



**UNIVERSIDADE FEDERAL DA BAHIA  
FACULDADE DE DIREITO  
CURSO DE GRADUAÇÃO**

**ALINE DA SILVA RIBEIRO**

**O REGIME DE RESPONSABILIDADE CIVIL ADOTADO NO  
ÂMBITO DA LEI Nº 13.709/2018 – LEI GERAL DE  
PROTEÇÃO DE DADOS (LGPD)**

Salvador  
2021

**ALINE DA SILVA RIBEIRO**

**O REGIME DE RESPONSABILIDADE CIVIL ADOTADO NO  
ÂMBITO DA LEI Nº 13.709/2018 – LEI GERAL DE  
PROTEÇÃO DE DADOS (LGPD)**

Monografia apresentada como trabalho de conclusão de curso de graduação em Direito, requisito parcial para a obtenção do grau de bacharela em Direito junto à Faculdade de Direito da Universidade Federal da Bahia.

Orientadora: Profa. Me. Teila Rocha Lins D'Albuquerque

Salvador  
2021

**ALINE DA SILVA RIBEIRO**

**O REGIME DE RESPONSABILIDADE CIVIL ADOTADO NO ÂMBITO DA LEI Nº  
13.709/2018 – LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)**

Monografia apresentada como trabalho de conclusão de curso de graduação em Direito, requisito parcial para a obtenção do grau de bacharela em Direito junto à Faculdade de Direito da Universidade Federal da Bahia.

Salvador, 16 de junho de 2021.

**Banca Examinadora**

**Teila Rocha Lins D’Albuquerque** – Orientadora \_\_\_\_\_

Mestre em Relações Sociais e Novos Direitos pela Universidade Federal da Bahia  
Universidade Católica do Salvador – UCSAL

**Maurício Requião de Sant’Ana** – Examinador(a) \_\_\_\_\_

Doutor em Direito das Relações Sociais pela Universidade Federal da Bahia  
Universidade Federal da Bahia – UFBA

**Leandro Reinaldo da Cunha** – Examinador(a) \_\_\_\_\_

Doutor em Direito pela Pontifícia Universidade Católica de São Paulo  
Universidade Federal da Bahia – UFBA

## **AGRADECIMENTOS**

Em primeiro lugar, agradeço aos meus pais, Vanusa e Esequiel, e ao meu irmão Alan, pelo amor e apoio incondicional durante toda a vida. Vocês são verdadeiros exemplos para mim e em cada passo que eu dou, levo vocês ao meu lado.

Agradeço aos meus familiares de Salvador, especialmente à minha tia Rosa, que incentivou minha mudança para Salvador e meu ingresso na UFBA. Saiba que a senhora faz parte da realização deste sonho.

Ao meu noivo, Gabriel, pelo amor e companheirismo e por sempre acreditar no meu potencial. Tem sido lindo compartilhar a vida com você.

Aos meus amigos da UFBA e da vida, os quais cito em especial, Alana, Kayque, Luana, Mayara, Karol e Rodrigo. Saibam que vocês tornaram minha trajetória mais leve e que carrego vocês aonde quer que eu esteja. Agradeço por todo carinho e ajuda, por todas as vezes que pacientemente me ouviram perguntando se conseguiria finalizar este trabalho a tempo e deram todo suporte.

Aos servidores da 19ª Vara das Relações de Consumo de Salvador, nas figuras de Dr. Moacir e Jane. A compreensão de vocês durante esse período foi essencial para o término deste trabalho.

À minha orientadora, Teila Rocha, por ter aceitado o convite para orientação.

Por fim e com muito orgulho, agradeço à minha Universidade Federal da Bahia, que possibilitou a concretização de um sonho e foi palco para tantos encontros e aprendizados. Que a universidade pública, gratuita e de qualidade continue viva e pulsante!

RIBEIRO, Aline da Silva. **O Regime de Responsabilidade Civil adotado no âmbito da Lei nº 13.709/2018 – Lei Geral de Proteção de Dados (LGPD)**. Orientadora: Profa. Me. Teila Rocha Lins D’Albuquerque. 2021. 72 f. Trabalho de Conclusão de Curso (TCC) – Curso de Direito, Faculdade de Direito, Universidade Federal da Bahia, Salvador, 2021.

## RESUMO

O trabalho em comento tem por objetivo central analisar, por força do regramento legislativo e das correntes doutrinárias, o instituto da responsabilidade civil adotado no âmbito da Lei nº 13.709/2018 – Lei Geral de Proteção de Dados (LGPD), em decorrência de violação das obrigações legais e/ou regulatórias previstas em nosso ordenamento jurídico, por parte dos agentes de tratamento. Para tanto, será abordado a análise histórica da regulamentação jurídica de proteção de dados no âmbito internacional, além da evolução do processo legislativo no Brasil, abarcando o Código de Defesa do Consumidor, Lei do Cadastro Positivo e Marco Civil da Internet, até chegar à LGPD. Por fim, serão expostos alguns dos principais conceitos previstos na legislação específica para proteção de dados, bem como examinados os principais argumentos utilizados pela doutrina para interpretar o que dispõe a lei em relação ao regime de responsabilidade.

Palavras-chave: Responsabilidade civil. Lei Geral de Proteção de Dados. Proteção de dados pessoais.

RIBEIRO, Aline da Silva. **The Civil Liability Regime adopted under Law No. 13.709/2018 - General Data Protection Law (GDPL)**. Monograph Advisor: Teila Rocha Lins D'Albuquerque. 2021. 72 s. Completion of course work, Faculdade de Direito, Universidade Federal da Bahia, Salvador, 2021.

## **ABSTRACT**

The work in question has as its main objective to analyze, under the legislative and doctrinal currents, the institute of civil liability adopted under Law No. 13.709/2018 - General Data Protection Law (GDPL), as a result of violation of legal and/or regulatory obligations provided for in our legal system, on the part of the treatment agents. Therefore, the historical analysis of the legal regulation of data protection in the international scope will be addressed, as well as the evolution of the legislative process in Brazil, covering the Consumer Defense Code, the Positive Registry Law and the Internet Civil Framework, until reaching the GDPL . Finally, some of the main concepts provided for in the specific legislation for data protection will be exposed, as well as the main arguments used by the doctrine to interpret the provisions of the law in relation to the liability regime will be examined.

Keywords: Civil liability. General Data Protection Law. Protection of personal data.

## LISTA DE ABREVIATURAS E SIGLAS

ADCT	Ato das Disposições Constitucionais Transitórias
ADIs	Ações Diretas de Inconstitucionalidades
ANPD	Autoridade Nacional de Proteção de Dados
ART	Artigo
CC	Código Civil
CDC	Código de Defesa do Consumidor
CIDH	Comissão Interamericana de Direitos Humanos
CF	Constituição Federal
CNDL	Confederação Nacional de Dirigentes Lojistas
CNIL	Comissão Nacional de Informática e Liberdade
COVID-19	<i>Coronavirus Disease 2019</i>
CPF	Cadastro de Pessoa Física
GDPR	<i>General Data Protection Regulation</i>
IBGE	Instituto Brasileiro de Geografia e Estatística
LC	Lei Complementar
LCP	Lei do Cadastro Positivo
LGPD	Lei Geral de Proteção de Dados
MCI	Marco Civil da Internet
MP	Medida Provisória
OAB	Ordem dos Advogados do Brasil
OMS	Organização Mundial da Saúde
ONU	Organização das Nações Unidas
PL	Projeto de Lei
PLC	Projeto de Lei da Câmara
PLS	Projeto de Lei do Senado
RG	Registro Geral
SARS-CoV-2	<i>Severe Acute Respiratory Syndrome Coronavirus 2</i>
SERPRO	Serviço Federal de Processamento de Dados
SMS	<i>Short Message Service</i>
STF	Supremo Tribunal Federal
STJ	Superior Tribunal de Justiça
UE	União Europeia

## LISTA DE FIGURAS

Figura 1	Mapa da proteção de dados pessoais ao redor do mundo.....	15
Figura 2	Período de aprovação das Leis de Proteção de Dados Pessoais na América-Latina.....	16
Figura 3	Conhecimento sobre a LGPD (consumidores).....	34
Figura 4	Conhecimento sobre a LGPD (pessoas jurídicas).....	35



## SUMÁRIO

<b>1. INTRODUÇÃO</b> .....	09
<b>2. BREVE HISTÓRICO DA REGULAMENTAÇÃO JURÍDICA DE PROTEÇÃO DE DADOS NO CENÁRIO INTERNACIONAL</b> .....	13
2.1 MODELO EUROPEU.....	16
2.2 MODELO NORTE-AMERICANO.....	23
<b>3. EVOLUÇÃO LEGISLATIVA BRASILEIRA</b> .....	26
3.1 LEI Nº 8.078/1990 – CÓDIGO DE DEFESA DO CONSUMIDOR (CDC).....	26
3.2 LEI Nº 12.414/2011 – LEI DO CADASTRO POSITIVO (LCP).....	28
3.3 LEI Nº 12.965/2014 – MARCO CIVIL DA INTERNET (MCI).....	29
3.4 LEI Nº 13.709/2018 – LEI GERAL DE PROTEÇÃO DE DADOS (LGPD).....	30
<b>4. APLICABILIDADE E PRINCÍPIOS DA LEI GERAL DE PROTEÇÃO DE DADOS</b> .....	34
4.1 ESCOPO DE APLICAÇÃO.....	35
4.2 PRINCIPAIS CONCEITOS.....	36
4.2.1 Dado Pessoal.....	37
4.2.2 Titular.....	37
4.2.3 Controlador e Operador.....	37
4.2.4 Tratamento de Dados.....	38
4.3 PRINCÍPIOS.....	39
4.3.1 Necessidade.....	40
4.3.2 Segurança.....	41
4.3.3 Prevenção.....	41
4.3.4 Responsabilização e Prestação de Contas.....	42
<b>5. RESPONSABILIDADE CIVIL NO ÂMBITO DA PROTEÇÃO DE DADOS</b> .....	44
5.1 O SURGIMENTO DA RESPONSABILIDADE CIVIL: BREVE HISTÓRICO.....	44
5.2 O INSTITUTO DA RESPONSABILIDADE CIVIL NO ORDENAMENTO BRASILEIRO.....	45
5.3 RESPONSABILIDADE CIVIL SUBJETIVA E OBJETIVA.....	48
5.4 PREVISÃO NA LEI GERAL DE PROTEÇÃO DE DADOS.....	49
<b>6. CONCLUSÃO</b> .....	60
<b>REFERÊNCIAS</b> .....	63

## 1. INTRODUÇÃO

O perfil da sociedade vem se transformando progressivamente ao longo dos anos. Se antes a preocupação era ter assegurado o direito à tranquilidade, apenas de ser deixado só e não ter os espaços privados invadidos, agora também é necessário que seja assegurado ao indivíduo o direito à autodeterminação afirmativa, ou seja, o poder de tomar as rédeas sobre suas próprias informações.

Essa mudança ocorreu sobretudo em decorrência do desenvolvimento tecnológico e aumento do fluxo informacional após meados do século XX. Desde então, a tecnologia assumiu uma posição relevante em nosso cotidiano, sendo praticamente impossível dissociar a vida *on-line* do mundo *off-line*. Assim, com a maior dependência dos meios digitais, houve também um aumento do compartilhamento dessas bases informacionais pelas redes. Cada vez mais vão sendo deixados para trás dados pessoais que vão muito além de nome, CPF, endereço ou telefone, mas verdadeiros rastros que identificam propriamente a personalidade dos indivíduos, suas preferências e características existenciais.

É por tais razões que se fala cada vez mais em uma sociedade da informação, onde as pessoas, sejam elas físicas ou jurídicas, estão sendo movimentadas e orientadas por dados. De um lado, esse avanço tem o condão de gerar diversos benefícios à população, ainda mais quando utilizados para conscientização e participação popular nos processos democráticos. No entanto, vê-se também que a captação e utilização desses dados se tornou um verdadeiro negócio lucrativo, servindo para os mais diversos fins, tais como *marketing*, informações financeiras e até mesmo políticos, o que pode mitigar a soberania e autonomia popular.

De uma rápida consulta é possível verificar que várias empresas divulgam pela *internet* a venda de base de dados confidenciais. Além disso, recentemente a Netflix, serviço de streaming por assinatura, lançou o documentário Dilema das Redes, que compilou depoimentos de especialistas e ex-funcionários de grandes empresas, expondo como funcionam os algoritmos das redes sociais e como eles podem ser utilizados para manipular os usuários e disseminar notícias falsas (*fake news*) em uma velocidade alarmante. Logo após, de acordo ao levantamento realizado pela Decode HUB, as buscas no *Google* por “como excluir ou desativar o *Facebook*” aumentaram em 250% no mês de lançamento do filme (DOLIVEIRA, 2020).

Dada essa realidade de exposição de dados pessoais e relações sociais cada vez mais complexas, houve constantes evoluções legislativas no cenário internacional e nacional, o que culminou, em 2018, na aprovação da Lei nº 13.709, a lei brasileira para proteção de dados. Até então o país possuía outros sistemas normativos que estavam regulando tema de acordo com suas finalidades precípuas, a saber, Lei nº 8.078/90 (Código de Defesa do Consumidor), Lei nº 12.414/11 (Lei do Cadastro Positivo) e Lei nº 12.965/14 (Marco Civil da Internet). Esse conjunto normativo se torna a prova concreta do risco provocado pela atividade de manuseio de dados.

Observa-se que Lei Geral de Proteção de Dados (LGPD) surgiu de forma um tanto tardia em nossa legislação pátria. O doutor e mestre em Direito Civil pela Universidade do Estado do Rio de Janeiro, Danilo Doneda (2019, p. 45), atribui essa demora ao perfil socioeconômico do país, sugerindo que diante dos graves problemas sistêmicos e estruturais do Brasil, “a proteção de dados pessoais seja, ao menos em termos quantitativos, uma demanda de menor apelo”.

Fato é que após inúmeras discussões sobre seu período de vacância, a Lei Geral de Proteção de Dados finalmente entrou em vigor em setembro de 2020, em meio a pandemia ocasionada pelo vírus SARS-Cov-2 (COVID-19). A própria situação vivenciada em esfera global desde março de 2020 provocou uma enorme aceleração do emprego de novas tecnológicas, visto que rapidamente todos os setores precisaram se reinventar para minimizar os impactos pelo isolamento e distanciamento social, medidas essenciais para conter a disseminação do vírus e salvaguardar vidas.

Por consequência, essa hiperconectividade elevou em escala a coleta, compartilhamento e armazenamento de dados. Já em junho de 2020, apenas três meses após a decretação da pandemia pela Organização Mundial de Saúde (OMS), um estudo da PSafe, startup brasileira que oferece soluções de segurança, revelou um aumento de 47% no vazamento de dados (DEMARTINI, 2020). Outros debates sobre o assunto surgiram em torno de medidas adotadas pelo Poder Público durante a pandemia, tais como câmeras de reconhecimento facial e detectores de temperatura corporal instalados, principalmente, em pontos de maior fluxo, como metrô e shoppings; monitoramento da geolocalização de celulares para fiscalizar o deslocamento das pessoas durante o período de isolamento e distanciamento social, etc.

Face ao exposto, a LGPD se torna um instrumento indispensável para coibir o tratamento e cessão de dados de forma irregular, criando regras claras e específicas sobre o processo de coleta, armazenamento e compartilhamento. Resta evidente, portanto, a importância de discutir seus dispositivos, especialmente aqueles referentes a responsabilidade civil dos agentes de tratamento dos dados pessoais (controladores e operadores), pois é com a concreta obrigação de reparação dos danos que se protege direitos fundamentais dos indivíduos. Sendo assim, indaga-se: Qual é o regime de responsabilidade civil adotado no âmbito da LGPD quando ocorre o descumprimento das obrigações legais e/ou regulatórias previstas no ordenamento jurídico?

A problemática, contudo, se torna ainda mais complexa quando se constata que a lei não trouxe um direcionamento concreto sobre quais os fundamentos dessa responsabilização, o que gerou uma amplitude de interpretação. Potencialmente, essas dúvidas em torno do tema serão levadas às vias judiciais para enfrentamento e solução dos conflitos, tanto por ações individuais, quanto coletivas, contribuindo para o aumento na morosidade do Poder Judiciário. Apenas a título exemplificativo, considerando que a maior parte dos tratamentos de dados são oriundos de uma relação de consumo, de acordo com o último relatório Justiça em Números, divulgado pelo Conselho Nacional de Justiça, a responsabilidade civil do fornecedor e ações indenizatórias já são o segundo assunto mais demandado na Justiça Estadual, representando 4,44% das ações em 2019.

Com efeito, o objetivo central do presente trabalho é analisar, por força do regramento legislativo e das correntes doutrinárias, o instituto da responsabilidade civil aplicado aos agentes de tratamento frente aos danos por eles ocasionados em decorrência de violação das obrigações legais e/ou regulatórias previstas em nosso ordenamento jurídico. Para que essa pesquisa fosse feita, a metodologia utilizada de forma preponderante foi a pesquisa qualitativa e exploratória, envolvendo levantamento bibliográfico, análise histórica, comparativo entre sistemas normativos e jurisprudências, todos relacionados ao Direito Civil, Direito do Consumidor e Direito Digital.

Para alcançar o objetivo acima mencionado, o primeiro capítulo começará de uma análise histórica da legislação de proteção de dados no cenário internacional e o contexto de seus surgimentos. Serão analisados dois processos legislativos, os quais se mostram de alta relevância para o tema, quais sejam, o europeu e o norte-

americano, cujos modelos serviram de referência para outros ordenamentos jurídicos, incluindo aquele adotado pelo Brasil. Ressalta-se que a adoção dessa trajetória de pesquisa é por considerar a importância de entender a sociedade a qual estamos inseridos, bem como a forma que ela se transformou ao longo do tempo, para, então, vislumbrar como se deu a aprovação de determinadas legislações.

O segundo capítulo partirá da mesma premissa, mas aproximando-se do cenário brasileiro para traçar uma linha do tempo das legislações que aqui surgiram, demonstrando como estas abriram caminho até a aprovação de um regramento específico para de proteção de dados. A ideia, novamente, é examinar como a sociedade foi se modificando e percebendo a relevância de salvaguardar informações pessoais e ter certo controle sobre elas, concretizando o direito à autodeterminação informativa já citado anteriormente. Dessa forma, o estudo se debruça a partir do Código de Defesa do Consumidor (1990), seguindo-se para a Lei do Cadastro Positivo (2011), Marco Civil da Internet (2014) e, finalmente, Lei Geral de Proteção de Dados (2018).

Ato contínuo, em que pese a própria LGPD já trazer de forma clara em seu Art. 5º a definição dos termos que utiliza ao longo de seu texto, bem como a explicação dos princípios a serem observados (Art. 6º), é preciso não perder de vista o fato de que a legislação ainda é muito recente, o que traz empecilhos ao exercício do pleno direito pela população que a desconhece. Assim, o capítulo 3 fará uma sucinta explanação dos principais conceitos e princípios dispostos na lei, dando enfoque àqueles necessários à compreensão do debate sobre o regime de responsabilidade civil.

O quinto e último capítulo é responsável por tratar do objetivo central do presente trabalho. Além de abordar o instituto da responsabilidade civil de um modo geral e fazer a distinção entre responsabilidade objetiva e subjetiva, serão analisados os principais argumentos doutrinários, que se dividem em, pelo menos, quatro correntes. Há os que defendem que a LGPD adota uma espécie de responsabilidade subjetiva, outros argumentam pela objetividade, mas também há autores que buscam fugir dessa dualidade, apresentando justificativas para uma responsabilidade subjetiva com alto grau de objetividade ou então uma responsabilidade que denominam como proativa.

## 2. BREVE HISTÓRICO DA REGULAMENTAÇÃO JURÍDICA DE PROTEÇÃO DE DADOS NO CENÁRIO INTERNACIONAL

A questão da privacidade e proteção de dados nunca esteve tão em voga como está no atual momento. Mais do que nunca as tecnologias e as redes sociais vem avançando com o passar do tempo, tendo, inclusive, sua utilização intensificada no último ano em decorrência da pandemia ocasionada pelo vírus SARS-Cov-2 (COVID-19) no âmbito mundial, vez que o uso da tecnologia se tornou a alternativa mais viável para o mercado de trabalho, ensino e entretenimento. Além disso, em meio a esse contexto, a lei brasileira de proteção de dados entrou em vigor em setembro de 2020, aumentando ainda mais os debates em torno da sua aplicação e abrangência.

Contudo, é possível remontar os primórdios da temática há mais de 130 anos, quando os advogados norteamericanos Samuel D. Warren e Louis D. Brandeis trouxeram a ideia – e não uma definição propriamente dita – do direito à privacidade (*right to privacy*), através de um ensaio publicado na *Harvard Law Review* em 1890. Conforme Doneda (2019), os autores começaram a se preocupar na época com o impacto da tecnologia na privacidade, tendo afirmado que “fotografias instantâneas e jornais invadiram os locais sagrados da vida privada e doméstica; e inúmeros dispositivos tecnológicos ameaçam cumprir a previsão de que “o que é sussurrado no armário será proclamado do telhado”” (BRANDEIS; WARREN, 1890, p. 195, tradução nossa).

Extrai-se, ainda, do referido trabalho, que os escritores se basearam na obra do juiz Thomas Cooley (1873), na qual havia a menção ao direito de ser deixado só (*right to be let alone*), para transcender tal expressão e dar origem, então, “a uma das vertentes pela qual se desenvolveria a tutela jurídica da privacidade ao longo do século XX, o direito de o indivíduo exercer o controle da informação sobre si.” (LEONARDOS; NAVARRO, 2012, p. 06). Dessa maneira, o direito à privacidade, que até a primeira metade do século XIX era confundido com a propriedade privada, ganhou outra dimensão, aproximando-se de uma tutela da personalidade humana.

Posteriormente, já em meados do século XX, a privacidade passou a ser discutida na seara do direito internacional, momento em que houve “uma crescente consciência de que a privacidade seria um aspecto fundamental da realização da pessoa e do desenvolvimento da sua personalidade” (DONEDA, 2019, p. 30). Assim, em 1948, foi realizada a IX Conferência Internacional Americana, que aprovou a

Declaração Americana dos Direitos e Deveres do Homem e mencionou, em seu Art. 5º que: “Toda pessoa tem direito à proteção da lei contra os ataques abusivos à sua honra, à sua reputação e à sua vida particular e familiar” (CIDH, 1948). No mesmo ano, a Organização das Nações Unidas (ONU) consignou no Art. 12 da Declaração Universal dos Direitos Humanos que: “Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques.” (ONU, 1948)

Em outros termos, vê-se que ao indivíduo é assegurado o direito de tomar suas próprias decisões na esfera privada, o que remete, novamente, ao conceito outrora mencionado do direito à tranquilidade, de ser deixado só, mas que agora passa a ter outros desdobramentos e adquirir características mais complexas. Inclusive, nos anos seguintes outras declarações internacionais também trataram sobre a privacidade (DONEDA, 2019), quais sejam, Convenção Europeia dos Direitos do Homem (1950), em seu Art. 8º; Convenção Americana dos Direitos do Homem (1969), mais conhecida como Pacto de São José da Costa Rica, no Art. 11; e, por fim e mais atual, a Carta dos Direitos Fundamentais da União Europeia (2000), que além de tratar no Art. 7º sobre o respeito pela vida privada e familiar, já menciona no dispositivo subsequente a proteção de dados pessoais.

Há de se ressaltar, outrossim, que é nesse contexto global, por volta de 1950, que se tem a chamada Terceira Revolução Industrial ou Revolução Informacional, onde há um acelerado desenvolvimento tecnológico e fluxo de informações e uma ruptura com os modelos tradicionais de produção e consumo (NETO, 2012). Com essa crescente dependência tecnológica, a privacidade, que já vinha adquirindo novos perfis, passou a ser também observada sob a ótica do aumento no tratamento de dados.

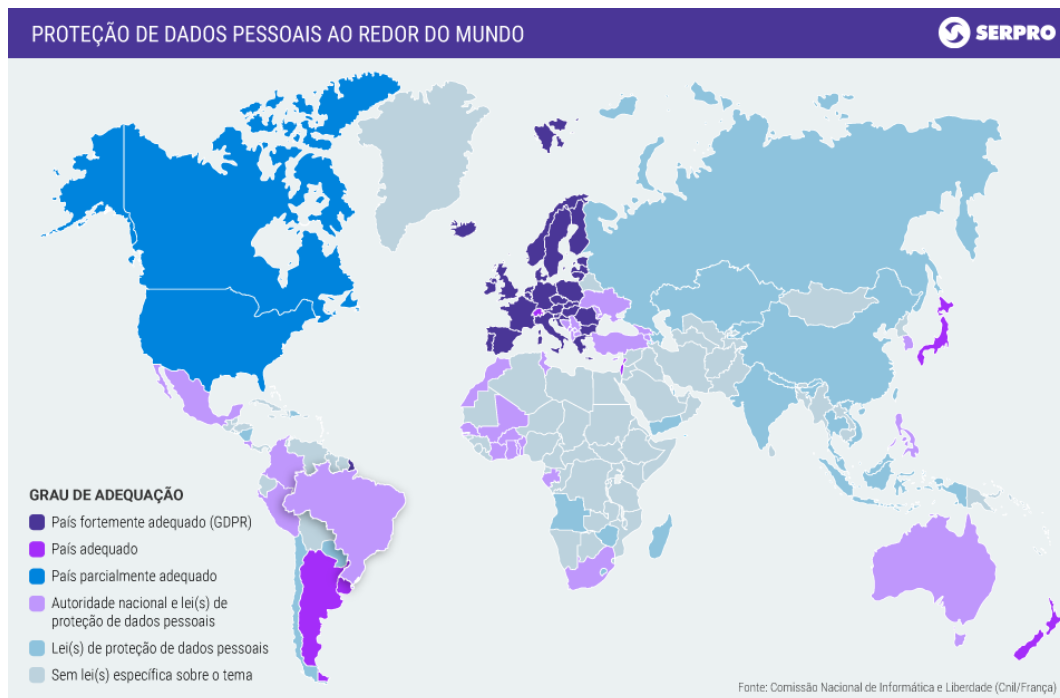
Ainda, é na década de 70, com o “boom” da informática e das telecomunicações, que surge o termo Sociedade da Informação, em substituição à de Sociedade pós industrial (WERTHEIN, 2000). Sobre a expressão, Dantas (1996, apud OLIVEIRA, A.; BAZI, 2008, p. 117) diz que esta

caracteriza uma etapa alcançada pelo desenvolvimento capitalista contemporâneo, no qual as atividades humanas determinantes para a vida econômica e social organizam-se em torno da produção, processamento e disseminação da informação através das

tecnologias eletrônicas.

É nesse sentido que ao longo das décadas outros avanços foram surgindo ao redor do mundo, sendo fato que nos dias atuais a maioria dos países possuem legislações que tratam sobre privacidade e, especificamente, proteção de dados, variando apenas o grau de adequação. É o que se extrai do mapa abaixo, divulgado no sítio do Serviço Federal de Processamento de Dados (Serpro), cujo levantamento foi realizado pela Comissão Nacional de Informática e Liberdade (Cnil), autoridade responsável por regular o funcionamento da internet na França.

Figura 1: Mapa da proteção de dados pessoais ao redor do mundo.



Fonte: Cnil/França apud Serpro

Ainda, restringindo a matéria para o panorama da América Latina, o Imprensa Digital 126, produto laboratorial da Oficina de Jornalismo Digital da Faculdade de Comunicação da Universidade Federal da Bahia, realizou em outubro de 2019 um mapeamento do território a fim de apurar como e quando se devolveram as legislações latinoamericanas. Nele, verifica-se que os primeiros países a legislarem sobre proteção de dados foram, em ordem cronológica, Chile (Lei nº 19.628/1999); Argentina (Lei nº 25.326/2000); Uruguai (Lei nº 18.331/2008) e México (Lei Federal de Proteção de Dados Pessoais em Poder de Particulares, 2010). Repisa-se que o Brasil,



em que pese sua potência regional, possui uma das legislações mais tardias, datada de 2018 e que será melhor abordada adiante, em tópico específico.

Figura 2: Período de aprovação das Leis de Proteção de Dados Pessoais na América-Latina.



Fonte: Impressão Digital 126 (ID126)

Superadas tais considerações, de modo a dar enfoque aos principais progressos legislativos no âmbito da proteção de dados, faz-se necessário mencionar que a União Europeia e Estados Unidos se destacam no assunto, vez que os modelos por eles adotados influenciaram diversos outros ordenamentos jurídicos.

## 2.1 MODELO EUROPEU

A comunidade Europeia é pioneira em legislar sobre proteção de dados pessoais, sendo que o marco desse surgimento foi na década de 1970, quando a Alemanha promulgou a lei do Land de Hesse, cujo objetivo era, segundo Ruaro, Rodriguez e Finger (2011, p. 58), “assegurar a proteção de dados, proibindo a consulta, modificação ou destruição das informações pelas pessoas que não têm legitimidade para tanto”, em outras palavras, protegia o direito do indivíduo ter certo controle sobre seus dados pessoais. Foi essa mesma lei que instituiu, inclusive, a figura do

comissário para vigilância dos dados. Posteriormente, em 1977, foi promulgada a lei federal alemã chamada *Bundesdatenschutzgesetz*, responsável por concretizar o direito fundamental à essa autodeterminação informativa (ASSMANN, 2014).

Em seguida, outros países europeus também passaram a normatizar a matéria, a exemplo da Suécia que em 1973 criou a primeira lei nacional, que, apesar de sua abrangência, possuía lacunas no que diz respeito à princípios gerais de proteção de dados ou quando e como tais dados deveriam ser processados (Öman, 20--). Posteriormente, em 1978, veio a Lei francesa de proteção das liberdades e processamento automatizado de dados, a chamada *Informatique et Libertés*, o que se seguiu por países como Noruega, Dinamarca, Áustria, Luxemburgo e Islândia (DONEDA, 2019).

Outro importante momento foi a inclusão do direito à privacidade de dados enquanto direito fundamental na Constituição de Portugal em 1976, que, em seu Art. 35º, referente à utilização da informática, mencionava que:

1. Todos os cidadãos tem o direito de tomar conhecimento do que constar de registos mecanográficos a seu respeito e do fim a que se destinam as informações, podendo exigir a rectificação dos dados e a sua actualização.
  2. A informática não pode ser usada para tratamento de dados referentes a convicções políticas, fé religiosa ou vida privada, salvo quando se trate do processamento de dados não identificáveis para fins estatísticos.
  3. É proibida a atribuição de um número nacional único aos cidadãos.
- (PORTUGAL, 1976)

O mesmo sucedeu, a nível constitucional, na Espanha, em 1978, que em seus Arts. 18 e 105, dispunha que:

Artigo 18 - (...) 4. A lei limitará o uso da informática para garantir a honra e a intimidade pessoal e familiar dos cidadãos e o pleno exercício dos seus direitos. (ESPANHA, 1978)

Artigo 105 - A lei regulará: (...) b) O acesso dos cidadãos aos arquivos e registos administrativos, salvo no que afete à segurança e defesa do Estado, a averiguação dos delitos e a intimidade das pessoas. (ESPANHA, 1978)

Foram todas essas movimentações legislativas que levaram à Convenção 108, ou também chamada de Convenção de Strasbourg, de 1981, elaborada pelos, até então, 47 países membros do Conselho Europeu e aderida por outros nove não membros,

conforme relação divulgada no sítio eletrônico do Conselho da Europa. A referida Convenção simboliza os crescentes debates e a preocupação sobre os contornos do assunto no âmbito do continente europeu, tendo como finalidade máxima a unificação das normas para o tratamento de dados pessoais, relacionando-os aos direitos humanos. É o que se depreende das considerações iniciais e do próprio Art. 1º:

O objetivo desta Convenção é proteger todas as pessoas físicas, quaisquer que sejam suas nacionalidades ou residência, no que diz respeito ao tratamento de dados pessoais, contribuindo assim para o respeito pelos seus direitos humanos e liberdades fundamentais e incluindo o direito à privacidade. (COUNCIL OF EUROPE, 1981, tradução nossa)

Após a Convenção supramencionada, diversos Estados começaram a adequar suas legislações internas, sendo que, em fevereiro de 1992, tem-se ainda um marco importante para coesão e integração dos países europeus, qual seja, a assinatura do Tratado de Maastricht, responsável pela criação da União Europeia (UE) enquanto bloco econômico, da forma como é conhecida atualmente.

Com efeito, durante seus primeiros anos, o bloco promulgou a Diretiva 95/46/CE, um modelo de legislação que obrigatoriamente precisava ser transposto para o ordenamento jurídico de cada país membro em um determinado período de tempo, e que serviu para padronizar a proteção de dados na Europa. Lado outro, apesar de sua estrutura, esse ato não possui força de lei, o que abre margens para que cada país acrescente ou subtraia disposições, de acordo com suas próprias realidades, gerando certa desigualdade em termos de proteção de dados no contexto da UE.

Discorrendo brevemente sobre a forma como foi organizada, a Diretiva em questão possui 72 considerandos, cabendo ressaltar, neste ponto, que em alguns itens é mencionado o termo Sociedade da Informação, já aludido no presente trabalho, evidenciando que os olhares estavam voltados à essa captação, utilização e compartilhamento de dados pessoais em virtude do avanço das novas tecnologias. Ademais, logo no primeiro artigo da Diretiva é exposto o seu objetivo, oportunidade que se destaca a menção à proteção das liberdades e dos direitos fundamentais em assunto de tratamento de dados pessoais:

1. Os Estados-membros assegurarão, em conformidade com a presente directiva, a protecção das liberdades e dos direitos,

fundamentais das pessoas singulares, nomeadamente do direito à vida privada, no que diz respeito ao tratamento de dados pessoais.

2. Os Estados-membros não podem restringir ou proibir a livre circulação de dados pessoais entre Estados-membros por razões relativas à protecção assegurada por força do nº 1. (UNIÃO EUROPEIA, 1995)

Além disso, os Arts. 6º e 7º, constantes na Seção I e II, respectivamente, trazem consigo fundamentos principiológicos, tanto no tocante à qualidade dos dados, quanto à legitimidade para tratamento desses dados. Esses princípios que compõem a seara do direito são essenciais para identificar a intenção do legislador ao elaborar a Diretiva e são, conforme Carraza (1998 apud TOVAR, 2005, p. 1):

um enunciado lógico, implícito ou explícito, que, por sua grande generalidade, ocupa posição de preeminência nos vastos quadrantes do direito e, por isso mesmo, vincula, de modo inexorável, o entendimento e a aplicação das normas jurídicas que com ele se conectam.

Outrossim, é nessa Diretiva que se vislumbra a definição de dados pessoais, semelhante a concepção adotada até os dias atuais, vide Art. 2º, alínea “a”, *in verbis*:

Dados pessoais: qualquer informação relativa a uma pessoa singular identificada ou identificável (« pessoa em causa »); é considerado identificável todo aquele que possa ser identificado, direta ou indiretamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, econômica, cultural ou social; (UNIÃO EUROPEIA, 1995)

Após essa Diretiva, que submetia tanto setor público quanto o privado à disciplina de proteção de dados (DONEDA, 2019), a já mencionada Carta dos Direitos Fundamentais da União Europeia, de 2000, levou adiante essa sistemática, consignando, em seu Art. 8º, a proteção de dados pessoais:

Artigo 8º - Proteção de dados pessoais.

1. Todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito.

2. Esses dados devem ser objecto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva rectificação.

3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente

Observa-se, outrossim, que essa Carta consolidou “a tutela dos dados pessoais como um direito autônomo em relação à tutela da privacidade” (BRASIL, 2010a, p. 49). Isso porque trata-se agora do direito ao respeito pela vida privada em familiar em dispositivo apartado, qual seja, Art. 7º.

Ato contínuo, em 1997 é publicada a Diretiva 97/66/CE, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Esse novo ato destinou-se à complementar e ampliar a Diretiva anterior, considerando que na época estavam sendo introduzidas tecnologias digitais avançadas específicas ao setor público de telecomunicação, aumentando, por consequência, a preocupação em garantir a privacidade dos consumidores, uma vez que eles depositaram suas confianças na prestação daqueles serviços.

Cinco anos depois, é promulgada a Diretiva 2002/58/CE, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrônicas. Embora esteja em processo de revisão e atualização atualmente, essa diretiva também não traz tantas inovações se comparada às demais. No entanto, conforme exposto no item 6 das considerações iniciais, haja vista que “a internet está a derrubar as tradicionais estruturas do mercado”, ela teve como propósito, na forma do Art. 1º, harmonizar

as disposições dos Estados-Membros necessárias para garantir um nível equivalente de protecção dos direitos e liberdades fundamentais, nomeadamente o direito à privacidade, no que respeita ao tratamento de dados pessoais no sector das comunicações electrónicas, e para garantir a livre circulação desses dados e de equipamentos e serviços de comunicações electrónicas na Comunidade. (UNIÃO EUROPEIA, 2002)

É nessa Diretiva que também encontramos já algumas orientações acerca do *marketing* eletrônico, através de chamadas automáticas, aparelhos de fax, correio eletrônico (*e-mails*) e mensagens SMS. Isso porque é ali adotado o sistema *opt-in*, onde “o consumidor aceita previamente e por escrito ser incluído nos cadastros dos fornecedores que lhe interessam, filtrando antecipadamente ofertas que certamente rejeitariam” (DAVANZO, 2015). É o que se extrai do item 40 dos considerandos da mencionada Diretiva:

(40) Devem ser previstas medidas de protecção dos assinantes contra a invasão da sua privacidade através de chamadas não solicitadas para fins de comercialização directa, em especial através de aparelhos de chamadas automáticas, aparelhos de fax e de correio electrónico, incluindo mensagens SMS. Essas formas de comunicações comerciais não solicitadas podem, por um lado, ser relativamente baratas e fáceis de efectuar e, por outro, acarretar um ónus e/ou custo ao destinatário. Além disso, em certos casos o seu volume pode também provocar dificuldades às redes de comunicações electrónicas e ao equipamento terminal. No que diz respeito a essas formas de comunicações não solicitadas para fins de comercialização directa, justifica-se que se obtenha, antes de essas comunicações serem enviadas aos destinatários, o seu consentimento prévio e explícito. O mercado único exige uma abordagem harmonizada para assegurar, a nível da Comunidade, regras simples para o comércio e os utilizadores. (UNIÃO EUROPEIA, 2002)

Por fim, de modo a concluir o aparato da legislação europeia, é necessário citar o mais recente Regulamento (UE) 2016/679, conhecido como Regulamento Geral de Protecção de Dados (do inglês, *General Data Protection Regulation* – GDPR, que entrou em vigor em maio de 2018 na UE, revogando a Diretiva 95/46/CE e incentivando outros países a criar ou atualizar suas legislações a respeito de proteção de dados pessoais, até mesmo como forma de não terem suas relações comerciais prejudicadas. Um dos exemplos a ser citado é o Brasil, que elaborou a LGPD, a ser melhor examinada em tópico posterior.

Ao contrário das Diretivas, que precisam ser transpostas, a GDPR é uma norma autoaplicável, ou também chamada de norma de eficácia plena, isto é, aquela que já possui todos os elementos para produzir seus efeitos e serem aplicadas imediatamente desde a sua entrada em vigor, não dependendo de outras leis regulamentadoras (DINIZ, 2001 apud LEITE, 2020).

Todavia, ainda assim é possível que coexistam legislações nacionais sobre o tema nos Estados-membros, ocupando as lacunas deixadas pela GDPR, justamente para que essas leis internas possam dar maior coerência e clareza às disposições, tornando-as compreensíveis para as pessoas a quem se aplicam e adequadas às suas conjunturas.

Dando seguimento, logo em seu primeiro considerando o Regulamento diz que “a proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental” (UNIÃO EUROPEIA, 2016). Nessa perspectiva, interessante fazer um rápido adendo para mencionar que no Brasil, em 2019 foi aprovada a proposta de Emenda à Constituição (PEC) nº 17, visando inserir expressamente no texto constitucional a proteção de dados no rol de direitos fundamentais.

De mais a mais, dois itens iniciais, abaixo transcritos, bem elucidam o contexto em que se é pensada a aprovação do GDPR, dada a maior necessidade de se ter um controle e segurança na captação e utilização de dados pessoais por empresas privadas e entidades públicas, bem como garantir a relação de confiança para com os titulares.

(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. (UNIÃO EUROPEIA, 2016)

(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. (UNIÃO EUROPEIA, 2016)

Conquanto a análise da LGPD há de ser feita adiante, vale a pena trazer à atenção que, em comparativo com a GDPR, esta acaba sendo mais abrangente e completa, estabelecendo critérios normativos mais rigorosos. A título exemplificativo, tem-se o modo como se dá a vinculação entre o responsável pelo tratamento ao subcontratante, vez que o Art. 28 prevê que o tratamento em subcontratação deverá ser formalizado através de contrato ou outro ato normativo, listando nas alíneas

seguintes as matérias que ali deverão constar. Em contrapartida, a LGPD não exige a formalização desse vínculo.

Além disso, na GDPR a multa para empresas em casos de descumprimento da norma podem chegar a 20 milhões de euros ou até 4% do faturamento anual a nível mundial, de acordo com o que for mais elevado, vide Art. 83. Enquanto a LGPD prevê multa simples, de até 2% do faturamento, limitada à R\$ 50.000.000,00 (cinquenta milhões de reais) por infração, conforme Art. 52, inciso II.

De tudo quanto exposto acima, observa-se que o modelo europeu de proteção de dados possuía legislações pontuais que, com o passar dos anos, foram sendo unificadas e uniformizadas. Assim, este caracteriza-se, principalmente, por ser sistemático, em paralelo ao modelo norte-americano, a ser explorado a seguir, igualmente relevante e influente no assunto, mas que apresenta legislações e entendimentos de forma fracionada (DONEDA, 2019).

## 2.2 MODELO NORTE-AMERICANO

Para examinar a experiência do sistema jurídico norte-americano no tocante à proteção de dados e, em consonância ao quanto exposto na parte introdutória da presente Seção, é necessário iniciar a discussão pelo artigo de Samuel D. Warren e Louis D. Brandeis, intitulado de *The Right to Privacy*. É partir desse momento, no final do século XIX, que direito à privacidade desvincula-se do direito à propriedade e passa a ser pensado de forma autônoma, aproximando-se, em verdade, de um direito geral da personalidade, muito em decorrência de uma mudança de perfil nos Estados Unidos, que passou de rural para urbano e somou-se aos avanços tecnológicos (BUBLITZ; MACEDO; RUARO, 2013).

Da circunstância acima, extrai-se que, embora os Estados Unidos adote o sistema Common Law, tendo como fontes jurídicas de seu direito a jurisprudência, predominantemente, e a legislação, esta representada pela Constituição de 1787, o debate em torno da *privacy* surge através de uma criação doutrinária e não de um *leading case*, definido como “aquele que estabelece a lei sobre algum ponto importante” (LEFROY, 1914 apud FRIEDE, 2019).

De acordo com Doneda (2019), a popularidade do artigo de Warren e Brandeis também teve, *a priori*, um impacto negativo para o reconhecimento do *right do privacy*, porquanto o surgimento de um direito através da doutrina não compactuava com a



cultura jurídica dos magistrados. Basta mencionar que em um primeiro momento, em 1902, a Corte negou a existência do *right to privacy*, vide o caso *Roberson x Rochester Folding Box Co*, sendo esse reconhecido apenas em 1905, com o caso *Pavesich x New England Life Ins. Co.*, ambos envolvendo a utilização da imagem para fins comerciais.

Em paralelo ao debate doutrinário, a nível constitucional, embora não haja menção explícita no texto, a proteção à privacidade baseia-se, principalmente, na 4ª Emenda, onde diz que

O direito do povo à inviolabilidade de suas pessoas, casas, papéis e haveres contra busca e apreensão arbitrárias não poderá ser infringido; e nenhum mandado será expedido a não ser mediante indícios de culpabilidade confirmados por juramento ou declaração, e particularmente com a descrição do local da busca e a indicação das pessoas ou coisas a serem apreendidas. (ESTADOS UNIDOS, 1787)

Em suma, essa emenda garantiu aos cidadãos norte-americanos que não seriam expedidos mandados de busca e apreensão ilícitas, sem prévio indício de culpabilidade. Em outras palavras, a privacidade versava sobre o direito do cidadão em regular a ação governamental, devendo ser observado o devido processo legal. Ressalta-se que é somente em 1967, com o caso *Katz x United States*, que se amplia-se o entendimento de que a quarta emenda “destina-se a proteger pessoas e não lugares” (DONEDA, 2019, p. 229).

Salienta-se que a modificação constitucional supramencionada é a que mais se aproxima com a proteção dos dados pessoais, tendo em consideração, novamente, que o direito à propriedade foi transfigurado para um direito de natureza pessoal. Contudo, verifica-se que a Corte norte-americana não vinculou, propriamente, o *right to privacy* à proteção de dados pessoais, trazendo apenas preocupações mais gerais.

De ora em diante, na seara infraconstitucional, surgem diversas leis federais, com múltiplas legislações específicas para proteção de dados, uma particularidade dos Estados Unidos, dentre as quais: a) *Freedom of Information Act*, de 1966; b) *Fair Credit Reporting Act*, de 1970; c) *Privacy Act*, de 1974; d) *Freedom of Information Reform Act*, de 1986; e) *Driver’s Privacy Protection Act*, de 1994; f) *Electronic Freedom of Information Act Amendments*, de 1996; g) *Health Insurance Portability and Accountability Act*, de 1996, h) *Children’s Online Pivacy Protection Act*, de 1998. Considerando que o objetivo do presente Seção é apresentar com brevidade como se

deu o histórico legislativo internacional, não será feita uma análise detalhada de cada uma dessas leis, citadas apenas com o fito de evidenciar a fragmentação do modelo em comento.

Destas, chama-se a atenção apenas para a Privacy Act (1974), que representou um avanço no que diz respeito à proteção de dados privados. Basicamente essa lei federal “proibia a divulgação de informações pessoais por agências governamentais sem o prévio consentimento da pessoa envolvida” (ALVAREZ e TAVARES, 2017, p. 166). Lado outro, se de um lado essa lei estabelecia diversas garantias e princípios para salvaguardar os dados pessoais durante a coleta e tratamento de dados, tais como adequação e livre acesso do titular, de outro, seu campo de atuação era restrito aos registros em órgãos federais (BUBLITZ; MACEDO; RUARO, 2013).

De mais a mais, como visto anteriormente, enquanto o modelo europeu partiu de legislações pontuais para legislações mais detalhadas e uniformes, os Estados Unidos possuem normas mais fragmentadas, por vezes sem muita coesão. Há pouco, a Lei de Proteção de Dados mais relevante e estruturada no país veio do estado da Califórnia, com a *California Consumer Privacy Act*, aprovada em 2018 e em vigor desde janeiro de 2020, impulsionada pela *GDPR*.

Segundo consta no projeto de lei, que a Califórnia “é uma das líderes mundiais no desenvolvimento de novas tecnologias e indústrias relacionadas”. Assim, dada a crescente proliferação de informações pessoais, fez-se necessário estabelecer normas para salvaguardar a proteção de dados no país. Outrossim, é citado no texto o escândalo de março de 2018 envolvendo a empresa americana *Cambridge Analytica*, que teria coletado informações pessoais de diversos usuários do Facebook, utilizando-os, sobretudo, para fins políticos. Daí parte o interesse do país em intensificar o controle de privacidade e transparência na prática de coleta, uso e armazenamento de dados pelas empresas.

### **3. EVOLUÇÃO LEGISLATIVA BRASILEIRA**

De maneira oposta ao contexto internacional, a legislação brasileira em torno da proteção de dados ainda é muito recente. Para compor essa linha do tempo, esse trabalho partirá de uma sucinta análise de alguns pressupostos históricos, especialmente no tocante à proteção ao consumidor nos Estados Unidos, dando prosseguimento com o exame do Código de Defesa do Consumidor (1990), seguido da Lei do Cadastro Positivo (2011) e do Marco Civil da Internet (2014), até chegar na aprovação da Lei Geral de Proteção de Dados (2018).

#### **3.1 LEI Nº 8.078/1990 – CÓDIGO DE DEFESA DO CONSUMIDOR (CDC)**

É notório que os Estados Unidos é uma grande potência capitalista financeira, não obstante seja pioneiro quando o assunto é proteção ao consumidor. Autores como Nunes (2018), cita como início dessa tutela a edição da Lei de Sherman, em 1890, a legislação antitruste americana. Em suma, essa lei foi concebida para “limitar o poder de empresas exercerem o controle monopolístico de setores da economia ou provocarem restrições significativas ao livre comércio” (SILVA, 1995). Denota-se, portanto, que já havia a preocupação em proteger o consumidor, vulnerável nessa cadeia, de eventuais abusos pelo surgimento de grandes monopólios e cartéis.

Outrossim, como exposto no capítulo anterior, o período pós-revolução industrial, ou também chamado de Revolução Informacional, rompeu com os modelos tradicionais de produção e consumo, máxime devido ao avanço da tecnologia e possibilidade concreta de maximizar os níveis de oferta de serviços ou produtos, atendendo, assim, ao aumento no mercado de consumo do período. Em vista disso, pensou-se em um processo para uniformizar e aumentar em escala a produção, a chamada “standartização” (NUNES, 2018), o que alterou profundamente a estrutura econômica dos países capitalistas e seus ideais de negócio.

Com essa indústria dos bens de consumo em massa, ampliou-se a distância entre as partes dessa relação jurídica (fornecedor, fabricante, produtor ou prestador de serviço e o consumidor). Assim, do mesmo modo que se utilizaram do fortalecimento da tecnologia para alcançar cada vez mais compradores, os modelos de contrato da época também precisariam ser planejados da mesma forma, ou seja, também precisariam dessa padronização para acelerar as negociações. A partir de

então, surge o contrato de massa, que veio a ser conhecido anos depois como contrato de adesão pelo CDC.

É justamente nesse período, mormente a partir de 1960, que a defesa do consumidor ganha fôlego. Destaca-se que em março de 1962 o então presidente John F. Kennedy, em mensagem ao Congresso Nacional dos Estados Unidos, afirma: “Todos nós somos consumidores”, mostrando, portanto, a importância de legislar e garantir direitos básicos dos consumidores, entre eles: o direito de consumir com segurança, direito à informação, direito de escolha e direito a ser ouvido.

Tais movimentos se seguiram em todo território mundial. No Brasil não foi diferente, tendo em consideração que no Rio de Janeiro, em 1974, foi criado o Conselho de Defesa do Consumidor, com o objetivo de “receber as reclamações das fraudes e abusos praticados contra os consumidores” (CÉSAR, 1974), seguidos de outros órgãos semelhantes. Em São Paulo, nos dois anos seguintes, foi publicado o Decreto nº 7.890/76, responsável pela criação do Sistema Estadual de Proteção ao Consumidor.

Não há dúvidas que a grande conquista para os consumidores se deu em 1988, com a Constituição Federal da República Federativa do Brasil, afamada como “constituição cidadã”. Esse avanço justifica-se pelo fato de a Constituição Federal ter promovido o direito do consumidor como direito fundamental de todos os cidadãos, basta ver o Art. 5º, inciso XXXII, *in verbis*:

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

(...)

XXXII - o Estado promoverá, na forma da lei, a defesa do consumidor;  
(BRASIL, 1988)

Além disso, coteja a defesa do consumidor como princípio para ordem econômica, vide Art. 170, inciso V da mesma Carta. Por fim, ainda é estabelecido no Art. 48 do Ato das Disposições Constitucionais Transitórias (ADCT) o prazo de 120 dias para elaboração do CDC. Embora decorrido tal prazo, em 11 de setembro de 1990 surge o CDC, superando, enfim, a aplicação do Código Civil de 1916 nas relações jurídicas de consumo.

Esse percurso cronológico é essencial para o tema ora pesquisado, porque o CDC surgiu através da constatação de uma sociedade em transformação, cada vez mais dependente de recursos tecnológicos. Foi trazido à tona o protagonismo dos consumidores, ditando as regras na relação entre fornecedores e consumidores na tentativa de equiparar essas partes. Desse modo, o CDC impactou diretamente na promulgação da LGPD, sendo importante destacar que muitos dos titulares de dados são consumidores, nos termos do Art. 2º do CDC.

Um dos principais pontos de convergência entre essas legislações está amparado no Art. 43 do referido Código, o qual tratou de disciplinar os bancos de dados e cadastro dos consumidores. Como Bioni (2019) pontua, esse dispositivo abarca não somente informações negativas para fins de concessão de crédito, mas todo e qualquer dado pessoal do consumidor. Com efeito, constata-se que a lei consumerista em tela confere ao consumidor o poder de controlar suas próprias informações, o chamado direito à autodeterminação informativa já mencionado anteriormente e disposto no Art. 2º, II da LGPD.

### **3.2 LEI Nº 12.414/2011 – LEI DO CADASTRO POSITIVO (LCP)**

Suscintamente, a ideia do cadastro positivo foi proposta ainda em 2003, através do Projeto de Lei (PL) nº 836, seguido de outro Projeto em 2007, identificado sob o nº 405, que visava acrescentar um parágrafo ao citado Art. 43 do CDC. Ato contínuo, três anos depois foi editada a Medida Provisória (MP) nº 518, de 30 de dezembro de 2010, que visava disciplinar “a formação e consulta a banco de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito” (BRASIL, 2010b), culminando na Lei nº 12.414.

Desta forma, em conformidade com a sistemática adotada pelo CDC, a LCP “disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito” (BRASIL, 2011a). Ela é assim chamada por incluir informações de adimplemento de pessoas naturais ou jurídicas, com o fito de diminuir juros bancários ao cadastrado pelo pagamento em dia de suas contas.

Enquanto o CDC prevê que o consumidor deve ser comunicado por escrito em caso de abertura de cadastro, ficha, registro e dados pessoais e de consumo (§2º do Art. 43), a LCP ia além, exigindo também o consentimento prévio desse titular dos

dados. Todavia, em 2019 foi sancionada a Lei Complementar (LC) nº 166, dando nova redação ao Art. 4º, que prevê, agora, a inclusão automática nessa base de dados, devendo o cadastrado ser comunicado em até 30 dias após a abertura do cadastro (Art. 4º, §4º).

Mesmo após tais alterações, a LCP permanece de acordo com a LGPD, haja vista que no Art. 7º, X, é prevista a proteção do crédito como uma das hipóteses para tratamento dos dados. Além disso, continua sendo assegurado ao titular dos dados o acesso às informações e revisão ou cancelamento do cadastro.

Salienta-se que em relação à temática, o próprio Superior Tribunal de Justiça (STJ) possui entendimento sumulado no sentido de que

Súmula 550 - A utilização de escore de crédito, método estatístico de avaliação de risco que não constitui banco de dados, dispensa o consentimento do consumidor, que terá o direito de solicitar esclarecimentos sobre as informações pessoais valoradas e as fontes dos dados considerados no respectivo cálculo.

### **3.3 LEI Nº 12.965/2014 – MARCO CIVIL DA INTERNET (MCI)**

O Marco Civil da Internet, por muitos chamado de “Constituição da Internet”, é voltado para regular o uso da internet no país através de princípios, garantias, direitos e deveres. Não obstante tenha sido sancionado em 2014, após ampla participação popular, seu PL foi apresentado ainda em 2011, sob o número 2.126, tendo sido posteriormente apensado ao Projeto nº 5.403, de 2001, visto que este já tratava de matéria idêntica, qual seja, o acesso a informações da internet.

Frise-se que em setembro de 2013 foi solicitado, através da Mensagem nº 391, do Poder Executivo, a atribuição do regime de urgência para a apresentação do Projeto de Lei em questão (BRASIL, 2011b). Isso porque, poucos meses antes, houve diversas denúncias de que o Brasil estaria sendo alvo de espionagem eletrônica pelos órgãos de inteligência Estados Unidos (Caso Snowden), urgindo a preocupação em garantir o sigilo dos dados pessoais dos milhares de brasileiros (PEREIRA, 2014).

Assim, embora as leis anteriores, especialmente o CDC, já fosse aplicado de forma análoga aos assuntos relacionados à internet, o ordenamento jurídico brasileiro precisava, conforme texto encaminhado à Presidência da República, de “um texto de lei específico para o ambiente cibernético que garanta direitos fundamentais e promova o desenvolvimento econômico e cultural” (BRASIL, 2011b). Novamente

pontua-se o crescimento vertiginoso da internet e das relações digitais, cabendo ao Direito se adequar a essa nova e complexa realidade da sociedade da informação, sob o risco da matéria e eventuais violações desaguarem no Poder Judiciário, com possíveis decisões conflitantes e contraditórias entre si.

Logo em seu Art. 3º, incisos II e III, o MCI evidencia sua preocupação com a proteção da privacidade e dos dados pessoais, definindo-os como princípios desse regramento. Já a Seção II trata, que trata sobre a proteção aos registros, aos dados pessoais e às comunicações privadas, prevê em seu Art. 12 as medidas sancionatórias na hipótese de violação das normas, sendo a mais gravosa aquela indicada no inciso IV, referente a proibição de exercer as atividades que envolvam a coleta, armazenamento, guarda e tratamento de registros pessoais ou de comunicações.

No entanto, conforme Bezerra e Waltz (2014 apud OLIVEIRA, G. e JÚNIOR, 2020, p. 260)

O Marco Civil constitui talvez uma das pedras fundamentais para a promoção da liberdade de expressão, combate à censura e promoção de direitos constitucionais da internet, mas não encerra o debate, uma vez que é preciso avançar em termos técnicos, políticos, legais e sociais.

E assim ocorreu. Os debates foram ampliados e a legislação teve que avançar em determinados pontos, resultando no surgimento da LGPD.

### **3.4 LEI Nº 13.709/2018 – LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)**

Da análise de todos os regramentos normativos vistos até o presente momento, depreende-se que o ponto em comum entre todos reside no fato de o avanço exponencial das ferramentas tecnológicas ter tornado o tratamento de dados uma forte realidade no dia a dia. Além da própria entrada em vigor da GDPR ter influenciado a aprovação final da LGPD, vemos que os constantes escândalos envolvendo vazamento de dados pessoais exigiu o cuidado e atenção para criar ou robustecer cada vez mais a temática dentro dos ordenamentos jurídicos ao redor do mundo.

Além do caso já exposto durante os trâmites do MCI, cinco anos depois dele, no início de 2018, houve uma nova polêmica, dessa vez envolvendo a empresa

privada de consultoria *Cambridge Analytica*, responsável por expor mais de 50 milhões de dados pessoais de usuários da rede social *Facebook*, para fins de campanhas políticas durante as eleições de Donald Trump, nos Estados Unidos (BBC NEWS, 2018). Tais notícias se tornaram cada vez mais frequentes, afligindo sobretudo a população brasileira, que necessitava de uma lei específica ao tema.

Em que pese a aprovação da LGPD tenha se dado apenas em 2018, muito em decorrência dessa pressão por uma maior segurança de dados, é importante dizer que as discussões para tanto se iniciaram muito antes. Durante setembro a outubro de 2010 ocorreu o I Seminário de Proteção à Privacidade e aos Dados Pessoais, que tinha por objetivo “apresentar conceitos e identificar os desafios na Sociedade da Informação”, além de discutir as “implicações em setores específicos, tais como: comércio eletrônico, proteção infanto-juvenil, e governo eletrônico” (Comitê Gestor da Internet no Brasil, 2010).

Em novembro de 2010, o Ministério da Justiça promoveu a primeira consulta pública acerca do anteprojeto de lei de dados pessoais, o qual tinha por objetivo “assegurar ao cidadão o controle e a titularidade sobre suas próprias informações pessoais, como forma de garantia do direito constitucional à privacidade” (BRASIL, 2011?). Conforme informação divulgada no sítio eletrônico do Ministério da Justiça, durante os cinco meses, a consulta rendeu 14 mil visitas e 795 comentários. Houve ainda a abertura de uma segunda consulta pública, em 2015, cuja versão já levou em consideração os comentários e sugestões pontuadas na consulta anterior.

Em junho de 2012 foi apresentado na Câmara dos Deputados o PL nº 4.060, com 3 capítulos e 25 artigos, sendo que o primeiro deles delimita o objetivo da proposta em questão: “Art. 1º. Esta lei tem por objetivo garantir e proteger, no âmbito do tratamento de dados pessoais, a dignidade e os direitos fundamentais da pessoa natural, particularmente em relação a sua liberdade, privacidade, intimidade, honra e imagem.” (BRASIL, 2012).

Segundo a organização não-governamental Artigo 19 (2016), uma das principais críticas a esse Projeto é o fato de não trazer em seu Art. 7º o conceito de consentimento e os graus desse consentimento. Ao contrário, ao trabalhar no Capítulo II sobre os requisitos para tratamento de dados pessoais, o Art. 9º diz apenas que “Os dados pessoais serão tratados com lealdade e boa-fé, de modo a atender aos legítimos interesses dos seus titulares” (BRASIL, 2012). Outrossim, o Art. 12º diz que “O início do tratamento de dados pessoais sensíveis, quando não solicitado pelo



titular, somente ocorrerá mediante autorização deste, por qualquer meio que permita a manifestação de sua vontade, ou na hipótese de imposição legal” (BRASIL, 2012). Desse modo, vê-se que o texto do projeto “não assegura padrões mínimos de proteção aos titulares dos dados pessoais, em total desacordo com os padrões internacionais de direitos humanos” (ARTIGO 19, 2016, p. 39).

Posteriormente, em agosto de 2013, é proposto no Senado Federal o PLS nº 330. Aqui, fazendo uma breve comparação, percebe-se que o texto é um pouco mais robusto que o PL supracitado, contendo 12 capítulos, 19 artigos e diversos incisos. Nesse sentido, o Projeto em questão já trata como princípio o consentimento prévio e expresso do titular de dados e em seu Capítulo XI, da responsabilidade civil, indica uma responsabilidade objetiva – independente da verificação de culpa –, do proprietário, do usuário, do gestor e do gestor aparente de banco de dados, traço esse importante para a discussão chave do presente trabalho.

Em maio de 2016 foi apresentado pelo Poder Executivo o PL nº 5.276, sob o regime de tramitação com urgência, fruto de um amplo debate e participação pública. De acordo com a Artigo 19 (2016, p. 25), “o principal ponto positivo e diferencial em relação aos outros projetos de lei é a atribuição a um órgão competente da responsabilidade pela implementação e fiscalização das disposições da lei.” Em julho do mesmo ano, foi deferido o requerimento para apensá-lo ao PL nº 4.060/2012, por se tratarem de matérias correlatas.

Em maio de 2018 é finalmente aprovado o PL nº 4.060/2012, que agora passa a tramitar no Senado Federal sob a identificação de PLC nº 53/2018. Quatro meses depois o projeto é sancionado pelo até então presidente interino Michel Temer, transformando-se na Lei nº 13.709/2018, mas com vetos significativos, dentre eles, a criação da Autoridade Nacional de Proteção de Dados (ANPD).

Já ao final de seu mandato, em dezembro de 2018, Michel Temer promulgou a MP nº 869, que “altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, e dá outras providências” (BRASIL, 2018c). É em julho de 2019 que Jair Bolsonaro converte a referida MP e aprova criação na ANPD através da Lei nº 13.853, que teve cinco vetos no total, posteriormente revistos e a maioria deles anulados pelo Congresso Nacional. A estruturação regimental dessa Autoridade veio através do Decreto nº 10.474, de agosto de 2020.

Por fim, em abril de 2020 foi editada a MP nº 959 que prorrogava a *vacatio legis* da LGPD para 03 de maio de 2021, conforme seu Art. 4º, gerando muitas dúvidas em relação ao início da aplicabilidade da nova lei. Contudo, ao ser convertida na Lei nº 14.058/2020, observa-se que o artigo em apreço foi removido, razão pela qual em setembro de 2020 finalmente entrou em vigor a legislação para proteção de dados pessoais brasileira.

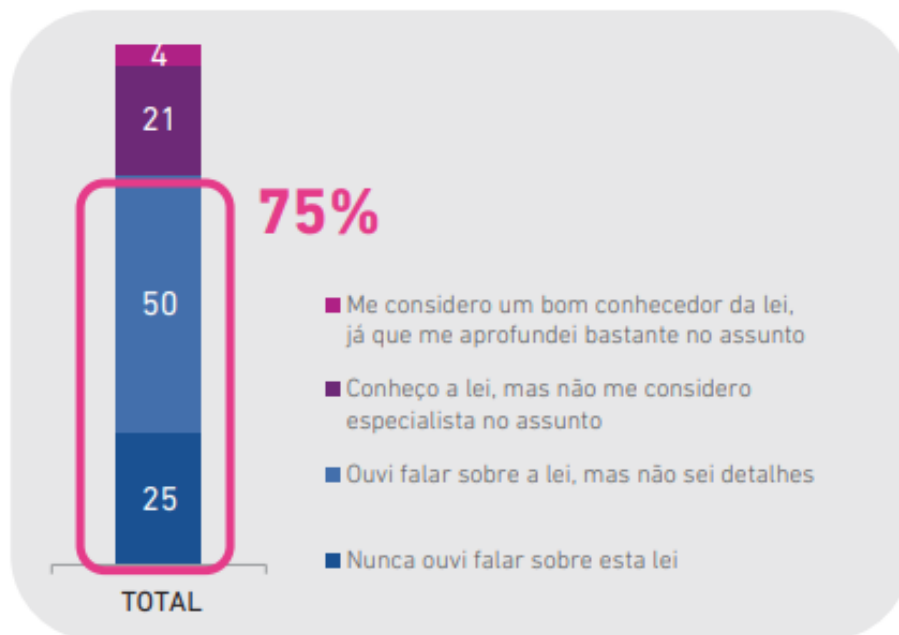
Ressalta-se que a Lei nº 14.010 de 10 de junho de 2020 prevê que as sanções administrativas só passarão a ser aplicadas a partir de 1º de agosto de 2021, dado ao período de pandemia.

#### 4. APLICABILIDADE E PRINCÍPIOS DA LEI GERAL DE PROTEÇÃO DE DADOS

Como pontuado, a LGPD entrou em vigor apenas em meados de 2020, sendo que seu conteúdo e aplicação ainda são pouco ou totalmente desconhecidos por boa parte dos brasileiros. É o que revelou o levantamento realizado pela Serasa Experian durante fevereiro e março de 2019 com 1.564 consumidores e 508 empresas de todas as regiões.

Da análise dos dados, constata-se que a maior parte dos consumidores nunca sequer ouviram falar da lei ou sabem muito pouco sobre ela, o que dificulta ou até mesmo impede o pleno exercício do direito que ela garante.

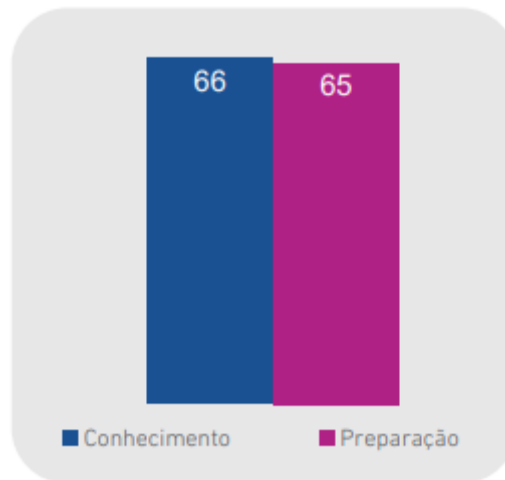
Figura 3: Conhecimento sobre a LGPD (consumidores)



Fonte: Serasa Experian

No entanto, se comparado às pessoas jurídicas, tais números sobem, indicando que 66% das empresas possuem o conhecimento da legislação.

Figura 4: Conhecimento sobre a LGPD (pessoas jurídicas)



Fonte: Serasa Experian

Além disso, em pesquisa publicada em fevereiro do ano corrente e noticiada no sítio eletrônico da Confederação Nacional de Dirigentes Lojistas (CNDL), a organização canadense OpenText, revelou que 60% dos brasileiros dizem ter uma “vaga ideia” da legislação, ao lado de 30% que dizem conhecer efetivamente e 10% que afirmam não saber do que se trata.

Logo, faz-se necessário uma resumida explanação acerca dos principais conceitos e princípios dispostos na LGPD, tendo em vista que isso facilitará no exame e interpretação do tópico concernente ao regime de responsabilidade adotado pela lei ora trabalhada, que frequentemente fará menção à tais termos.

#### 4.1 ESCOPO DE APLICAÇÃO

Entre os seus 10 capítulos e 65 artigos, logo no início a LGPD é clara ao dispor que se aplica a qualquer operação de tratamento de dados pessoais, realizados por pessoas físicas ou pessoas jurídicas de direito público ou privado, assim como às pessoas físicas que tenham seus dados tratados por tais agentes.

Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. (BRASIL, 2018b)

Apesar de mencionadas no artigo acima transcrito, é possível verificar que a LGPD não se aplica aos dados de pessoas jurídicas, sendo estas tão somente realizadoras desse tratamento. Isso porque seus dados já são tutelados no âmbito da Lei nº 9.279, de 14 de maio de 1996 (Lei da Propriedade Industrial). Há quem critique tal opção legislativa, a exemplo de FILHO e SOUSA (2021), que entendem que a proteção deveria ser estendida às pessoas jurídicas, especialmente porque a maioria são de pequenos negócios, cuja Constituição Federal já relaciona, em seu Art. 170, IX, como princípio da ordem econômica o “tratamento favorecido para as empresas de pequeno porte constituídas sob as leis brasileiras e que tenham sua sede e administração no País.” (BRASIL, 1988). Assim, eventuais danos oriundos do tratamento indevido de dados impactaria, efetivamente, a pessoa natural por trás da empresa.

Para mais, consoante Art. 4º da LGPD, também não se aplica a lei em evidência ao tratamento de dados realizados por pessoas naturais para fins exclusivamente particulares e não econômicos; jornalístico, artísticos, acadêmicos; assim como quando tratados pelo Poder Público para fins de segurança pública, defesa nacional, segurança do Estado, atividades de investigação e repressão de infrações penais; ou provenientes de fora do território nacional e que não tenha como destino agentes de tratamento brasileiros.

Por fim, embora não faça citação expressa, a lei também não se aplica a pessoas falecidas, pois em vários de seus artigos menciona que se destina às pessoas naturais, cuja personalidade se encerra com a morte, nos termos do Art. 6º do CC. Interessante pontuar que no regulamento europeu essa previsão é explícita, constante no item 27 das considerações iniciais, nos seguintes termos:” O presente regulamento não se aplica aos dados pessoais de pessoas falecidas. Os Estados-Membros poderão estabelecer regras para o tratamento dos dados pessoais de pessoas falecidas.”

## **4.2 PRINCIPAIS CONCEITOS**

O Art. 5º traz um rol de 19 incisos contendo as definições que norteiam a LGPD, dentre os quais serão destacados apenas cinco, citados ao longo dos Arts. 42 a 45, referentes a responsabilidade e ressarcimento de eventuais danos causados pela violação da legislação de proteção de dados.

### 4.2.1 DADO PESSOAL

A *priori*, considerando que o Art. 5º, I, da LGPD diz que dado pessoal é a “informação relacionada a pessoa natural identificada ou identificável”, Doneda (2019, p. 136) traz uma distinção entre informação e dado, entendendo que este “estaria associado a uma espécie de “pré-informação”, anterior à interpretação e a um processo de elaboração”, enquanto aquele “alude a algo além da representação contida no dado, chegando ao limiar da cognição”.

Dito isso, conforme Vainzof (2020), a LGPD adotou a interpretação expansionista do conceito de dados pessoais, pois se protege não apenas a informação relacionada à uma pessoa identificada (dados pessoais diretos), mas também aquela que tem o condão de tornar essa pessoa identificável (indiretos).

Tem-se como exemplo de dados pessoais: nome, RG, CPF, telefone, endereço, data de nascimento, estado civil, profissão, *cookies*, etc.

Salienta-se que o Art. 12 da referida lei exclui dos dados pessoais aqueles anonimizados, isto é, aqueles que passaram por um processo técnico durante o tratamento para que o titular não seja identificado, salvo se puderem ser revertidos.

### 4.2.2 TITULAR

Conforme Art. 5º, V, da LGPD, titular é toda “pessoa natural a quem se referem os dados pessoais que são objeto de tratamento”. Neste ponto menciona-se o Art. 2º do CC dispõe que a personalidade civil da pessoa natural, ou também chamada de pessoa física, “começa do nascimento com vida; mas a lei põe a salvo, desde a concepção, os direitos do nascituro”. Desse modo, a LGPD também reconhece como titular de dados pessoais os nascituros, tendo em vista que estes possuem personalidade jurídica formal desde a sua concepção (VAINZOF, 2020).

Reforça-se, como já explanado anteriormente, que pessoas jurídicas não são enquadradas como titulares de dados da LGPD.

### 4.2.3 CONTROLADOR E OPERADOR

Tais definições serão tratadas em conjunto neste subtópico, tendo em vista que tanto o controlador quanto o operador figuram-se como agentes de tratamento na LGPD, vide inciso IX do regramento em tela.

O primeiro diz respeito, de acordo com o inciso VI, à “pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais” (BRASIL, 2018b). Enquanto o segundo, conforme inciso subsequente, seria a “pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador”.

Isto significa que o controlador é o maior responsável na tomada de decisões nas operações envolvendo tratamento de dados, possuindo uma série de obrigações previstas no corpo da LGPD. Já o operador é subordinado ao controlador, podendo ser igualmente responsabilizado caso viole a legislação de proteção de dados (Art. 42, caput, LGPD), bem como responder solidariamente caso não siga as instruções lícitas do primeiro agente, situação em que será equiparado ao controlador (Art. 42, I, da LGPD).

Segundo Vainzof (2020, p. 98), é muito importante que seja precisamente identificado quem é o controlador e o operador nessa cadeia de proteção de dados, embora essa seja uma tarefa complicada dado que “devido à evolução da tecnologia da informação e da comunicação e à tendência de entidades serem e proverem serviços multidisciplinares, por vezes, haverá situações em que uma mesma pessoa jurídica será controladora e operadora”. É justamente por isso que a lei prevê no Art. 9º, III, em observância ao princípio do livre acesso, que o controlador se identifique ao titular.

#### **4.2.4 TRATAMENTO DE DADOS**

Por fim, o último conceito a ser visto é o de tratamento de dados, colocado na lei como sendo

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

Constata-se, portanto, uma ampla abrangência do que seria o tratamento de dados, abarcando desde a sua coleta até sua completa eliminação. Assim, o simples fato de os agentes armazenarem um dado já será considerado tratamento para fins leis, ainda que não haja propriamente uma utilização deles.

Por tais razões, é essencial que haja um mapeamento desses dados, vez que é dever dos agentes de tratamento manter registro de todas as operações (Art. 37, LGPD), sob as penas da lei.

### **4.3 PRINCÍPIOS**

Em conformidade com Lucca (2015 apud VAINZOF, 2020, p. 126), os princípios podem ser entendidos como “toda norma jurídica considerada determinante de outra ou outras que lhe são subordinadas, que a pressupõem, desenvolvendo e especificando ulteriormente o preceito em direções mais particulares”. Com efeito, e em consenso ao quanto já pontuado, examinar a base principiológica de uma legislação permite identificar a intenção real do legislador no momento da elaboração de uma norma jurídica.

Desde a Convenção 108 de 1981, relevante instrumento internacional no que tange a proteção de dados, já eram previstos princípios básicos a serem observados, basta visualizar os Arts. 4º e seguintes do Capítulo II, dentre os quais estão: legitimidade, segurança e transparência no processamento de dados, etc.

Os demais regramentos ao redor do mundo seguiram a mesma linha, inclusive a LGPD, cujos fundamentos principiológicos encontram-se no Art. 6º, sendo ali listados 11 princípios, contando aquele previsto no caput, quais sejam, boa-fé, finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e, por último, responsabilização e prestação de contas.

Destes, o trabalho ora desenvolvido se limitará à exposição de apenas quatro: necessidade, segurança, prevenção e responsabilização e prestação de contas. Tal recorte é em razão de serem os principais princípios na discussão sobre as bases de responsabilização civil dos agentes de tratamento, sendo pertinente que haja um maior enfoque no tema.



### 4.3.1 NECESSIDADE

Na literalidade do Art. 6º, III da LGPD, esse princípio diz respeito a “limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados”. De outro modo, a captação de dados ou qualquer outra operação prevista na lei devem ser estritamente necessárias à finalidade que motivou a coleta.

Esse princípio é refletido em outros artigos da LGPD, tal como Art. 9º, I, V e §2º, Art. 15, I e Art. 16, caput. Em suma, eles estabelecem o direito do titular em saber a finalidade do tratamento e consentir ou não, de forma prévia, caso haja alteração dessa finalidade. Para mais, atingir a finalidade a que se propôs representa o término do tratamento, devendo os dados pessoais serem eliminados pelos agentes.

A citar como exemplo, durante a pandemia foi editada a MP nº 954/2020, que versava sobre

o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020. (BRASIL, 2020)

Basicamente, estabelecia-se que as empresas de telecomunicações e prestadoras de serviço telefônico deveriam fornecer ao Instituto Brasileiro de Geografia e Estatística (IBGE) a relação dos nomes, números de telefones e endereços dos seus consumidores, sejam eles pessoas físicas ou jurídicas, vide Art. 2º da referida MP. A finalidade prevista era realizar entrevistas não presenciais para mapear novos casos de COVID-19 no país, dentre outras informações econômico-sociais.

No entanto, a medida em questão foi alvo de diversos questionamentos relacionados à necessidade na transferência desses dados, ainda mais por não disciplinar como se daria a supervisão durante esse tratamento. Essa MP foi alvo, inclusive, de diversas Ações Diretas de Inconstitucionalidades (ADIs), identificadas

sob as seguintes numerações: 6387, 6388, 6390, 6393 e teve sua vigência encerrada em agosto de 2020.

#### **4.3.2 SEGURANÇA**

O tratamento de dados pessoais sem um nível de segurança adequado é considerado irregular, visto que aumenta as chances de utilização de forma abusiva ou indevida, potenciando o vazamento de tais informações. É por isso que a LGPD, em seu Art. 6º, VII, determina a “utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão” (BRASIL, 2018b).

Esse princípio é fundamental para que os titulares de dados pessoais também tenham confiança nos agentes de tratamento e foi, em parte, aprofundado na Seção I do Capítulo VII da legislação, atinente a segurança e sigilo dos dados. Por certo, qualquer sujeito que intervir nesse tratamento deverá garantir a segurança da informação, mesmo após o seu término (Art. 47).

Eventuais danos pela inobservância da segurança dos dados, os agentes de tratamento deverão ser responsabilizados nos termos do Art. 42 a 45 da LGPD, sendo que as sanções administrativas estão disciplinadas a partir do Art. 52.

Para ilustrar a importância do respeito por tal princípio, em agosto do ano passado, houve o vazamento de dados pessoais de advogados brasileiros, decorrente de falhas de segurança no sítio eletrônico da Ordem dos Advogados do Brasil – OAB (RIBEIRO, 2020), situação essa que poderia ter sido evitada caso tivessem sido adotadas medidas adequadas de proteção.

#### **4.3.3 PREVENÇÃO**

O Art. 6º, VIII da LGPD estabelece que prevenção é a “adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais” (BRASIL, 2018b). Logo, a norma brasileira visa não apenas reparar os danos, mas agir de forma a evita-los, reduzindo os riscos antes mesmo de iniciado o tratamento.

Como colocado por Vainzof (2020, p. 146)

A prevenção esperada no princípio ora analisado deve ser pautada no conceito Privacy by Design (PbD), de Ann Cavoukian, pelo qual a proteção à privacidade advém da trilogia (i) sistemas de tecnologia informação (IT systems); (ii) práticas negociais responsáveis (accountable business practices); e (iii) design físico e infraestrutura de rede (physical and networked infrastructure)

É sob essa lógica que a LGPD trata na Seção II sobre boas práticas e governança. Além disto, a figura do encarregado, responsável por atuar como intermediário na comunicação entre o controlador, titulares e ANPD, se torna imprescindível, visto que entre suas atividades está “orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais” (Art. 41, III, LGPD).

Ainda, o relatório de impacto à proteção de dados pessoais, elaborado pelo controlador também se mostra indispensável no cumprimento desse princípio, já que descreve “medidas, salvaguardas e mecanismos de mitigação de risco”, veja Art. 5º, XVII da LGPD.

#### **4.3.4 RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS**

Por fim, o último princípio a ser visto encontra-se disciplinado no inciso X, onde diz que a responsabilização e proteção de dados representa a “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”. Aqui vislumbra-se que os agentes de tratamento estão sujeitos a responsabilização em caso de descumprimento da lei.

Segundo Vainzof (2020, p. 153),

Prever a responsabilização e a prestação de contas como princípio demonstra a intenção da Lei em alertar os controladores e os operadores de que são eles os responsáveis pelo fiel cumprimento de todas as exigências legais para garantir todos os objetivos, fundamentos e demais princípios nela estabelecidos. E não basta somente pretender cumprir a Lei, é necessário que as medidas adotadas para tal finalidade sejam comprovadamente eficazes. Ou seja, os agentes deverão, durante todo ciclo de vida de tratamento de dados sob sua responsabilidade, analisar a conformidade legal e implementar os procedimentos de proteção dos dados pessoais de acordo com a sua própria ponderação de riscos.

Quanto à prestação de contas, já foi mencionado durante a explanação da definição de tratamento de dados, que os agentes devem manter o registro de todas as operações realizadas para fins de tratamento de dados, haja vista que tais informações podem ser solicitadas a qualquer tempo, inclusive por determinação judicial no curso de uma ação (Art. 42, §2º, LGPD).

## 5. RESPONSABILIDADE CIVIL NO ÂMBITO DA PROTEÇÃO DE DADOS

Tal como visto, as legislações trabalhadas foram surgindo e se adaptando aos novos contornos da sociedade contemporânea, que é responsável por aumentar o tráfego e compartilhamento de dados pessoais através dos meios digitais. Assim, diante da alta possibilidade na captação e utilização indevida ou abusiva desses dados, foi essencial a criação de instrumentos que trazem consigo uma série de direitos e garantias aos titulares dos dados pessoais. Tanto é que constantemente vemos escândalos envolvendo o vazamento de informações.

Dessa forma, necessário se faz a análise do regime de responsabilidade adotado no âmbito da LGPD em caso de cessão indevida de dados pessoais, pois, “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.” (BRASIL, 2010a, p. 39)

### 5.1 O SURGIMENTO DA RESPONSABILIDADE CIVIL: BREVE HISTÓRICO

A responsabilidade civil é oriunda do direito das obrigações, vez que o cometimento de um ilícito gera o dever de reparar o dano (GONÇALVES, 2017).

Fazendo uma sucinta digressão histórica, Figueiredo e Figueiredo (2020) dizem que é possível remontar seu surgimento desde a fase pré-romana, onde imperava a vingança privada, normalmente coletiva e não racional. Sucessivamente, a Pena de Talião, conhecida pela máxima “olho por olho, dente por dente”, foi a principal caracterizadora dessa responsabilidade civil. Com ela, o Estado passa a ter do domínio de decidir quando e como se daria sua aplicação, mas a vítima que a executava e o próprio corpo do ofensor era utilizado como forma de reparação pelo delito cometido (SOUZA, 2015).

É apenas depois que essa vingança privada começou a ser substituída por uma reparação econômica. Com a criação da Lei das XII Tábuas, previu-se o pagamento de uma determinada quantia em dinheiro como consequência do dano cometido. A partir de então, se ingressa na fase romana, época houve uma tentativa de diferenciação entre pena e reparação e delitos públicos e privados (FIGUEIREDO; FIGUEIREDO, 2020). Assim, tendo em conta que o Estado toma para si, de forma

exclusiva, a função punitiva, ou seja, retira da vítima o papel de fazer justiça com as próprias mãos, surge para esta, por consequência, o direito de ação indenizatória civil (SOUZA, 2015).

Em continuidade cronológica, surge, no século III a.C, a *Lex Aquilia de Damno*, a qual cuidou de estabelecer as bases jurídicas da responsabilidade civil, sendo até hoje mencionada para se referir a responsabilidade civil extracontratual (aquiliana). Se antes a preocupação era apenas punir o ofensor (ROSENVALD, 2013), agora o objetivo era realmente indenizar a vítima do dano, o que representou um avanço para a temática e teve reflexos pelo mundo, perdurando até os dias atuais.

## **5.2 O INSTITUTO DA RESPONSABILIDADE CIVIL NO ORDENAMENTO BRASILEIRO**

No ordenamento brasileiro, foi a Constituição de 1824 que determinou a criação de um Código Civil separado do Criminal, tendo em vista que até então havia uma dependência entre as instâncias (FIGUEIREDO; FIGUEIREDO, 2020).

Art. 179. A inviolabilidade dos Direitos Civis, e Politicos dos Cidadãos Brasileiros, que tem por base a liberdade, a segurança individual, e a propriedade, é garantida pela Constituição do Imperio, pela maneira seguinte.

XVIII. Organizar-se-ha quanto antes um Codigo Civil, e Criminal, fundado nas solidas bases da Justiça, e Equidade. (BRASIL, 1824)

É somente em 1916 que advém o Código Civil, cuja responsabilidade civil foi tratada apenas no Art. 159 e fundamentada na culpa (subjativa).

Art. 159. Aquele que, por ação ou omissão voluntária, negligência, ou imprudência, violar direito, ou causar prejuízo a outrem, fica obrigado a reparar o dano. A verificação da culpa e a avaliação da responsabilidade regulam-se pelo disposto neste Código, arts. 1.518 a 1.532 e 1.537 a 1.553. (BRASIL, 1916)

Como já visto na Seção 3, após as mudanças no modelo de produção e de consumo ocasionadas pelo avanço tecnológico, o aumento no mercado de consumo e a complexidade das relações sociais poderia aumentar, em igual proporção, a possibilidade de danos, especialmente aqueles de natureza moral (NADER, 2016). Somado a isso, o distanciamento entre as partes integrantes daquela relação jurídica

dificultaria na identificação do ofensor e, por consequência, na verificação da culpa deste (OLIVEIRA, J., 2019).

É nesse sentido que Farias, Rosenvald e Netto (2015, p. 7) concluem que

em virtude dos desafios científicos e técnicos da contemporaneidade, exige-se um horizonte hermenêutico mais amplo para o conceito de responsabilidade. Por muito tempo essa responsabilidade moral se forjou na obrigação de reparar danos decorrentes de culpa. Mas aquele era o mundo das relações interindividuais. Atualmente, no amplo campo dos conflitos sociais e danos anônimos, atemporais e globais, o agente moral deliberará pela prevenção, como forma ética e virtuosa de comportamento. Esse é um caminho seguro para uma ordem jurídica que se queira justa.

De modo a seguir uma linha cronológica, a Constituição Federal promulgada em 1988, embora não trate expressamente da responsabilidade civil, teve sua importância ao prever a indenização por danos morais no rol de direitos e garantias fundamentais do Art. 5º, V e X, abaixo transcritos.

V - é assegurado o direito de resposta, proporcional ao agravo, além da indenização por dano material, moral ou à imagem;  
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; (BRASIL, 1988)

Para mais, é prevista também, no Art. 37, §6º, a responsabilidade de forma objetiva do Estado.

§ 6º As pessoas jurídicas de direito público e as de direito privado prestadoras de serviços públicos responderão pelos danos que seus agentes, nessa qualidade, causarem a terceiros, assegurado o direito de regresso contra o responsável nos casos de dolo ou culpa. (BRASIL, 1988)

O mesmo sucede nos Arts. 225, §3º e Art. 21, XXIII, alínea “d”, ambos da CF, quando ocorre dano ao meio ambiente devido ao risco da atividade desenvolvida ou danos nucleares. Vejamos:

Art. 225. Todos têm direito ao meio ambiente ecologicamente equilibrado, bem de uso comum do povo e essencial à sadia qualidade de vida, impondo-se ao Poder Público e à coletividade o dever de defendê-lo e preservá-lo para as presentes e futuras gerações. (...)

§ 3º As condutas e atividades consideradas lesivas ao meio ambiente sujeitarão os infratores, pessoas físicas ou jurídicas, a sanções penais e administrativas, independentemente da obrigação de reparar os danos causados. (BRASIL, 1988)

Art. 21. Compete à União:

(...)

XXIII - explorar os serviços e instalações nucleares de qualquer natureza e exercer monopólio estatal sobre a pesquisa, a lavra, o enriquecimento e reprocessamento, a industrialização e o comércio de minérios nucleares e seus derivados, atendidos os seguintes princípios e condições:

(...)

d) a responsabilidade civil por danos nucleares independe da existência de culpa; (BRASIL, 1988)

O CDC (1990), por seu turno, representou um marco com relação a responsabilidade civil no âmbito privado, dispondo que esta se dá, predominantemente, independente da comprovação de culpa (objetiva). Repita-se, isso ocorre em decorrência da complexidade das relações sociais na sociedade informacional. Cabe pontuar que o regime ora adotado pelo CDC, para fins de melhor compreensão da temática, será aprofundado adiante, quando em comparação com a LGPD, até para que se possa chegar à conclusão da pergunta central da pesquisa em comento.

Finalmente, em 2002, é promulgado o novo Código Civil, cujo anteprojeto já caminhava desde junho de 1975, sob a identificação do PL nº 634. Apesar de já nascer insuficiente para diversos desafios impostos pela sociedade contemporânea, agora a responsabilidade civil já é tratada nos Arts. 186 a 188, 927 a 943 e 944 a 954. Diversamente do Código anterior, é trazida a previsão da responsabilidade independentemente de culpa, compatibilizando ambos os sistemas.

De acordo com a classificação feita por Farias, Rosenvald e Netto (2015, p. 37), a responsabilidade civil possui três funções no direito brasileiro, sendo elas:

(1) função reparatória: a clássica função de transferência dos danos do patrimônio do lesante ao lesado como forma de reequilíbrio patrimonial; (2) função punitiva: sanção consistente na aplicação de uma pena civil ao ofensor como forma de desestímulo de comportamentos reprováveis; (3) função precaucional: possui o objetivo de inibir atividades potencialmente danosas.



É fato que muito falou-se em uma responsabilidade civil fundamentada na culpa ou, diversamente, independente dela. Logo, é imperioso que se faça uma distinção entre as teorias subjetiva e objetiva, cuja análise será feita sob o estudo da função reparatória da responsabilidade, “espinha dorsal do Código Civil”, nas palavras de Farias, Rosenvald e Netto (2015, p. 121). Tanto é que logo no primeiro parágrafo da Subseção 5.1 associou-se a responsabilidade civil ao dever de reparação do dano.

### 5.3 RESPONSABILIDADE CIVIL SUBJETIVA E OBJETIVA

De forma prática, tanto na responsabilidade civil subjetiva quanto na objetiva, é necessário que haja o total exaurimento dos seguintes pressupostos: a) ato ilícito, que, em síntese, é toda prática que vai de encontro à lei, ao ordenamento jurídico e interliga-se à conduta do agente ofensor; b) dano, que seria o resultado, a ofensa à um interesse juridicamente tutelado, seja ele de natureza material ou moral; c) nexo de causalidade, que é uma relação de causa e efeito, o liame entre o ato ilícito/conduta e o dano (NADER, 2016).

Lado outro, a principal diferença entre ambas as teorias reside na presença ou ausência do elemento subjetivo da conduta do agente, qual seja, a culpa em sentido *lato sensu*, que abarca tanto o dolo (intenção em praticar o ato danoso), quanto a culpa propriamente dita (*stricto sensu*). Se for necessário comprovar a culpa do agente causador do dano, trata-se da responsabilidade subjetiva, mas se o ofensor tiver que reparar a vítima independentemente de culpa, o caso é de responsabilidade objetiva (GONÇALVES, 2017).

Como já mencionado, o Código de 2002 começa a tratar da matéria em análise no Art. 186, que prevê: “Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito.” (BRASIL, 2002). Observa-se, dessa forma, que o referido Códex adota, predominantemente, a teoria subjetiva ou teoria da culpa para responsabilização, seguindo na mesma linha do Código de 1916 e com redação parecida, vide Art. 159 já reproduzido anteriormente.

Adiante é que se consagra a responsabilidade objetiva, com a expressão “independentemente de culpa”, ou também conhecida por Teoria do Risco, dada a segunda parte do parágrafo único do Art. 927, *in verbis*:

Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo.

Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem. (BRASIL, 2002)

A referida Teoria significa, em síntese, que “os danos provocados por quem mantém atividade perigosa por natureza devem ser reparados, ainda que o agente tenha envidado esforços no sentido de evitar os resultados nocivos” (NADER, 2016, p. 147). No mesmo sentido compreendem Farias, Rosenvald e Netto (2015, p. 443), pontuando que a mensagem trazida pela leitura do artigo há pouco reproduzido é de que

o risco é especial e inerente à particular potencialidade lesiva de uma atividade, pois a despeito de quem a coordena, o seu simples desenvolvimento induzirá a produção de danos quantitativamente numerosos ou qualitativamente graves. A atividade em si é lícita e tolerada por sua utilidade social, apesar de ser fonte de cometimento de danos.

Diante do exposto, a chegada da LGPD provocou uma série de questionamentos em relação à qual seria o regime de responsabilidade civil ali adotado, inaugurando verdadeiro debate doutrinário sobre o assunto. Dada a relevância que a proteção de dados foi adquirindo ao longo das décadas e a potencialidade de danos que podem ser causadas aos titulares em caso de tratamento irregular. Destarte, se torna imprescindível e ideal uma análise da redação da lei, confrontando-a com um conjunto de outras fontes, visto que o país está inserido em uma nova realidade.

#### **5.4 PREVISÃO NA LEI GERAL DE PROTEÇÃO DE DADOS**

Já caminhando ao término do presente trabalho, foi possível observar que a nossa legislação para proteção de dados levou anos até sua construção, visivelmente impulsionada pela rápida transformação da sociedade, que está cada vez mais hiperconectada, trocando centenas de informações em milésimos de segundos no mundo virtual.

Para que chegasse até a sua redação atual, houve diversos debates e contribuições através consultas públicas, as quais acabam se tornando, neste momento, uma importante ferramenta para tentar entender a intenção do legislador ao dispor do tema. Fato é que as significativas alterações nos textos geraram confusão quanto ao regime de responsabilidade civil adotado na LGPD, disciplinado entre os Arts. 42 a 45, inaugurando um verdadeiro debate doutrinário.

Dentre as principais mudanças, o anteprojeto submetido à consulta pública em 2010 pelo Ministério da Justiça aparentemente favoreceu em seu Art. 6º uma responsabilização objetiva ao mencionar que “O tratamento de dados pessoais é atividade de risco (...)”. Logo, de acordo a teoria já vista, aquele que causasse dano a outrem deveria promover sua imediata reparação, ainda que isento de culpa, dado o risco da atividade que exerce.

Da mesma forma o anteprojeto de 2015 dispõe, em seu Art. 31, que “O cedente e o cessionário têm responsabilidade solidária pelo tratamento de dados realizado no exterior ou no território nacional, em qualquer hipótese, independente de culpa.” (BRASIL, 2015). Novamente a expressão dirige-se à uma objetividade, no entanto, esse artigo se relaciona aos casos de transferência de dados, sendo que no Art. 35 do Capítulo VII, exclusivo da responsabilidade dos agentes, a responsabilidade adotada já se assemelha, em teoria, à subjetiva. Senão, vejamos: “Todo aquele que, por meio do tratamento de dados pessoais, causar a outrem dano material ou moral, individual ou coletivo, é obrigado a ressarcir-lo.”. (BRASIL, 2015)

Essa mescla de sistemas gerou, até mesmo, comentários nesse sentido dos participantes da consulta.

[O Art. 31] prevê a responsabilidade solidária e objetiva, exclusivamente quanto à transferência de dados. Mais à frente, a Lei estabelece responsabilidade subjetiva aos agentes, nas demais formas de tratamento. (Comentário feito por Associação Brasileira de Direito da Tecnologia da Informação e das Comunicações – ABDTIC, em 2 de julho de 2015 às 02:56)

Ainda assim os participantes defenderam a adoção da responsabilidade objetiva dos agentes.

Apoiamos a proposta de determinar a aplicação da disciplina da responsabilidade objetiva ao tratamento de dados pessoais. Ocorrendo qualquer espécie de dano, em âmbito individual, coletivo

ou difuso, o encarregado pelo tratamento será responsável independentemente de culpa, isto é, independentemente de ter agido com negligência, imprudência ou imperícia. São admitidas aqui as exceções comuns à essa disciplina - culpa exclusiva da vítima ou força maior. (Comentário feito por Veridiana Alimonti – Intervenções, em 6 de julho de 2015 às 02:07)

[...] o sistema a ser adotada deve ser o da atividade de risco, a fim de que quem processa dados pessoais seja responsabilizado objetivamente - independentemente de culpa. Essa é a tendência nas demais relações de consumo em que quem exerce uma atividade de risco somente não será responsabilizado havendo culpa exclusiva da vítima e/ou força maior. (Comentário feito por Grupo de Pesquisa em Políticas Públicas para o Acesso à Informação/GPoPAI da USP, em 8 de junho de 2015 às 21:07)

O PLC nº 53/2018, por sua vez, aproximou-se aparentemente mais do Art. 35 do anteprojeto de 2015. Sua redação teve poucas mudanças quando transformada, de fato, na LGPD, sendo substituída apenas o termo “o responsável ou o operador” por “o controlador ou o operador” no caput do Art. 42. Vejamos o comparativo:

Art. 42. **O responsável ou o operador** que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo. (BRASIL, 2018a, grifo nosso)

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

Em razão dessas modificações ao longo da tramitação do projeto, autores como Gustavo Tepedino, Aline Terra e Gisela Guedes (2021) defendem que a LGPD se pautou em um regime subjetivo de responsabilização, porquanto os vestígios de objetividade foram omitidos na aprovação do texto final. Embora os autores reconheçam que há as semelhanças entre a LGPD e o CDC, afirmam que há diferenças substanciais em algumas passagens, tais como o próprio Art. 42 supracitado e os Arts. 12 e 14 do CDC, que expressamente trazem o termo “independentemente da existência da culpa” para tratar da responsabilidade do fornecedor pelo fato do produto e do serviço.

Ademais, asseguram que quando se compara o Art. 43 da LGPD com o Art. 12, §3º do CDC, embora ambos também tenham redações similares, o inciso II seria a chave central para distingui-los.

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

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

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

III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro. (BRASIL, 2018b)

Art. 12. O fabricante, o produtor, o construtor, nacional ou estrangeiro, e o importador respondem, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos decorrentes de projeto, fabricação, construção, montagem, fórmulas, manipulação, apresentação ou acondicionamento de seus produtos, bem como por informações insuficientes ou inadequadas sobre sua utilização e riscos.

(...)

§ 3º O fabricante, o construtor, o produtor ou importador só não será responsabilizado quando provar:

I - que não colocou o produto no mercado;

**II - que, embora haja colocado o produto no mercado, o defeito inexistente;** (grifo nosso)

III - a culpa exclusiva do consumidor ou de terceiro. (BRASIL, 1990)

Isso porque no CDC, alegam que o inciso II faz referência ao nexo de causalidade, um dos pressupostos da responsabilidade civil, entendimento esse que também é seguido pela jurisprudência.

APELAÇÃO CÍVEL – AÇÃO DE INDENIZAÇÃO POR DANOS MATERIAIS E MORAIS – UTILIZAÇÃO DE PROTETOR SOLAR DE FABRICAÇÃO DA RÉ – REAÇÃO ALÉRGICA – RELAÇÃO ENTRE AS LESÕES DE PELE E O USO DO PRODUTO NÃO COMPROVADA – DIAGNÓSTICO DO AUTOR DE DERMATITE CRÔNICA – LAUDO PERICIAL MÉDICO NO SENTIDO DE QUE O AUTOR NÃO POSSUI ALERGIA AOS COMPONENTES DO PROTETOR SOLAR – DOENÇA CAUSADA POR OUTROS FATORES – **AUSÊNCIA DE DEFEITO NO PRODUTO – NEXO DE CAUSALIDADE NÃO CONFIGURADO – DEVER DE INDENIZAR INEXISTENTE – INTELIGÊNCIA DO ARTIGO 12, §3º, II DO CDC** – SENTENÇA MANTIDA – MAJORAÇÃO DOS HONORÁRIOS EM GRAU RECURSAL – INTELIGÊNCIA DO ART. 85, §11 DO CPC. RECURSO DE APELAÇÃO NÃO PROVIDO. (TJ-PR – APL - 0002993-06.2016.8.16.0108; Relator: Juiz Alexandre Barbosa Fabiani, Data de

Julgamento: 23/03/2020, Data de Julgamento: 23/03/2020, 8ª Câmara Cível, Data de Publicação, 24/03/2020) (grifo nosso)

Ao passo em que o dispositivo na LGPD estaria ligado à culpa, eximindo os agentes de tratamento da responsabilização caso comprovem que não houve violação da legislação de proteção de dados.

Além disso, justificam seus posicionamentos igualmente amparados nos diversos deveres e padrões de conduta (*standards*) que são atribuídos aos agentes de tratamento de dados ao longo da legislação, maiormente no Capítulo VII, chegando à conclusão de que “não haveria razão para o legislador impor tantos deveres, fixando preciso padrão de conduta, se fosse para responsabilizar os agentes, independentemente de terem esses agido ou não com culpa” (TEPEDINO, TERRA; GUEDES, 2021, p. 438)

Por fim, um dos últimos argumentos defendidos é de que, embora se diga que o Art. 927 do CC/2002 tenha sido inspirado, respectivamente, nos Arts. 2.050 e 493 dos Códigos italiano e português, da análise destes, depreende-se que trazem, efetivamente, uma noção de culpa presumida e não uma autêntica cláusula de responsabilidade objetiva como o Código brasileiro. Assim, conclui que a LGPD estaria muito mais próxima dessas legislações estrangeiras do que com a brasileira.

Art. 2050 Responsabilidade pelo exercício de atividades perigosas: Quem causar danos a outrem no exercício de uma atividade perigosa, pela sua natureza ou pela natureza dos meios utilizados, está obrigado a pagar uma indenização, **se não provar** que tomou todas as medidas adequadas para evitar o dano. (ITÁLIA, 1942, grifo e tradução nossa)

ARTIGO 493º (Danos causados por coisas, animais ou actividades) 1. Quem tiver em seu poder coisa móvel ou imóvel, com o dever de a vigiar, e bem assim quem tiver assumido o encargo da vigilância de quaisquer animais, responde pelos danos que a coisa ou os animais causarem, salvo se provar que nenhuma culpa houve da sua parte ou que os danos se teriam igualmente produzido ainda que não houvesse culpa sua. 2. Quem causar danos a outrem no exercício de uma actividade, perigosa por sua própria natureza ou pela natureza dos meios utilizados, é obrigado a repará-los, **excepto se mostrar** que empregou todas as providências exigidas pelas circunstâncias com o fim de os prevenir. (PORTUGAL, 1966, grifo nosso)

Neste ponto em específico, embora ambos os dispositivos falem de uma atividade perigosa, a teoria do risco não se confunde com a da culpa presumida, pois

na primeira sequer discute-se a existência ou não de culpa, o dever de reparar ocorre independentemente disso (FARIAS; ROSENVALD; NETTO, 2015). Então, se os dispositivos acima dão a possibilidade de comprovar que não houve aquele ato ilícito culposo, eles encaixam-se na teoria subjetiva, motivo pelo qual os autores defendem a convergência da LGPD com eles. Tanto o é que o Art. 43, caput, traz a locução “(...) só não serão responsabilizados quando provarem(...)”.

As alterações substanciais na redação durante o processo de tramitação da LGPD e as diferenças com o CDC também são dois dos argumentos utilizados por Bioni e Dias (2020), que sustentam que é preciso ir além da visão binária de responsabilidade civil (objetiva x subjetiva), entendendo que, em verdade, a LGPD adota um regime subjetivo com alto grau de objetividade.

Ambos sinalizam que a inclusão do princípio da *accountability*, na lei chamado de princípio da responsabilização e prestação de contas (Art. 6º, X) e aqui trabalhado na Subseção 4.3.4, assim como a previsão de relatórios de impacto, reitera o direcionamento subjetivo da lei. Na mesma ótica dos autores da corrente anterior, Bioni e Dias (2020, p. 8) entendem que há um “juízo de valor em torno da conduta do agente de tratamento de dados para a sua responsabilização”, pois ele teria que demonstrar que cumpriu a lei e que as medidas adotadas foram eficazes.

Além disso, os autores sustentam que a LGPD não classifica toda e qualquer atividade de tratamento como de risco, o que a afasta da responsabilidade objetiva. É o que extraem da definição de relatório de impacto trazido no Art. 5º, XVII da LGPD, e como igualmente pode ser observado no Art. 55-J do mesmo regramento.

XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que **podem gerar riscos** às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco; (BRASIL, 2018b, grifo nosso)

Art. 55-J. Compete à ANPD:

XIII - editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os **casos em que o tratamento representar alto risco** à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei; (Incluído pela Lei nº 13.853, de 2019) (BRASIL, 2018b, grifo nosso)

Em conclusão, os autores apontam o alto grau de objetividade da lei, em decorrência do princípio há pouco referido, pois ali se fala em adoção de “medidas eficazes” pelos agentes de tratamento. Assim, a lei estaria deixando subtendido uma obrigação de resultado ou, em outros termos, que “(...) não basta apenas adotar (...) medidas a evitar o tratamento inadequado de dados, mas, tais ações devem ser eficientes.” (BIONI; DIAS, 2020, p. 20). Com efeito, essa corrente deduz que embora haja a possibilidade de afastar a culpa os agentes de tratamento, dificilmente isso ocorreria.

A terceira corrente que aqui se propõe analisar é a objetiva. Conforme apontam Tepedino, Terra e Guedes (2021), o principal argumento para os que seguem essa linha de posicionamento é a similitude da LGPD com o CDC.

Não obstante nem todo tratamento de dados seja oriundo de uma relação de consumo, a maioria dos interesses dos titulares de dados partirão dessa seara. Com efeito, Doneda e Mendes (2018) destacam que a LGPD preceitua logo em seu Art. 2º, VI, dentre outros fundamentos, a defesa do consumidor, consolidando a interação e diálogo entre as fontes. O mesmo verifica do Art. 18, § 8º e Art. 45 da LGPD.

Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

(...)

§ 8º O direito a que se refere o § 1º deste artigo também poderá ser exercido perante os organismos de defesa do consumidor. (BRASIL, 2018b)

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

Complementando a ideia, Vainzof (2020, p. 46) assinala que

Tal ênfase na defesa do consumidor quanto ao tema proteção de dados deriva da era em que produtos e serviços são definidos e customizados de acordo com as opiniões e interesses de cada pessoa, mediante a publicidade direcionada, seja ela contextual, seja segmentada.

É o que Miragem (2019), outro defensor da responsabilidade objetiva, atribui como característico de uma “economia da especialização flexível”, onde fornecedores buscam direcionar publicidades à um determinado público-alvo. Para tanto, faz-se



necessário uma maior captação de dados pessoais a fim de identificar tais consumidores e suas respectivas preferências no mercado.

O autor supracitado também destaca como efeito prático do Art. 45 o fato de que os consumidores afetados pelo tratamento irregular de dados poderão ingressar com uma ação indenizatória dentro do prazo de cinco anos, conforme Art. 27 do CDC. Além disso, Miragem (2019) enfatiza que a LGPD adotou expressamente uma interpretação sistemática com os direitos dos consumidores e demais instrumentos normativos ao preceituar, em seu Art. 64, que: “Os direitos e princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.” (BRASIL, 2018b)

Além disso, tal como o CDC em seu Art. 6º, VIII, a LGPD traz a previsão do ônus da prova (Art. 42, §2º), de modo a assegurar o equilíbrio e a paridade de armas entre os sujeitos da relação.

Art. 42 (...) § 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa. (BRASIL, 2018b)

Art. 6º São direitos básicos do consumidor: (...) VIII - a facilitação da defesa de seus direitos, inclusive com a inversão do ônus da prova, a seu favor, no processo civil, quando, a critério do juiz, for verossímil a alegação ou quando for ele hipossuficiente, segundo as regras ordinárias de experiências; (BRASIL, 1990)

Outra tese defensiva de tal regime já foi parcialmente aventada em parágrafos anteriores. Trata-se da redação praticamente idêntica entre o Art. 43 da LGPD e os Arts. 12, §3º e 14, §3º do CDC. Conquanto Tepedino, Terra e Guedes (2021) sustentem que o inciso II do Art. 43 da LGPD estaria ligado à culpa e não ao nexo de causalidade, Miragem (2019) pontua que no caso da LGPD, o defeito do serviço se caracterizaria pelo tratamento irregular dos dados, em desconformidade à legislação. Portanto, as hipóteses de excludentes de responsabilidade do CDC estão em simetria com aquelas previstas na LGPD.

O Art. 44 também é alvo de interpretações distintas entre aqueles que defendem a responsabilidade subjetiva e objetiva. O dispositivo em questão assim dispõe:

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

I - o modo pelo qual é realizado;

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

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

Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano. (BRASIL, 2018b)

O primeiro grupo de doutrinadores examinam sob a ótica do parágrafo único acima transcrito, afirmando que o legislador optou por responsabilizar os agentes de tratamento somente quando eles não provarem que seguiu todas as medidas de segurança previstas na lei, ou seja, novamente seria preciso a verificação de culpa (TEPEDINO; TERRA; GUEDES, 2021). Em contrapartida, o segundo grupo nota, mais uma vez, proximidade com os dispositivos da norma consumerista, pois ambos os sistemas estabelecem as regras que devem ser observadas para o cumprimento do dever de segurança, dado o risco inerente à atividade (MIRAGEM, 2019). Enfatiza-se que a LGPD elenca como princípio a segurança no tratamento de dados pessoais, trabalhado na Subseção 4.3.2.

Dando continuidade aos fundamentos elencados, Doneda e Mendes (2018 apud MULHOLLAND, 2020) entendem também que os princípios que norteiam a LGPD apontam para o enquadramento do tratamento de dados como atividade de risco, a começar pelo princípio da necessidade, previsto no Art. 6º, III da LGPD e explanado na Subseção 4.3.1 do presente trabalho, o qual limita o tratamento “ao mínimo necessário para a realização de suas finalidades”. A intenção da legislação seria justamente impor que os agentes de tratamento captem a menor quantidade possível de dados pessoais, reduzindo os riscos de causar danos aos titulares.

Ainda de acordo com Doneda e Mendes (2018 apud MULHOLLAND, 2020), o princípio da responsabilização e prestação de contas também um indicativo dessa objetividade. Para os autores, ao exigir-se que os agentes tomem medidas de acordo com as boas práticas e de governança impostas pela lei e prestem conta disso ao titular dos dados, prioriza-se uma relação de transparência entre as partes envolvidas nessa atividade. Entre essas boas práticas incluem a elaboração de um relatório de impacto à proteção de dados pessoais.

Se de um lado Bioni e Dias (2020) defendem acima que a expressão “podem causar riscos” na definição de relatório de impacto colocada no Art. 5º, XVII da LGPD, significa que nem toda atividade de tratamento é de risco, por outro Doneda e Mendes (2018 apud MULHOLLAND, 2020) dão enfoque no texto ao final do artigo, que menciona “mecanismos de mitigação de risco”, concluindo que a legislação já parte do pressuposto dos riscos inerentes à essa atividade, tanto é que determina a adoção de medidas para mitiga-los, diminui-los, assim como os danos por ele potencialmente poderão ser causados.

Por fim, autores como Maria Celina Bodin de Moraes e João Quinelato de Queiroz (2019) seguem uma quarta linha, para além de uma classificação binária de responsabilidade civil, defendendo um novo regime denominado ativo ou proativo e, em tese, mais maduro que os demais. Os autores baseiam essa teoria igualmente no princípio a responsabilização e prestação de contas e na intenção do legislador em não somente reparar, mas prevenir a ocorrência de danos.

Desse modo, conforme pontuam os autores,

esta responsabilidade especial, à semelhança do que ocorre no Regulamento europeu, está articulada em torno de três noções fundamentais, que devem ser somadas: i) dano, ii) violação da legislação de proteção dos dados por parte do controlador e/ou operador e iii) reparação.

Em linhas gerais, é possível reparar que os autores não repelem categoricamente que a LGPD teria adotado o regime de responsabilidade subjetiva, mas unicamente que o legislador teria transcendido-o, inovando ao determinar que os agentes de tratamento atuem conscientemente, com uma postura proativa para identificar o próprio risco de suas atividades e, por conseguinte, evita-las, da mesma forma como prega o princípio da prevenção disposto no Art. 6º, VIII da LGPD.

Em suma, a partir da análise das correntes apontadas, bem como de todo o contexto normativo brasileiro, o presente trabalho filia-se aos argumentos doutrinários que entendem pela previsão de uma responsabilidade objetiva no âmbito da LGPD. Soma-se à tais apontamentos o episódio semelhante já ocorrido com o Marco Civil da Internet, onde a responsabilidade dos provedores de internet virou alvo de discussão no Supremo Tribunal Federal (STF), através do Tema 987, ainda em trâmite.

Resumidamente, questiona-se a constitucionalidade do Art. 19 do MCI, transcrito abaixo, haja vista que este imputa ao usuário o dever de recorrer à justiça para tornar indisponível determinado conteúdo tido como infringente e, eventualmente, requerer a responsabilização dos provedores.

Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário. (BRASIL, 2014)

De acordo com Frazão e Medeiros (2021), o dispositivo supracitado coloca a liberdade de expressão em um patamar superior em relação a outros princípios e garantias constitucionais. As autoras também se valem do princípio da *accountability*, já mencionado anteriormente, para ratificar a necessidade que os *designs* das plataformas adotem padrões mínimos de zelo e segurança, ponderando os riscos que dali decorrem.

Como sinalizado, debate semelhante pode ocorrer por conta da amplitude interpretativa da LGPD. No entanto, a leitura mais assertiva ao caso deve se valer da observância do conjunto normativo brasileiro e do potencial danoso da atividade de tratamento de dados.

## 6. CONCLUSÃO

Foi possível notar com o presente trabalho que o direito à privacidade foi inicialmente pensado sob a ótica do direito de ser deixado só (*right to be let alone*). No entanto, com o passar dos anos esse direito foi ganhando novos contornos, tornando-se mais complexo e aproximando-se, efetivamente, de uma tutela da personalidade humana. Não basta apenas ter direito à tranquilidade, de não ter os espaços privados violados, mas ter a garantia da autodeterminação afirmativa, de poder ter o controle das próprias informações.

É em meados do século XX que se tem a chamada revolução informacional, com um vertiginoso desenvolvimento tecnológico e fluxo de informações. A partir desse momento, constata-se uma ruptura nos modelos tradicionais de produção e consumo e a privacidade agora começa a ser também observada pela perspectiva do tratamento de dados, razão pela qual foi surgindo ao redor do mundo diversas legislações específicas à essa proteção, dentre as quais analisou-se aqui o modelo europeu e norte-americano, influenciadores de diversos outros ordenamentos jurídicos, inclusive do Brasil.

No cenário brasileiro, especificamente, viu-se que a Lei Geral de Proteção de Dados surgiu de forma tardia, entrando em vigor apenas em setembro de 2020. Contudo, havia outros sistemas normativos que já atuavam na defesa dos consumidores, entendida como parte mais vulnerável dentro de uma relação jurídica, bem como na proteção de dados, ainda que de forma limitada em razão das suas extensões e finalidades inicialmente previstas. São eles o Código de Defesa do Consumidor, a Lei do Cadastro Positivo e o Marco Civil da Internet.

Notou-se, igualmente, que a LGPD falhou ao deixar margens interpretativas sobre qual seria o regime de responsabilidade civil ali adotado. Com efeito, tal como ocorreu com o Marco Civil da Internet, a temática tem um elevado potencial de desaguar no Poder Judiciário, que já enfrenta uma enorme morosidade em decorrência do alto número de ações ajuizadas anualmente.

Foi nessa trilha que, rapidamente, surgiram diversas discussões doutrinárias e correntes de entendimentos, cujos argumentos foram expostos na última seção desta monografia. Em apertada síntese, os defensores da responsabilidade subjetiva alegam que houve alterações significativas na redação legal durante seu histórico de tramitação, sendo suprimidas expressões chaves da responsabilidade civil objetiva,

tal como “independentemente de culpa”, além de entenderem que outros dispositivos da LGPD apontam para necessidade de verificação de culpa dos agentes de tratamento.

Sob outra perspectiva, há autores que invocam fundamentos para uma responsabilidade subjetiva com alto grau de objetividade. Aqui, a despeito de entenderem que no geral a lei curva-se à uma subjetividade, sustentam que dificilmente os agentes conseguiriam demonstrar que não tiveram culpa pela cessão indevida dos dados pessoais, daí porque concordam que há certa combinação entre os regimes.

Por seu turno, apoiadores da responsabilidade objetiva elencam diversas semelhanças entre a LGPD e as normas consumeristas. Além de terem dispositivos praticamente idênticos, a legislação de dados demonstra ao longo do seu corpo textual a compatibilização e harmonia entre ambos os regramentos. Outrossim, são dispostas diversas medidas que buscam mitigar o potencial danoso do tratamento de dados, logo, isso indicaria que a legislação parte do pressuposto que há riscos inerentes à essa atividade.

Por fim e como tentativa de fuga à uma classificação binária entre subjetiva versus objetiva, a quarta corrente abraça a chamada responsabilidade proativa, amparando suas justificativas no fato de a LGPD ter não apenas se preocupado em reparar os danos ocasionados por agentes de tratamento, mas também em agir de forma diligente e proativa, de modo a evita-los.

Em atenção à problemática levantada para conduzir a pesquisa, o presente trabalho chega à conclusão que embora todos os fundamentos apresentados para classificar qual seria o regime de responsabilidade civil adotado no âmbito da LGPD se mostrem contundentes, é imprescindível analisar e aplicar a LGPD sob a perspectiva do diálogo das fontes. A influência dessas normas, sobretudo do CDC, na legislação de proteção de dados é evidente ao longo do texto, seja pela própria semelhança entre as redações, mas como também a previsão de complementação e harmonia entre os regramentos, vide Arts. 2, VI, 18, §8º, 45 e 64 da LGPD.

Diga-se, também, que vários dos princípios relacionados na LGPD apontam para necessidade de adotar medidas capazes de proteger, efetivamente, os dados pessoais, limitando seu tratamento à estrita finalidade a qual se propõe. É o que se depreende da leitura e aprofundamento dos princípios da necessidade, segurança, prevenção e responsabilização e prestação de contas.

Resta evidente, portanto, que o tratamento de dados deve ser sim enquadrado como uma atividade de risco, ainda que esses níveis possam variar em virtude do tipo de dado, como os dados sensíveis. Mesmo que os agentes de tratamento adotem posturas cautelosas (ou proativas, como defende a quarta corrente exposta no presente trabalho), a natureza da atividade continuará tendo o condão de provocar danos gravosos, em massa. O cenário não é outro quando se está diante de uma sociedade da informação, com crescentes compartilhamentos de dados em fração de segundos.

Não é possível conter o avanço tecnológico e nem se deve tentar, tendo em vista que essas transformações geraram inúmeros benefícios para a sociedade contemporânea. A questão é que essa vida *on-line* não mais se dissocia do mundo *off-line* e a tecnologia que antes era vista como opcional, passou a se tornar um elemento necessário, quase que obrigatório para as relações sociais. Dessa forma, é cabível que o ordenamento jurídico brasileiro adote providências rigorosas e bem estruturadas a fim de coibir o tratamento irregular de dados pessoais, pois isso incorre, na mesma medida, em violação de direitos e garantias fundamentais.

## REFERÊNCIAS

ALVAREZ, Bruna Acosta; TAVARES, Letícia Antunes. **Da proteção dos dados pessoais: uma análise comparada dos modelos de regulação da Europa, dos Estados Unidos da América e do Brasil**. In: Marcus Vinicius Kiyoshi Onodera e Thiago Baldani Gomes De Filippo (Org.). *Brasil e EUA: temas de direito comparado*. São Paulo: Escola Paulista da Magistratura, 2017, p. 155-203. Disponível em: <<https://api.tjsp.jus.br/Handlers/Handler/FileFetch.ashx?codigo=94288>>. Acesso em 11 de maio de 2021.

ARTIGO 19. **Proteção de dados pessoais no Brasil: Análise dos projetos de lei em tramitação no Congresso Nacional**. São Paulo, 2016. Disponível em: <<https://artigo19.org/wp-content/blogs.dir/24/files/2017/01/Prote%ca7%ca3o-de-Dados-Pessoais-no-Brasil-ARTIGO-19.pdf>>. Acesso em 15 de maio de 2021.

ASSMANN, Jhonata. **O direito à autodeterminação informativa no direito germânico e brasileiro**. Orientador: Ailton Lisle Cerqueira L. Seelaender. 2014. 65 p. TCC (Graduação) – Curso de Direito, Universidade Federal de Santa Catarina, Florianópolis, 2014. Disponível em: <<https://repositorio.ufsc.br/handle/123456789/117169>> Acesso em 01 de maio de 2021.

Biblioteca Virtual de Direitos Humanos. **Constituição dos Estados Unidos da América (1787)**. Disponível em: <<https://cutt.ly/EbCljcX>>. Acesso em 11 de maio de 2021.

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

BIONI, B.; DIAS, D. **Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor**. *Civilistica.com*, v. 9, n. 3, p. 1-23, 22 dez. 2020. Disponível em: <<https://civilistica.emnuvens.com.br/redc/article/view/662>>. Acesso em 03 de junho de 2021

BRANDEIS, Louis, D.; WARREN, Samuel D. **The Right to Privacy**. *Havard Law Review*, Vol 4, No. 5, December, 1890, pp. 193-220. Disponível em: <<https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf>> Acesso em 11 de abril de 2021.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 405, de 14 de março de 2007**. Brasília: Câmara dos Deputados, 2007. Disponível em: <<https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=344631>>. Acesso em 15 de maio de 2021.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 836, de 24 de abril de 2003**. Brasília: Câmara dos Deputados, 2003. Disponível em: <<https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=112893>>. Acesso em 15 de maio de 2021.



BRASIL. Câmara dos Deputados. **Projeto de Lei nº 2126, de 24 de agosto de 2011**. Brasília: Câmara dos Deputados, 2011b. Disponível em: <<https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=517255>>. Acesso em 15 de maio de 2021.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 4060, de 13 de junho de 2012**. Brasília: Câmara dos Deputados, 2012. Disponível em: <<https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=548066>>. Acesso em 15 de maio de 2021.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 5276, de 13 de maio de 2016**. Brasília: Câmara dos Deputados, 2016. Disponível em: <<https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378>>. Acesso em 15 de maio de 2021.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 5403, de 24 de setembro de 2001**. Brasília: Câmara dos Deputados, 2001. Disponível em: <<https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=34462&ord=1>>. Acesso em 15 de maio de 2021.

BRASIL. Câmara dos Deputados. **Projeto de Lei da Câmara nº 53, de 2018**. Brasília: Câmara dos Deputados, 2018a. Disponível em: <<https://www25.senado.leg.br/web/atividade/materias/-/materia/133486>>. Acesso em 15 de maio de 2021.

BRASIL. **Constituição Federal (1988)**. Brasília DF, 5 de out 1988. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/constituicao/constituicao.htm](http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm)>. Acesso em 15 de maio de 2021.

BRASIL. **Constituição Política do Império do Brasil (1824)**. Brasília DF, 25 de março de 1824. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/constituicao/constituicao24.htm](http://www.planalto.gov.br/ccivil_03/constituicao/constituicao24.htm)>. Acesso em 15 de maio de 2021.

BRASIL. Escola Nacional de Defesa do Consumidor. **A proteção de dados pessoais nas relações de consumo: para além da informação creditícia**. Escola Nacional de Defesa do Consumidor; elaboração Danilo Doneda. – Brasília: SDE/DPDC, 2010a. Disponível em: <<https://www.justica.gov.br/seus-direitos/consumidor/Anexos/manual-de-protecao-de-dados-pessoais.pdf>>. Acesso em 11 de maio de 2021.

BRASIL. **Lei Complementar nº 166, de 8 de abril de 2019**. Altera a Lei Complementar nº 105, de 10 de janeiro de 2001, e a Lei nº 12.414, de 9 de junho de 2011, para dispor sobre os cadastros positivos de crédito e regular a responsabilidade civil dos operadores. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/leis/lcp/Lcp166.htm](http://www.planalto.gov.br/ccivil_03/leis/lcp/Lcp166.htm)>. Acesso em 15 de maio de 2021.

BRASIL. Lei nº 3.071, de 1º de janeiro de 1916. **Institui o Código Civil dos Estados Unidos do Brasil.** Diário Oficial dos Estados Unidos do Brasil, Brasília, 2 de Janeiro de 1916. Disponível em <[http://www.planalto.gov.br/ccivil\\_03/LEIS/L3071.htm](http://www.planalto.gov.br/ccivil_03/LEIS/L3071.htm)>. Acesso em 10 de março de 2021.

BRASIL. Lei nº. 8.078, de 11 de setembro de 1990. **Código de Defesa do Consumidor.** Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/leis/l8078compilado.htm](http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm)>. Acesso em 15 de maio de 2021.

BRASIL. Lei n. 10.406, 10 de janeiro de 2002. **Institui o Código Civil.** Diário Oficial da União, Brasília, DF, 11 de janeiro de 2002. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/Leis/2002/L10406compilada.htm](http://www.planalto.gov.br/ccivil_03/Leis/2002/L10406compilada.htm)>. Acesso em 10 de março de 2021.

BRASIL. Lei nº 12.414, de 9 de junho de 2011. **Lei do Cadastro Positivo.** Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. 2011a. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2011/lei/l12414.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm)>. Acesso em 15 de maio de 2021.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. **Marco Civil da Internet.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília DF, 23 abril 2014. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2014/lei/l12965.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm)>. Acesso em 15 de maio de 2021.

BRASIL. Lei nº 13.709/2018, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados (LGPD).** Brasília, DF, 2018a. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm)>. Acesso em 10 de abril de 2021.

BRASIL. **Medida Provisória nº 518, de 30 de dezembro de 2010.** Diário Oficial da República Federativa do Brasil, Poder Executivo, Brasília, 2010b. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_Ato2007-2010/2010/Mpv/518.htm](http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2010/Mpv/518.htm)>. Acesso em 15 de maio de 2021.

BRASIL. **Medida Provisória nº 869, de 27 de dezembro de 2018.** Diário Oficial da República Federativa do Brasil, Poder Executivo, Brasília, 2018c. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/Mpv/mpv869.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Mpv/mpv869.htm)>. Acesso em 15 de maio de 2021.

BRASIL. **Medida Provisória nº 954, de 17 de abril de 2020.** Diário Oficial da República Federativa do Brasil, Poder Executivo, Brasília, 2020. Disponível em: <[http://www.planalto.gov.br/CCIVIL\\_03/\\_Ato2019-2022/2020/Mpv/mpv954.htm](http://www.planalto.gov.br/CCIVIL_03/_Ato2019-2022/2020/Mpv/mpv954.htm)>. Acesso em 15 de maio de 2021.

BRASIL. Ministério da Justiça e Segurança Pública. **Proteção de Dados Pessoais.** Brasília, DF, 2011?. Disponível em: <<https://www.justica.gov.br/seus->

direitos/elaboracao-legislativa/participacao-social/protecao-de-dados-pessoais/protecao-de-dados-pessoais>. Acesso em 15 de maio de 2021.

BRASIL. Ministério da Justiça. **Anteprojeto de Lei para a Proteção de Dados Pessoais**. Pensando o Direito, 2015. Disponível em:

<<http://pensando.mj.gov.br/dadospessoais/texto-em-debate/anteprojeto-de-lei-para-a-protecao-de-dados-pessoais/>>. Acesso em 15 de maio de 2021.

BRASIL. Senado Federal. **Projeto de Lei do Senado nº 330, de 2013**. Brasília, DF, 2013. Disponível em: <<https://www25.senado.leg.br/web/atividade/materias/-/materia/113947>>. Acesso em 15 de maio de 2021.

BRASIL. Senado Federal. **Proposta de Emenda à Constituição nº 17**, de 03 de julho de 2019. Brasília, DF, 2019. Disponível em: <<https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2210757>>. Acesso em 21 de maio de 2021.

BRASIL. Superior Tribunal de Justiça (STJ). **Súmula 550**. A utilização de escore de crédito, método estatístico de avaliação de risco que não constitui banco de dados, dispensa o consentimento do consumidor, que terá o direito de solicitar esclarecimentos sobre as informações pessoais valoradas e as fontes dos dados considerados no respectivo cálculo. Segunda Seção. Diário da Justiça Eletrônico, 19 out. 2015

BUBLITZ, M.D; MACEDO, F.S; RUARO, R.L. **A *privacy* norte-americana e a relação com o direito brasileiro**. *In*: Revista Jurídica Cesumar - Mestrado, v. 13, n. 1, p. 161-178, jan./jun. 2013 - ISSN 1677-64402. Disponível em: <<https://periodicos.unicesumar.edu.br/index.php/revjuridica/article/view/2666>>. Acesso em 11 de maio de 2021.

CALIFORNIA LEGISLATIVE INFORMATION. **California Consumer Privacy Act of 2018 [1798.100 - 1798.199.100]**. Disponível em: <[https://leginfo.ca.gov/faces/codes\\_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5](https://leginfo.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5)>. Acesso em 11 de maio de 2021.

CÉSAR, Genilson. **Consumo: Dos Estados Unidos para o Brasil**. Opinião, Rio de Janeiro, 1974. Disponível: <<http://memoria.bn.br/DocReader/Hotpage/HotpageBN.aspx?bib=123307&pagfis=2045&url=http://memoria.bn.br/docreader#>>. Acesso em 15 de maio de 2021.

COMISSÃO INTERAMERICANA DE DIREITOS HUMANOS. **Declaração Americana dos Direitos e Deveres do Homem**: aprovada na Nona Conferência Internacional Americana, Bogotá, 1948. Disponível em <[https://www.cidh.oas.org/basicos/portugues/b.declaracao\\_americana.htm](https://www.cidh.oas.org/basicos/portugues/b.declaracao_americana.htm)>. Acesso em 17 de abril de 2021.

COMITÊ GESTOR DA INTERNET NO BRASIL. **Seminário de Proteção à Privacidade e aos Dados Pessoais, de 30 de setembro e 1º de outubro de 2010** – São Paulo, SP. Disponível em: <<https://seminarioprivacidade.cgi.br/2010/>>. Acesso em 05 de junho de 2021.

CONSELHO NACIONAL DE JUSTIÇA. **Justiça em Números 2020: ano-base 2019**. Brasília: CNJ, 2020. Disponível em: <<https://www.cnj.jus.br/pesquisas-judiciarias/justica-em-numeros/>>. Acesso em 03 de junho de 2021.

COUNCIL OF EUROPE. **Chart of signatures and ratifications of Treaty 108**. Disponível em: <[https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p\\_auth=uEvXRQbk](https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=uEvXRQbk)>. Acesso em 01 de maio de 2021.

COUNCIL OF EUROPE. **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981)**. Strasbourg, 1981. Disponível em: <<https://rm.coe.int/16808ade9d>>. Acesso em 01 de maio de 2021.

DAVANZO, Danilo. **E-mail marketing: Sistema opt-in e opt-out de envio: A ausência de legislação específica sobre o assunto não é razão para deixar de se ater às imposições da vigente Lei nº. 8.078/90, o Código de Defesa do Consumidor**. 2015. Disponível em: <<https://danilodavanzo.jusbrasil.com.br/artigos/208357821/e-mail-marketing-sistema-opt-in-e-opt-out-de-envio>>. Acesso em 11 de maio de 2021.

DEMARTINI, Felipe. **Vazamento de dados cresceram 47% desde o início da pandemia**. Canaltech PSafe, 2020. Disponível em: <<https://canaltech.com.br/seguranca/vazamentos-de-dados-cresceram-47-desde-o-inicio-da-pandemia-166537/>>. Acesso em 03 de junho de 2021.

DOLIVEIRA, Matheus. **Buscas por “excluir Facebook” crescem 250% após filme “Dilema das Redes”**. Exame, 2020. Disponível em: <<https://exame.com/casual/buscas-por-excluir-facebook-crescem-250-apos-filme-o-dilema-das-redes/>>. Acesso em 03 de junho de 2021.

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

DONEDA, Danilo; MENDES, Laura Schertel. **Comentário à Nova Lei De Proteção De Dados (Lei 13.709/2018): O Novo Paradigma da Proteção de Dados no Brasil**. In: Revista de Direito do Consumidor, vol. 120/2018, p. 555 – 587, Nov - Dez / 2018.

**Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades**. BBC News Brasil, 2018. Disponível em: <<https://www.bbc.com/portuguese/internacional-43461751>>. Acesso em 11 de maio de 2021.

ESPANHA. **Constituição Espanhola (1978)**. Disponível em: <<https://www.tribunalconstitucional.es/es/tribunal/normativa/Normativa/CEportugu%C3%A9s.pdf>> Acesso em 01 de maio de 2021.

FARIAS, Cristiano Chaves de; ROSENVALD, Nelson; NETTO, Felipe Peixoto Braga. **Curso de direito civil: responsabilidade civil, volume 3**. 2. ed. rev., ampl. e atual. – São Paulo: Atlas, 2015.

FIGUEIREDO, Luciano L.; FIGUEIREDO, Roberto L. **Direito Civil: obrigações e responsabilidade civil**. 9 ed. ver., atual. e ampl. – Salvador: Editora Juspodivm, 2020.

FILHO, Eduardo T.; SOUZA, Mariana A. **A proteção de dados da pessoa jurídica e a Lei Geral de Proteção de Dados**. Revista Consultor Jurídico, jan-2021. Disponível em: < <https://www.conjur.com.br/2021-jan-22/opinioao-protECAo-dados-pessoa-juridica-lgpd>>. Acesso em 21 de maio de 2021.

FRAZÃO, Ana; MEDEIROS, Ana Rafaela. **Responsabilidade Civil dos provedores de internet: a liberdade de expressão e o art. 19 do Marco Civil**. Migalhas, 2021. Disponível em: < <https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/340656/responsabilidade-civil-dos-provedores-de-internet>>. Acesso em 05 de junho de 2021.

FRIEDE, Reis. **O emprego da jurisprudência no direito estadounidense**. Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 24, n. 5791, 2019. Disponível em: <<https://jus.com.br/artigos/73768>>. Acesso 11 de maio de 2021.

GONÇALVES, Carlos Roberto. **Direito das obrigações: parte especial: responsabilidade civil**. 14. ed. Coleção Sinopses jurídicas, v. 6, t. II, São Paulo : Saraiva, 2017.

ITÁLIA. **II Codice Civile Italiano, 16 marzo 1942, n. 262 Approvazione del testo del Codice Civile**. Disponível em: <[http://www.jus.unitn.it/Cardozo/Obiter\\_Dictum/codciv/Codciv.htm](http://www.jus.unitn.it/Cardozo/Obiter_Dictum/codciv/Codciv.htm)>. Acesso em 11 de março de 2021.

LEGISLATIVE COUNSEL'S DIGEST. **AB-375 Privacy: personal information: businesses**. Disponível em: < [https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill\\_id=201720180AB375](https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375)> . Acesso em 11 de maio de 2021.

LEITE, George Salomão. **Eficácia e aplicabilidade das normas constitucionais**. Brasília: Senado Federal, Conselho Editorial, 2020. 160 p. Disponível em: <[https://www2.senado.leg.br/bdsf/bitstream/handle/id/570639/Eficacia\\_aplicabilidade\\_normas\\_constitucionais.pdf?sequence=3&isAllowed=y](https://www2.senado.leg.br/bdsf/bitstream/handle/id/570639/Eficacia_aplicabilidade_normas_constitucionais.pdf?sequence=3&isAllowed=y)>. Acesso em 11 de maio de 2021.

LEONARDOS, Gabriela; NAVARRO, Ana Maria Neves de Paiva. **Privacidade Informacional: Origem e Fundamentos No Direito Norte-Americano**. Publica Direito. 2012. Disponível em: < <http://www.publicadireito.com.br/artigos/?cod=34f9a343f945196b>> Acesso em 11 de abril de 2021.

Mapa da proteção de dados pessoais ao redor do mundo. Serviço Federal de Processamento de Dados (SERPRO). Disponível em: <<https://www.serpro.gov.br/lgpd/menu/a-lgpd/mapa-da-protecao-de-dados-pessoais>>. Acesso em 10 de abril de 2021.

MIRAGEM, Bruno. **A Lei Geral De Proteção De Dados (Lei 13.709/2018) e o Direito Do Consumidor**. Revista dos Tribunais, vol. 1009/2019, Nov-2019. Disponível em: < <https://www.brunomiragem.com.br/wp-content/uploads/2020/06/002-LGPD-e-o-direito-do-consumidor.pdf>>. Acesso em 05 de junho de 2021.

MORAES, Maria Cecilia B.; QUEIROZ, João Q. **Autodeterminação informativa e responsabilização proativa: novos instrumentos de tutela da pessoa humana na LGPD**. In: Cadernos Adenauer XX (2019), nº3 *Proteção de dados pessoais: privacidade versus avanço tecnológico* Rio de Janeiro: Fundação Konrad Adenauer, p. 113-135, 2019.

MULHOLLAND, Caitlin. **A LGPD e o fundamento da responsabilidade civil dos agentes de tratamento de dados pessoais: culpa ou risco?**. Migalhas, 2020. Disponível em: < <https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/329909/a-lgpd-e-o-fundamento-da-responsabilidade-civil-dos-agentes-de-tratamento-de-dados-pessoais--culpa-ou-risco>>. Acesso em 03 de junho de 2021.

NADER, Paulo. **Curso de direito civil, volume 7: responsabilidade civil**. 6. ed. rev., atual. e ampl. – Rio de Janeiro: Forense, 2016

NETO, Raimundo Nonato de Araújo Soares. **Revolução informacional, novas tecnologias e consumo imediatista**. Cadernos de Campo: Revista de Ciências Sociais, Araraquara, n. 16, p. 111-124, 2012. Disponível em: < <https://periodicos.fclar.unesp.br/cadernos/article/view/7319/5181>> Acesso em 27 de abril de 2021.

NUNES, Rizzatto. **Curso de direito do consumidor**. 12. ed. São Paulo: Saraiva Educação, 2018.

OLIVEIRA, Antônio F.M; BAZI, Rogério Eduardo R. **Sociedade da Informação, transformação e inclusão social: A questão da produção de conteúdos**. Revista Digital de Biblioteconomia e Ciência da Informação, Campinas, v.5, n. 2, p.115-131, jan/jun. 2008– ISSN: 1678-765X. Disponível em: < <https://brapci.inf.br/index.php/res/download/114440>>. Acesso em 17 de abril de 2021.

OLIVEIRA, Guilherme Eduardo; JUNIOR, Cildo Giolo. **A tutela do direito à privacidade na internet**. Revista de Iniciação Científica e Extensão. Franca, vl. 5, n.1, p. 247-265, 2020. Disponível em: < <http://www.revista.direitofranca.br/index.php/icfdf/article/view/1094>>. Acesso em 15 de maio de 2021.

OLIVEIRA, José Eduardo da Silva. **Responsabilidade Civil dos Agentes de Proteção de Dados no Brasil**. Orientador: Adriano Marteleto Godinho. 2019. 49 p.

TCC (Graduação) – Curso de Direito, Universidade Federal da Paraíba, Santa Rita, 2019. Disponível em:  
<<https://repositorio.ufpb.br/jspui/bitstream/123456789/16584/1/JESO04102019.pdf>>. Acesso em 25 de maio de 2021.

Öman, Sören. **Implementing Data Protection in Law**. Estocolmo, Institute for Scandianvian Law, p. 389-403, 20--. Disponível em:  
<<https://scandinavianlaw.se/pdf/47-18.pdf>> Acesso em 01 de maio de 2021.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS, **Convenção Americana de Direitos Humanos (“Pacto de San José de Costa Rica”)**, 1969. Disponível em: <<http://www.pge.sp.gov.br/centrodeestudos/bibliotecavirtual/instrumentos/sanjose.htm>> Acesso em 17 de abril de 2021.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos**: adotada e proclamada pela Resolução 217 A (III) da Assembleia Geral das Nações Unidas em 10 de dezembro de 1948. Disponível em:  
<<https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos>> Acesso em 11 de abril de 2021.

PEREIRA, Jonas. **Marco Civil, resposta à espionagem**. Revista Em Discussão, Brasília (DF), Senado Federal, ano 5, n. 21, p. 56-57, 2014. Disponível em: <<http://www.senado.gov.br/noticias/jornal/emdiscussao/espionagem/espionagem.pdf>>. Acesso em 15 de maio de 2021.

Período de aprovação das Leis de Proteção de Dados Pessoais na América-Latina. Impressão Digital 126. Disponível em: <<http://impressaodigital126.ufba.br/panorama-leis-de-protecao-de-dados-pessoais/>>. Acesso em 10 de abril de 2021.

PORTUGAL. **Constituição da República Portuguesa (1976)**. Disponível em: <<https://www.parlamento.pt/parlamento/documents/crp1976.pdf>> Acesso em 01 de maio de 2021.

PORTUGAL. **Decreto-Lei nº 47344/99, de 25 de Novembro de 1966**. Diário Oficial da República de Portugal. Portugal, Lisboa. Disponível em:  
<<https://www.igac.gov.pt/documents/20178/358682/C%c3%bdigo+Civil.pdf/2e6b36d8-876b-433c-88c1-5b066aa93991>>. Acesso em 03 de junho de 2021.

RIBEIRO, Igor. **Falha de segurança vaza dados de todos os advogados brasileiros!**. Portal Exame de Ordem, 2020. Disponível em:  
<<https://portalexamedeordem.com.br/falha-de-seguranca-vaza-dados-da-oab/>>. Acesso em 03 de junho de 2021.

ROSENVALD, Nelson. **As funções da responsabilidade civil: a reparação e a pena civil**. São Paulo: Atlas, 2013.

RUARO, R.L; RODRIGUEZ, D.P; FINGER, B. **O direito à proteção de dados pessoais e a privacidade**. Revista da Faculdade de Direito – UFPR, Curitiba, n. 53, p. 45-66, 2011. Disponível em: <<http://dx.doi.org/10.5380/rfdufpr.v53i0.30768>> Acesso em 01 de maio de 2021.

SÃO PAULO. **Decreto nº 7.890, de 06 de maio de 1976**. Disponível em: <<http://dobuscadireta.imprensaoficial.com.br/default.aspx?DataPublicacao=19760507&Caderno=Poder%20Executivo&NumeroPagina=1>>. Acesso em 15 de maio de 2021.

**Seis em cada 10 brasileiros têm ‘vaga ideia’ do que é a LGPD**. Confederação Nacional de Dirigentes Lojistas (CNDL), 2021. Disponível em: <<https://cndl.org.br/varejosa/6-em-cada-10-brasileiros-tem-vaga-ideia-do-que-e-a-lgpd/>> Acesso em 03 de junho de 2021.

O que os consumidores e as empresas sabem sobre LGPD e o que estão fazendo a respeito?. Serasa Experian, 2019. Disponível em: <[https://s3-sa-east-1.amazonaws.com/serasaexperian-site-institucional-wp-content/wp-content/uploads/20190716115509/LGPD-Resultados-Pesquisa-Consumidores-e-Empresas\\_2019\\_minimo.pdf](https://s3-sa-east-1.amazonaws.com/serasaexperian-site-institucional-wp-content/wp-content/uploads/20190716115509/LGPD-Resultados-Pesquisa-Consumidores-e-Empresas_2019_minimo.pdf)> Acesso em 03 de junho de 2021.

SILVA, Carlos Eduardo Lins da. **Lei americana tem um século**. Folha de São Paulo, 1995. Disponível em: <<https://www1.folha.uol.com.br/fsp/1995/12/10/brasil/18.html>>. Acesso em 15 de maio de 2021.

SOUZA, Wendell L.B. **A perspectiva histórica da responsabilidade civil**. In: Alexandre Dartanhan de Mello Guerra, Marcelo Benacchio (coord.). Responsabilidade Civil. São Paulo: Escola Paulista da Magistratura, 2015, p. 9-31. Disponível em: <[http://www.mpsp.mp.br/portal/page/portal/documentacao\\_e\\_divulgacao/doc\\_biblioteca/bibli\\_servicos\\_produtos/BibliotecaDigital/BibDigitalLivros/TodosOsLivros/Responsabilidade\\_civil.pdf](http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/BibliotecaDigital/BibDigitalLivros/TodosOsLivros/Responsabilidade_civil.pdf)>. Acesso em 25 de maio de 2021.

TEPEDINO, Gustavo; TERRA, Aline de Miranda Valverde; GUEDES, Gisela Sampaio da Cruz. **Fundamentos do direito civil: responsabilidade civil**. 2. ed. – Rio de Janeiro: Forense, 2021.

TOVAR, Leonardo Zehuri. **O papel dos princípios no ordenamento jurídico**. Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 10, n. 696, 1 jun. 2005. Disponível em: <<https://jus.com.br/artigos/6824>>. Acesso em 11 de maio de 2021.

TRIBUNAL EUROPEU DOS DIREITOS DO HOMEM. **Convenção Europeia dos Direitos do Homem**. 1950. Disponível em: <[https://www.echr.coe.int/documents/convention\\_por.pdf](https://www.echr.coe.int/documents/convention_por.pdf)> Acesso em 17 de abril de 2021.

UNIÃO EUROPEIA. **Carta dos Direitos Fundamentais da União Européia**. 2000. Disponível em: <[https://www.europarl.europa.eu/charter/pdf/text\\_pt.pdf](https://www.europarl.europa.eu/charter/pdf/text_pt.pdf)> Acesso em 17 de abril de 2021.

UNIÃO EUROPEIA. **Directiva 95/46/CE do Parlamento Europeu e do Conselho**. 1995. Disponível em: <<https://eur-lex.europa.eu/legal->



content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=EN>. Acesso em 10 de maio de 2021.

UNIÃO EUROPEIA. **Directiva 97/66/CE do Parlamento Europeu e do Conselho**. 1997. Disponível em: <<https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31997L0066&from=PT>>. Acesso em 10 de maio de 2021

UNIÃO EUROPEIA. **Directiva 2002/58/CE do Parlamento Europeu e do Conselho**. 2002. Disponível em: <<https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32002L0058&from=PT>>. Acesso em 10 de maio de 2021.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho**. 2016. Disponível em: <<https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT>>. Acesso em 10 de maio de 2021.

VAINZOF, Rony. Capítulo I – Disposições Preliminares. In: **LGPD: Lei Geral de Proteção de Dados comentada [livro eletrônico]**. Coord. Viviane Nóbrega Maldonado e Renato Opice Blum. – 2. ed. rev., atual. e ampl. – São Paulo: Thomson Reuters Brasil, 2020.

WERTHEIN, Jorge. **A sociedade da informação e seus desafios**. *Ci. Inf.* [online]. Brasília, 2000, vol.29, n.2, pp.71-77. ISSN 1518-8353. Disponível em: <<https://doi.org/10.1590/S0100-19652000000200009>> Acesso em 17 de abril de 2021.