técnico (ferramentas), documentar (atualizar normas, políticas, contratos), procedimental (adequar a governança e a gestão dos dados pessoais) e cultura (realizar treinamentos e campanhas de conscientização das equipes, dos parceiros, fornecedores e clientes) (2020, p. 65).

Danilo Doneda pondera que a proteção de dados pessoais deve definir, mais que tudo, a quem cabe o controle sobre os dados pessoais – e assim, conseqüentemente, realizar uma forma de distribuição de poder na sociedade (2019, p. 328).

A empresa eletrônica, dependendo do ramo de negócio e da maturidade da governança de dados, é essencial criar um programa de *compliance* digital, com *risk assessment*, plano de respostas a incidentes, treinamentos e comunicação, *due diligence* de terceiros em um contexto que abarque todos os setores dentro do negócio e com visão abrangente para legislação nacional e internacional (PINHEIRO, 2020).

Desse modo, a empresa corporativa conseguirá êxito na coleta e tratamento de dados, e conseqüentemente, estar em consonância com a LGPD.

5 CONCLUSÃO

Com a evolução tecnológica, e conseqüentemente o surgimento do comércio eletrônico, a modernidade cada vez menos nos dá privacidade e cada dia mais nossos dados são coletados, compartilhados, usados e expostos sem nosso consentimento. A palavra “dados”, que pouco tempo atrás não representava mais do que simples informação da pessoa, é a palavra do futuro, ao uso de um dos ativos mais valioso da sociedade digital, que são as bases de dados relacionados às pessoas.

A proteção de dados pessoais é um tema que compreende, em grande parte, questões relacionadas ao direito da privacidade, sendo este, um instrumento fundamental para a construção da própria esfera privada e, por conseguinte, o livre desenvolvimento da personalidade, além disto, o processo evolutivo das normas relacionadas à Internet buscou constantemente a garantia do direito fundamental à privacidade.

A Lei de Proteção de Dados Pessoais é um símbolo de grande impacto, tanto para as instituições privadas como para as públicas, por ser extremamente necessário uma lei específica e para tratar sobre a proteção dos dados pessoais dos indivíduos em qualquer relação que envolva o tratamento de informações classificadas como dados pessoais, por qualquer meio, seja por pessoa natural ou jurídica.

Dessa forma, o presente trabalho monográfico procurou adentrar na problemática da regulamentação da LGPD no âmbito do comércio eletrônico. No primeiro capítulo discorreu-se acerca do contexto histórico da Internet e o desenvolvimento do e-commerce como uma nova forma de transacionar entre as pessoas via Internet, estabelecendo definições e conceitos importantes para o tema, como: contratos eletrônicos, lojas virtuais e a legislação aplicada à estas.

Já segundo capítulo, ratifica-se a relevância do tratamento dos dados pessoais com o advento da LGPD, e se destaca que a vigência desta lei traz consigo uma mudança de pensamento sobre privacidade e de como agir com seus dados. Para isso, investigou-se acerca de sua origem, termos e definições da lei, campo de aplicação, princípios e o Marco Civil da Internet.

No terceiro capítulo partiu-se para análise da regulamentação da LGPD no âmbito do comércio eletrônico, bem como discorreu sobre a Autoridade Nacional de Proteção de Dados,

agentes de tratamento, responsabilidades inerentes à função, importância do consentimento pelo titular de dados, e, por último, as penalidades aplicadas pela ANPD.

De todo exposto, conclui-se que, tão logo a Autoridade Nacional de Proteção de Dados esteja devidamente constituída e atuando em casos concretos e a Lei Geral de Proteção de Dados entre em vigência, não há como garantir o quanto a privacidade realmente será preservada e quais medidas serão tomadas pelas empresas de comércio eletrônico.

Também é preciso acentuar que as empresas do ramo têm buscado se adaptar à nova legislação, é certo que os obstáculos estão apenas no início, e o usuário brasileiro titular de dados pessoais precisará saber o que é proteção de dados pessoais e quais são seus direitos, por tal razão, mostra-se oportuno debater e se ambientar com o tema, diante da nova realidade que nos é apresentada.

REFERÊNCIAS

ANDRADE, Ronaldo Alves de. **Contrato Eletrônico no Novo Código Civil e no Código do Consumidor**. Barueri: Manole, 2004. E-book. Acesso restrito via Minha Biblioteca.

ARAÚJO, Marcelo Barreto de. **Comércio eletrônico**; marco civil da internet; direito digital. Rio de Janeiro: Confederação Nacional do Comercio de Bens, Serviços e Turismo, 2017. E-book. Acesso restrito via Minha Biblioteca.

BARBAGALO, Erica Brandini. **Contratos eletrônicos**: contratos formados por meio de rede de computadores: peculiaridades jurídicas da formação do vínculo. São Paulo: Saraiva, 2001. E-book. Acesso restrito via Minha Biblioteca.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 5 mai. 2020.

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. Brasília, DF: Presidência da República, 2013. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Decreto/D7962.htm. Acesso em: 16 mai. 2020.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Brasília, DF: Presidência da República, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/110406.htm. Acesso em: 12 mai. 2020.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm. Acesso em: 16 mai. 2020.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 5 mar. 2020.

BRASIL. **Lei nº 13.853, de 8 de julho de 2019**. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art1. Acesso em: 5 mar. 2020.

BRASIL. **Lei nº 4.657, de 4 de setembro de 1942**. Lei de Introdução às normas do Direito Brasileiro. Presidência da República, 1942. Disponível em:

http://www.planalto.gov.br/ccivil_03/decreto-lei/del4657compilado.htm. Acesso em: 20 mar. 2020.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: Presidência da República, 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/18078.htm. Acesso em: 5 mar. 2020.

BRASIL. **Medida Provisória nº 959, de 29 de abril de 2020**. Estabelece a operacionalização do pagamento do Benefício Emergencial de Preservação do Emprego e da Renda e do benefício emergencial mensal de que trata a Medida Provisória nº 936, de 1º de abril de 2020, e prorroga a vacatio legis da Lei nº 13.709, 14 de agosto de 2018, que estabelece a Lei Geral de Proteção de Dados Pessoais – LGPD. Brasília, DF: Presidência da República, 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv959.htm. Acesso em: 11 mai. 2020.

BRUNO, Gilberto marques. As relações do “business to consumer” (B2C) no âmbito do e-commerce. **Revista Jus Navigandi**, Teresina, ano 6, n. 52, p. dez. 2001. Disponível em: <https://jus.com.br/artigos/2319/as-relacoes-do-business-to-consumer-b2c-no-ambito-do-e-commerce>. Acesso em: 23 mar. 2020.

CARVALHO, Ana Paula Gambogi. **Contratos via internet segundo os ordenamentos jurídicos alemão e brasileiro**. Belo horizonte: Del Rey, 2001. E-book. Acesso restrito via Minha Biblioteca.

CASTELLS, Manuel. **A sociedade em rede**. 6. ed. rev. e ampl. Tradução: Roneide Venancio Majer. São Paulo. Paz e Terra. 1999. E-book. Acesso restrito via Minha Biblioteca.

CASTRO, Aldemario Araujo. Os meios eletrônicos e a tributação. **Revista Jus Navigandi**, Teresina, ano 5, n. 48, 1 dez. 2000. Disponível em: <https://jus.com.br/artigos/1813>. Acesso em: 29 mar. 2020.

CHIOVENDA, Giuseppe. **Instituições de direito processual civil**. Tradução de Paolo Capitanio. 4. ed. Campinas: Bookseller, 2009. E-book. Acesso restrito via Minha Biblioteca.

COÊLHO, Amanda Carmen Bezerra. **A lei geral de proteção de dados pessoais brasileira como meio de efetivação dos direitos da personalidade**. 2019. Monografia (Especialização) - Curso de Direito, Universidade Federal da Paraíba, João Pessoa. 2019. Disponível em: <https://repositorio.ufpb.br/>. Acesso em: 02 abr. 2020.

COELHO, Fábio Ulhoa. **Curso de direito comercial**. Direito de empresa. 24. ed. São Paulo: Saraiva, 2012. E-book. Acesso restrito via Minha Biblioteca.

COELHO, Fábio Ulhoa. **Curso de Direito Comercial: Contratos, Falência e Recuperação de Empresas**. São Paulo: Saraiva, 2008. E-book. Acesso restrito via Minha Biblioteca.

COLHO, Fábio Ulhoa. **Manual de direito comercial**. Direito de Empresa. 23. ed. São Paulo: Saraiva, 2011. E-book. Acesso restrito via Minha Biblioteca.

COTS, Marcio. **Lei Geral de Proteção de Dados Pessoais Comentada** / Márcio Cots e Ricardo Oliveira. 3.ed. atual e ampl. São Paulo: Thomson Reuters Brasil, 2019.

DE LUCCA, Newton. **Aspectos da responsabilidade civil no âmbito da internet**. São Paulo: Saraiva, 2009. E-book. Acesso restrito via Minha Biblioteca.

DE LUCCA, Newton. **Aspectos jurídicos da contratação informática e telemática**. São Paulo: Saraiva, 2003. E-book. Acesso restrito via Minha Biblioteca.

DINIZ, Maria Helena. **Código Civil Anotado**. 18. ed. São Paulo: Saraiva, 2017. E-book. Acesso restrito via Minha Biblioteca.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: elementos da formação da lei geral de proteção de dados** / Danilo Doneda. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

FINKELSTEIN, Maria Eugênia Reis. **Aspectos jurídicos do comércio eletrônico**. Porto Alegre: Síntese, 2004. E-book. Acesso restrito via Minha Biblioteca.

FINKELSTEIN, Maria Eugênia Reis. **Direito do comércio eletrônico**. 2. ed. Rio de Janeiro: Forense, 2011. E-book. Acesso restrito via Minha Biblioteca.

FLORENÇO, Larissa Brito. **A proteção de dados pessoais nas relações de consumo como um direito fundamental: Perspectivas de um marco regulatório para o Brasil**. v. 23, n. 29, 2016. Disponível em: <https://revista.esmesc.org.br/re/article/view/144/123>. Acesso em: 02 mai 2020.

FUENZALIDA, Carlos Vattier. **En torno a los contratos electrónicos**. In: Alterini, Maria Fernandes Novaes (Coord.). Direito e responsabilidade. Belo Horizonte: Del Rey, 2001, p. 51-52. E-book. Acesso restrito via Minha Biblioteca.

GASIOLA, Gustavo Gil. **Criação e desenvolvimento da proteção de dados na Alemanha – a tensão entre a demanda estatal por informações e os limites jurídicos impostos**. 29 mai. 2019. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/criacao-e-desenvolvimento-da-protecao-de-dados-na-alemanha-2905019>. Acesso em: 04 de maio de 2020.

GETTING, Brian. Basic definitions: web 1.0, web. 2.0, web 3.0. **Practical Ecommerce**, abr. 2007. Disponível em: <https://www.practicalecommerce.com/Basic-Definitions-Web-1-0-Web-2-0-Web-3-0>. Acesso em: 05 mai. 2020.

GLANZ, Semy. Internet e contrato eletrônico. **Revista dos Tribunais**, v.1, n.3, 1998. Disponível em: <https://core.ac.uk/download/pdf/79118914.pdf>. Acesso em: 07 mai. 2020

GOMES, Orlando. **Contratos**. Atualização Humberto Theodoro Junior. 18. ed. Rio de Janeiro: Forense, 1998. E-book. Acesso restrito via Minha Biblioteca.

GONÇALVES, Carlos Roberto. **Direito civil brasileiro**. Responsabilidade civil. 13.ed. v. 4. São Paulo: Saraiva, 2018. E-book. Acesso restrito via Minha Biblioteca.

KONDER COMPARATO, Fabio. A democratização dos Meios de Comunicação de Massa. **Revista USP**, São Paulo, n. 48, pp. 6-17, dez. /2000-fev. /2001.

LAWAND, Jorge José. **Teoria Geral dos Contratos Eletrônicos**. Juarez de Oliveira. São Paulo: 2003, p. 44. E-book. Acesso restrito via Minha Biblioteca.

LEONARDI, Marcel. **Tutela e privacidade na internet**. São Paulo: Saraiva, 2011. Disponível em: <http://leonardi.adv.br/wp-content/uploads/2012/01/mltpi.pdf>. Acesso em: 1 mar. 2020.

LORENZETTI, Ricardo Luis. **Comércio eletrônico**. RT, 2004, p.19. E-book. Acesso restrito via Minha Biblioteca.

LORENZETTI, Ricardo Luis. **Fundamentos do direito privado**. São Paulo: Revista dos Tribunais, 1998. E-book. Acesso restrito via Minha Biblioteca.

MACIEL, Rafael Fernandes. **Manual prático sobre a Lei geral de proteção de dados pessoais (Lei nº 13.709/2018)**. 1ª ed. Goiânia: RM Digital Education. 2019. E-book. Acesso restrito via Minha Biblioteca.

MAGRANI, Eduardo. **A internet das coisas**. Rio de Janeiro: FGV Editora. 2018. E-book. Acesso restrito via Minha Biblioteca.

MARQUES. Claudia Lima. **Confiança no comércio eletrônico e a proteção do consumidor** (um estudo dos negócios jurídicos de consumo no comércio eletrônico). São Paulo: RT, 2004. E-book. Acesso restrito via Minha Biblioteca.

OPICE, Blum, Bruno, Abrusio e Vainzof Advogados Associados. **Direito Digital Coletânea de Artigos**. 2017. Disponível em: <https://opiceblum.s3-sa-east-1.amazonaws.com/ColetaneaDireitoDigital.pdf>. Acesso em: 10 mai. 2020.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos**. 1948. Disponível em: <https://nacoesunidas.org/wp-content/uploads/2018/10/DUDH.pdf>. Acesso em: 25 abr. 2020.

PINHEIRO, Patricia Peck. Contratos digitais ou eletrônicos: apenas um meio ou uma nova modalidade contratual? **Revista dos Tribunais**. Brasil. vol. 966, abril.2016. Disponível em: <http://www.tjpa.jus.br/CMSPortal/VisualizarArquivo?idArquivo=340926>. Acesso em: 27 abr. 2020.

PINHEIRO, Patrícia Peck. **Direito digital**. 6. ed. São Paulo: Saraiva, 2016. E-book. Acesso restrito via Minha Biblioteca.

PINHEIRO, Patricia Peck. **Proteção de dados pessoais**: Comentários à Lei n. 13.709/2018 (LGPD). 2. ed. São Paulo: Saraiva Educação, 2020.

RAPOSO E SILVA, João Francisco. **Governança algorítmica e publicização das marcas: estudo de casos sob o paradigma da propagabilidade no ambiente numérico do Facebook**. 2018. 177 f. Dissertação (Mestrado). Programa de Pós-graduação em Ciências da Comunicação, Escola de Comunicações e Artes, Universidade de São Paulo, São Paulo, 2018. https://edisciplinas.usp.br/pluginfile.php/4601140/mod_resource/content/1/JoaoFranciscoRaposoSilva.pdf. Acesso em: 20 mai. 2020.

RIBEIRO, Cinthya Imano Vicente. **Privacidade digital das instituições bancárias**. 2019. 123 f. Dissertação (Mestrado em Direito) - Programa de Estudos Pós-Graduados em Direito, Pontifícia Universidade Católica de São Paulo, São Paulo, 2019. Disponível em: <https://tede2.pucsp.br/handle/handle/22990>. Acesso em: 15 abr. 2020.

RIBEIRO, Lígia Maria. **Algumas notas sobre a história da internet**. Curso de Engenharia da Universidade do Porto, abr. 1998. Disponível em: <https://paginas.fe.up.pt/~mgi97018/historia.html>. Acesso em: 10 abr. 2020.

ROCCO, Alfredo. **Princípios do direito comercial**. Campinas: LZN Editora, 2003, traduzido por Ricardo Rodrigues Gama, Título original: *Principios de derecho comercial*. E-book. Acesso restrito via Minha Biblioteca.

ROPPO, Enzo. **O contrato**. Tradução de Ana Coimbra e M. Januário C Gomes. Coimbra. Almedina, 2009, p. 73. E-book. Acesso restrito via Minha Biblioteca.

SANTOS, Manoel J. Pereira dos; ROSSI, Mariza Delapieve. Aspectos legais do comércio eletrônico: contrato de adesão. **Revista de Direito do Consumidor**. São Paulo: RT, n. 36: 105-129, out. /dez. 2000, p. 108. Disponível em: http://ead2.fgv.br/ls5/centro_rec/pag/textos/aspectos_legais_comercio_eletronico.htm. Acesso em: 18 abr. 2020.

SOUZA, Carlos Affonso; LEMOS, Ronaldo. **Marco civil da internet**: construção e aplicação. Juiz de Fora: Associada, 2016. E-book. Acesso restrito via Minha Biblioteca.

TEIXEIRA, Tarcisio. **Comercio eletrônico**: conforme o Marco Civil da Internet e a regulamentação do e-commerce no Brasil. São Paulo: Saraiva, 2015.

TEIXEIRA, Tarcisio. **Curso de direito e processo eletrônico**: doutrina jurisprudência e pratica. 2. Ed. Atual. E ampl. São Paulo: Saraiva, 2014, p. 131. E-book. Acesso restrito via Minha Biblioteca.

TEIXEIRA, Tarcisio. **Direito empresarial sistematizado**: doutrina, jurisprudência e prática. 2. ed. atual. e ampl. São Paulo: Saraiva, 2015. E-book. Acesso restrito via Minha Biblioteca.

VAINZOF, Rony; MALDONADO, Viviane Nobrega; BLUM, Renato Opice. **LGPD: Lei Geral de proteção de dados Comentada**. Coordenação. São Paulo: Thomson Reuters Brasil, 2019.

VERÇOSA, Haroldo Malheiros Duclerc. Agente fiduciário do consumidor em compras pela internet: um novo negócio nascido da criatividade mercantil. **Revista de Direito Mercantil, Industrial, Econômico e Financeiro**, n. 118, São Paulo: Malheiros, abr./jun. 2000, p. 90. Disponível em: <https://livros-e-revistas.vlex.com.br/vid/agente-fiduciario-do-consumidor-583095298>. Acesso em: 15 mar. 2020.

VERÇOSA, Haroldo Malheiros Duclerc. **Contratos mercantis e a teoria geral dos contratos**: o código civil de 2002 e a crise do contrato. São Paulo: Quartier Latin, 2010, p. 292-293. E-book. Acesso restrito via Minha Biblioteca.

ZULIANI, Ênio Santarelli. **Responsabilidade civil pelos vícios dos bens informáticos e pelo fato do produto**. In: SILVA, Regina Beatriz Tavares da; SANTOS, Manoel J. Pereira dos (Coords.). Responsabilidade civil na internet e nos demais meios de comunicação. São Paulo: 2012, p.370 (Série GVlaw). E-book. Acesso restrito via Minha Biblioteca.