

**UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
CENTRO DE CIÊNCIAS JURÍDICAS E ECONÔMICAS
FACULDADE DE DIREITO**

**A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS NO DIREITO DO
CONSUMIDOR E O AUMENTO DAS RELAÇÕES DE CONSUMO ON-LINE EM
DECORRÊNCIA DA PANDEMIA DE COVID-19**

BEATRIZ SOARES FERREIRA BRAGA

RIO DE JANEIRO

2021

BEATRIZ SOARES FERREIRA BRAGA

A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS NO DIREITO DO
CONSUMIDOR E O AUMENTO DAS RELAÇÕES DE CONSUMO ON-LINE EM
DECORRÊNCIA DA PANDEMIA DE COVID-19

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de Bacharel em Direito sob a orientação da Professora Dr^a. Daniela Silva Fontoura de Barcellos.

RIO DE JANEIRO

2021

CIP - Catalogação na Publicação

BB8131 Braga, Beatriz Soares Ferreira
A Lei Geral de Proteção de Dados Pessoais no
Direito do Consumidor e o aumento das relações de
consumo on-line em decorrência da pandemia de Covid
19 / Beatriz Soares Ferreira Braga. -- Rio de
Janeiro, 2021.
77 f.

Orientadora: Daniela Silva Fontoura de Barcellos.
Trabalho de conclusão de curso (graduação) -
Universidade Federal do Rio de Janeiro, Faculdade
Nacional de Direito, Bacharel em Direito, 2021.

1. Direito do Consumidor. 2. Dados Pessoais. 3.
E-commerce. 4. Covid-19. I. Barcellos, Daniela
Silva Fontoura de, orient. II. Título.

BEATRIZ SOARES FERREIRA BRAGA

A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS NO DIREITO DO
CONSUMIDOR E O AUMENTO DAS RELAÇÕES DE CONSUMO ON-LINE EM
DECORRÊNCIA DA PANDEMIA DE COVID-19

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de Bacharel em Direito sob a orientação da Professora Dr^a. Daniela Silva Fontoura de Barcellos.

Data da Aprovação: ___ / ___ / ___.

Banca Examinadora:

Daniela Silva Fontoura de Barcellos
Orientadora

Fabiana Rodrigues Barletta
Membro da Banca

Felipe Mendes
Membro da Banca

RIO DE JANEIRO

2021

AGRADECIMENTOS

Chegar até aqui é a realização de um sonho e o apoio de cada um de vocês foi essencial.

Agradeço, primeiramente, a Deus por mais essa conquista em minha vida.

À minha amada mãe Adriana, que venceu todas os obstáculos para me proporcionar as melhores oportunidades. Com todo o amor, me guiou pelo caminho da honestidade e da perseverança. Você é meu orgulho e minha inspiração, sem o seu apoio não seria possível.

Aos meus queridos avós, Maria Ranuzia e Evaldo, pelo amor incondicional e por cuidarem de mim com tanto carinho e dedicação. Sou eternamente grata por ter vocês.

Aos meus tios e primos, por todo amor e apoio dado durante toda a minha vida.

Ao Lucas, por ter sido compreensivo nos momentos de ausência e por nunca ter me deixado duvidar que seria capaz.

À Ana Lúcia, Denise, Márcia Revoredo e Marcia Calaza, sei que sempre posso contar com vocês.

Aos amigos da Procuradoria Federal, pela experiência e conhecimentos compartilhados.

À minha orientadora Prof^a. Dr^a. Daniela Silva Fontoura de Barcellos pela oportunidade e apoio na elaboração deste trabalho.

À Faculdade Nacional de Direito, todo meu orgulho e minha gratidão.

A todos que torcem e vibram pelas minhas conquistas, dedico mais esta à vocês.

E que esse seja o primeiro passo nessa longa jornada em busca de equidade e justiça.

RESUMO

A pandemia de Covid-19, que teve início em 2020, gerou a necessidade de isolamento social e a impossibilidade de acesso físico a diversos lugares. Com isso, o crescimento de compras e vendas on-line foi exponencial, tornando os dados pessoais ainda mais vulneráveis. Nesse contexto, este estudo teve como objetivo avaliar se a Lei Geral de Proteção de Dados Pessoais (LGPD) oferece meio efetivo de resguardos e limites a que se propôs os dados pessoais dos consumidores com o aumento do e-commerce impulsionado pela Covid-19. Com o propósito de atender a este objetivo, foi realizada uma pesquisa exploratória documental. Inicialmente contextualiza-se acerca da conjuntura dos dados pessoais e sua proteção como um direito fundamental, logo em seguida, as principais normativas no âmbito internacional e nacional em que envolve a matéria, explana-se sobre a pandemia de 2020 provocada pela Covid-19 no mundo e no Brasil e a mudança do comportamento do consumidor com o aumento das relações de consumo on-line e por fim, busca-se fazer uma análise dos principais tópicos da Lei Geral de Proteção de Dados Pessoais no direito do consumidor. A pesquisa permitiu apresentar que a LGPD abrange uma série de medidas que preservam os dados pessoais dos consumidores, sendo de grande importância que as organizações que exercem o e-commerce readequem as suas regras e os seus procedimentos para que possam atender o acréscimo da demanda virtual e preservar ou conquistar um bom prestígio no mercado. Logo, a LGPD é requisito para o Brasil prosseguir como participante de uma economia global.

Palavras-chave: covid-19; dados pessoais, e-commerce, direito do consumidor; LGPD.

ABSTRACT

The Covid-19 pandemic, which began in 2020, generated the need for social isolation and the impossibility of physical access to many places. As a result, the growth of online shopping was exponential, making personal data even more vulnerable. In this context, this study aimed to assess whether the Brazilian General Data Protection Law (LGPD) offers an effective means of safeguarding and limiting consumers' personal data with the increase in e-commerce driven by Covid-19. To attain the objective, an exploratory documentary research was carried out. Initially, it contextualizes the situation of personal data and your protection as a fundamental right, then the main international and national regulations about data privacy, explains about the coronavirus pandemic in the world and in Brazil and the change in consumer behavior with the increase of online consumer relationships and finally, seeks to analyze the main topics of the Brazilian General Data Protection Law in Consumer Law. The research allowed to show that the LGPD covers a series of measures that preserve the personal data of consumers, being of great importance that e-commerce companies readjust their rules and procedures to attend the increase of virtual demand and preserve or gain good prestige in the market. Therefore, the LGPD is a requirement for Brazil to continue as a participant in a global economy.

Keywords: covid-19, personal data, e-commerce, consumer law; LGPD.

LISTA DE QUADROS

Quadro 1 - Comparação entre a LGPD e o GDPR de definição e distinção do que são dados pessoais e dados sensíveis	20
--	----

LISTA DE FIGURAS

Figura 1 - Modelo de solicitação para o uso de cookies.....	59
Figura 2 - Controlador, Operador e Encarregado da Proteção de Dados	60

LISTA DE GRÁFICOS

Gráfico 1 - Percentual de consumidores realizando a primeira compra on-line	49
Gráfico 2 - Participação do comércio eletrônico nas vendas totais	50
Gráfico 3 - Volume mensal de vendas do varejo on-line no Brasil em 2020 (R\$ bilhões) ...	51
Gráfico 4 - Top 10 países, ranqueados pelo crescimento do varejo eletrônico em 2020	52

LISTA DE ABREVIATURAS E SIGLAS

ABComm Associação Brasileira de Comércio Eletrônico

APPI Act on the Protection of Personal Information

CCPA California Consumer Privacy Act

CDC Código de Defesa do Consumidor

CF Constituição Federal

CNC Confederação Nacional do Comércio de Bens, Serviços e Turismo

COVID 19 Coronavirus Disease 2019

GDPR General Data Protection Regulation

LAI Lei de Acesso à Informação

LCP Lei do Cadastro Positivo

LGPD Lei Geral de Proteção de Dados Pessoais

MCI Marco Civil da Internet

PIPEDA Personal Information Protection and Electronic Documents Act

OMS Organização Mundial da Saúde

SARS-CoV-2 Coronavírus da Síndrome Respiratória Aguda Grave 2

UTIs Unidades de Terapia Intensiva

SUMÁRIO

1	INTRODUÇÃO	14
2	DADOS PESSOAIS E SUA PROTEÇÃO COMO DIREITO FUNDAMENTAL	17
2.1	Definições de Dados Pessoais	17
2.2	A Proteção de Dados Pessoais como Direito Fundamental.....	21
3	PRINCIPAIS INSTRUMENTOS REGULATÓRIOS DA PROTEÇÃO DE DADOS PESSOAIS NO MUNDO E NO BRASIL.....	28
3.1	A proteção de dados pessoais no mundo	28
3.1.1	General Data Protection Regulation (GDPR).....	28
3.1.2	California Consumer Privacy (CCPA)	30
3.1.3	Personal Information Protection and Electronic Documents Act (PIPEDA)	32
3.1.4	Act on the Protection of Personal Information (APPI)	33
3.2	A proteção de dados pessoais no Brasil.....	35
3.2.1	Constituição Federal e legislações esparsas de proteção de dados pessoais no Brasil	35
3.2.1.1	Constituição Federal (1988)	36
3.2.1.2	Código de Defesa do Consumidor (Lei nº 8.078/90)	37
3.2.1.3	Código Civil (Lei nº 20.406/2002)	38
3.2.1.4	Lei do Cadastro Positivo (Lei nº 12.414/2011)	39
3.2.1.5	Lei de Acesso à Informação Pública (Lei nº 12.527/2011)	39
3.2.1.6	Marco Civil da Internet (Lei nº 12.965/2014).....	40
3.2.2	Lei Geral de Proteção de Dados (Lei nº 13.709/2018).....	41
4	MUDANÇA DO COMPORTAMENTO DO CONSUMIDOR MEDIANTE À PANDEMIA DE COVID-19.....	45
4.1	A pandemia provocada pelo COVID-19 no mundo e no Brasil	45
4.2	A mudança do comportamento do consumidor com o aumento das relações de consumo on-line	48
5	PRINCIPAIS ASPECTOS DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS NO DIREITO DO CONSUMIDOR	54

6	CONCLUSÃO.....	65
7	REFERÊNCIAS BIBLIOGRÁFICAS	69

1 INTRODUÇÃO

No Brasil, a proteção dos dados pessoais, que corresponde a toda e quaisquer informações que identifique ou que possa vir a identificar uma pessoa, é uma preocupação no ordenamento jurídico, já que possui status constitucional.

A Constituição Federal de 1988 dispõe em seu artigo 5º, inciso X, ser inviolável a intimidade, a vida privada, a honra e a imagem das pessoas; inciso XII, ser intocável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal; e por fim o inciso LXXII, assegura que um cidadão tenha acesso a dados e informações pessoais que estejam sob posse do Estado brasileiro, ou de entidades privadas que tenham informações de caráter público.

No âmbito infraconstitucional, destaca-se o Código de Defesa do Consumidor, Lei nº 8.078 de 11 de setembro de 1990, que basicamente estabelece uma série de direitos e garantias para o consumidor em relação às suas informações pessoais presentes em bancos de dados e cadastros.

De acordo com Doneda (2010, p.49):

O reconhecimento da proteção de dados como um direito autônomo e fundamental, portanto, não deriva de uma dicção explícita e literal, infere-se da consideração dos riscos que o tratamento automatizado traz à proteção da personalidade à luz das garantias constitucionais de igualdade substancial, liberdade e dignidade pessoal humana, juntamente com a proteção da intimidade e da vida privada.

A disseminação do mercado e do fomento de novas tecnologias, com o avanço da internet cada vez mais presente, faz-se imprescindível a particularização de conceitos como intimidade e privacidade diante da propagação acelerada de dados pessoais de um indivíduo, principalmente de dados pessoais de um consumidor, que passam a ser mais interessantes ao mercado, podendo ser utilizados para diversos fins, o deixando de certa forma vulneráveis.

Nesse novo cenário, surge a necessidade da defesa do consumidor proporcionar respostas a tal gravame, fornecendo proteção contra a utilização imprópria dessas informações por meio de instrumentos garantidores, limitadores e transparentes quanto à divulgação dos dados pessoais.

Dessa forma, a Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709, foi sancionada em agosto de 2018, estabelecendo uma série de obrigações para organizações com referência à coleta, à armazenamento, ao tratamento e ao compartilhamento de dados pessoais, tanto on-line quanto off-line.

Atualmente, a pandemia de coronavírus que se espalha por todo mundo gerou medidas de isolamento social, a fim de evitar a proliferação do Coronavirus Disease 2019 (Covid-19), doença infecciosa causada pelo novo coronavírus, identificado pela primeira vez em dezembro de 2019, em Wuhan, na China.

O estado de calamidade pública no Brasil foi estabelecido pelo Decreto Legislativo nº 06 de 20 de março de 2020, surgindo com determinações de isolamento social e impactando fortemente as relações de consumo. Os estabelecimentos foram fechados, com exceção daqueles estipulados pelas autoridades como essenciais, e conseqüentemente houve um aumento significativo no *e-commerce*, abreviação em inglês de comércio eletrônico, ou seja, toda transação comercial (compra e venda) realizada através da internet com a ajuda de um equipamento eletrônico. No atual cenário, com o objetivo de evitar frequentar locais públicos, o e-commerce ganhou força e passou a ser a melhor opção de venda, pois o consumidor recebe o seu produto em casa, com o menor contato físico possível, evitando, assim, o risco de contaminação pelo novo coronavírus.

Contudo, em virtude do aumento de consumo via Internet em decorrência da pandemia de Covid-19, o presente estudo busca resposta para o seguinte questionamento: a Lei Geral de Proteção de Dados Pessoais garante não somente mais segurança jurídica para os consumidores, como também para organizações empresariais, conciliando a proteção dos

direitos fundamentais individuais constitucionalmente protegidos, como a privacidade e a intimidade, com as atividades impulsionadas pela economia digital?

Para solucionar tal questionamento, inicialmente, contextualizar-se-á acerca da conjuntura dos dados pessoais e sua proteção como um direito fundamental, logo em seguida, as principais normativas no âmbito mundial em que envolve a matéria, assim como os instrumentos regulatórios brasileiros; expor-se-á sobre a pandemia de 2020 provocada pelo Covid-19 no mundo e no Brasil e a mudança do comportamento do consumidor com o aumento das relações de consumo on-line e por fim, buscar-se-á fazer uma análise dos principais tópicos da Lei Geral de Proteção de Dados Pessoais no direito do consumidor.

Cabe ressaltar a importância da análise do impacto da Lei Geral de Proteção de Dados Pessoais no direito do consumidor, em virtude principalmente do Brasil ter registrado um aumento expressivo das relações de consumo pela internet durante a pandemia de Covid-19. Espera-se com essa monografia colaborar para o desenvolvimento de pesquisas na área de Defesa do Consumidor, proporcionando um real progresso da ciência.

2 DADOS PESSOAIS E SUA PROTEÇÃO COMO DIREITO FUNDAMENTAL

A definição de dados pessoais é a primeira delimitação fundamental à qualquer disciplina que diz respeito a proteção destes dados.

2.1 Definição de Dados Pessoais

A partir do momento que a sociedade passa a ser conduzida por dados, estes se tornam um importante ativo financeiro capaz de guiar decisões estratégicas para os agentes do mercado, inclusive nas relações de consumo. Através de dados fidedignos sobre os consumidores é viável traçar um planejamento de produtos e vendas mais eficazes, ou ainda uma publicidade direcionada às reais características dos consumidores; na genética, possibilitam o mapeamento completo do genoma humano; em campanhas eleitorais, permitem a aferição de intenções de votos de acordo com cada perfil; na busca por relacionamentos, facilitam a identificação de pessoas com perfis compatíveis, entre inúmeras outras aplicações.

Nesse contexto, Carneiro (2020) expõe:

Ao navegar na internet, você deixa um “rastros”, uma série de “pegadas digitais”, como os sites que você visitou, as interações que você fez, quanto tempo ficou em determinada página, o que curtiu e descurtiu... E essa informação tem valor econômico. Quanto mais alguém sabe sobre o como você se comporta na internet, mais vai saber sobre seu perfil: seu gênero, sua orientação sexual, sua religião, sua orientação política, seu endereço, seu estado de saúde, profissão e muito mais. Empresas coletam estas informações através de vários mecanismos tecnológicos de vigilância e a partir dos dados obtidos, podem desenvolver modelos complexos para prever o comportamento dos consumidores e para extrair inferência potencialmente sensíveis sobre eles.

Acrescenta ainda Roque, Baptista e Rocha (2019, p.394):

Os dados pessoais, na sociedade contemporânea, assumem importância estratégica cada vez maior. Podem ser utilizados em inúmeras aplicações, como o direcionamento de propagandas e anúncios específicos para o perfil de determinado consumidor, com base nas páginas que este visita na internet, para a identificação de preferência ideológica ou mesmo sexual, mediante análise dos gastos realizados pelo cartão de crédito, ou para a investigação de doenças com maior probabilidade de se manifestarem durante a vida de determinado indivíduo, por meio da análise de seu material genético. Os exemplos são praticamente inesgotáveis e, cada vez mais, presentes no cotidiano – basta lembrar do seu smartphone, que sugere trajetos para o trabalho mesmo nos feriados.

Nesse sentido, o inciso I, do artigo 5º, da Lei nº 13.709/18, Lei Geral de Proteção de Dados Pessoais (LGPD), considera dado pessoal como: “informação relacionada a pessoa natural identificada ou identificável”. Essa informação permite individualizar o titular do dado, pessoa natural viva, através, por exemplo do nome, sobrenome, apelido, endereço residencial e CPF.

Para Mendes (2014): “Com relação ao conceito de dados pessoais, pode-se dizer que são os fatos, comunicações e ações que se referem a circunstâncias pessoais ou materiais de um indivíduo identificado ou inidentificável.”

Para maior entendimento, Matos e Ruzyk (2019, p.109) explicam o significado dos dados pessoais como informação relacionada a uma pessoa natural identificada ou identificável: “são abrangidas pelo conceito não apenas as informações sensíveis, mas, também, quaisquer outras informações pertinentes à pessoa, incluindo dados cadastrais, não sendo essencial para a definição de dados pessoais a precisa e definitiva identificação da pessoa.”

De acordo com Konder (2019, p.262):

A marca característica do dado pessoal, em geral, é a identificabilidade da pessoa natural a que ele se refere. Ou seja, o dado será considerado pessoal não somente se ele próprio servir a identificar o seu titular (por exemplo, o nome ou o número de CPF), mas também se, a partir da integração com outras informações, essa identificação for possível (por exemplo, o endereço ou o Internet Protocol - IP, o número que identifica o computador na rede). Sob esse conceito amplo de dado pessoal, há dado pessoal não apenas quando houver a presença de identificadores diretos ou indiretos que diferem precisamente um indivíduo. Os dados que potencialmente conduzem à individuação da pessoa são igualmente tomados como informação pessoal.

Nessa circunstância, acrescentam Menezes e Colaço (2019, p.77):

No conceito de dados, inclui até aquelas informações que não se prestam a identificar a pessoa quando usadas isoladamente (IP, faixa etária, altura etc), mas que poderão fazê-lo se conjugadas com outros dados, são portanto, identificáveis. Diferente do que chama de dado anonimizado que é aquele que não implicará, em definitivo, a identificação do seu titular, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

Pinheiro (2020) define dados pessoais:

Toda informação relacionada a uma pessoa identificada ou identificável, não se limitando, portanto, a nome, sobrenome, apelido, idade, endereço residencial ou eletrônico, 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. (grifo do autor)

Segundo Doneda (2010, p. 39) :

Os dados pessoais, por definição, representam algum atributo de uma pessoa identificada ou identificável e, portanto, mantém uma ligação concreta e viva com a pessoa titular destes dados. Os dados pessoais são a pessoa e, portanto, como tal devem ser tratados, justificando o recurso ao instrumental jurídico destinado à tutela da pessoa e afastando a utilização de um regime de livre apropriação e disposição contratual destes dados que não leve em conta seu caráter personalíssimo.

Oliva e Pessoa (2016) expõem:

Os dados pessoais devem ser integrados ao entendimento da própria construção da pessoa e de sua personalidade, como decorrência de não haver meio de serem dissociados referidos conceitos na atual sociedade pós-moderna de registros e classificações. Por esse motivo, necessário estender a conceituação da intimidade, para nele se incluir o controle dos dados pessoais e de suas formas de captação e de uso.

Portanto, para Doneda (2010, p.39):

A utilização sempre mais ampla de dados pessoais para as mais variadas atividades – identificação, classificação, autorização e tantas outras – torna tais dados elementos essenciais para que a pessoa possa se mover com autonomia e liberdade no que hoje costumamos denominar de Sociedade da Informação.

No Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho (General Data Protection Regulation - GDPR), item 1 do seu artigo 4º, entende-se por Dados Pessoais:

1) Dados pessoais, informação relativa a uma pessoa singular inidentificável (titular dos dados); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa singular.

Cumpra ressaltar que em relação a LGPD e o GDPR, “ambas as legislações têm como objetivo o regramento do tratamento de dados pessoais, buscando em si a defesa dos direitos fundamentais das pessoas naturais.” (PINHEIRO, 2021).

No Quadro 1 é apresentado a comparação de definição e distinção do que são dados pessoais e dados sensíveis entre a LGPD e o GDPR:

ITEM DE CONFORMIDADE	REGIME BRASILEIRO (LGPD)	REGIME EUROPEU (GDPR)
Definição e distinção do que são dados pessoais e dados sensíveis. Tal conceituação busca delimitar os direitos e as informações protegidas pelo ordenamento jurídico.	Define que dado pessoal é qualquer informação que identifique ou torne identificável a pessoa natural; já dados sensíveis são dados pessoais sobre etnia, raça, crenças religiosas, opiniões políticas, dados genéticos/biométricos, além de informações sobre filiações e organizações quaisquer da pessoa natural.	Adota os mesmos princípios e conceitos para realizar a distinção e delimitação dos direitos relativos aos dados pessoais e dados sensíveis, e ainda pontua considerações acerca dos dados genéticos, biométricos e os relativos à saúde.

Quadro 1 - Comparação entre a LGPD e o GDPR de definição e distinção do que são dados pessoais e dados sensíveis.

Fonte: Pinheiro (2021)

A LGPD, no seu inciso II, do artigo 5º, também trouxe a definição de dado pessoal sensível: “dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural”.

Explicam Tepedino e Teffé (2019, p.170):

Os dados denominados de sensíveis representam espécie de dado pessoal e se encontram presentes em todos os conjuntos informacionais do ser humano. Na LGPD, entendeu o legislador que a melhor forma de os proteger seria trazendo exemplos claros de dados assim considerados. Portanto, dados sensíveis versam sobre origem racial ou étnica, convicção religiosa, opinião política e filiação a sindicato ou a organização de caráter religioso, filosófico ou político. São também sensíveis aqueles referentes à saúde ou à vida sexual e dados genéticos ou biométricos.

Xavier, Xavier e Spaler (2019, p.286), com base na LGPD, apresentam:

Os dados pessoais sensíveis, segundo a literalidade da lei, são os que versam sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. Há hipóteses legais próprias que autorizam o tratamento de tais dados, que, apesar de estarem dispostas em seção própria da lei, muito se assemelham aos requisitos relativos ao tratamento de dados pessoais em sentido estrito. Entende-se que a proteção conferida a esses dados, considerados sensíveis, tem grande importância para evitar práticas discriminatórias em relação a grupos de indivíduos com características semelhantes.

Pinheiro (2020) também conceitua dados pessoais sensíveis:

São dados que estejam relacionados a características da personalidade do indivíduo e suas escolhas pessoais, tais como origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização de caráter religioso, filosófico ou político, dado referente a saúde ou a vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. (grifo do autor)

Doneda (2010, p.27) afirma:

Hoje, no entanto, o próprio conceito de dados sensíveis como fator que fundamenta uma proteção de nível mais elevado tende a ceder à noção de tratamento sensível de dados pessoais. Esta tendência provém do reconhecimento de que não é possível, hoje, prever os efeitos que um tratamento de dados pessoais possa causar ao seu titular apenas a partir da consideração da natureza dos dados que são tratados. Com as modernas técnicas estatísticas e de análise de dados, até mesmo informações pessoais que, em si, não são sensíveis podem causar tanto (i) um tratamento discriminatório em si, quanto (ii) a dedução ou inferência de dados sensíveis obtidos a partir de dados pessoais não-sensíveis. Em ambos os casos ocorre, efetivamente, justamente aquilo que se procura inibir com a criação de um regime especial para os dados sensíveis, que é a discriminação a partir do tratamento de dados pessoais.

Enfim, Xavier, Xavier e Spaler (2019, p.290) relatam:

Em um tempo em que dados pessoais passaram a orientar e ditar os rumos da sociedade, transformando-se em um valioso ativo que influencia e determina tomadas de decisões em diferentes setores, torna-se imprescindível avaliar os mecanismos voltados à proteção aos direitos fundamentais de privacidade e de liberdade de seus titulares.

2.2 Proteção de dados pessoais como Direito Fundamental

Um dos novos recursos do nosso tempo é a utilização dos dados pessoais em comércio, estatística, comunicação, marketing e tantas outras áreas, muitas empregam o

tratamento de dados pessoais para alcançar um determinado aumento de eficiência. O aumento de eficiência ocasionado pela utilização de dados pessoais deve ser equilibrado com a necessidade de proteger a pessoa, evitando que esta se submeta à devassa de sua privacidade, permitindo que mantenha intacta sua dignidade, integridade, autonomia e liberdade pessoal.

Carneiro (2020) menciona:

Diante desta geração e entrega voluntária de dados e informações, não podemos falar em um direito ao segredo, à privacidade em sentido estrito, pois isto é incompatível com a vida online, onde geramos e transferimos informações sobre nós o tempo todo, voluntariamente. No entanto, estas informações devem ser usadas de maneira responsável, para fins legítimos e da forma como autorizada pelo titular. As informações sobre localização que você cedeu para uma rede social não podem (pelo menos, não deveriam) ser usadas para, por exemplo, fazer ofertas diferentes de preço. Se antes o controle sobre as nossas informações era representado pelo trinômio “pessoa-informação-sigilo”, o eixo agora é composto por quatro elementos: “pessoa-informação-circulação-controle”. Ou seja, é preciso que nossos dados estejam protegidos e sua circulação seja controlada. O direito à proteção de dados pessoais angaria autonomia própria. É um novo direito da personalidade que não pode ser amarrado a uma categoria específica, em particular ao direito à privacidade. Pelo contrário, demanda-se uma correspondente ampliação normativa que clareie a sua tutela.

Neste sentido, a proteção de dados ganha relevo como um novo direito fundamental, que surge a partir de aumento do fluxo de informações pessoais na internet. Não apenas como um direito de manter seus dados em segredo (privacidade), mas também como o direito de o titular permitir, autorizar, retificar, solicitar exclusão, reduzir, e contestar o tratamento de suas informações pessoais por terceiros.

Segundo Doneda (2010, p.40):

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

Ainda sobre proteção de dados pessoais, Doneda (2010, p. 39) explica:

A proteção de dados pessoais é uma maneira indireta de atingir um objetivo último, que é a proteção da pessoa. Ao estabelecer um regime de obrigações para os responsáveis pelo tratamento de dados, bem como de direitos para os titulares destes, não se está meramente regulando um objeto externo à pessoa, porém uma representação da própria pessoa.

A importância da proteção de dados pessoais segundo Tepedino e Teffé (2019, p. 164):

A proteção dos dados pessoais compõe uma das partes essenciais da tutela da dignidade da pessoa humana, mostrando-se essencial para a garantia das liberdades fundamentais, da igualdade e da integridade psicofísica. O desenvolvimento de mecanismos destinados a regular o tratamento dos dados auxilia a evitar discriminações que não encontrem fundamento constitucional, como aquelas que possam dificultar o acesso ao crédito ou a empregos por determinados grupos. Além disso, afasta práticas que possam reduzir a liberdade e autonomia dos indivíduos, como decisões a partir de análises de dados não informadas ao titular e sob critérios não transparentes. A tutela dos dados relativos à pessoa natural mostra-se hoje vital para que ela se realize integralmente e se relacione na sociedade, representando garantia de maior segurança às informações dos cidadãos e impedindo práticas autoritárias e de vigilância por parte de instituições públicas e privadas.

No entanto, apesar de ser possível pleitear a tutela de dados pessoais baseado na proteção ao direito fundamental a partir dos incisos X, XII e LXXII do art. 5º da Constituição Federal à luz do princípio da dignidade da pessoa humana, esse mecanismo foi se apresentando pouco eficaz, demonstrando cada vez mais a necessidade de uma lei específica que conceda tanto segurança jurídica como garantias adequadas às partes.

Mendes (2014, p.235) expõe:

Sob as modernas condições de processamento de dados, a inviolabilidade da intimidade e da vida privada pressupõe a proteção do indivíduo contra a coleta, o armazenamento, o uso e a transmissão irrestrita de seus dados pessoais. Essa proteção é abrangida pelo direito fundamental do art. 5º, X, c/c o art. 5º, LXXII, da Constituição Federal (CF/88), à luz do princípio da dignidade da pessoa humana, de modo que atribui ao cidadão de controlar livremente a divulgação, transmissão e uso de seus dados pessoais, bem como garante o tratamento leal e lícito dos seus dados, conforme o princípio da boa-fé objetiva e da proteção das suas legítimas expectativas.

Tepedino e Teffé (2019, p.164) esclarecem:

No Brasil, até agosto de 2018, não se dispunha de lei específica para a proteção dos dados pessoais. Entretanto, sua tutela já poderia ser pleiteada com base em determinadas previsões estabelecidas na Constituição Federal, como a inviolabilidade da intimidade e da vida privada (art. 5º, X); a inviolabilidade do sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas (art. 5º, XII); e a ação de habeas data (art. 5º, LXXII). Como aponta a doutrina, o País já contava com mais de 40 normas que direta ou

indiretamente tratavam de questões relacionadas à privacidade e aos dados pessoais, como o Código de Defesa do Consumidor, o Marco Civil da Internet, a Lei de Acesso à Informação e a Lei do Cadastro Positivo. Todavia, esse arcabouço regulatório mostrava-se pouco preciso e não oferecia garantias adequadas às partes, o que, além de gerar insegurança jurídica, acabava tornando o País menos competitivo no contexto de uma sociedade cada vez mais movida a dados.

Nesse sentido, foi aprovada em 2018 a Lei Geral de Proteção de Dados Pessoais no Brasil (Lei 13.709/18 – LGPD) que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

No que concerne o direito à proteção de dados pessoais, Guedes e Meireles (2019, p.118) expressam:

O direito à proteção dos dados pessoais nasce como direito de defesa perante o Estado, mas atualmente encontra alcance em todos os espaços, públicos e privados. Chegou-se a afirmar que o potencial ofensivo do tratamento de dados pessoais pode se igualar ou mesmo exceder aquele representado pelo Estado. Importa assim, inicialmente, compreender qual o objeto dessa proteção. Os dados pessoais são projeções diretas da personalidade. Sendo assim, qualquer tratamento de dados, por influenciar na representação da pessoa na sociedade, pode afetar a sua personalidade e, portanto, tem o potencial de violar os seus direitos fundamentais.

O tratamento de dados é conceituado no art. 5º, inciso X, da Lei 13.709/2018:

X – tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Doneda (2010, p.39) expõe sobre o tratamento de dados:

O tratamento de dados pessoais, em particular por processos automatizados, é, no entanto, uma atividade de risco. Risco que se concretiza na possibilidade de exposição e utilização indevida ou abusiva de dados pessoais; na eventualidade destes dados não serem corretos e representarem erroneamente seu titular; em sua utilização por terceiros sem o conhecimento de seu titular, somente para citar algumas hipóteses reais. Daí a necessidade de mecanismos que proporcionem à pessoa efetivo conhecimento e controle sobre seus próprios dados, dados estes que são expressão direta de sua própria personalidade. **Por este motivo a proteção de dados pessoais é tida em diversos ordenamentos jurídicos como um instrumento essencial para a proteção da pessoa humana e é considerada como um direito fundamental.** (grifo nosso)

Conforme Schreiber (2019, p.218):

A proteção dos dados pessoais é certamente um dos mais sensíveis desafios que o direito contemporâneo enfrenta, em decorrência do extraordinário avanço tecnológico verificado nas últimas décadas. No Brasil, a proteção de dados pessoais encontra seu fundamento normativo na Constituição da República, que proclama no inciso X do artigo 5º a inviolabilidade da intimidade e da vida privada. Doutrina e jurisprudência reconhecem que o direito à privacidade abrange, hoje, não apenas a proteção à vida íntima do indivíduo, mas também a proteção de seus dados pessoais, alcançando qualquer ambiente no qual circulem dados de uma pessoa humana. É certo que, longe de representar “informações sem dono” livremente coletáveis na internet, esse conjunto de dados exprime uma abrangente projeção da personalidade humana, exigindo firme proteção da ordem jurídica.

A Constituição Federal de 1988 estatui em seu inciso X do artigo 5º:

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

X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.

Doneda (2010, p.49) explica:

No ordenamento brasileiro, o reconhecimento da proteção de dados como um direito autônomo e fundamental não deriva de uma dicção explícita e literal, porém da consideração dos riscos que o tratamento automatizado traz à proteção da personalidade à luz das garantias constitucionais de igualdade substancial, liberdade e dignidade da pessoa humana, juntamente com a proteção da intimidade e da vida privada.

Acrescenta, ainda, Doneda (2011):

A proteção de dados pessoais no ordenamento brasileiro não se estrutura a partir de um complexo normativo unitário. A Constituição Brasileira contempla o problema da informação inicialmente por meio das garantias à liberdade de expressão e do direito à informação, que deverão eventualmente ser confrontados com a proteção da personalidade e, em especial, com o direito à privacidade. Além disso, a Constituição considera invioláveis a vida privada e a intimidade (art. 5º, X), veja-se especificamente a interceptação de comunicações telefônicas, telegráficas ou de dados (artigo 5º, XII), bem como instituiu a ação de habeas data (art. 5º, LXXII), que basicamente estabelece uma modalidade de direito de acesso e retificação dos dados pessoais. Na legislação infraconstitucional, destaque-se o Código de Defesa do Consumidor, Lei 8.078/90, cujo artigo 43 estabelece uma série de direitos e garantias para o consumidor em relação às suas informações pessoais presentes em “bancos de dados e cadastros”.

Carneiro (2020) expõe:

A afirmação de um direito fundamental à privacidade e à proteção de dados pessoais deriva, ao contrário, de uma compreensão integrada do texto constitucional lastreada (i) no direito fundamental à dignidade da pessoa humana, (ii) na concretização do compromisso permanente de renovação da força normativa da proteção constitucional à intimidade (art. 5º, inciso X, da CF/88) diante do espraiamento de novos riscos derivados do avanço tecnológico e ainda (iii) no reconhecimento da centralidade do Habeas Data enquanto instrumento de tutela material do direito à autodeterminação informativa.

O tratamento de dados pessoais e a sua proteção como um fenômeno mundial praticado, conforme apresenta Menezes e Colaço (2019, p.77):

Uma vez que o tratamento de dados pessoais é um fenômeno mundial praticado, a proteção desses dados também tem merecido atenção especial e muitos países tem reconhecido novas dimensões do direito à privacidade como o direito à autodeterminação informativa, assim considerado como a faculdade de o indivíduo decidir, por si só, sobre a exibição e o uso de seus dados pessoais. A totalidade dessas informações que circulam sobre a pessoa acaba por configurar um verdadeiro corpo virtual – extensão da personalidade que deve receber idêntica proteção.

No item 4 das considerações do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho (General Data Protection Regulation - GDPR) estabelece:

(4) O direito à proteção de dados pessoais não é absoluto; deve ser considerado em relação à sua função na sociedade e ser equilibrado com outros direitos fundamentais, em conformidade com o princípio da proporcionalidade. O presente regulamento respeita todos os direitos fundamentais e observa as liberdades e os princípios reconhecidos na Carta, consagrados nos Tratados, nomeadamente o respeito pela vida privada e familiar, pelo domicílio e pelas comunicações, a proteção dos dados pessoais, a liberdade de pensamento, de consciência e de religião, a liberdade de expressão e de informação, a liberdade de empresa, o direito à ação e a um tribunal imparcial, e a diversidade cultural, religiosa e linguística.

Sobre a privacidade, Oliveira e Lopes (2019, p.26) explanam:

No Brasil, pode-se considerar que a privacidade há muito é objeto de proteção tanto pela legislação ordinária – a Lei do Habeas Data, Código Civil, a Lei de Arquivos Públicos, o Código de Defesa do Consumidor, a Lei de Acesso à Informação, Lei do Cadastro Positivo e, mais recentemente, o Marco Civil da Internet – como constitucional – inciso X do art. 5º. Não obstante, uma legislação específica sobre a proteção de dados foi muito desejada por nossos juristas e necessária do ponto de vista de uma estratégia internacional.

Cueva (2019, p.50) acrescenta, ainda, sobre a privacidade:

Logo, a privacidade hoje, longe de se restringir à intimidade e ao direito de ser deixado só, ampliou seus domínios para abranger o controle sobre as informações que digam respeito ao sujeito, a autodeterminação informativa, o direito à não discriminação, a liberdade, a igualdade, o direito ao acesso e acompanhamento dos dados pessoais quando se tornam objeto de disponibilidade de outros, dentre outros.

No que refere-se à defesa da privacidade, Tepedino e Teffé (2019, p.166) dizem:

A defesa da privacidade deve também integrar os controles individuais e coletivos de proteção aos direitos fundamentais. Quando se controla o tratamento de dados, não se resguarda apenas o indivíduo cujos dados estão relacionados, mas também o grupo social do qual ele faz parte, interesses coletivos e as futuras gerações. Nesse sentido, entende-se que também às coletividades devem ser garantidos meios jurídicos, técnicos e sociais que aumentem seu poder e controle sobre os dados.

Em suma, a proteção de dados pessoais é vista em diversos ordenamentos jurídicos e doutrinas como um instrumento fundamental para a proteção da pessoa humana e como um direito fundamental.

3 PRINCIPAIS INSTRUMENTOS REGULATÓRIOS DA PROTEÇÃO DE DADOS PESSOAIS NO MUNDO E NO BRASIL

A proteção dos dados pessoais passou por diversas evoluções, e isso deve-se ao fato do direito à privacidade, dos avanços socioeconômicos e tecnológicos e da inserção das relações na sociedade da informação, portanto surge a necessidade de aprimorar essa proteção, fazendo com que o mundo passasse a regulamentar a matéria.

Segundo Souza Neto (2020, p. 47) :

Assim, a adoção de leis de proteção de dados em vários países demonstra que a temática já faz parte de um movimento internacional. Isto enseja um enorme ganho para a toda sociedade, vez que possibilita que a internet seja uma ferramenta cada vez mais integrada, colaborativa e participativa, sem que seja necessário a fragmentação da rede para se preservar direitos fundamentais como o direito a privacidade dos usuários-cidadãos, o que, feito de outra maneira, poderia comprometer o gozo de outros direitos, como o direito à liberdade de informação e de expressão, por exemplo.

3.1 - A proteção de dados pessoais no mundo

Proteção de dados é um assunto relativamente novo no Brasil, mas na Europa e em outros países a segurança de dados já é prática comum.

Algumas das principais leis de proteção de dados pessoais no mundo são:

- **Europa : General Data Protection Regulation (GDPR)**
- **Califórnia: California Consumer Privacy Act (CCPA).**
- **Canadá: Personal Information Protection and Electronic Documents Act (PIPEDA)**
- **Japão: Act on the Protection of Personal Information (APPI)**

3.1.1 - General Data Protection Regulation (GDPR)

A atual lei da União Européia é a **General Data Protection Regulation (GDPR)** que representa o Regulamento Geral sobre a Proteção de Dados da Europa, criado em 2016, com início de vigência em 25 de maio de 2018.

Souza Neto (2020, p. 26) expõe sobre o início das tratativas da proteção aos dados pessoais na União Europeia:

As tratativas de proteção aos dados pessoais têm seu início a partir da segunda metade do século XX. Foi no Conselho da Europa, durante sessões ocorridas em 1967 e 1968, que a temática da vulnerabilidade do direito à privacidade dos cidadãos frente aos novos avanços tecnológicos teve início.

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

Proteção de dados é um assunto relativamente novo no Brasil, mas na Europa o tema é discutido desde 1940. Na década de 1970, surgiu a primeira geração de normas de proteção de dados na Europa, como a Lei de Dados da Suécia (1973) e a Lei Federal de Proteção de Dados da Alemanha (1977). As leis europeias foram evoluindo nas últimas quatro décadas em busca de devolver ao titular do dado o poder da autodeterminação informativa, que concede a ele o controle sobre o compartilhamento ou não de seus dados pessoais. Essa evolução culminou na recente lei europeia de proteção de dados, conhecida como RGPD – Regulamento Geral de Proteção de Dados que entrou em vigor em maio de 2018.

Nos itens 6 e 7 das considerações do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho (General Data Protection Regulation - GDPR) estabelece a importância de se ter uma norma eficaz de proteção de dados:

6. A rápida evolução tecnológica e a globalização criaram novos desafios em matéria de proteção de dados pessoais. A recolha e a partilha de dados pessoais registaram um aumento significativo. As novas tecnologias permitem às empresas privadas e às entidades públicas a utilização de dados pessoais numa escala sem precedentes no exercício das suas atividades. As pessoas singulares disponibilizam cada vez mais as suas informações pessoais de uma forma pública e global. As novas tecnologias transformaram a economia e a vida social e deverão contribuir para facilitar a livre circulação de dados pessoais na União e a sua transferência para países terceiros e organizações internacionais, assegurando simultaneamente um elevado nível de proteção dos dados pessoais.

7. Esta evolução exige um quadro de proteção de dados sólido e mais coerente na União, apoiado por uma aplicação rigorosa das regras, pois é importante gerar a confiança necessária ao desenvolvimento da economia digital no conjunto do mercado interno. As pessoas singulares deverão poder controlar a utilização que é feita dos seus dados pessoais. Deverá ser reforçada a segurança jurídica e a segurança prática para as pessoas singulares, os operadores económicos e as autoridades públicas.

Os principais pontos-chaves que constituem a GDPR, enfatizando a relevância dessa regulamentação em um negócio e indicando as obrigações gerais da empresa (DocuSign, 2018):

1. A disponibilização obrigatória da identidade e do contato do controller, que consiste na companhia que estabelece os meios e as finalidades de processamento de dados.
2. O fornecimento dos contatos da corporação de data protection, que é o responsável pela supervisão da estratégia e a implantação da proteção de dados, garantindo a conformidade com as especificações normativas da GDPR.
3. O detalhamento ao usuário sobre quais informações serão coletadas, de que forma acontecerá a sua utilização, as razões do processamento de dados e os fundamentos legais para isso.
4. A listagem dos destinatários dos dados armazenados, caso haja.
5. A apresentação do período de tempo em que uma determinada informação ficará armazenada ou, se não houver possibilidade, o critério empregado para determinar esse espaço temporal necessário
6. A explicitação das principais consequências da ausência de disponibilização de dados.
7. A especificação do tipo de base de informações – se uma fonte pública, isto é, em que a coleta não é feita diretamente do usuário, ou privada.
8. A concessão do direito ao cliente de corrigir, sempre que necessário, as informações que foram inicialmente fornecidas.
9. A atribuição do direito de o usuário, a qualquer momento, retirar o seu consentimento para a empresa processar os seus dados.
10. A proteção específica quanto à coleta de dados mais sensíveis, como aqueles que indicam convicções filosóficas ou religiosas, origem étnica ou racial, dados genéticos e biométricos, orientação sexual, opiniões políticas, condições de saúde e filiação sindical.
11. O tratamento de dados de um indivíduo menor de 16 anos somente nos casos de consentimento expresso pelo titular de sua responsabilidade parental.

Em suma, a entrada em vigor da GDPR na Europa, continente mais avançado do mundo quando o assunto são leis de proteção de dados, proporcionou um impulso para que outros países buscassem também uma legislação mais apropriada com o mundo atual.

3.1.2 - California Consumer Privacy Act (CCPA)

A **California Consumer Privacy Act (CCPA)** é a lei de proteção de dados pessoais do estado da Califórnia, nos Estados Unidos. Esta lei entrou em vigor a partir de 01 de Janeiro de 2020.

A Gatefy (2021) expõe sobre a California Consumer Privacy Act (CCPA):

Como o próprio nome sugere, a California Consumer Privacy Act (CCPA) é uma lei de proteção de dados da Califórnia, nos Estados Unidos. Ela reúne regras que devem ser seguidas por empresas que lidam com dados pessoais. A CCPA surgiu no embalo da GDPR (General Data Protection Regulation), a regulamentação europeia, e na necessidade da Califórnia de proteger melhor os seus residentes, visto que não há uma única lei geral de proteção de dados no país.

A CCPA foi aprovada em 2018 e entrou em vigor em janeiro de 2020. Em suma, a principal mudança que a lei traz é que os cidadãos da Califórnia têm mais direitos sobre os seus dados. Em outras palavras, a lei concede às pessoas os direitos de acessar dados, de saber como eles são usados e de proibir o uso deles.

A CCPA procura garantir os seguintes direitos para os consumidores da Califórnia (AWS, 2021):

- O direito de os californianos saberem quais informações pessoais estão sendo coletadas sobre eles.
- O direito de os californianos saberem se suas informações pessoais são vendidas ou divulgadas, e para quem.
- O direito de os californianos não autorizarem a venda de informações pessoais.
- O direito de os californianos acessarem suas informações pessoais.
- O direito de os californianos terem o mesmo atendimento e pagarem o mesmo preço, mesmo que exerçam seus direitos de privacidade.

É uma das leis de proteção de dados mais abrangentes dos Estados Unidos e é extremamente imprescindível conhecer as principais obrigações trazidas pela CCPA.

A BL Consultoria Digital (2020) apresenta as principais obrigações abordadas pela CCPA:

- Publicar uma Política de Privacidade que esteja em conformidade com as regras da CCPA e seja atualizada pelo menos uma vez a cada 12 meses;
- Informar aos consumidores sobre o que acontece com seus dados pessoais ou informações de identificação pessoal quando compartilhados com a empresa;
- Manter um mapeamento de dados (data mapping) para rastrear o histórico de processamento de dados;
- Notificar o consumidor antes ou no momento da coleta de dados sobre o desejo da empresa ter permissão para coletar esses dados;
- Conceder aos consumidores o direito de acessar os dados pessoais que estão sob custódia da empresa;
- Explicar como os consumidores podem fazer uma solicitação para que a empresa exclua seus dados pessoais (em outras palavras, o direito de ser esquecido); e
- Garantir que os consumidores conheçam seus direitos sob o CCPA.

Portanto, esses procedimentos visam garantir e preservar a privacidade e a proteção de dados dos consumidores californianos.

3.1.3 - Personal Information Protection and Electronic Documents Act (PIPEDA)

A **Personal Information Protection and Electronic Documents Act (PIPEDA)** é a lei do Canadá para proteção à privacidade de dados pessoais dos canadenses. Em vigor desde 2001, permite que cada estado do Canadá tenha sua própria lei de privacidade de dados pessoais, desde que sejam similares com a PIPEDA.

No que concerne à lei do Canadá para a proteção à privacidade de dados pessoais, AWS (2021) coloca que:

A PIPEDA é uma lei federal canadense que se aplica à coleta, ao uso e à divulgação de informações pessoais durante o exercício de atividades comerciais em todas as províncias do Canadá, conforme complementação por leis regionais de privacidade substancialmente semelhantes em Alberta, Colúmbia Britânica e Quebec. A PIPEDA também se aplica a transferências internacionais e interregionais de informações pessoais.

Acrescenta, ainda, Dalmaso (2020) sobre a PIPEDA:

A PIPEDA tem como propósito regulamentar o uso e a divulgação de informações pessoais (informações sobre um indivíduo identificável) de uma maneira que reconheça o direito à privacidade dos indivíduos com relação a suas informações pessoais e a necessidade das organizações de coletar, usar ou divulgar informações pessoais para fins, que uma pessoa consideraria razoavelmente apropriada. Essa última informação é de suma importância pois o tratamento dos dados necessita de um propósito razoável.

A PIPEDA opera sobre dez princípios de boas práticas a serem seguidos pelas empresas, González (2021) enumera:

- as empresas são responsáveis pelos dados pessoais que coletaram e que usam;
- é preciso identificar claramente os propósitos por trás de uma coleta de dados;
- é preciso ter o consentimento do titular para coleta, uso e compartilhamento de seus dados, salvo exceções previstas por lei;

- podem ser coletados somente os dados necessários dentro do propósito informado;
- os dados solicitados podem ser usados, divulgados e mantidos pela empresa apenas da maneira informada e enquanto cumprirem os propósitos;
- as informações pessoais devem ser verídicas e mantidas atualizadas;
- os dados devem ser protegidos sob medidas adequadas de acordo com a sensibilidade das informações;
- a organização precisa fornecer amplamente informações claras e detalhadas sobre suas políticas e práticas de segurança e proteção de dados;
- o titular dos dados tem o direito de receber informações sobre a existência de tratamentos de suas informações, assim como questionar se seus dados são verídicos e estão completos;
- o titular dos dados tem o direito de questionar as organizações que tratam e coletam suas informações pessoais, dentro dos nove princípios anteriores.

Em síntese, os principais procedimentos da PIPEDA são de suma importância para às questões de privacidade e de proteção de dados dos canadenses.

3.1.4 - Act on the Protection of Personal Information (APPI)

O Japão teve sua primeira lei de proteção de dados criada em 2003. A **Act on the Protection of Personal Information (APPI)** foi atualizada em 2015 e teve as novas regras aplicadas a partir de 2017.

No que refere-se a lei de proteção de dados do Japão, Novaes (2020) expõe:

O primeiro contato do Japão com uma lei que regulamenta o tratamento de dados pessoais se deu com a adoção da Act on the Protection of Personal Information (APPI) em 2003. Dessa forma, o APPI se estabelece como uma das primeiras regulamentações de proteção de dados na Ásia.

A lei sofreu significativa reforma em setembro de 2015, após que uma série de violações de dados no Japão serem trazidas à público, deixando claro que os requisitos da lei não atendiam mais às necessidades atuais de proteção de dados do país. O APPI, então remodelado, entrou em vigor em 30 de maio de 2017, um ano antes do GDPR.

A APPI contém preceitos básicos para a proteção de dados pessoais, menciona González (2021):

A APPI traz regras sobre compartilhamento de dados com terceiros, manutenção de informações em bancos de dados, anonimização de dados e vazamentos, estabelecendo diretrizes para proteger os titulares. Por causa da nova legislação, o Japão foi incluído na “lista branca” da União Europeia de países com leis adequadas de proteção de dados.

Quanto à aplicabilidade da lei de proteção de dados do Japão, Novaes (2020) cita:

A lei é aplicável a todas as empresas que processam dados pessoais para fins comerciais, mesmo àquelas com bancos de dados enxutos. Organizações governamentais centrais, governos locais, agências administrativas independentes e agências administrativas locais incorporadas, que se enquadram no escopo de outros regulamentos, estão isentos do cumprimento da APPI.

A APPI é utilizada em duas espécies de dados, Durbano (2020) define:

A regulamentação é aplicada em dois tipos de dados, as informações pessoais e as informações que requerem cuidados especiais. Assim como na União Europeia, empresas que não tratem os dados dos japoneses de forma adequada também podem sofrer sanções.

No país, os cidadãos têm o direito de pedir a revisão e a exclusão de seus dados se acharem necessário. Assim como também poderá ser possível no Brasil com a Lei Geral de Proteção de Dados (LGPD).

Novaes (2020) esclarece o que são “informações pessoais” e “informações que requerem cuidados especiais”:

A APPI estabelece duas categorias distintas de dados: informações pessoais e informações pessoais que requerem “cuidados especiais”. A primeira hipótese se refere a informações de identificação pessoal como nome, data de nascimento, e-mail ou dados biométricos. Já a segunda, configura-se como uma nova categoria introduzida na lei após a remodelação, que se refere a dados que possam vir a causar tratamentos discriminatórios ou preconceituosos. Histórico médico, estado civil, raça, crenças religiosas e antecedentes criminais são exemplos desta nova categoria da APPI.

Resumindo, a APPI é uma legislação ampla a ponto da União Europeia considerar o país oriental totalmente adequado quanto à proteção de dados.

Por fim, o mundo vivenciou período de inexistente ou reduzida normatização a respeito do uso de dados pessoais. No entanto, considerando a intensificação de usos de dados

e os efeitos negativos provenientes de usos abusivos, modelos regulatórios têm sido elaborados capazes de limitar as falhas no desempenho dos agentes de mercado e da atividade de instituições públicas, proporcionando melhor fluxo de informações, mais segurança nas transações e relações cada vez mais complexas. É nessa circunstância que muitos países ao redor do mundo implementaram ou aprimoraram sua legislação sobre proteção de dados.

3.2 - A proteção de dados pessoais no Brasil

A proteção de dados pessoais no Brasil é matéria de preocupação dos legisladores há algumas décadas. A regulamentação inicialmente deu-se por meio de legislações esparsas, que não abordavam a matéria com a profundidade suficiente, culminando finalmente na Lei Geral de Proteção de Dados (LGPD), sancionada em 14 de agosto de 2018.

3.2.1 - Constituição Federal e legislações esparsas de proteção de dados pessoais no Brasil

Antes da LGPD não existia no Brasil uma legislação específica sobre proteção de dados pessoais, a matéria era regulada pela Constituição Federal e por leis esparsas, conforme apresenta Porto (2019, p. 6):

No Brasil, a Constituição de 1988 tem previsto no artigo 5, inciso X, o direito fundamental à intimidade e a vida privada. Há também leis ordinárias que tutelam a privacidade e proteção de dados, das quais podemos citar o Código de Defesa do Consumidor (lei n.º 8.078/90), o Código Civil (lei n.º 10.406/2002), a Lei do Cadastro Positivo (lei n.º 12.414/2011), Lei de Acesso a Informação Pública (lei n.º 12.527/2011), Marco Civil da Internet (lei n.º 12.965/2014) dentre outras.

Somente em 2012 foi proposto na Câmara o projeto de lei n.º 4.060, o qual regulou especificamente o tratamento de dados pessoais. Em 2013, é proposto no Senado o projeto de Lei n.º 330/2013, que tinha como tema a proteção, tratamento e o uso de dados pessoais. Em 2016, após consulta pública feita pelo Ministério da Justiça e, impulsionado pela aprovação do Regulamento Geral de Proteção de Dados europeu, é instaurado o PL n.º 5.276/2016 na Câmara, que acaba sendo apensado ao PL n.º 4.060/2012. Em 2017, estavam em tramitação no Congresso Nacional dois projetos relativos privacidade e proteção de dados: o PL 5.276/2016 na Câmara e o PLS 330/2013 no Senado. Os Projetos de Lei foram unificados no Projeto de Lei Complementar n.º 53/2018 que resultou na Lei Geral de Proteção de Dados Pessoais.

3.2.1.1 - Constituição Federal (1988)

A Constituição abrange as normas gerais e abstratas para a proteção dos dados pessoais no Brasil, como direitos fundamentais a intimidade, a vida privada, a honra e a imagem das pessoas, bem como o sigilo de correspondência e comunicações telegráficas, de dados e comunicações telefônicas, além de um dos meios processuais adequados para o exercício dos direitos de conhecimento e retificação de dados pelo titular, o habeas data.

A proteção dos dados pessoais na Constituição Federal é exposta por Souza Neto (2020, p. 32):

Antes mesmo da aprovação da Lei Geral de Proteção de Dados (BRASIL, 2018), a tutela da matéria já era prevista em nossa Magna Carta, a qual, assim como faz a Carta dos Direitos Fundamentais da União Europeia, consagra a privacidade como um direito fundamental em seu art. 5º, inciso X (BRASIL, 1988), tutelando de igual modo a inviolabilidade do sigilo das correspondências, das comunicações telegráficas, dos dados e das comunicações telefônicas (art. 5º, inciso XII). A proteção conferida no inciso XII aos dados em tráfego não se refere à tutela dos dados pessoais. Estes estão protegidos de forma genérica pelo inciso X do art. 5º da Constituição Federal.

Souza (2019, p. 246) relata sobre o habeas data na Constituição Federal:

O habeas data, segundo o artigo 5º, LXXII, será ainda concedido “para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público” e para a retificação de dados.

Ainda sobre a proteção de dados pessoais, Souza (2019, p. 246) divulga:

A partir da tutela prevista na Constituição, coube a outros dispositivos na legislação infraconstitucional detalhar o regime de aplicação da proteção de dados, ora dotando-a de medidas práticas para prevenir o dano ou responsabilizar o autor de um ilícito, bem como garantindo ao titular de dados pessoais uma série de deveres.

Exemplos de outros dispositivos que tratam da proteção de dados pessoais, além da Constituição Federal: o Código de Defesa do Consumidor (lei n.º 8.078/90), o Código Civil (lei n.º 10.406/2002), a Lei do Cadastro Positivo (lei n.º 12.414/2011), a Lei de Acesso a Informação Pública (lei n.º 12.527/2011) e o Marco Civil da Internet (lei n.º 12.965/2014).

3.2.1.2 - Código de Defesa do Consumidor (Lei n.º 8.078/90)

O Código de Defesa do Consumidor (CDC) concede alguns direitos de privacidade para acessar e corrigir dados do consumidor, ou seja, garante aos consumidores o acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre a suas respectivas fontes.

Souza Neto (2020, p.34) pronuncia sobre o Código de Defesa do Consumidor:

Em 1990 foi aprovado o Código de Defesa do Consumidor. A legislação, voltada para regular as relações de consumo e proteger o consumidor, foi por muito tempo responsável por suprir as lacunas em decorrência da ausência de um marco normativo para a proteção dos dados pessoais, impondo limites ao fornecedor quanto ao uso indiscriminado das informações pessoais do consumidor.

A Relação de Consumo é aquela na qual existe um consumidor, um fornecedor e um produto ou serviço. Portanto, para haver essa relação é indispensável a presença dos três elementos, concomitantemente.

O Código de Defesa do Consumidor (CDC), no caput do artigo 2º define que “Consumidor é toda pessoa física ou jurídica que adquire ou utiliza produto ou serviço como destinatário final”, e no caput do artigo 3º do CDC estabelece que “Fornecedor é toda pessoa física ou jurídica, pública ou privada, nacional ou estrangeira, bem como os entes despersonalizados, que desenvolvem atividade de produção, montagem, criação, construção, transformação, importação, exportação, distribuição ou comercialização de produtos ou prestação de serviços.”

Quanto ao Produto e Serviço, o CDC estabelece em seus parágrafos 1º e 2º do artigo 3º que:

Art. 3º [...]

§1º Produto é qualquer bem, móvel ou imóvel, material ou imaterial.

§2º Serviço é qualquer atividade fornecida no mercado de consumo, mediante remuneração, inclusive as de natureza bancária, financeira, de crédito e securitária, salvo as decorrentes das relações de caráter trabalhista.

A comunicação entre a LGPD e o CDC, segundo Cardoso (2020, p.11):

O Código de Defesa do Consumidor (Lei nº 8.078/90) contém as primeiras normas sobre a regulação da formação dos bancos de dados no Brasil. Com a entrada em vigor da Lei Geral de Proteção de Dados, o CDC deve ser aplicado em conjunto para reger especificamente as práticas de tratamento de dados pessoais nas relações de consumo. O diálogo das fontes entre a LGPD e o CDC para a regulação da obtenção, tratamento e proteção de dados nas relações de consumo (entre outras atividades relacionadas aos dados pessoais) deve ser, na prática, a combinação de normas legais mais utilizada.

3.2.1.3 - Código Civil (Lei n.º 10.406/2002)

O Código Civil garante a privacidade como direito da personalidade, direito que regulamento os aspectos mais essenciais e relevantes da personalidade humana.

Schreiber (2019, p.2018) discorre sobre o artigo 21 do Código Civil:

[...] embora verse sobre a proteção à privacidade em termos amplos, representa, a rigor, uma inútil duplicação do que já afirma a própria Constituição da República. Diante da insuficiência dessas disposições, os esforços para a construção sistemática de um direito à proteção de dados pessoais no Brasil acabaram recaindo sobre a doutrina. Tais esforços, associados a uma bem-sucedida estratégia de articulação política e à confluência de fatores externos, conduziram, não sem algum atraso, à aprovação da Lei 13.709/2018, a Lei Geral de Proteção de Dados Pessoais.

O diálogo entre LGPD e o Código Civil, Cardoso (2020, p.17) profere:

Apesar de não ser, no aspecto temporal, a primeira norma analisada nas interações da LGPD com outras leis de Direito Privado na proteção dos dados pessoais (porque o CDC regulou anteriormente a matéria, na tutela dos consumidores), o Código Civil é a norma geral das relações jurídicas privadas no país.

Portanto, nas relações jurídicas entre pessoas naturais e pessoas jurídicas de direito privado acerca da proteção de dados pessoais, em primeiro lugar deve ser avaliada a aplicação conjunta da LGPD com o Código Civil. Na sequência, caso se trate de relação de consumo, passa-se ao exame das normas do Código de Defesa do Consumidor incidentes ao caso.

O Código Civil (Lei nº 10.406/2002) é a norma básica e geral das relações jurídicas privadas no país, o que significa que é a lei que rege a vida das pessoas naturais e das pessoas jurídicas de direito privado, do nascimento até a morte. Especificamente para as pessoas naturais (titulares dos dados pessoais), a maior parte dos direitos e obrigações que tiver ao longo de sua vida será regulada por pelo menos um dispositivo do Código Civil.

Por isso, as suas normas também devem ser utilizadas na regulação da obtenção e do tratamento de dados pessoais, em conjunto com a Lei Geral de Proteção de Dados.

3.2.1.4 - Lei do Cadastro Positivo (Lei n.º 12.414/2011)

A Lei do Cadastro Positivo prevê a criação de bancos de dados com informações relativas a adimplimento do indivíduo cadastrado para a formação de histórico de crédito.

Souza Neto (2020, p.34) relata sobre a Lei do Cadastro Positivo:

Contados mais de duas décadas desde a aprovação do CDC, adveio a Lei nº 12.414/2011, denominada de Lei do Cadastro Positivo (BRASIL, 2011), legislação que instituiu o banco de dados sobre bons pagadores. A lei surgiu como contraponto aos cadastros negativos de crédito e, em sua versão original, exigia o consentimento do consumidor para que seus dados financeiros e comerciais pudessem ser analisados pelas agências a fim de pontuar e classificar o seu nível de adimplimento, de modo a influenciar no acesso ao mercado de consumo e em futuras disponibilizações de linhas de crédito.

Cardoso (2020, p.30) também expõe sobre a Lei do Cadastro Positivo:

A Lei do Cadastro Positivo (LCP – Lei nº 12.414/2011, derivada da Medida Provisória nº 518/2010) foi elaborada com o objetivo principal de ampliar o acesso ao crédito e reduzir os encargos dos contratos bancários, a partir da análise completa do histórico dos clientes, levando em consideração não apenas a inadimplência anterior, mas especialmente a adimplência das pessoas em suas relações anteriores com as instituições financeiras.

Assim, além de eventual inscrição em cadastro negativo, os usuários (pessoas naturais ou jurídicas) dos serviços bancários são inscritos em cadastros positivos, que são bancos de dados mantidos pelas instituições financeiras contendo uma pontuação ou nota de cada pessoa, baseada em sua situação econômica e nas relações e contratações realizadas no sistema bancário (ou seja, o histórico de crédito).

3.2.1.5 - Lei de Acesso à Informação Pública (Lei n.º 12.527/2011)

A Lei de Acesso à Informação já considerava informação pessoal aquela relacionada à pessoa natural identificada ou identificável e regulamentava o tratamento de dados feito em especial pela Administração Pública.

A Lei de Acesso à Informação segundo Cardoso (2020, p.54):

Além das leis anteriores, que se aplicam principalmente a relações jurídicas de Direito Privado, a LGPD também mantém um diálogo com leis de Direito Público, entre as quais se destaca a Lei de Acesso à Informação (Lei nº 12.527/2011), regulamentada pelo Decreto nº 7.724/2012. A Lei de Acesso à Informação (LAI) foi

editada com o objetivo principal de permitir a publicidade, a abertura e o acesso amplo de dados e de informações da Administração Pública à sociedade, com fundamento nos direitos à informação de interesse particular ou coletivo (art. 5º, XXXIII, da Constituição) e de acesso dos usuários aos registros administrativos e a informações sobre atos de governo (art. 37, § 3º, II, da Constituição), e nos deveres da Administração Pública de gestão da documentação governamental e de adoção das providências necessárias para permitir a consulta dos documentos públicos pelos interessados e por quem necessitar de seu uso (art. 216, § 2º, da Constituição).

A LAI tem como destinatários todos os entes da Administração Pública direta e indireta da União, dos Estados, do Distrito Federal e dos Municípios. Na Administração direta, abrange o Executivo, o Legislativo (inclusive os Tribunais de Contas), o Judiciário e o Ministério Público.

Além disso, a LAI contém uma regulação (parcial) do tratamento de dados pessoais dos administrados pelos entes públicos, a partir da regra de proteção das informações sigilosas e dos dados pessoais (art. 6º, III) e das regras de tratamento de dados previstas no Decreto nº 7.724/2012. Em resumo, a LAI e o decreto referido autorizam que os dados armazenados em registros públicos sejam divulgados aos titulares, seus sucessores e até mesmo à sociedade. Com isso, permitiu o aumento da transparência na prestação de informações pela Administração Pública, o que facilita o exercício de direitos e as atividades de fiscalização.

3.2.1.6 - Marco Civil da Internet (Lei n.º 12.965/2014)

Marco Civil da Internet disciplina o uso da internet no Brasil e dispõe sobre a proteção da privacidade e de dados pessoais, ou seja, o marco regula o processamento de dados pessoais, incluindo a obtenção, armazenamento, retenção, processamento e transferência de dados pessoais.

Souza Neto (2020, p.35) expressa sobre o Marco Civil da Internet:

Um marco no avanço da tutela dos dados pessoais de forma ampla e genérica no Brasil se deu com a aprovação e sanção do Marco Civil da Internet (MCI), em 2014. Tal legislação foi fruto de um processo em que se garantiu a ampla participação da sociedade civil por meio de debates. O projeto de lei teve como referência as recomendações do Comitê Gestor da Internet.

Acrescenta, ainda, Cardoso (2020, p. 103) sobre Marco Civil da Internet:

O Marco Civil da Internet (Lei nº 12.965/2014 – MCI) é a lei que contém os parâmetros de uso da internet no país, por meio da definição de princípios e regras e, de modo mais específico, das relações jurídicas (direitos e deveres) de usuários e provedores de serviços de internet (conexão e aplicações) no Brasil.

O MCI contém uma regulação do tratamento de dados pessoais mais específica em comparação com as leis existentes até então [...], mas se restringe aos dados obtidos por meio da internet.

Em 2016 foi aprovado o decreto regulamentador do Marco Civil da Internet, que é o Decreto nº 8.771/2016, que trata especialmente da neutralidade de rede e da segurança da informação, com critérios técnicos a ser observados por quem realiza o tratamento de dados na internet, principalmente com padrões para a guarda desses dados.

Os três principais fundamentos do Marco Civil da Internet são a neutralidade de rede, a privacidade online e a fiscalização dos acessos.

O Marco Civil da Internet é o ato normativo que mais se aproxima da Lei Geral de Proteção de Dados e que, por isso, manterá um diálogo frequente com ela na proteção de dados na rede mundial de computadores. Apenas os dados pessoais tratados em meio externo à internet (e que não tenham alguma etapa do tratamento realizado por meio dela) não exigirão a interpretação e aplicação conjunta da LGPD e do MCI.

Em síntese, o Brasil já contava com inúmeras regulamentações que direta ou indiretamente tratavam de questões relacionadas à proteção de dados pessoais, tais como: Constituição Federal, Código de Defesa do Consumidor, Código Civil, Lei do Cadastro Positivo, Lei de Acesso à Informação e Marco Civil da Internet, como foi visto anteriormente.

Todavia, esse arcabouço regulatório mostrava-se pouco preciso e não oferecia garantias adequadas às partes, o que, além de gerar insegurança jurídica, acabava tornando o Brasil menos competitivo no contexto de uma sociedade cada vez mais movida a dados. Sendo assim, foi criada em agosto de 2018, a Lei Geral de Proteção de Dados (LGPD) do Brasil.

3.2.2 - Lei Geral de Proteção de Dados (Lei nº 13.709/2018)

O Brasil, a partir de 14 de agosto de 2018, passou a fazer parte dos países que contam com uma legislação específica para proteção de dados e da privacidade e intimidade dos seus cidadãos, a Lei Geral de Proteção de Dados (LGPD). Esta foi inspirada no General Data Protection Regulation (GDPR), de 27 de abril de 2016, regulamento europeu relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação destes dados. A LGPD é um grande avanço para a proteção dos direitos fundamentais do cidadão brasileiro na sociedade da informação.

A importância da criação da Lei Geral de Proteção de Dados (LGPD), segundo Tepedino e Teffé (2019, p. 165):

A partir do desenvolvimento de tecnologias cada vez mais sofisticadas para o tratamento de dados, da maior aplicação da inteligência artificial em sistemas e processos e da ampliação da capacidade de armazenamento de informações, mostrou-se urgente a edição e a atualização de normas para tratar de maneira mais específica as questões enfrentadas no que concerne à proteção da privacidade e dos dados pessoais, especialmente no que tange aos dados sensíveis e aos dados de crianças e adolescentes.

Souza (2019, p. 248) expõe sobre a LGPD:

A Lei Geral de Proteção de Dados é marco regulatório que estabelece as diretrizes para o tratamento de dados pessoais, inclusive nos meios digitais, realizado por pessoa natural ou por pessoa jurídica de direito público ou privado. Dessa forma, ela supera os entraves que poderiam existir na aplicação de legislações setoriais, que ora se voltam para relações de consumo, ora apenas para as relações travadas por meio da Internet.

“É inegável que a lei veio em momento necessário, em sincronia com posicionamento internacional de inevitável regulação do tratamento de dados pessoais” (MATOS; RUZYK, 2019, p. 114).

Murad e Requena (2019, p. 360) mencionam os parâmetros da LGPD:

A promulgação da LGPD tem como principal norte a tutela da privacidade, liberdade e autodeterminação informativa da pessoa humana, direitos em alta posição na ordem constitucional brasileira que se encontram notoriamente afetados pelo progresso tecnológico. Assim, a LGPD promove avanço no marco legal, cujas bases foram instituídas com a Lei do Habeas Data e com o Marco Civil da Internet (MCI) – e, em alguma extensão, por meio do Código de Defesa do Consumidor.

A LGPD foi motivada pelo Modelo Europeu de Proteção de Dados, a GDPR, Tepedino e Teffé (2019, p. 165) mostra a semelhança entre a LGPD e a GDPR:

A Lei Geral de Proteção de Dados brasileira e o Regulamento Geral Europeu sobre a Proteção de Dados 2016/679 (General Data Protection Regulation – GDPR) representam no contexto atual instrumentos para a proteção e garantia da pessoa humana, uma vez que facilitam o controle dos dados tratados, impõem deveres e responsabilidades aos agentes de tratamento e proporcionam segurança para que as informações circulem. Os dois sistemas encontram-se fortemente alinhados, como desejou o legislador brasileiro, para que a norma nacional, nos próximos anos, seja reconhecida como adequada ao sistema europeu, uma vez que isso facilitará a realização de transações e cooperações com países do bloco.

A LGPD adota as premissas e fundamentos necessários para que a proteção dos dados seja instrumento de preservação dos direitos fundamentais, como também, da autonomia

informativa, do controle sobre a informação e das questões relacionadas à igualdade e à própria liberdade, a fim de contornar, dentro do possível, os efeitos nefastos de um capitalismo cada vez mais baseado na vigilância e na opacidade (FRAZÃO, 2019).

Quanto ao impacto da LGPD, Tepedino e Teffé (2019, p.166) abordam:

O impacto da LGPD será efetivo nos mais diversos setores da sociedade, trazendo direitos aos titulares e deveres e responsabilidades aos agentes de tratamento. Todos os sujeitos terão que se adaptar a uma nova cultura de tutela dos dados pessoais, cabendo à doutrina, ao Judiciário e à autoridade nacional de proteção de dados harmonizarem a interpretação e aplicação da Lei.

Souza Neto (2020, p. 38) divulga o alcance da LGPD:

Assim como o regulamento europeu, a LGPD atinge a todos os setores da economia, sendo aplicável a entidades públicas e privadas, e possui efeito até mesmo extraterritorial, isto porque a norma é aplicável a qualquer operação de tratamento que seja efetuada por pessoa natural ou pessoa jurídica de natureza pública ou privada, independentemente do meio, do país de sua sede ou do país em que estejam localizados os dados, desde que: (I) a operação de tratamento tenha se realizado em território nacional; (II) a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; (III) os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

Os requisitos para o tratamento de dados pessoas na LGPD:

A LGPD cria regras para a coleta, uso, armazenamento e tratamento de dados pessoais. Ela afeta as mais diversas relações - de comércio, de serviços, trabalhistas, ou seja, qualquer relação que implique o uso dessas informações dentro ou fora do Brasil. Há, no entanto, exceções, como em caso de segurança nacional e pública; pesquisa pura, fins artísticos e jornalísticos.

A lei determina o tratamento especial para dados como número de identidade, CPF ou e-mail. Além desses códigos que identificam as pessoas, ela também cria a figura do dado pessoal sensível que envolve a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato, religião ou partido político. Ela resguarda também os dados referentes a saúde, vida sexual, dado genético ou biométrico (FUNCEF, 2020).

Resumindo, a LGPD aborda sobre diversos pontos fundamentais, a HASA (2019) destaca alguns pontos:

Aplicação

Abrange diversos setores, e vale tanto na esfera pública quanto privada, seja online ou offline. Além disso, assim com a GDPR, tem validade extraterritorial, então qualquer empresa estrangeira que oferecer serviços ao Brasil precisará se adequar às regras.

Conceito de dados pessoais

Estabelece de forma clara o conceito, tanto dos dados pessoais quanto dos dados pessoais sensíveis (aqueles que podem deixar seus titulares a mercê de práticas discriminatórias). Todos estes dados estarão sujeitos à regulação.

Princípios gerais de proteção e tratamento de dados

Proporciona mais transparência no tratamento e utilização dos dados pessoais. A lei estabelece 10 princípios definidos que precisam ser considerados no tratamento dos dados. Além disso, todo o tratamento precisa necessariamente ter um fundamento legal.

Direito dos titulares e responsabilidade dos agentes

Proporciona mais transparência, pois lista todos os direitos dos titulares dos dados. Por sua vez, os agentes responsáveis pelo tratamento podem ser penalizados por uso indevido de informações ou incidentes relacionados a segurança da informação.

Órgão fiscalizador

A lei estabelecerá a criação de uma autoridade pública denominada Autoridade Nacional de Proteção de Dados (ANPD), que fará o papel de uma agência reguladora e de fiscalização, que terá papel fundamental para garantir a aplicação e vigência da nova lei.

Por fim, possivelmente grande parte das pessoas já tiveram seus dados tratados indevidamente e/ou vazados em determinada circunstância de vulnerabilidade de alguma instituição. Tal constatação aumenta a necessidade por regulamentos nacionais e internacionais voltadas aos novos desafios tecnológicos e que assegurem tanto mecanismos adequados para a proteção e reparação das pessoas quanto deveres e responsabilidades próprias para todo aquele que desempenhar o tratamento de dados pessoais.

Por essa razão, foi criada a LGPD, com a enunciação de princípios, direitos, responsabilidades e demais aplicações decorrentes do tratamento de dados pessoais, mas a lei não detém a exclusividade no tratamento do tema da proteção de dados pessoais, sendo o mesmo igualmente inserido em outros diplomas legais, como exemplo: Constituição Federal, Código de Defesa do Consumidor, Código Civil, Lei do Cadastro Positivo, Lei de Acesso à Informação e Marco Civil da Internet, o que caracteriza a importância do diálogo entre essas diversas fontes, com a finalidade de assegurar a unidade do sistema, bem como o reconhecimento de que a LGPD concede eixo valorativo que facilitará a interpretação e a aplicação das demais legislações na problemática da proteção de dados, portanto um importante avanço da ordem jurídica de nosso país na proteção dos direitos fundamentais de seus cidadãos.

4 MUDANÇA DO COMPORTAMENTO DO CONSUMIDOR MEDIANTE À PANDEMIA DE COVID-19

A pandemia mundial de 2020 provocada pelo COVID-19 impactou o mercado de produtos de consumo provocando uma mudança de hábito nos consumidores.

4.1 A pandemia provocada pelo COVID-19 no mundo e no Brasil

Em 11 de março de 2020, a Organização Mundial da Saúde (OMS) declarou o novo coronavírus como uma pandemia mundial. Na época, o vírus já havia se espalhado por 114 países. De acordo com o dicionário *Priberam*, pandemia é o “surto de uma doença com distribuição geográfica internacional muito alargada e simultânea”. Em outras palavras, a OMS define pandemia como a disseminação mundial de uma nova doença e explica que o termo passa a ser usado quando uma epidemia, surto que afeta somente uma região, se espalha por diferentes continentes com transmissão sustentada de pessoa por pessoa.

O vírus Sars-CoV-2, o novo coronavírus causador da doença COVID-19, foi identificado pela primeira vez em dezembro de 2019 na cidade de Wuhan, na província de Hubei, na China. Logo o vírus começou a se espalhar e, ainda em janeiro, casos foram notificados em vários países asiáticos e até mesmo nos Estados Unidos.

Com o aumento repentino dos casos, alguns países se tornaram o epicentro da pandemia, sendo a China o primeiro deles. Em março de 2020, a Itália passou a ser o epicentro fora do continente asiático. Em abril do mesmo ano, os Estados Unidos registram um grande número de casos e se tornam o novo epicentro da pandemia. Em maio, o Brasil foi apontado. Já em outubro, a Europa era considerada o epicentro novamente. Mais recentemente, em março do 2021, o Brasil tornou-se mais uma vez o epicentro da doença, juntamente com a Índia a partir de abril de 2021.

Como primeiro epicentro do novo coronavírus, a China agiu rapidamente após a identificação dos casos de COVID-19. Conseguiram, inclusive, zerar os novos casos locais da

doença no país por um tempo, passando a serem monitorados individualmente. Para isso, foram aplicadas grandes campanhas de testagem e medidas de distanciamento social. A cidade de Wuhan, por exemplo, ficou em lockdown por 76 dias, a partir de 23 de janeiro de 2020. A circulação de pessoas entre uma região e outra do país também foi limitada e diversas cidades determinaram que apenas um dos membros da família tinha permissão de sair para comprar os itens essenciais durante o período de isolamento social. No dia 1 de setembro de 2021, a China contabilizava 123.068 casos de Covid-19 e foram registradas 5.683 mortes pela doença desde o início da pandemia (WHO, 2021).

A partir de março de 2020, depois da China, a Itália era o país com o maior número de casos de coronavírus. Entre os dias 9 e 11 de março de 2020, foram decretadas pelo governo italiano as primeiras medidas de distanciamento social com o intuito de frear a disseminação do vírus colocando em quarentena 16 milhões de pessoas na região da Lombardia, que inclui as cidades de Milão e Veneza. Logo em seguida, novas medidas restritivas foram anunciadas pelo Primeiro-ministro italiano Giuseppe Conte, entre elas, o fechamento de todos os estabelecimentos não essenciais, chamando a crise de saúde pública como a maior crise que o país já enfrentou desde a Segunda Guerra Mundial.

Em poucas semanas, o sistema de saúde italiano entrou em colapso, o que fez com que os outros países europeus se atentassem para a gravidade da doença e o quão importante são as medidas preventivas, como restrições de viagens e de circulação, para diminuir os índices de contágio e evitar a sobrecarga em seus sistemas de saúde. No dia 1 de setembro de 2021, a Itália contava com cerca de 4.539.991 casos confirmados de Covid-19, sendo que 129.221 pessoas morreram desde o início da pandemia no país (WHO, 2021).

Em seguida, o epicentro da pandemia passou a ser os Estados Unidos. Em 21 de janeiro de 2020 foi registrado o primeiro caso de coronavírus no país. Em fevereiro do mesmo ano, a Covid-19 foi declarada como uma emergência nacional pelo governo Trump e, em março de 2020, já era considerada uma emergência nacional. O número de casos cresceram muito rápido e, em 28 de maio de 2020, a marca de 100.000 mortos pelo vírus Sars-CoV-2 foi ultrapassada.

Na época, para tentar achatar a curva de contágio, o governo fez um apelo para que a população aderisse as recomendações estatais de distanciamento social, higiene das mãos e uso de máscara, prática que muitas pessoas nos Estados Unidos recusavam-se a fazer. Em contrapartida à população chinesa que aderiu à prática rapidamente por experiências passadas, como o surto do Sars-CoV em 2002 na Ásia causado por outro tipo de coronavírus. No dia 1 de setembro de 2021, o país contava com 38.923.013 casos contabilizados da doença e era o líder em mortes com um total de 634.320 vidas perdidas para a Covid-19 (WHO, 2021).

Em maio de 2020, o Brasil se tornou o epicentro da pandemia. O primeiro caso confirmado do coronavírus foi em 26 de fevereiro. No mesmo mês, o Ministério da Saúde declarou Emergência em Saúde Pública de Importância Nacional, alegando ser um evento complexo que demanda esforço conjunto de todo o Sistema Único de Saúde (SUS). No entanto, as medidas de restrição e isolamento estavam sendo aplicadas de forma descentralizada no país até que, no dia 15 de abril de 2020, o Supremo Tribunal Federal (STF) determinou que, além do governo federal, o governo dos estados e municípios também teriam o poder para definir as suas medidas de isolamento e de quarentena. Desde então, medidas estão sendo aplicadas pelos governos estaduais para o controle da proliferação do vírus.

No início de maio de 2020, o número de pessoas infectadas pelo coronavírus já ultrapassava os 100.000, com 7.000 mortes registradas. Já em junho do mesmo ano, o Brasil atingiu a marca de 1 milhão de casos confirmados e cerca de 60.000 mortos pela Covid-19. No mês seguinte, já eram mais de 2.660.000 milhões de brasileiros infectados pelo vírus Sars-CoV-2 e mais de 90.000 mortos pelas complicações da doença. Em dezembro do mesmo ano, o sistema de saúde de Manaus ficou tão sobrecarregado que faltou oxigênio nas unidades de internação da região.

Assim, em 2021, o sistema de saúde do Brasil entrou em colapso. Em março, a ocupação nas unidades de terapia intensiva (UTIs) dos hospitais do país era de mais de 90%, ultrapassando, inclusive, os 100% em 3 estados: Mato Grosso (104,2%), Mato Grosso do Sul (102%) e Rondônia (100%). Isso significa que nesses estados os pacientes precisavam

aguardar pela internação mesmo apresentando sintomas graves da doença. No dia 6 de abril de 2021, 4.211 brasileiros perderam a vida para a Covid-19, o dia com mais mortes registradas no país durante toda a pandemia. No mês seguinte, o Brasil se tornou o terceiro maior país com casos confirmados no mundo com 15.003.353 de casos e o segundo maior no número de mortes registradas pela Covid-19 com 416.949 mortes. Em 1 setembro de 2021, o Brasil registava 20.752.281 casos confirmados de coronavírus e um total de 579.574 mortes (WHO, 2021).

Agora, com mais de 190 países atingidos pela pandemia, inclusive estações da Antártida, de acordo com a Organização Mundial da Saúde (OMS), fica claro que o mundo está diante de um processo de intensa transformação. A pandemia da Covid-19 instaurou uma crise nunca antes vista na história recente da humanidade, além das milhões de vidas perdidas para a doença, presenciamos o mais rígido distanciamento social da história, o qual confinou as pessoas e transformou definitivamente a rotina diária e empresarial exercidas até então.

Paradoxalmente, efeitos positivos podem ser extraídos desse momento atípico que estamos passando. A crise gerada pela pandemia mundial provocada pela COVID-19 impulsionou o fenômeno da transformação digital. As medidas estatais de isolamento e fechamento ou redução de frequência dos estabelecimentos empresariais, promoveram grandes mudanças de ordem estrutural nas organizações econômicas empresariais, forçando a aceleração do processo de digitalização nos seus modelos de negócios e, conseqüentemente, elevando o consumo digital.

4.2 A mudança do comportamento do consumidor com o aumento das relações de consumo on-line

No cenário atual, frente à pandemia de Covid-19, houve um grande avanço no número de compras pela internet, aumentando as relações de consumo on-line. Com a necessidade das pessoas permanecerem em suas casas para o cumprimento das recomendações de isolamento social, muitas empresas foram obrigadas a migrar para o *e-commerce* como medida de manutenção de suas atividades durante a pandemia, o que alavancou a expansão do comércio

eletrônico que já apresentava uma trajetória de crescimento ao longo dos últimos 5 anos.

Com o fechamento das lojas físicas em muitas cidades, houve uma mudança no comportamento de compra dos brasileiros que já pôde ser sentida em alguns setores logo nas primeiras semanas de isolamento social. De acordo com o Compre&Confie, o *e-commerce* brasileiro faturou R\$ 9,4 bilhões em abril, aumento de 81% em relação ao mesmo período do ano passado. Com 24,5 milhões de pedidos feitos no mês, 98% a mais em relação a abril de 2019, o novo coronavírus acelerou vendas de setores ainda pouco explorados no comércio eletrônico (saúde, alimentos e bebidas) e consolidou produtos que já eram comuns nos carrinhos (eletrônicos e brinquedos).

Essa migração para o *e-commerce* se deu tanto com compradores já habituados às compras on-line quanto com os que nunca haviam experimentado esse canal. A Associação Brasileira de Comércio Eletrônico (ABComm) estima que 20,2 milhões de consumidores realizaram pela primeira vez uma compra pela internet em 2020. De acordo com uma pesquisa da Infobase Interativa, desde o início da pandemia, 13% dos brasileiros fizeram compras pela internet pela primeira vez, 24% passaram a realizar mais compras on-line e 52% consumiram mais conteúdos pela internet. Inclusive, a tendência é que essas pessoas que tiveram suas primeiras experiências com o *e-commerce*, adaptados à comodidade do comércio eletrônico, consumam de forma mais recorrente e busquem produtos em diversas categorias.

O número de brasileiros que realizaram a primeira compra on-line apresenta um crescimento acima da média desde o mês de março de 2020, como mostra o Gráfico 1.

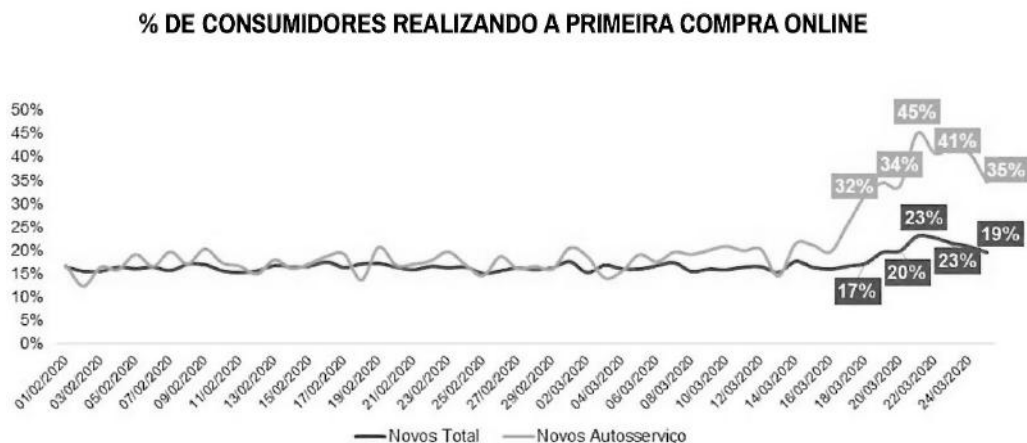


Gráfico 1 – Percentual de consumidores realizando a primeira compra on-line

Fonte: Ebit | Nielsen - Novos consumidores e-commerce Brasil - Total E-commerce e Total Autosserviço - 01/02 a 06/04

Com o aumento da demanda em razão da pandemia de Covid-19 e com o aumento do número de empresas que passaram a integrar o comércio eletrônico, o setor de *e-commerce* registrou um salto recorde em 2020. De acordo com a Associação Brasileira de Comércio Eletrônico (ABComm), entre os dias 23 de março e 31 de maio de 2020, por exemplo, houve o surgimento de 107 mil novas lojas on-line no Brasil. Isto significa quase um novo *e-commerce* a cada minuto durante este período.

Com isso, segundo o levantamento da ABComm, em parceria com a Neotrust, o crescimento nas vendas foi de 68% na comparação com 2019, elevando a participação do *e-commerce* no faturamento total do varejo, que passou de 5% no final de 2019 para um patamar acima de 10% em alguns meses do ano passado. Foram mais de 301 milhões de compras pela internet, com um valor médio de R\$ 419, segundo o balanço.

PARTICIPAÇÃO DO COMÉRCIO ELETRÔNICO NAS VENDAS TOTAIS

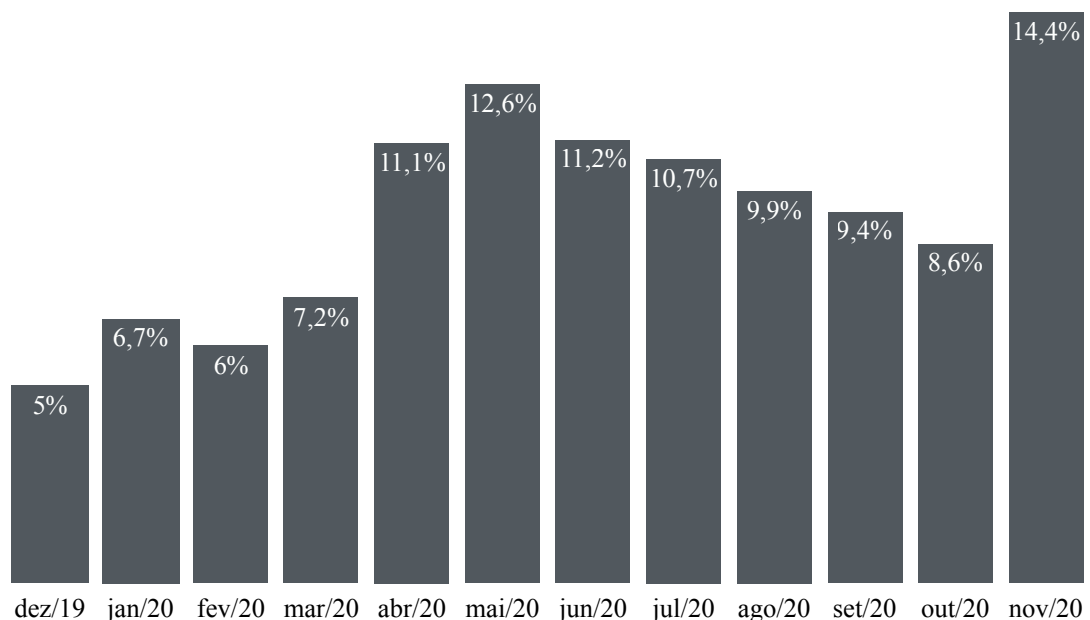


Gráfico 2 - Participação do comércio eletrônico nas vendas totais
Fonte: ABComm

Outro recorde alcançado pelo comércio eletrônico em 2020 foi quanto ao faturamento total. Segundo a Confederação Nacional do Comércio de Bens, Serviços e Turismo (CNC), dados da Receita sobre notas fiscais eletrônicas mostram que o faturamento real do *e-commerce*, descontada a inflação, avançou 37% em comparação com 2019, totalizando o valor recorde de R\$ 224,7 bilhões no ano passado. Como mostra o gráfico abaixo:

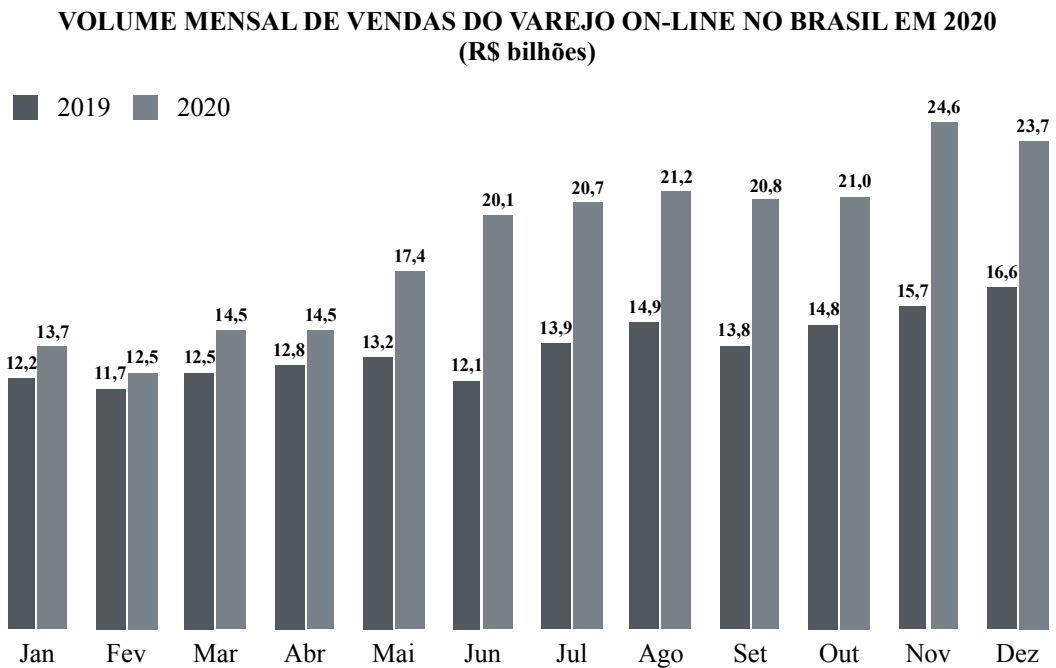


Gráfico 3 - Volume mensal de vendas do varejo on-line no Brasil em 2020 (R\$ bilhões)
Fonte: CNC

O grande crescimento das vendas on-line somada ao maior número de empresas que passaram a integrar o comércio eletrônico e a digitalização da sociedade brasileira foram os motivos pelos quais o Brasil alavancou na lista de países com os *e-commerce* mais bem desenvolvidos. É o que mostra a pesquisa da eMarketer, que compara o “top 10” países que tiveram o maior número de vendas por *e-commerce* nos últimos meses.

Nota-se que o Brasil aparece em sétimo lugar, à frente do Reino Unido, Tailândia e Espanha, mas ainda atrás de outros países do continente americano, como Canadá, Argentina e México. Vale destacar que a média de crescimento global é de 25,7%, ao passo que a média de crescimento do Brasil ficou em torno de 50,1%, quase o dobro. Em território nacional, a maior parte dos acessos é feito por meio do smartphone, em algum site de busca ou pelas redes sociais.

**TOP 10 PAÍSES , RANQUEADOS PELO CRESCIMENTO DO VAREJO
ELETRÔNICO EM 2020**

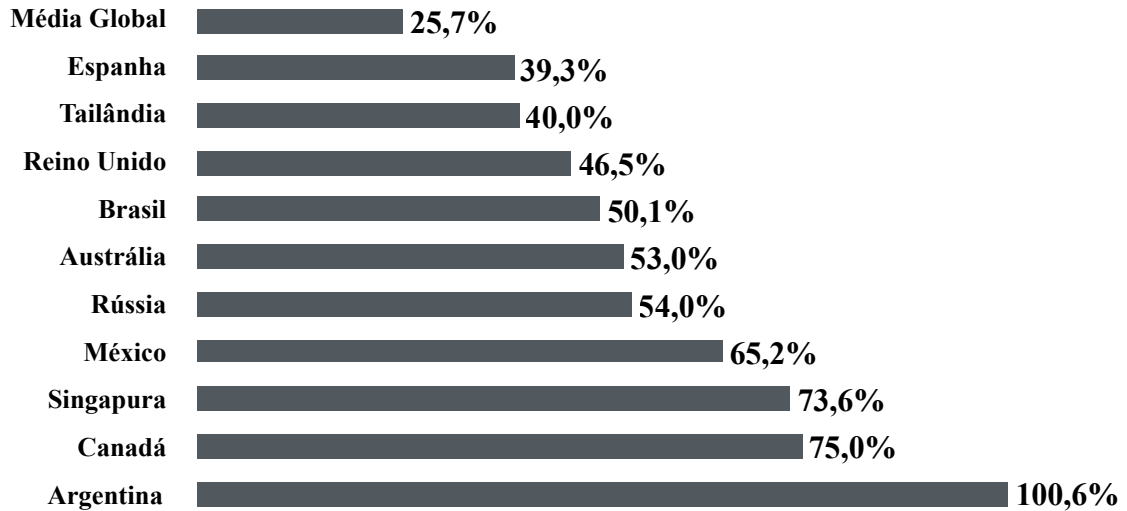


Gráfico 4 - Top 10 países, ranqueados pelo crescimento do varejo eletrônico em 2020
Fonte: eMarketer

Não obstante a pandemia tenha causado um profundo colapso na economia global, com milhões de novos desempregados no Brasil, os números do *e-commerce* seguiram em ascensão durante o ano de 2020, apresentando, inclusive, recordes históricos. Desse modo, a expectativa para 2021 é que as compras on-line continuem em alta, com um crescimento previsto superior a 32% de acordo com o relatório da XP Investimentos. Além disso, segundo dados da ABComm, de 20 a 30% das lojas virtuais criadas durante a pandemia irão permanecer nas plataformas de vendas on-line.

Portanto, fica claro que a pandemia trouxe mudanças em nosso comportamento em relação ao universo on-line que muito provavelmente vieram para ficar. Tendências relacionadas a como trabalhamos, aprendemos e usamos a tecnologia são mudanças aceleradas por este cenário que levará a um possível "novo normal" mesmo após a crise.

No entanto, apesar do eminente crescimento do comércio eletrônico, é normal que parte dos consumidores ainda não se sintam seguros em realizar transações que solicitem a descrição de seus dados em sites e plataformas desconhecidas, dado que, em contrapartida às compras em lojas físicas, para realizar a transação no ambiente virtual é necessário a realização de um cadastro no qual são requisitados dados relevantes e que permitem ligação direta a quem os declara, fato que pode deixar o consumidor em uma situação vulnerável, já

que raramente este tem acesso as informações sobre o tratamentos dos dados que foram coletados no momento da compra.

Mesmo o Brasil sendo um dos países com maior número de usuários de Internet do mundo, a falta de confiança ao efetuar compras on-line ainda é tida como um obstáculo para o crescimento do comércio eletrônico no país. Segundo Pinheiro (2013), “a insegurança do ambiente de rede é um dos maiores empecilhos para a expansão definitiva do e-commerce”.

Conforme pesquisa realizada pelo NZN Intelligence, 74% dos consumidores brasileiros preferem comprar on-line pela disponibilidade de ofertas mais vantajosas e comodidade de receber os produtos em casa. No entanto, a insegurança de informar seus dados pessoais e de cartão de crédito, ainda impede muitas pessoas de realizar compras pelo *e-commerce*, tanto pelo medo de ser enganado quanto ao pagamento, como de não receber o produto ou, ainda, de ter seus dados compartilhados ou utilizados indevidamente.

Dessa forma, com o aumento do consumo on-line é imprescindível que haja, cada vez mais, uma relação transparente no que diz respeito ao fornecimento, tratamento e armazenamento de dados pessoais. O aprimoramento das medidas voltadas à privacidade e proteção de dados, mediante a implantação de políticas transparentes que despertem a confiança dos consumidores, é a chave para a retenção dos novos consumidores que surgiram durante o período de isolamento social tornando sua experiência positiva para que as compras on-line se mantenham como um hábito (SOUZA, 2020).

E, ainda, poderão ser trabalhadas de forma alinhada à estratégia de negócio para atrair novos adeptos do e-commerce entre aquela parcela da população que ainda não se sente segura demonstrando que o compartilhamento de seus dados ocorrerá somente nas hipóteses previstas em lei e de acordo com o que lhe foi previamente informado no momento da compra (SOUZA, 2020). A questão agora é a conformidade com a Lei Geral de Proteção de Dados para promover um crescimento sustentável da economia baseada em dados (AMARAL, 2020).

5 PRINCIPAIS ASPECTOS DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS NO DIREITO DO CONSUMIDOR

A LGPD nasceu com o claro objetivo de "proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural", como descrito em seu art. 1º. Seus fundamentos dialogam tanto com os princípios constitucionais e direitos fundamentais, quanto com as proteções que o Código Civil e o Código de Defesa do Consumidor conferem às situações existenciais dos usuários, como apresentado no art. 2º da referida lei:

Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:

I - o respeito à privacidade;

II - a autodeterminação informativa;

III - a liberdade de expressão, de informação, de comunicação e de opinião;

IV - a inviolabilidade da intimidade, da honra e da imagem;

V - o desenvolvimento econômico e tecnológico e a inovação;

VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e

VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Nota-se que, além da privacidade e dos direitos dos consumidores, são mencionados expressamente, entre outros, a autodeterminação informativa, os direitos humanos, o livre-desenvolvimento da personalidade, a cidadania e a dignidade. Desse modo, segundo Frazão (2019, p.48), "fica claro que o objetivo da LGPD é o de conferir uma ampla proteção ao cidadão e às situações existenciais mais importantes que são afetadas pelo tratamento de dados".

Cumprido destacar que o termo "tratamento de dados", conforme o art. 5º, X da LGPD, refere-se a:

X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Além disso, quanto ao fundamento da "autodeterminação informativa", ou seja, o poder de escolha do proprietário do dado, este se refere à nova regra que exige o consentimento do titular dos dados para o uso das informações. Para os fins da LGPD,

considera-se consentimento a “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada” (art. 5º, XII). Com isso, o titular poderá inclusive revogar o consentimento, ter acesso facilitado a informações sobre o tratamento de seus dados, requisitar a correção de dados incompletos, inexatos ou desatualizados e, ainda, solicitar a sua transferência para outro fornecedor do mesmo produto (art. 18). Nesse contexto, a lei busca conscientizar a população sobre o uso dos dados “e mostrar que esses dados não pertencem aos que os recebem ou os tratam, mas sim ao próprio indivíduo” (LINHARES, 2020).

No entanto, quanto a preocupação com a tutela de dados pessoais, cumpre ressaltar que existem algumas poucas hipóteses em que a LGPD não se aplica, como previsto no art. 4º, quais sejam: o tratamento de dados pessoais por pessoa natural para fins exclusivamente particulares e não econômicos; e aquele que se realiza para fins a) jornalístico, artístico ou acadêmico (embora neste caso, continue a exigir o consentimento); b) de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais ou c) dados em trânsito, ou seja, que não tem como destino Agentes de Tratamento no Brasil.

Em contrapartida, nas demais situações em que se aplica a lei no tratamento de dados, visando a transparência no tratamento e utilização dos dados pessoais, deve-se observar os dez princípios elencados no art. 6º da LGPD, quais sejam:

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. (grifo nosso)

Nota-se que os princípios da finalidade, da adequação e da necessidade, estabelecidos pelo art. 6º, norteiam as atividades de tratamento de dados. Portanto, a realização do tratamento de dados deve ocorrer para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; de forma compatível ou adequada com as finalidades informadas ao titular, de acordo com o contexto do tratamento; e ainda no limite do 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.

Contudo, as hipóteses estabelecidas pela lei que autorizam o tratamento de dados pessoais estão presentes no art. 7º da LGPD.

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I - mediante o fornecimento de consentimento pelo titular;

II - para o cumprimento de obrigação legal ou regulatória pelo controlador;

III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;

VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;

VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Quanto ao primeiro requisito que diz respeito ao consentimento do titular, destaca-se que este deve ser livre, informado e inequívoco. Deverá ser fornecido ao controlador por escrito ou por outro meio que demonstre a manifestação de vontade do titular, correspondendo a uma finalidade determinada para o tratamento de dados, visto que autorizações genéricas serão consideradas nulas. Inclusive, em uma eventual mudança quanto à finalidade do tratamento desses dados que seja incompatível com o consentimento originalmente fornecido pelo titular, este deverá ser previamente informado, podendo revogar o consentimento caso discorde das alterações.

Na lógica do consentimento informado, o artigo 9º da referida lei dispõe que o titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca da: I) finalidade específica do tratamento; II) forma e duração do tratamento, observados os segredos comercial e industrial; III) identificação do controlador; IV) informações de contato do controlador; V) informações acerca do uso compartilhado de dados pelo controlador e a finalidade; VI) responsabilidades dos agentes que realizarão o tratamento; e VII) direitos do titular, com menção explícita aos direitos contidos no art. 18.

Além disso, a LGPD também apresenta hipóteses de tratamento específicas para dados pessoais sensíveis (art. 11) e para dados pessoais de crianças e adolescentes (art. 14). De acordo com o art. 5º, II, dado pessoal sensível é aquele “sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural” e sua coleta deve ser cautelosa a fim de evitar solicitações abusivas e práticas discriminatórias.

Quanto à proteção aos dados pessoais de crianças e adolescentes, o art. 14 da LGPD estabelece que o tratamento deverá ser realizado no melhor interesse desses sujeitos, atentando-se sempre as normas protetivas estabelecidas na Constituição Federal, no Estatuto da Criança e do Adolescente e na Convenção sobre os Direitos da Criança. “A proteção dos dados dos menores implica evitar que eles sejam mapeados e tenham suas preferências e escolhas pregressas utilizadas e manipuladas, preservando, dessa forma, sua liberdade na

construção da própria identidade e o livre desenvolvimento da personalidade” (TEIXEIRA; RETTORE, 2019, p.300). Nas palavras de Tepedino e Teffé (2019, p.171), “busca-se, assim, assegurar seu desenvolvimento físico, mental, moral, espiritual e social em condições de liberdade e dignidade, reconhecendo a criança e o adolescente não como meras partes integrantes do complexo familiar, mas como protagonistas da dinâmica familiar”.

Portanto, para que o consentimento do titular dos dados pessoais seja considerado válido e o tratamento destes dados possa ser realizado de forma lícita visando uma finalidade específica, esse deve ser prévio, expresso, livre, inequívoco, em cláusula destacada e devidamente informado na forma dos artigos 5º, XII, 8º e 9º da LGPD.

Cardoso (2021, p.81) explica que:

Por isso, os sites na internet passaram a destacar a sua política de privacidade e o uso de cookies, com a utilização, como regra, de cookies essenciais ou necessários (registro do usuário, armazenamento de preferências, login e outros necessários para a navegação na página) e a possibilidade de ampliação do uso de cookies para outras finalidades (como a localização e a definição do idioma do usuário, ou para gravar uma sessão de chat de atendimento ao usuário, ou para uso em ações de marketing) apenas se houver a opção expressa do titular dos dados pessoais coletados por meio deles. Quando o site não mostra as opções, significa que há somente o registro dos cookies essenciais, que derivam do cumprimento de um dever legal pelo controlador (especialmente, no Brasil, nos deveres de guarda previstos no Marco Civil da Internet). Assim, além das opções de aceitar ou de rejeitar os cookies, é possível realizar a personalização, com a definição pelo usuário do rastro que ele quer deixar naquele site.

Sobre os cookies, estes são uma espécie de arquivo utilizado nos sites para armazenar informações sobre os acessos à página da internet com o intuito de facilitar o retorno e para rastrear a navegação dos usuários visando analisar e conhecer os clientes. Tais arquivos ficam guardados na própria memória do computador. O Google Analytics e o Facebook são exemplos mais comuns de plataformas que utilizam cookies para saber as preferências dos usuários e mostrar a eles anúncios relevantes de acordo com o que andaram pesquisando online. Por isso, a LGPD determina que ao acessar o site, o usuário deve ser informado da utilização de cookies e solicitado seu consentimento. Cumpre ressaltar que alguns sites não permitem o acesso caso o usuário não aceite os cookies, no entanto, outros concedem mesmo não os aceitando (Porto, 2019).

Fato que podemos observar claramente na imagem abaixo retirada do site *The Weather Channel*:

Sobre as Cookies neste site

Além dos cookies necessários para o funcionamento adequado dos sites, sujeitos às suas preferências, usamos dados ou cookies no seu navegador para fornecer os recursos do clima, otimizar a funcionalidade do site e exibir anúncios com base em seus interesses (sua atividade neste e em outros sites) e em seu local. Clique "Concordar e continuar" para aceitar todos os cookies, conforme descrito em "Visualizar configurações de cookies", e acessar o site diretamente. Clique "Continuar só com cookies obrigatórios" para aceitar somente cookies necessários para o funcionamento do nosso site. Se você não quiser aceitar todos os cookies e preferir personalizar suas opções, clique "Visualizar configurações de cookies".

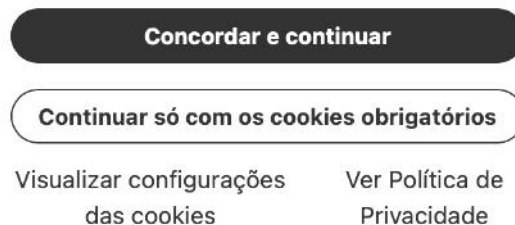


Figura 1 - Modelo de solicitação para o uso de cookies
Fonte: The Weather Channel

Além dos cookies, manter um link para a política de privacidade também é indispensável. Esta é uma declaração que explica a todos os interessados como os dados adquiridos através dos sites, dos cookies ou das próprias informações cedidas pelos titulares, serão usados, tratados e eliminados após o uso. Quais informações serão usadas e para quais finalidades. Além disso, como será feita a segurança desses dados para não haver vazamentos e nem roubos. Na política de privacidade, ainda deve conter os direitos dos usuários e a forma pela qual ele pode exercê-los, como também quem é o encarregado responsável pela proteção destes dados (Porto, 2019).

Vale ressaltar que o consentimento não implica transferência da titularidade dos dados para os agentes de tratamento, a LGPD apenas permite o controle do tratamento de dados pessoais pelo próprio titular estabelecendo limites aos agentes. No art. 15 da Lei temos as hipóteses de término do tratamento de dados pessoais, que se dá: I) pelo esgotamento funcional da utilização dos dados; II) pelo término do período de tratamento; III) pela autodeterminação do titular; e IV) por ilegalidade. Em suma, a regra é a eliminação dos dados

peçoais quando seu tratamento se encerra, na forma do art. 16, visando diminuir os riscos do uso não autorizado ou indevido dos dados pessoais.

Contudo, além da figura do titular dos dados, que é a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento (art. 5º V), a LGPD ainda prevê a criação de categorias de agentes de tratamento de dados, que corresponderão a novas funções, podendo ser desempenhadas tanto por pessoa natural quanto por pessoa jurídica, de direito público ou privado. Trata-se das figuras do controlador, aquele a quem compete a tomada de decisões referente ao tratamento de dados (art. 5º, VI), e do operador, que será o responsável por realizar o tratamento de dados em nome do controlador e segundo as informações por ele fornecidas (art. 5º, VII) (XAVIER; XAVIER; SPALER, 2019).

Além dos agentes de tratamento, a LGPD também estabelece a figura do encarregado de proteção de dados nas organizações, figura esta que corresponde ao DPO (data protection officer) previsto no Regulamento Europeu. De acordo com o art. 5º, VIII da lei, ele será indicado “pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)” – a qual corresponde ao órgão da Administração Pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD (XAVIER; XAVIER; SPALER, 2019).



Figura 2 - Controlador, Operador e Encarregado da Proteção de Dados
Fonte: Asseso

Conforme Xavier, Xavier e Spaler (2019, p.287):

Em suma, esses profissionais “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 de equipe”. Ambos deverão ainda manter registro de suas operações de tratamento de dados e estarão sujeitos à responsabilidade civil se, no exercício de suas atividades, causarem dano patrimonial, moral, individual ou coletivo a terceiros, em violação às normas de proteção de dados.

Segundo Linhares (2020), somente com a atuação da ANPD, será possível aplicar as sanções e assim, tornar a lei eficaz. No âmbito jurídico, o poder de força de uma lei depende muito das sanções e das penalidades que venham a ser aplicadas, caso essa disposição não seja cumprida. Caso contrário, ela passa a ser meramente educativa e perde o impacto de cumprimento pelas diversas empresas e instituições.

Portanto, para Souza Neto (2020, p. 53):

Como visto, a existência da autoridade nacional de proteção de dados é essencial para dar efetividade à LGPD e torná-la uma legislação integrante da quarta geração de leis de proteção de dados pessoais. É de salutar importância também que esta autoridade possua maior liberdade e independência para que não sofra ingerência ou subordinação a qualquer interesse escuso no exercício de sua função de fiscalização, regulamentação e aplicação das sanções constantes na norma, o que pode fazer, inclusive, com que o Brasil não seja considerado pela Comissão da Europa como país que apresenta nível de proteção adequada na tutela dos dados pessoais, conforme interpretação do art. 45/ 2, “a”, da GDPR, o que criaria empecilho à transferência de dados dos cidadãos europeus para o Brasil e acarretando até mesmo problemas para as relações comerciais entre ambos os mercados.

Inclusive, a não adequação a lei poderá resultar na aplicação de penalidades (art. 52), tais como: advertência; multa simples de até R\$ 50.000.000,00 (cinquenta milhões de reais); multa diária; publicização da infração; bloqueio ou eliminação dos dados pessoais tratados em desconformidade com a lei e suspensão ou proibição do exercício da atividade de tratamento por período de até 6 (seis) meses.

A LGPD também estabeleceu em seu art. 52, §1º, que as penalidades serão aplicadas de forma gradativa, podendo ser isoladas ou cumulativas. Além disso, deverá ser levado em consideração para a aplicação da pena: I) a gravidade e natureza da infração e dos direitos afetados; II) a boa-fé do infrator; III) a vantagem econômica auferida ou pretendida pelo infrator; IV) a condição econômica do infrator; V) se houve reincidência; VI) o grau do dano;

VII) a cooperação do infrator; VIII) a adoção de mecanismos capazes de minimizar o dado; IX) a adoção de políticas 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 (PORTO, 2020).

Ainda, a incidência da LGPD se dará independente da sede da empresa controladora ou operadora ou da localização geográfica, desde que a operação de tratamento seja realizada no território nacional. De acordo com o art. 3º, se quaisquer das fases de tratamento tiver sido realizada no Brasil, seja a coleta, o acesso, o processamento e/ou transferência das informações, incidirá a regulamentação legal da lei de proteção (COLAÇO, 2019).

Contudo, a Lei Geral de Proteção de Dados, publicada em 15 de agosto de 2018, possui vigência progressiva na forma do art. 65, dividida em três datas: (a) a partir do dia 28 de dezembro de 2018, para os dispositivos que autorizam a criação da Autoridade Nacional de Proteção de Dados (ANPD) e seus órgãos, de suas atribuições e receitas, e que preveem a criação e as atribuições do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (arts. 55-A a 55-L e arts. 58-A e 58-B); (b) a partir do dia 1º de agosto de 2021, para as sanções administrativas que podem ser aplicadas pela ANPD (arts. 52, 53 e 54); (c) e 24 (vinte e quatro) meses após a data de sua publicação, para todos os demais dispositivos da LGPD. Portanto, somente a partir do dia 1º de agosto de 2021, a LGPD entrou integralmente em vigor no país.

Em resumo, a lei regulamenta desde a coleta, classificação, utilização, acesso, reprodução, transmissão, compartilhamento, transferência internacional, armazenamento e controle dos dados, até o arquivamento e eliminação. Nas palavras de Souza Neto (2020, p.46):

Depreende-se, então, que a LGPD confere maior controle aos cidadãos sobre suas informações pessoais, exigindo o consentimento prévio e explícito para coleta e utilização dos dados em rede, além de estabelecer a obrigação de ser disponibilizada a possibilidade de o usuário visualizar, corrigir e excluir esses dados. A regulamentação da temática, apesar de exigir mudanças severas na atuação dos vários seguimentos da economia e nos órgãos públicos, não deve ser vista como freio ou entrave para o desenvolvimento econômico e para a inovação, eis que o foco principal da norma é assegurar o livre desenvolvimento da pessoa natural, resguardando seus direitos fundamentais de liberdade e privacidade.

Além do mais, o início dos debates e a aprovação da legislação no Brasil se deram demasiadamente tarde quando comparado com o desenvolvimento da temática na União Europeia e em outros países. Com a LGPD, o Brasil passou a integrar um conjunto de países os quais possuem regramentos para assegurar maior segurança e proteção no compartilhamento de informações pessoais entre si, o que conseqüentemente possibilita a atração de investimentos de empresas de tecnologia e o desenvolvimento de relações comerciais com outros países (SOUZA NETO, 2020).

A Lei Geral de Proteção de Dados brasileira e o General Data Protection Regulation – GDPR representam no contexto atual instrumentos para a proteção e garantia da pessoa humana, uma vez que facilitam o controle dos dados tratados, impõem deveres e responsabilidades aos agentes de tratamento e proporcionam segurança para que as informações circulem. Os dois sistemas encontram-se fortemente alinhados, como desejou o legislador brasileiro, para que a norma nacional, nos próximos anos, seja reconhecida como adequada ao sistema europeu, uma vez que isso facilitará a realização de transações e cooperações com países do bloco. Na América Latina, apenas Argentina e Uruguai até o momento conseguiram tal reconhecimento (TEPEDINO; TEFFÉ, 2019)

Dessa forma, percebe-se que a LGPD impactará bastante nas relações de consumo e sob o ponto de vista do Direito do Consumidor. A base dos e-commerces são formadas por armazenamento de dados. A partir dos cadastros dos clientes, se torna possível destinar ofertas personalizadas e fazer um contato mais próximo, por isso é uma das áreas que mais terá que se adaptar às novas demandas.

Com o aumento das vendas pela internet e com a entrada em vigor da LGPD, é preciso que haja uma relação cada vez mais transparente no que tange o fornecimento, tratamento e armazenamento de dados pessoais, com um olhar atento à segurança do consumidor e da empresa que detém seus dados, o que torna mais que necessária a utilização de uma política de proteção de dados eficiente que norteie o processamento adequado dos dados de usuários registrados em suas plataformas e assegure conformidade e adequação à lei.

Existem alguns passos básicos para manter o negócio adequado à lei, como garantir a obtenção do consentimento do consumidor final para a utilização dos seus dados pessoais; permitir que o cliente modifique ou mesmo exclua um dado pessoal; desenvolver políticas de privacidade e mantê-las atualizadas; e investir em tecnologias que garantam a segurança dos dados armazenados (AMORIM, 2020). A LGPD quer garantir que os consumidores possam escolher entre ter ou não seus dados compartilhados, tanto as informações cadastrais como aquelas armazenadas pelos cookies, que registram nossos movimentos no espaço on-line.

Tal adequação do *e-commerce* à LGPD significa adequar as atividades da empresa aos padrões internacionais de legislação protetiva de dados, trazendo um aumento da confiança dos clientes. Isso permite não somente a diminuição do risco perante eventual punição da autoridade pública constituída, como também pode corresponder a uma vantagem competitiva para empresas que pretendem se posicionar no mercado internacional, possibilitando que os negócios brasileiros sejam levados a estes mercados nos quais a legislação de data privacy está em pleno vigor (AMORIM, 2020).

Logo, é de suma importância a adequação aos termos da LGPD, visto que ao ter a concordância do usuário cria-se um negócio jurídico firmado entre a plataforma e o cliente, e, nesse interim, é preciso aumentar a confiança do consumidor e inovar o mercado digital para que haja cada vez mais segurança nas relações de consumo pela internet. Só assim, a expansão do e-commerce poderá ocorrer de maneira segura e eficaz. A adequação à LGPD não representa somente uma segurança para o titular, mas também para empresas que são responsáveis pelo tratamento dos dados pessoais e por assegurar a credibilidade das plataformas utilizadas. Portanto, estar em conformidade com a LGPD é promover ainda mais o avanço do e-commerce (MORAES, 2021).

6 CONCLUSÃO

Com a disseminação do mercado e o fomento de novas tecnologias, os dados pessoais passaram a conduzir os rumos da sociedade, transformando-se em um valioso ativo financeiro que influencia e determina as decisões estratégicas em diversos setores, especialmente nas relações de consumo. Junto a isso, surgiu um dos mais sensíveis desafios que o direito deve enfrentar nos tempos atuais: a proteção dos dados pessoais.

Neste cenário, faz-se imprescindível avaliar os mecanismos voltados à proteção dos direitos fundamentais de privacidade e de liberdade de seus titulares. O uso do tratamento de dados pessoais visando o aumento da eficiência deve dar-se de forma equilibrada, atentando-se à necessidade de proteger a privacidade do consumidor, permitindo-o, assim, manter intacta sua dignidade, integridade, autonomia e liberdade pessoal.

Logo, apesar do Brasil já contar com mais de 40 normas que direta ou indiretamente tratavam de questões relacionadas à privacidade e aos dados pessoais, como o Código de Defesa do Consumidor, o Código Civil, a Lei de Arquivos Públicos, a Lei de Acesso à Informação, a Lei do Cadastro Positivo, o Marco Civil da Internet e, inclusive, a Constituição Federal, esses mecanismos se mostravam pouco eficaz, demonstrando cada vez mais a necessidade de uma legislação específica sobre a proteção de dados que pudesse oferecer garantias adequadas às partes, segurança jurídica e que permitisse tornar o País mais competitivo no contexto de uma sociedade cada vez mais movida a dados.

Assim, em 14 de agosto de 2018 foi sancionada a Lei Geral de Proteção de Dados Pessoais, mas apenas em 1º de agosto de 2021 entrou totalmente em vigor, estabelecendo uma série de obrigações para organizações com referência à coleta, ao armazenamento, ao tratamento e ao compartilhamento de dados pessoais, por pessoa natural ou jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Dessa forma, o Brasil passou a fazer parte dos países que contam com uma legislação específica para proteção de dados e da privacidade e intimidade dos usuários. A LGPD foi inspirada principalmente no regulamento europeu, o General Data Protection Regulation (GDPR). No entanto, considerando a intensificação de usos de dados e os efeitos negativos provenientes de usos abusivos, muitos países implementaram ou aprimoraram seus modelos regulatórios visando limitar as falhas no desempenho dos agentes de mercado e da atividade de instituições públicas, proporcionando melhor fluxo de informações, mais segurança nas transações e relações cada vez mais complexas. Entre eles, destacamos o California Consumer Privacy Act (CCPA) da Califórnia, o Personal Information Protection and Electronic Documents Act (PIPEDA) do Canadá e o Act on the Protection of Personal Information (APPI) do Japão.

Assim, a adoção de leis de proteção de dados em diversos países demonstra que a temática já faz parte de um movimento internacional. O que representa um enorme ganho para toda a sociedade, vez que possibilita que a internet seja uma ferramenta cada vez mais integrada, colaborativa e participativa, sem que seja necessário a fragmentação da rede para se preservar direitos fundamentais dos usuários-cidadãos. Ao proporcionar uma maior segurança e proteção no compartilhamento de informações pessoais entre si, consequentemente, possibilita-se a atração de investimentos de empresas de tecnologia e o desenvolvimento de relações comerciais entre os países.

Junto à isso, em março de 2020, a pandemia de Covid-19 que assolou o Brasil e o mundo, instaurou uma crise nunca antes vista na história recente da humanidade. Com as medidas estatais de isolamento e fechamento ou redução de frequência dos estabelecimentos empresariais, muitas empresas foram obrigadas a migrar para o *e-commerce* como medida de manutenção de suas atividades durante a pandemia, o que alavancou a expansão do comércio eletrônico e elevou o consumo digital.

Os números do *e-commerce* seguiram em ascensão durante todo o ano de 2020, apresentando, inclusive, recordes históricos. Dessa forma, com o aumento do consumo on-line é imprescindível que haja, cada vez mais, uma relação transparente no que diz respeito ao

fornecimento, tratamento e armazenamento de dados pessoais. A LGPD visa um equilíbrio entre o uso em massa de informações pessoais pelos novos negócios na era digital e a privacidade, visando não proibir sua utilização, mas garantir um mínimo de controle ao titular. Deve ser respeitado o direito deste tanto de manter seus dados em segredo, como de autorizar, retificar, solicitar exclusão, reduzir e contestar o tratamento de suas informações pessoais por terceiros.

A adequação do *e-commerce* à LGPD significa adequar as atividades da empresa aos padrões internacionais de legislação protetiva de dados, aprimorando as medidas voltadas à privacidade e proteção de dados, mediante a implantação de políticas transparentes que despertem a confiança dos consumidores. Isto permite não somente a retenção dos novos consumidores que surgiram durante o período de isolamento social, como também àquela parcela da população que ainda não se sente segura demonstrando que o compartilhamento de seus dados ocorrerá somente nas hipóteses previstas em lei e de acordo com o que lhe foi previamente informado no momento da compra, tornando sua experiência positiva para que as compras on-line se mantenham como um hábito.

Além disso, também representa diminuição do risco perante eventual punição por parte da Autoridade Nacional de Proteção de Dados (ANPD), como também pode corresponder a uma vantagem competitiva para empresas que pretendem se posicionar no mercado internacional, possibilitando que os negócios brasileiros sejam levados a estes mercados nos quais as legislações de proteção de dados estão em pleno vigor.

Perante o contexto tecnológico atual e a importância dos dados para a economia, o marco legal imposto pela LGPD se mostra fundamental para a formação de uma verdadeira cultura de proteção de dados pessoais. A lei junto a todos os seus respectivos princípios impõem uma nova forma de lidar com os dados, transformando tanto os hábitos dos usuários em relação ao compartilhamento dessas informações quanto ao modo pelo qual empresas passam a tratar os dados de outrem. A proteção da privacidade é um pré requisito para a competitividade das empresas, tendo em visto que cada vez mais os cidadãos e consumidores estão exigindo cuidado e maior transparência no uso dos dados pessoais. Quem não zelar

pelos dados de seus clientes, perderá mercado para aqueles que buscarem se adequar às novas regras.

Portanto, a adequação à LGPD não representa somente uma segurança para os consumidores, mas também para as organizações empresariais que são responsáveis pelo tratamento dos dados pessoais e por assegurar a credibilidade das plataformas utilizadas. O objetivo agora deve ser a conformidade com a Lei Geral de Proteção de Dados para promover um crescimento sustentável da economia baseada em dados e, conseqüentemente, o avanço do e-commerce.

7 REFERÊNCIAS BIBLIOGRÁFICAS

AGUILAR, Alirio. O que é a Economia Digital?. **BLOG de Ambiente de Negócios**, 2020. Disponível em: <<http://www.blogdoideies.org.br/o-que-e-a-economia-digital/>>. Acesso em: 06 set. 2020.

AMARAL, Bruno do. Oi e Google acreditam na transformação digital de olho na LGPD. **Teletime**, 2020. Disponível em: <<https://teletime.com.br/30/06/2020/oi-e-google-acreditam-na-transformacao-digital-de-olho-na-lgpd/>>. Acesso em: 01 jul 2021.

AMORIM, Luiza. O impacto da LGPD na transformação digital acelerada pelo COVID-19. **VTEX/ Blog**, 2020. Disponível em: <<https://vtex.com/pt-br/blog/gestao/lgpd-transformacao-digital-covid/>>. Acesso em: 04 out. 2020.

ATHENIENSE, Alexandre. Impactos das mudanças na Lei de Proteção de Dados Pessoais. **SiplanControl-M**, 2019. Disponível em: <<https://spcm.com.br/blog/impactos-das-mudancas-na-lei-de-protecao-de-dados-pessoais/>>. Acesso em: 05 set. 2020.

BÉLGICA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho (General Data Protection Regulation)**, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Disponível em: <<https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016R0679>>. Acesso em: 01 set. 2020.

BEZERRA, Alexia Santos; BAPTISTA, Rafaela Ferreira; DESTRO, Carla R. F. Aplicabilidade do Código de Defesa do Consumidor no comércio eletrônico. **Âmbito Jurídico**, 2020. Disponível em: <<https://ambitojuridico.com.br/cadernos/direito-do-consumidor/aplicabilidade-do-codigo-de-defesa-do-consumidor-no-comercio-eletronico/>>. Acesso em: 05 set. 2020.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 01 set. 2020.

_____. **Decreto Legislativo no 06, de 20 de março de 2020**. Reconhece a ocorrência do estado de calamidade pública. Disponível em: <http://www.planalto.gov.br/ccivil_03/portaria/DLG6-2020.htm>. Acesso em: 01 set. 2020.

_____. **Lei na 8.078, de 11 de setembro de 1990**. Código de Defesa do Consumidor, Disponível em: <http://www.planalto.gov.br/CCIVIL_03/Leis/L8078.htm>. Acesso em: 01 set. 2020.

_____. **Lei no 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 01 set. 2020.

BUCAR, Daniel; VIOLA, Mario. **A Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.** São Paulo: Thomson Reuters Brasil, 2019.

CARDOSO, Guilherme. O Que Faço Para Me Adequar A Lgpd?. **Jusbrasil**, 2020. Disponível em: < <https://advgui.jusbrasil.com.br/artigos/1105873836/o-que-faco-para-me-adequar-a-lgpd?ref=feed> >. Acesso em: 23 out. 2020.

CARDOSO, Oscar Valente. **Legislação sobre a Proteção de Dados Pessoais.** 1. ed. Xangri-Lá, 2020.

CARNEIRO, Ramon. A proteção de dados como direito humano fundamental. *Master Juris*, 2020. Disponível em: <<https://masterjuris.com.br/a-protecao-de-dados-como-direito-humano-fundamental/>>. Acesso em: 01 set. 2020.

CARVALHO, Diógenes; FERREIRA, Vitor Hugo. DEFESA do consumidor ganha com a nova lei de proteção de dados pessoais. **Consultor Jurídico**, 2018. Disponível em: <<https://www.conjur.com.br/2018-ago-15/garantias-consumo-defesa-consumidor-ganha-lei-protecao-dados>>. Acesso em: 05 set.2020.

CCPA: Lei de Privacidade do Consumidor da Califórnia. **BL Consultoria Digital**, 2020. Disponível em: < <https://blconsultoriadigital.com.br/ccpa-lei-de-privacidade-da-california/>>. Acesso em: 26 abr. 2021.

COELHO, F.U. **Curso de direito comercial: direito de empresa.** 10a. ed. rev. e atual. São Paulo: Saraiva, 2015, V. III.

COELHO, Ludmilla. A proteção das relações de consumo na era digital. **Migalhas**, 2019. Disponível em: <<https://migalhas.uol.com.br/depeso/303209/a-protecao-das-relacoes-de-consumo-na-era-digital>>. Acesso em: 15 set. 2020.

COLLIS, Jill; HUSSEY, Roger. **Pesquisa em Administração: um guia prático para alunos de graduação e pós-graduação.** 2. ed. São Paulo: Bookman, 2005.

COM pandemia, e-commerce cresce 81% em abril e fatura R\$ 9,4 bilhões. **E-Commerce Brasil**, 2020. Disponível em: <<https://www.ecommercebrasil.com.br/noticias/e-commerce-cresce-abril-fatura-compreconfie-coronavirus/>>. Acesso em: 10 set. 2020.

CONHEÇA os principais números do e-commerce no Brasil. **Mailbiz**, 2021. Disponível em: < <https://www.mailbiz.com.br/conheca-os-principais-numeros-do-e-commerce-no-brasil/>>. Acesso em: 01 jul 2021.

COVID-19: 61% dos consumidores aumentaram volume de compras online. **E-Commerce Brasil**, 2020. <<https://www.ecommercebrasil.com.br/noticias/consumidores-aumentaram-compras-online-coronavirus/>>. Disponível em: 10 set. 2020.

CUEVA, Ricardo Villas Bôas. **A Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019.

DALMASSO, Alexandre. PIPEDA – A segunda Lei de Privacidade de Dados no Canadá. **Ética e Compliance**, 2020. Disponível em: <<https://alexandredalmasso.com/pipeda-a-segunda-lei-de-privacidade-de-dados-no-canada/>>. Acesso em: 26 abr. 2021.

DONEDA, Danilo. **A proteção de dados pessoais nas relações de consumo: para além da informação creditícia**. Escola Nacional de Defesa do Consumidor. Brasília: SDE/ DPDC, 2010.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. Espaço Jurídico Journal of Law, 2011. Disponível em: https://www.researchgate.net/publication/277241112_A_protecao_dos_dados_pessoais_como_um_direito_fundamental>. Acesso em: 06 jan. 2021.

DURBANO, Vinicius. Leis de Proteção de Dados pelo Mundo: como aplicar a devida prioridade e importância dos dados pessoais. **ECOIT Segurança Digital**, 2020. Disponível em: <<https://blog.ecoit.com.br/leis-de-protecao-de-dados-pelo-mundo-como-aplicar-a-devida-prioridade-e-importancia-dos-dados-pessoais/>>. Acesso em: 26 abr. 2021.

E-COMMERCE no Brasil bate recorde e atinge R\$ 53 bilhões no 1º semestre, mostra Ebit| Nielsen. **e-commercebrasil**, 2021. Disponível em: <<https://www.ecommercebrasil.com.br/noticias/e-commerce-no-brasil-bate-recorde-e-atinge-r-53-bilhoes-ebit-nielsen-webshoppers/>>. Acesso em: 01 set. 2021.

FILHO, Carlos Edison do Rêgo Monteiro; CASTRO, Diana Paiva de. **A Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019.

FLORENÇO, Larissa Britto. **A proteção de dados pessoais nas relações de consumimos como um Direito Fundamental**: Perspectivas de um margo regulatório para o Brasil. REVISTA DA ESMESC, v.23, n.29, p. 165-182, 2016.

FRAZÃO, Ana. **A Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019.

FORATO, Fidel. Retrospectiva COVID-19: o que aconteceu em um ano de coronavírus?. **Canaltech**, 2020. Disponível em: <<https://canaltech.com.br/saude/retrospectiva-covid-19-um-ano-de-coronavirus-176704/>>. Acesso em: 01 jul 2021.

GANDOLFE, Lucas. O Impacto do Coronavírus na Proteção de Dados. **Jusbrasil**, 2020. Disponível em: <<https://lucasgandolfe9.jusbrasil.com.br/artigos/1146970034/o-impacto-do-coronavirus-na-protecao-de-dados>>. Acesso em: 01 jul 2021.

GARCIA, Lara Rocha et al. **Lei Geral de Proteção de Dados Pessoais (LGPD): guia de implantação**. São Paulo: Blucher, 2020.

GERENCIAR direitos dos dados. **The Weather Channel**, 2021. Disponível em: <<https://weather.com/pt-BR/data-rights>>. Acesso em: 15 set. 2021.

GDPR: entenda o que é o Regulamento Geral de Proteção de Dados. **DocuSign**, 2018. Disponível em: <<https://www.docusign.com.br/blog/gdpr-entenda-o-que-e-o-regulamento-geral-de-protecao-de-dados>>. Acesso em: 26 abr. 2021.

GIL, Antonio Carlos. **Métodos e técnicas de pesquisa social**. São Paulo: Atlas, 2002.
GOLDENBERG, Mirian. **A arte de pesquisar: como fazer pesquisa qualitativa em Ciências Sociais**. 3. ed. Rio de Janeiro: Record, 1999.

GOMES, Laís D. O comércio eletrônico e o amparo do consumidor no direito brasileiro. **JUS.COM.BR**, 2018. Disponível em: <<https://jus.com.br/artigos/66508/o-comercio-eletronico-e-o-amparo-do-consumidor-no-direito-brasileiro>>. Acesso em: 06 out. 2020.

GONÇALVES, Ellen. O consumidor conectado e a sua relação com o Direito. **E-Commerce Brasil**, 2020. Disponível em: <<https://www.ecommercebrasil.com.br/artigos/consumidor-conectado-relacao-direito/>>. Acesso em: 15 set. 2020.

GONZÁLEZ, Mariana. Conheça o cenário das leis de proteção de dados ao redor do mundo. **Idblog**, 2020. Disponível em: <<https://blog.idwall.co/protecao-de-dados-cenario-mundial-das-leis/>>. Acesso em: 26 abr. 2021.

GUIMARÃES, Ana Helena. LGPD: O que é e como isso me impacta?. **Jusbrasil**, 2020. Disponível em: <<https://anahelenaguimaraes.jusbrasil.com.br/artigos/1106121563/lgpd-o-que-e-e-como-isso-me-impacta?ref=feed>>. Acesso em: 23 out. 2020.

GUEDES, Carla. Como a Covid-19 interferiu no comportamento de compra online?. **Nação Digital**, 2020. Disponível em: <<https://nacao.digital/blog/comportamento-de-compra/>>. Acesso em: 04 out. 2020.

GUEDES, Gisela Sampaio; MEIRELES, Rose Melo Vencelau. **A Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019.

GUEDES, Maria Julia. Covid-19: o que aconteceu em um ano de pandemia no Brasil e no mundo?. **Politize**, 2021. Disponível em: <<https://www.politize.com.br/covid-19-um-ano-de-pandemia/>>. Acesso em: 01 jul 2021.

HACKEROTT, Nadia. AUMENTO de vendas pela internet em decorrência do Covid-19 e direitos do consumidor. **Fenalaw Digital**, 2020. Disponível em: <<https://digital.fenalaw.com.br/especialistas/aumento-de-vendas-pela-internet-em-decorrncia-do-covid-19-e-direitos-do-consumidor>>. Acesso em: 20 set. 2020.

IMPORTÂNCIA da LGPD. **HASA** - Certificação Digital, 2019. Disponível em: <<https://www.certificadodigitalhasa.com.br/importancia-da-lgpd/>>. Acesso em: 26 abr. 2021.

KNEBEL, Patricia. Com entrada em vigor da LGPD, empresas correm para se adequar. **Jornal do Comércio**, 2020. Disponível em: <https://www.jornaldocomercio.com/_conteudo/colunas/mercado_digital/2020/08/754342-com-entrada-em-vigor-da-lgpd-empresas-correm-para-se-adequar.html>. Acesso em: 30 set. 2020.

KONDER, Calos Nelson. **A Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019.

LEGISLAÇÃO de privacidade do setor privado federal do Canadá. **Amazon Web Services (AWS)**, 2021. Disponível em: <<https://aws.amazon.com/pt/compliance/pipeda/>>. Acesso em: 26 abr. 2021.

LEI de proteção da privacidade do consumidor da Califórnia (CCPA). **Amazon Web Services (AWS)**, 2021. Disponível em: <<https://aws.amazon.com/pt/compliance/california-consumer-privacy-act/>> Acesso em: 26 abr. 2021.

LEI Geral de Proteção de Dados: entenda os impactos para as empresas brasileiras. **Assesso**, 2019. Disponível em: <https://www.assesso.com.br/lgpd-entenda-os-impactos-para-as-empresas-brasileiras/infografico_lgpd/>. Acesso em: 15 set. 2021.

LEI LGPD – Como se adequar à nova lei. **Itamarati Contábil**, 2019. Disponível em: <<https://www.itamaraticontabil.com.br/lei-lgpd/>>. Acesso em: 13 out. 2020.

LGPD: a versão brasileira do regulamento europeu. **Serpro**, 2020. Disponível em: <<https://www.serpro.gov.br/lgpd/noticias/lgpd-versao-brasileira-gdpr-dados-pessoais/>>. Acesso em: 13 out. 2020.

LOPES, Ana Karla. **Dissecando a LGPD Entenda a Lei Geral de Proteção de Dados em uma linguagem simples e como ela interfere, na prática, em seus negócios online**. eBook Kindle, 2021.

LUARO, Regina L.; RODRIGUES, Daniel Piñero; FINGER, Brunize (col). **O direito à proteção de dados pessoais e a privacidade**. Curitiba: Revista da Faculdade de Direito – UFP. n. 53, 2011.

MACIEL, Rafael Fernandes. **Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais** (Lei nº 13.709/18). 1. ed. Goiânia: RM Digital Education, 2019.

MARTINO, Natalye Dornelles. Tempo de “Primeiras Vezes”: As Transformações nos Hábitos de Consumo Online durante a Quarentena. **UFSM**, 2020. Disponível em: <<https://www.ufsm.br/app/uploads/sites/820/2020/06/Textos-para-Discussão-05-Tempo-de-Primeiras-Vezes.pdf>>. Acesso em: 04 out. 2020.

MARTINS, Rose. Quem vai acelerar a transformação digital na sua empresa, a área de TI, Projetos, Diretoria ou a COVID-19?. **Mercado&Consumo**, 2020. Disponível em: <<https://>

mercadoeconsumo.com.br/2020/04/14/quem-vai-acelerar-a-transformacao-digital-na-sua-empresa-a-area-de-ti-projetos-diretoria-ou-a-covid-19/>. Acesso em: 04 out. 2020.

MATOS, Ana Carla Harmatiuk; RUZVK, Carlos Eduardo Pianovski. **A Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019.

MEDEIROS, Davi. Pandemia impulsiona aumento de compras online no país. Olhar Digital, 2020. Disponível em: <<https://olhardigital.com.br/noticia/pandemia-impulsiona-aumento-de-compras-online-no-pais/105621>>. Acesso em: 01 set. 2020.

MELO, Carla. Impactos do COVID-19 no varejo brasileiro. **Linx**, 2020. Disponível em: <<https://www.linx.com.br/blog/impactos-do-covid-19-no-varejo-brasileiro/>>. Acesso em: 04 out. 2020.

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

MENEZES, Joyceane Bezerra; COLAÇO, Hian Silva. **A Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019.

MONTEIRO, Renato L. *Lei Geral de Proteção de Dados do Brasil – Análise*. Disponível em: <<https://baptistaluz.com.br/institucional/lei-geral-de-protecao-de-dados-do-brasil-analise/>>. Acesso em: 20 out. 2020.

MORAES, Nathalya da Silva de. Proteção de dados e e-commerce: a importância da implementação da LGPD nas plataformas de compra e venda virtuais. **Migalhas**, 2021. Disponível em: <<https://www.migalhas.com.br/depeso/341620/protecao-de-dados-e-e-commerce-a-importancia-da-implementacao-da-lgpd>>. Acesso em: 01 set. 2021.

MURAD, Raul; REQUENA, Rodrigo. **A Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019.

NOVAES, Manuela. Proteção de dados: Japão introduz reconhecimento facial em investigações criminais. **LGPD News**, 2020. Disponível em: <<https://lgpdnews.com/2020/09/protecao-de-dados-japao-introduz-reconhecimento-facial-em-investigacoes-criminais/>>. Acesso em: 26 abr. 2021.

OLIVA, Afonso Carvalho; PESSOA, Flávia Moreira Guimarães. Bancos de Dados e a Proteção do Consumidor Brasileiro: o Panóptico Pós-Moderno. **academia.edu**, 2016. Disponível em: <https://www.academia.edu/38391576/Bancos_de_Dados_e_a_Proteção_do_Consumidor_Brasileiro_o_Panóptico_Pós_Moderno>. Acesso em: 06 jan. 2021.

OLIVEIRA, Marco Aurélio Bellizze; LOPES, Isabela Maria Pereira Lopes. **A Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019.

OLIVEIRA, M.M. **Como fazer pesquisa qualitativa**. Petrópolis. Vozes, 2007.

O QUE é a CCPA, a lei de privacidade e proteção de dados da Califórnia?. **Gatefy**, 2021. Disponível em: < <https://gatefy.com/pt-br/blog/o-que-e-ccpa-lei-privacidade-dados-california/> >. Acesso em: 26 abr. 2021.

O QUE é uma pandemia e por que o atual surto de coronavírus ainda não é uma. **BBC News Brasil**, 2020. Disponível em: <<https://www.bbc.com/portuguese/geral-51633275>>. Acesso em: 01 jul 2021.

OS IMPACTOS da LGPD nas nossas vidas. **Funcef**, 2020. Disponível em: <<https://www.funcef.com.br/portal/menu-principal/comunicacao/os-impactos-da-lgpd-nas-nossas-vidas.htm>> Acesso em: 02 set. 2020.

O QUE muda com a LGPD. **Serpro**, 2020. Disponível em: <<https://www.serpro.gov.br/lgpd/menu/a-lgpd/o-que-muda-com-a-lgpd>>. Acesso em: 06 out. 2020.

PANDEMIA. In: Dicionário Priberam da Língua Portuguesa. **Priberam Dicionário**, 2021. Disponível em: <https://dicionario.priberam.org/Pandemia>. Acesso em: 01 set. 2021.

PERONGINI, Maria F.H. Lei Geral de Proteção de Dados: Um Resumo da LGPD (ATUALIZADO). Legalcloud, 2018. Disponível em: <<https://legalcloud.com.br/lei-geral-de-protecao-de-dados-resumo-lgpd/>>. Acesso em: 02 set. 2020.

PEZZOTTI, Renato. Compras pela internet disparam com crise do coronavírus. **UOL ECONOMIA**, 2020. Disponível em: < <https://economia.uol.com.br/noticias/redacao/2020/03/23/compras-pela-internet-disparam-com-crise-do-coronavirus.htm> >. Acesso em: 01 out. 2020.

PICON, Rodrigo. A PROTEÇÃO de dados pessoais já é uma realidade mesmo a LGPD não entrando em vigor. **JUS.COM.BR**, 2020. Disponível em: < <https://jus.com.br/artigos/83487/a-protecao-de-dados-pessoais-ja-e-uma-realidade-mesmo-a-lgpd-nao-entrando-em-vigor>>. Acesso em: 01 set. 2020.

PINHEIRO, Patrícia Peck. **Direito Digital**. 6.ed. São Paulo: Saraiva, 2019.

PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais**. São Paulo: Saraiva, 2021.

PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais**: comentários à Lei n. 13.709/2018 (LGPD). São Paulo: Saraiva Educação, 2020.

PORTO, Viviane de Araújo. **Descomplicando a Lei Geral de Proteção de Dados**. Clube dos Autores, 2019.

QUEM vai regular a LGPD?. **Serpro**, 2020. Disponível em: <<https://www.serpro.gov.br/lgpd/governo/quem-vai-regular-e-fiscalizar-lgpd>> . Acesso em: 10 set. 2020.

RIBEIRO, Davi. Qual é a relação entre a Lgpd e o CDC?. **Jusbrasil**, 2020. Disponível em: <<https://davirdr.jusbrasil.com.br/artigos/814465325/qual-e-a-relacao-entre-a-lgpd-e-o-cdc>>. Acesso em: 10 out. 2020.

ROCHA, William. Entenda como a LGPD Influencia nos Direitos do Consumidor. **Mundo do Marketing**, Disponível em: <<https://www.mundodomarketing.com.br/lgpd/38856/entenda-como-a-lgpd-influencia-nos-direitos-do-consumidor.html>>. Acesso em: 06 set. 2020.

ROQUE, Andre Vasconcelos; BAPTISTA, Bernardo Barreto; ROCHA, Henrique de Moraes Fleury. **A Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019.

SANTOS, Flavia; PAPPERT, Milena. A importância da aplicação da Lei Geral de Proteção de Dados Pessoais - (LGPD) nas empresas. **Migalhas**, 2020. Disponível em: <<https://migalhas.uol.com.br/depeso/331831/a-importancia-da-aplicacao-da-lei-geral-de-protecao-de-dados-pessoais-lgpd-nas-empresas>>. Acesso em: 20 set. 2020.

SCHREIBER, Anderson. **A Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019.

SILVA, Cleide; ROMANI, Bruno. Compras pela internet disparam até 40% com impacto do novo coronavírus. **UOL ECONOMIA**, 2020. Disponível em: <<https://economia.uol.com.br/noticias/estadao-conteudo/2020/03/20/compras-pela-internet-disparam-ate-40-com-impacto-do-novo-coronavirus.htm>>. Acesso em: 10 set. 2020.

SOUZA, Carlos Affonso Pereira de. **A Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019.

SOUZA, Nara. LGPD no E-commerce: a proteção de dados como estratégia de negócios. **Nextlaw academia**, 2020. Disponível em: <<https://www.nextlawacademy.com.br/blog/lgpd-no-e-commerce-a-protecao-de-dados-como-estrategia-de-negocios>>. Acesso em: 01 jul 2021.

SOUZA NETO, José Luiz. **A proteção dos dados pessoais na era da informação**. Independently Published, 2020.

TEIXEIRA, Ana Carolina Brochado; RETTORE, Anna Cristina de Carvalho. **A Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019.

TEPEDINO, Gustavo; TEFFÉ, Chiara. **A Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019

TERMOS de Uso e Política de Privacidade: o que são e qual a sua importância?. **ADV Junior Consultoria Jurídica**, 2020. Disponível em: <<http://advjunior.com/publicacoes/noticias/termos-de-uso-e-politica-de-privacidade/>>. Acesso em: 04 out. 2020.

VAZQUEZ, Rafael Ferraz. **A proteção de dados pessoais nos Estados Unidos, União Europeia e América do Sul: interoperabilidade com a proposta de marco normativo no Brasil**. XXI Congresso Nacional do CONPEDI/UFF, outubro de 2012.

VILELE, Luiza. Brasil está na lista dos 10 países com maior crescimento de e-commerce. **NOVAREJO**, 2021. Disponível em: <<https://www.consumidormoderno.com.br/2021/07/05/brasil-e-commerce-top-dez/>>. Acesso em: 01 set. 2021.

WHO - World Health Organization. **COVID-19**, 2021. Disponível em: <<https://covid19.who.int/region/amro/country/br>>. Acesso em: 01 set. 2021.

XAVIER, Luciana Pedrosa; XAVIER, Marília Pedrosa; SPALER, Mayara Guibor. **A Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019.

XIMENES, Alexia Praia; PIETZSCH, Ingo Dieter. A Proteção dos Consumidores nas compras pela internet em tempos de pandemia. **Âmbito Jurídico**, 2020. Disponível em: <<https://ambitojuridico.com.br/cadernos/direito-do-consumidor/a-protecao-dos-consumidores-nas-compras-pela-internet-em-tempos-de-pandemia/>>. Acesso em: 05 set. 2020.