UNIVERSIDADE DO SUL DE SANTA CATARINA

GUILHERME CARDOSO TEIXEIRA

O PAPEL SOCIAL DA LEI GERAL DE PROTEÇÃO DE DADOS NO BRASIL

Araranguá

2020

GUILHERME CARDOSO TEIXEIRA

O PAPEL SOCIAL DA LEI GERAL DE PROTEÇÃO DE DADOS NO BRASIL

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

Orientador: Profª Fátima Hassan Caldeira Drª

Araranguá

2020

GUILHERME CARDOSO TEIXEIRA

O PAPEL SOCIAL DA LEI GERAL DE PROTEÇÃO DE DADOS NO BRASIL

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

Araranguá, 08 de julho de 2020.

_____
Professora e orientadora Fátima Hassan Caldeira, Drª
Universidade do Sul de Santa Catarina

_____
Profª Nádila da Silva Hassan, Esp.
Universidade do Sul de Santa Catarina

_____
Profª Rejane da Silva Johansson, Esp.
Universidade do Sul de Santa Catarina

To the one who has always been there for me.

AGRADECIMENTOS

Agradeço à minha família e aos amigos pelo apoio, e à professora doutora Fátima Hassan Caldeira, que foi minha orientadora, a quem sou muito grato, pois sua orientação foi fundamental para a realização deste trabalho, e sempre vou lembrar com carinho o suporte que tive.

“O conhecimento é poder”. Thomas Hobbes.

RESUMO

Este trabalho trata do papel social da Lei Geral de Proteção de Dados, Lei nº 13.709, de 14 de Agosto de 2018, conhecida como LGPD. Utilizou-se das pesquisas bibliográfica e documental a fim de analisar o cenário contemporâneo no que se refere à proteção de dado pessoais e, ainda para verificar como a nova lei produzirá seus efeitos diante das circunstâncias vivenciadas diariamente pelos usuários da Internet. Era notável que o Brasil possuía uma falta na legislação no que tangia especificamente à proteção de dados dos usuários, no entanto, com a criação desta lei, toda e qualquer operação de coleta e tratamento de dados ou informações estarão sujeitos ao crivo do ordenamento jurídico do país. A importância deste estudo é sustentada pelo valor econômico dos dados pessoais e pela necessidade de proteger os proprietários dos mesmos para que seus direitos e sua privacidade não sejam violados. Assim, em 2018, foi proposta uma legislação que lida diretamente com os problemas com os quais os usuários e as empresas têm convivido, sendo promulgada no mesmo ano, porém só entrando em vigor ao fim da *vacatio legis*. Assim, o presente estudo buscou verificar como a nova lei produzirá seus efeitos na sociedade. Concluiu-se que, com a entrada integral da lei em vigor, espera-se que esta produza a consolidação do uso íntegro, protetivo e legal dos dados pessoais dos usuários/consumidores na internet, respeitando-se os princípios legais apresentados nesse trabalho, a fim de garantir, acima de tudo, a proteção dos dados pessoais, e especialmente, o respeito ao direito fundamental à privacidade. Pôde-se compreender que, em razão da promulgação da Lei nº 13.709/2018, o direito à privacidade passou a receber amparo jurídico específico, com enfoque na proteção de dados.

Palavras-chave: Lei Geral de Proteção de Dados. Privacidade. Dados Pessoais. Consentimento.

ABSTRACT

The subject of this coursework is the social role of the General Data protection Law, which is Law No. 13.709, August 14 2018, known as LGPD. For this monograph, it has used bibliographic and documentary research. Its aim, is to analyze the contemporary scenario which deals with the protection of personal data, and as a new law, producing its legal effects, based on experiences lived by internet users. It was perceived that Brazil had a lack of legislation on what was applicable to the protection of user data. However, with the creation of this law, any and all operations to collect and process data or information will be subject to the new regulations. The importance of this study is underpinned by the economic value of personal data and the need to protect data owners, so that their rights, as well as their privacy, are not violated. Then, in 2018, a legislation that deals directly with the issues users and companies have been dealing with, is proposed. It was concluded that, with the full entry into force of the law, it is expected that it will consolidate the full, protective and legal use of personal data of users / consumers on the internet, respecting the legal principles presented in this work, the in order to guarantee, above all, the protection of personal data, and especially, respect for the fundamental right to privacy. It was possible to understand that, due to the enactment of Law No. 13.709, August 14 2018, the right to privacy started to receive specific legal protection, with a focus on data protection.

Keywords: General Data Protection Law. Privacy. Personal data. Consent.

SUMÁRIO

1 INTRODUÇÃO

É essencial compreender o atual panorama da sociedade diante das inúmeras mudanças decorrentes das inovações tecnológicas cada vez mais velozes e frequentes no campo da informação e que afeta diretamente as relações entre as pessoas e suas próprias vidas.

Antes dessas inúmeras mudanças, as atividades e situações eram sempre concretizadas pessoalmente, hoje, porém, muitas migraram para a forma virtual, transformando a maneira como nos relacionamos. Nessa nova configuração social, onde a troca de informações e de dados é constante, estes começaram ser o cerne de um sistema econômico virtual gigantesco.

Em uma esfera cujas mídias digitais prestam seus serviços aos usuários sem que estes paguem alguma tarifa diretamente, não se percebe que a conjuntura financeira vai além disso. Mesmo não havendo boletos ou débito em conta para poder acessar determinado website ou rede social, o fim econômico, neste caso, está na coleta dos dados dos usuários, que, na maior parte dos casos, fornecem eles involuntariamente. Assim, há a coleta de dados que, além de passarem por tratamento, são, em muitos casos, vendidos ou compartilhados com terceiros, girando enormes somas de dinheiro, resultado de um mercado que se apoia na publicidade direcionada (GUIMARÃES, 2015).

Conforme aponta Krieger (2019), diante deste cenário, pode-se citar como exemplo as ferramentas chamadas *cookies*, as quais ficam armazenados nos dispositivos de mídia dos usuários rastreando suas navegações e pesquisas. O resultado é uma segmentação em várias categorias com correlação a determinados anúncios de marketing e de publicidade. Percebe-se, então, que o usuário é o tempo inteiro vigiado, tendo seus dados coletados e armazenados, para então, receberem propaganda conforme seus gostos e preferências. Diante dessa conjectura, se não houver regramento, percebe-se uma invasão sobre as informações pessoais de cada indivíduo, até mesmo com a violação dos direitos dos titulares em relação aos seus dados, que são usados por empresas para fins econômicos, sem o próprio titular saber que sua vida íntima online está sendo comercializada. Esta é uma das razões para que se pense na proteção de dados pessoais, o que é intrínseco quando se fala em resguardar a privacidade de cada usuário. A partir daí, pode-se

imaginar legislações que abordem o assunto, desde o que diz respeito ao consentimento até a responsabilização por eventuais danos (KRIEGER, 2019).

Pode-se entender que os dados estão sendo trafegados em qualquer lugar da Internet, não importa se foi em uma busca no Google, uma aquisição de assinatura na Netflix, a inscrição de perfis nas redes sociais ou até mesmo a pesquisa de um determinado lugar em aplicativos e websites de localização. Compreende-se que todas essas atividades, realizadas no âmbito on-line, serão vistas e analisadas como dados que serão armazenados e tratados, inclusive havendo transferência para outros países, seja com finalidade comercial ou até política, como poderá ser visto ao longo deste estudo.

Assim, insta salientar ser necessário haver legislação própria quando se trata de proteção de dados pessoais, em razão do grande desenvolvimento tecnológico e informacional que houve no planeta. A globalização e suas características deram, com resultado expressivo, valor para a informação, transformando esta em um ativo de muita relevância no mercado, tanto para a iniciativa pública quanto para a iniciativa privada, assim, “quem tem acesso aos dados, tem acesso ao poder” (PINHEIRO, 2018, p. 50).

Então, ao tratar da Lei Geral de Proteção de Dados - LGPD, que ainda não entrou totalmente em vigor, é importante salientar que o presente estudo não possui como finalidade esgotar o assunto abordado. No entanto, procura-se, com esta pesquisa, desenvolver uma análise neste ambiente acadêmico e o compartilhamento das experiências estudadas no decorrer de sua criação.

Para realização da pesquisa, utilizamos a pesquisa bibliográfica e documental. E, em termos de estrutura, o trabalho foi dividido em três capítulos: o primeiro apresenta o cenário dos dados pessoais e à cultura da informação; o segundo aborda o processo de criação da Lei nº 13.709 e; por fim, o terceiro trata dos principais conceitos relativos a tema, abordando a possibilidade de responsabilização civil e das sanções aplicáveis no que concerne à violação das normas definidoras do tema.

2 DADOS PESSOAIS E A CULTURA DA INFORMAÇÃO

No ordenamento jurídico brasileiro, em especial diante do que está previsto no artigo 5°, inciso X, da Carta Magna, bem como no art. 21 do Código Civil, tem-se a base sobre a proteção do âmbito privado de um cidadão, seja em sua vida particular ou em sua intimidade.

Em relação ao direito à privacidade, em especial no que toca ao direito à intimidade, visualiza-se a segurança que um indivíduo possui em relação à sua vida íntima contra intromissões externas, aleatórias e desconvidadas, inclusive prevendo-se que a exposição na sociedade não pode acontecer sem a autorização de quem é o titular de tais direitos. A definição de privacidade é, em grande parte, resultado do veloz crescimento de como as informações e dados são colhidos e disseminados.

De acordo com Carvalho e Pedrini (2019), não há como negar que essa era de tecnologia facilitou a vida dos seres humanos, é visível o quanto a sociedade modificou-se em razão das constantes modernizações trazidas pelo momento tecnológico vivenciado. Os celulares, computadores e muitos outros dispositivos eletrônicos com acesso à internet fazem com que informações em massa sejam processadas, os dados podem atingir escalas altíssimas em sua produção e alcance. Também, pode-se considerar que as pessoas estão vivendo uma era comunicacional, há busca maciça por notícias e o desejo de estar informado. Percebe-se que os instrumentos tecnológicos podem potencializar formação de conhecimento e disseminação de informações. Quando se fala em conhecimento, constata-se que a Internet e seus produtos podem minimizar obstáculos do tempo e do espaço, proporcionando que o objeto envolvido alcance imediatamente número expressivo de usuários. Já quando se fala em propagação de informações, visualiza-se o espaço democrático em que estas são criadas e depois exibidas, inúmeras vezes sendo viralizadas em redes sociais, em que muitos podem acessar pelo próprio celular e até criar conteúdo a partir deste. Claro que nem tudo o que se está na rede é verdade. “Fake News” aparecem o tempo todo, já que divulgar conteúdo na Internet não é só exclusivo para uns, existe a possibilidade de todos os usuários fazerem divulgações também. Compreende-se então, segundo os autores acima mencionados, que o usuário da Internet não é só destinatário de informação, mas também veiculador. No entanto, com todo esse ambiente democrático que permite a muitos poderem exercer suas opiniões, existem chances de haver violação de

direitos constitucionais, especialmente no que diz respeito à privacidade, sendo este um direito fundamental, como atesta a Carta Magna no art. 5°, inciso 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, CRFB, 2020). Sob o ângulo desta configuração constitucional, não somente o direito à intimidade, à vida privada e à honra são garantidos, como também a correspondente proteção que possa resultar das possíveis violações de tais direitos, quer delas decorram danos morais ou materiais.

Não há como não mencionar a influência da internet na vida dos usuários. Nesse sentido Silva e Silva afirmam que

> O crescente uso das tecnologias da informação e da comunicação, em especial da Internet, imprimiu maior dinamicidade às relações econômicas, à participação política e às interações sociais, redesenhando as formas de ser e estar no mundo. Em nenhum outro momento histórico foi tão fácil e rápido acessar informações, produzir e compartilhar conteúdos, comunicar e interagir em sites de redes sociais, blogs e microblogs, tudo de maneira instantânea. O intenso desenvolvimento capitaneado pelo segmento de Tecnologias da Informação (TI) acelera ainda mais esse processo, pois a cada dia são lançados no mercado novos equipamentos, aplicativos, plataformas e ferramentas que maximizam a experiência de navegação na web, o que faz com que um número crescente de pessoas almeje a inclusão digital (2013, p. 2).

Porém, nem tudo deve ser visto apenas pelo lado otimista, sabe-se que há inúmeros problemas que precisam ser encaradas, principalmente no que diz respeito ao viés legal. Por isso, mesmo havendo essa difusão das facilidades do acesso à rede, as autoras continuam a afirmar que

> Mas ao lado desse panorama de otimismo e de novas oportunidades também se revelam inéditos problemas e desafios decorrentes do grande fluxo informacional, especialmente quando as informações assumem a forma de dados pessoais e saem do controle do seu titular. Essa situação de vulnerabilidade tanto pode ocorrer quando os dados são espontaneamente disponibilizados nas interações sociais, como ocorre com publicações feitas em sites de redes sociais; nos casos em que são recolhidos pelo fornecedor para permitir a abertura de contas que garantirão o acesso a serviços e produtos ou nas situações de captura indevida por meio de algum programa espião. A pluralidade de formas de recolhimento de informações demonstra a complexidade do tema, pois mesmo o internauta mais cauteloso e com seletivas atuações no ambiente virtual não fica a salvo de sofrer ataques aos seus dados pessoais (SILVA; SILVA, 2013, p. 2).

Com a expansão da internet e diante de tudo o que ela trouxe, como as plataformas digitais e as redes sociais, entende-se que ficou mais fácil a difusão de dados na rede. Isso pode trazer formas elevadas de atentados contra a proteção

individual que cada um de nós tem quando se trata da vida privada, como pode ocorrer quando terceiros não autorizados conseguem acessar o que é íntimo do ser. Assim, compreende-se que a privacidade começa a ser estudada não somente como um direito a ser respeitado, mas também como um direito ao poder de controlar os dados pessoais e não permitir que sejam expostos livremente (MULHOLLAND, 2012).

A segurança, quando se trata de dados pessoais, decorre de princípios relacionados à pessoa humana e sabe-se que, em uma democracia, o direito da privacidade é indispensável a seus cidadãos. Diante do cenário atual, Mulholland compreende que

> A capacidade de tratamento de dados pessoais das mais diversas ordens vem aumentando exponencialmente, principalmente devido ao advento de tecnologias avançadas de inteligência artificial, com o uso de algoritmos sofisticados e com a possibilidade de aprendizado por máquinas (*machine learning*). Significa dizer que o tratamento de "*big data*" literalmente, grandes bases de dados por meio de técnicas computacionais cada vez mais desenvolvidas pode levar a análises probabilísticas e resultados que, ao mesmo tempo que atingem os interesses de uma parcela específica da população, retiram a capacidade de autonomia do indivíduo e o seu direito de acesso ao consumo de bens e serviços e a determinadas políticas públicas, por exemplo (2018, p. 173).

De acordo com Vergili (2019, p. 1), quando se fala na esfera dos direitos da personalidade, é preciso esclarecer que há uma diferença considerável entre o direito à privacidade e o direito à proteção de dados pessoais, uma vez que são direitos autônomos. Ao falar de direito à privacidade, especialmente após o fim das Grandes Guerras Mundiais, com a lembrança de regimes autoritários, estabeleceu-se, no artigo XII, da Declaração Universal dos Direitos Humanos, a chamada inviolabilidade da vida privada, da residência, do seio familiar, inclusive no que se refere à correspondência. É, na verdade, um meio para que o indivíduo exerça sua vida privada sem interferências em seu proceder e em seu pensar interior, inclusive sem a interferência do poder estatal. A Constituição Federal do Brasil positiva este direito no artigo 5°, incisos X e XII, que preveem a proteção da privacidade, com abrangência especial da vida íntima de cada um, onde ninguém é obrigado a partilhar de sua intimidade quer com o Estado quer com outros que busquem forçá-lo a fazer o oposto. Assim, entende-se que a privacidade protege o direito à intimidade bem como a independência de cada indivíduo.

Segundo Vergili,

> Insta salientar que a delimitação entre o que é público e o que é privado parte do princípio democrático como forma de preservação do indivíduo frente ao poder do Estado. Neste sentido, por impor um limite à interferência estatal no núcleo individual, tem-se que o direito à privacidade é uma liberdade negativa. O Estado não pode invadir a esfera de proteção que este direito cria ao redor de seu titular. Simultaneamente, gera a este mesmo sujeito o poder de reivindicar, frente à autoridade pública, a proteção contra a violação deste direito por terceiros ou pelo próprio Poder Público (2019, p. 1).

Já, no que concerne à proteção de dados pessoais, tem sua origem a partir do direito à privacidade, como produto de uma sociedade da informação. Sabe-se que, com a criação e produção em massa de computadores, aparecem os bancos de dados, que armazenam dados pessoais, e aqueles que têm acesso a esses bancos cheios de informações podem ser considerados detentores de um sistema de poder. Assim, diante da abrangência e do domínio sobre os dados das pessoas, surge uma preocupação acerca de como esses dados são usados.

No Brasil, a partir deste vislumbre, tal direito começou a ser positivado de forma progressiva. Pode-se destacar o Código de Defesa do Consumidor, em 1990, bem como o Marco Civil da Internet, de 2014. A partir destes, para preencher determinadas lacunas que o mundo contemporâneo atual trouxe, foi elaborada a Lei n° 13.709, de 2018, chamada de Lei Geral de Proteção de Dados, cuja inspiração veio da norma geral do continente europeu, que entrou em vigor em 2020, trazendo proteção especial no que tange aos dados pessoais e sobre as informações que reconhecem ou tornam reconhecível a pessoa natural, pelas definições da lei.

Compreende-se que o modo como os dados são usados e até mesmo divulgados faz surgir uma preocupação: de que os titulares desses dados podem estar em situação de insegurança. Entende-se que, embora a Constituição Federal seja clara sobre o direito à privacidade, pode não haver a mesma abrangência quando se trata da proteção dos dados pessoais.

Na forma como o mercado age, atualmente, sabe-se que as informações das pessoas são profundamente observadas e, até mesmo, utilizadas por mecanismos automatizados. Neste presente modelo, diversos problemas ocorrem, tais como a assimetria das informações, a criação de perfis virtuais indevidos, a busca por determinados usuários ou solicitantes de serviços de forma indevida e até mesmo discriminatória. Percebe-se que tal circunstância é nociva aos cidadãos porque afeta os seus direitos fundamentais. Daí a importância de haver um

procedimento de normatização e supervisionamento por parte do Estado para proteger que tal direito seja ameaçado (VERGILI, 2019, p. 1).

2.1 EXEMPLOS DE CASOS PARA MELHOR APROFUNDAMENTO

No ano de 2016, uma entidade cuja atividade era captação de sangue humano para doação, a *Red Cross Blood Service*, passou por um período demasiado difícil quando teve o seu sistema de segurança de dados invadido. Neste sistema, havia informações de mais de 500 mil doadores de sangue que vieram a público em razão de uma transferência das mesmas em um ambiente desprotegido, quando houve o envio de um determinado arquivo que continha as informações de cada doador. Neste arquivo, existiam dados das coletas de sangue que ocorreram entre 2010 a 2016. Os dados foram divulgados, porém, não somente aqueles relacionados à identificação dos doadores (nome, data de nascimento e endereço), mas também informações sigilosas que estavam nos questionários também vieram a público, tais como comportamento sexual de cada doador e a avaliação se este era doador de risco ou não. O questionário possuía várias questões que, conforme as repostas, determinavam uma relação com os doadores, que estavam separados por nome, dentre outras informações confidenciais. A organização coletora de sangue desculpou-se pela situação ocorrida e ofereceu suporte para aqueles cujos dados foram desrespeitados (RED CROSS..., 2016).

Um segundo caso interessante a ser mencionado, apresentado por Braun (2018), foi o que ocorreu na China em 2014. Tratava-se de um sistema de crédito social que seria instalado no país até o ano de 2020. Neste sistema, que era implementado pelo governo chinês, pretendia-se analisar o quão fiéis eram os 1,3 bilhão de pessoas ao Estado no que versava sobre valores e princípios. Com tal serviço, seria possível organizar e determinar certos comportamentos das pessoas como positivos ou negativos, havendo algo como uma classificação de cada cidadão, cuja finalidade seria apontar se o cidadão poderia ter direito a certas políticas públicas que iam desde a aquisição de serviços de saúde até a matrícula de seus filhos em escolas. Os planejadores de tal sistema de crédito entendiam que a proposta engendraria um espaço em que possuir confiança seria algo imprescindível. No momento da criação de tal sistema, a adesão era voluntária,

porém, espera-se que, no decorrer de 2020, todos sejam obrigados a aderir, inclusive empresas cuja sede seja em solo chinês (BRAUN, 2018).

Sobre este assunto, Doneda já tinha uma opinião relevante, quando afirmava que

> Tome-se por exemplo uma negativa de um empréstimo bancário baseada em uma avaliação da capacidade de endividamento do solicitante que utilizou dados pessoais coletados de forma abusiva, ou que não correspondiam à realidade, sem que o solicitante sequer tenha a consciência de que tais dados falsos estavam sendo levados em conta. Ou igualmente em outras situações, como a de uma apólice de seguro-saúde de uma pessoa que pode eventualmente ser mais restritiva para ela do que para as demais pelo fato da seguradora ter tido acesso às suas informações genéticas que atestam uma propensão para o desenvolvimento de uma determinada patologia, dificultando o acesso à saúde em relação às demais pessoas (2008, p. 1).

Ambos os casos narrados, mesmo discorrendo sobre diferentes temas, trazem um ponto em comum: a violação de dados, especialmente os sensíveis. Estes foram utilizados com grande amplitude, sendo que o perigo reside no uso com caráter de discriminação, tanto pelo Estado como pelo setor privado. Assim, tais situações podem apresentar possíveis violações dos direitos fundamentais, em virtude da natureza e da definição dos dados sensíveis. Diante desse quadro, é que Mulholland (2018) afirma que o entendimento deste assunto sob a ótica da Lei Geral de Proteção de Dados Pessoais é essencial.

Sobre o assunto, Silva e Silva (2013, p. 6) entendem que “portanto, deve haver cautela redobrada quando se trata de dados sensíveis, seja no momento do recolhimento, seja quanto à segurança em seu armazenamento, afim de garantir que seu uso não se dissocie da finalidade para a qual foi obtida”.

2.2 A IMPORTÂNCIA DE UMA LEGISLAÇÃO PARA A PROTEÇÃO DOS USUÁRIOS DA INTERNET

Inspirada pelo Regulamento Europeu de Proteção de Dados Pessoais, chamado de *General Data Protection Regulation* - GDPR, a Lei n° 13.709/2018, também conhecida como Lei Geral de Proteção de Dados - LGDP, promulgada no dia 14 de agosto de 2018, propõe uma maneira eficaz de tratamento dos dados pessoais dos indivíduos tanto pela iniciativa privada quanto pelo poder público.

Além do mais, Silva e Silva argumentam que

> [...] os estados europeus desde a década de oitenta normatizam a matéria a partir de sucessivas Diretivas, aperfeiçoadas sempre que o desenvolvimento tecnológico impôs novos ritmos às interações sociais e às transações econômicas. Essa abertura, garantida pela adoção de princípios (lealdade, respeito à finalidade do recolhimento aos dados, proporcionalidade) e as constantes revisões empreendidas permitem que a legislação não se cristalize e se mantenha em constante sintonia com os usuários. Como se percebe, o foco de proteção é a pessoa, e não meramente os interesses econômicos (2013, p. 24).

Ao analisar esta nova legislação, segundo Pinheiro, deve-se lembrar que a presente lei atua diretamente no uso de um dos ativos mais preciosos nas relações digitais, que é a base de dados pertencente às pessoas. Sendo esta uma lei com profunda apresentação técnica, engloba também um conjunto de normas que visam a cumprir as garantias no campo da proteção aos direitos humanos também no âmbito digital (PINHEIRO, 2018).

Para Pinheiro (2018), ao considerar o momento econômico contemporâneo, a nova lei vem como uma garantia quando se trata de liberdade, de segurança e de dignidade. Segundo a autora,

> Destaque-se que a proteção das pessoas físicas relativamente ao tratamento dos seus dados pessoais é um direito fundamental, garantido por diversas legislações em muitos países. Na Europa, já estava previsto na Carta dos Direitos Fundamentais da União Europeia e no Tratado sobre o Funcionamento da União Europeia; no Brasil, já tinha previsão no Marco Civil da Internet e na Lei do Cadastro Positivo, mas a questão ainda era, muitas vezes, observada de forma difusa e sem objetividade no tocante aos critérios que serão considerados adequados para determinar se houve ou não guarda, manuseio e descarte dentro dos padrões mínimos de segurança condizentes (PINHEIRO, 2018, p. 18).

Assim, compreende-se que a importância de uma legislação própria relacionada à proteção de dados pessoais vem a partir do atual cenário em que os negócios digitais estão inseridos, entendendo ser a informação a novíssima moeda de troca utilizada pelas pessoas, para poder adquirir bens, produtos e serviços.

Ao visar uma segurança de informações, percebeu-se a importância de criar legislações que viessem a preencher determinadas lacunas. E é isto que a LGDP vem suprir.

Com a presença dos brasileiros cada vez maior no mundo virtual, esperava-se a proteção do titular e de seus dados. Assim, Silva e Silva afirmam que

> Observa-se que a necessidade em proteger juridicamente o cidadão resulta do fato de que os dados pessoais adquiriram nos últimos anos forte componente econômico devido à possibilidade de sua comercialização, o que atrai empresas e fornecedores que atuam no ambiente virtual a utilizarem as mais variadas estratégias para obter dados dos internautas. Com efeito, os dados pessoais de um consumidor traduzem aspectos de

> sua personalidade e revelam comportamentos e preferências, tornando-o um alvo fácil de mensagens publicitárias. Quando se trata da Internet o tema ganha inda mais interesse tendo em vista a possibilidade de criação de perfis psicológicos que revelam os hábitos de consumo, os gostos e preferências do indivíduo e, uma vez formado o perfil, posteriormente esse consumidor passa a ser alvo de publicidades indesejadas, e-mails que oferecem serviços, produtos e uma série de outras “promoções” que parecem elaboradas e direcionadas especialmente a ele, tudo articulado com base nos dados antes recolhidos. Percebe-se, pois, que as novas tecnologias informacionais, especialmente a Internet, convertem a informação em uma riqueza fundamental da sociedade, o que acentua a necessidade de sua proteção (2013, p. 6).

No que tange ao direito digital, percebe-se que serão abrangentes os efeitos da nova lei. Contudo, é importante salientar que tal legislação não alcança somente as redes sociais e afins, mas qualquer empresa ou organização que faça coleta de dados dos seus clientes e que os guarde em seus bancos de informações.

É oportuno atentar para o que diz o artigo 1° da Lei Geral de Proteção de Dados:

> 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, LGPD, 2020).

Então, ao analisar um paralelo em relação a LGPD e o GDPR, percebe-se que ambas as leis possuem como finalidade a regulamentação dos dados pessoais, objetivando, consequentemente, a proteção de direitos fundamentais dos cidadãos.

O regulamento europeu define as normas referentes ao tratamento aos dados pessoais referentes aos cidadãos do bloco europeu, seja por uma única pessoa ou por uma corporação ou organização. No entanto, ele não abrange as pessoas que já faleceram ou os organismos sociais dotados de personalidade jurídica. Percebe-se, então, que a nova legislação brasileira, com efeito, tem como base a lei europeia quando se trata deste tema. É na verdade uma tendência mundial, resultado da conjectura contemporânea. Vale lembrar que, somente no Brasil, a rede social Facebook possui mais de 127 milhões de usuários (BASTOS, 2018).

Compreende-se, então, que mesmo havendo leis, no Brasil, em relação ao tratamento da privacidade e à proteção de dados pessoais de uma maneira geral, como consta na Carta Magna, no Código Civil (CC), Código de Defesa do Consumidor (CDC), Marco Civil da Internet (MCI) e inclusive a Lei de Acesso à Informação (LAI), era necessário uma lei mais específica, que abrangesse o tema

por completo. Então, tal possibilidade veio com o exemplo do Regulamento de Proteção de Dados Pessoais europeu - RGPD, que inspirou os legisladores brasileiros.

Para Doneda,

> Enfim, a natureza do problema da tutela da privacidade requer uma solução de política do direito que assegure a maior eficácia possível a proteção de dados pessoais dentro do espectro de questões levantadas pelo tratamento de informações pessoais em bancos de dados automatizados. Para isto, o marco legislativo da codificação da temática da privacidade pelo CC2002 representa pouco mais do que uma referência, longe de refletir o perfil da realidade subjacente à temática. Para uma concreta composição desta, hão de ser levados em consideração todos os fatores envolvidos, como a importância estratégica que a privacidade e a informação representam para o desenvolvimento da personalidade, além da necessidade de tratar do problema com instrumentos específicos, capazes de operar dentro da complexidade do panorama tecnológico e pessoal no qual se desenrolam (2008, p. 1).

De acordo com Lanchester (2017), sabe-se que, em virtude da expansão do mundo digital e do aparecimento de diversas redes sociais que são provedoras de incontáveis dados fornecidos por usuários, o ato de enviar propaganda considerando os gostos e os interesses de cada indivíduo tornou-se atividade costumeira, gerando muito lucro para quem faz o chamado marketing direcionado. O próprio Facebook, em um curto período de tempo, já estava com valor de mercado bilionário, apesar da tenra idade de seu surgimento. Em relação a isso, é interessante o que Lanchester afirma:

> No final de junho deste ano, Mark Zuckerberg anunciou que o Facebook havia alcançado um novo patamar: 2 bilhões de usuários mensais ativos. Ou seja: 2 bilhões de pessoas diferentes acessaram o Facebook no mês anterior. É difícil aquilatar um conjunto desses. E pensar que “thefacebook” – o nome original do site – foi lançado para uso exclusivo dos alunos de Harvard em 2004. Nenhum empreendimento, nenhuma nova tecnologia, nenhum serviço jamais obteve tal difusão em tão pouco tempo (2017, p. 1).

Sobre o assunto, Krieger, pondera que

> A rede social, logo de início, apresentou um programa que prometia transformar cada usuário em uma ferramenta de marketing direcionada às empresas do e-commerce, denominado então como “o Santo Graal da publicidade”. Tal projeto tinha a premissa de monitorar intensivamente as compras e vendas realizadas entre os integrantes da rede, não estando mais restrito àqueles gostos e preferências anteriormente visados – os atos como consumidores de seus usuários tornaram-se o principal destaque (2019, p. 23).

É de conhecimento geral que a internet faz parte da vida diária de muitas pessoas, sendo as informações enviadas e recebidas a cada momento, de forma instantânea. Isso faz da rede mundial de computadores algo como que onipresente

na sociedade e, nessa situação, com os dados das pessoas transitando o tempo todo, os anúncios publicitários têm uma ampla vantagem ao poder direcionar seus produtos para determinados consumidores. Pode-se verificar, como exemplo, a questão dos celulares que detectam e enviam a localização física de seus donos, dando permissão para que a propaganda, de forma célere, possa percorrer seu caminho e até mesmo ode apenas potenciais seguidores. Um grande exemplo disso tudo, para demostrar a dimensão grandiosa da situação, foi a venda do aplicativo Waze para o Google, no valor de US$ 1,3 bilhão, cuja finalidade da aquisição era poder ter acesso aos dados da localização de cada usuário (BIONI, 2018b, p. 22).

Silva e Silva são enfáticas ao afirmar o quão urgente era a criação de uma lei específica sobre o tema. Para as autoras seria essencial, pois se trata da proteção de direitos inerentes à dignidade da pessoa humana. *In verbis*:

> Assim, no ano em que a Carta Constitucional brasileira completa vinte e cinco anos mostra-se oportuno e necessário trazer à discussão a ampliação do rol de direitos fundamentais, de modo a abarcar aqueles decorrentes do intenso desenvolvimento tecnológico experimentados nos últimos anos, notadamente na área da informação e comunicação. Essa reflexão não pode mais ser postergada, sobretudo porque o tratamento de dados pessoais na Internet oferece uma série de riscos ao seu titular, com claro potencial para fomentar discriminações e preconceitos de origem, raça, sexo, cor, idade, o que por certo viola a dignidade humana. O reconhecimento de novas categorias de direitos fundamentais, como os dados pessoais e a autodeterminação informativa, revela-se medida necessária não só para a concretização dos objetivos da República Federativa do Brasil, elencados no art. 3º da Carta Magna, como também para o alinhamento jurídico do país aos demais Estados que já adotaram igual postura em favor da dignidade da pessoa, a exemplo da União Europeia. Com efeito, enquanto a discussão sobre o tema é ainda incipiente no Brasil, a União Europeia se preocupa com a tutela desse direito desde 1995, momento em que os Estados integrantes perceberam a necessidade de garantir um adequado grau de proteção aos dados pessoais dos usuários das novas tecnologias, tratando-os como direitos fundamentais (2013, p. 8).

Leis que resguardam os direitos das pessoas são sempre imprescindíveis para manutenção e proteção da sociedade, o que engloba também a questão da proteção de dados. Assim, Carvalho e Pedrini afirmam que

> Por fim, constata-se que, com a edição de legislações infraconstitucionais com a finalidade de tutelar juridicamente a proteção de dados pessoais nas plataformas informatizadas e tecnológicas, houve ampliação na segurança jurídica, principalmente, por respaldar direitos como: à liberdade, à privacidade, ao livre desenvolvimento da personalidade da pessoa natural, à honra, à imagem. Colabora-se, dessa maneira, com a previsibilidade de mais garantias específicas no tratamento e disponibilização de informações, momento em que, geram-se mais obrigações às empresas, que devem aderir aos comandos legislativos e respeitar princípios norteadores na relação empresa e usuário, sob pena de aplicação de multa (2019, p. 379).

2.3 O CÓDIGO DE DEFESA DO CONSUMIDOR COMO PREDECESSOR NA PROTEÇÃO DE DIREITOS NO TOCANTE AO MERCADO

Na visão de Gonçalves e Lotufo (2020, p. 1), ao longo de 30 anos de existência do Código de Defesa do Consumidor, muitas foram as mudanças nas relações de consumo, inclusive aquelas feitas grandemente com o crescimento da internet. E é em consequência disso que surge a LGPD.

Importante destacar que, em um momento inicial, o CDC não deixou de atender aos consumidores no que diz respeito a suas dúvidas e necessidades no que se trata de questões consumeristas. Também é importante mencionar que, quando se fala dos consumidores e da influência que estes possuem, não se deve esquecer que os mesmos devem agir cautelosamente quando se trata de suas privacidades. Assim, em um mundo em que uma infinidade de pessoas acessa redes sociais o tempo inteiro, podem aparecer problemas relacionados à falta de privacidade, e é nesse momento que leis como a LGPD e o CDC podem se comunicar. Tais legislações apontam para o consentimento quando se trata do uso de dados pessoais. Isso quer dizer que mesmo que alguém exponha sua vida privada inúmeras vezes na internet, a rede social/empresa coletiva de dados deverá comunicar o consumidor acerca dessa coleta, com fundamento no artigo 43 do CDC e do artigo 7° da LGPD.

Ribeiro (2020) aponta que assim como o Código de Defesa do Consumidor transformou as relações comerciais quando surgiu, assim será com a nova Lei Geral de Proteção de Dados, cuja finalidade, para o autor, é normatizar o modo como as organizações utilizam os dados pessoais de pessoas naturais identificadas ou identificáveis. Tal legislação traz determinações que as empresas devem seguir, tais como a obrigação de atender todo titular de dado, que em muitas situações, também é consumidor, nos moldes do art. 2° do CDC.

Um dos artigos da LGPD que é interessante analisar, trata-se de o titular de dados/cliente poder solicitar, junto a determinada empresa, uma cópia com todas as suas informações, bem como saber para que finalidades estas estão sendo usadas. O artigo 9°, da LGPD afirma que

> Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:

> I - finalidade específica do tratamento;
> II - forma e duração do tratamento, observados os segredos comercial e industrial; III - identificação do controlador;
> IV - informações de contato do controlador;
> V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;
> VI - responsabilidades dos agentes que realizarão o tratamento; e
> VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei (BRASIL, LGPD, 2020).

Compreende-se que a LGPD possui sistemas de proteção semelhantes aos mencionados no CDC. Em relação ao segundo, é interessante averiguar o que diz o art. 43: “O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes” (BRASIL, CDC, 2020).

Isso revela uma espécie de conexão entre estas duas legislações: o consentimento do uso de dados.

O CDC deixou claro que o consumidor pode, como direito, solicitar correções de quaisquer erros que possam ser encontrados em seu cadastro, dando o prazo de até cinco dias para a empresa corrigi-lo. A LGPD aborda o mesmo assunto, concedendo ao dono dos dados/usuário poder de ter sua informação corrigida de qualquer inexatidão existente. A diferença entre os ordenamentos, no entanto, é o meio pelo qual poderá pleitear esse direito, pois não é mais necessário o titular dos dados ir até um local físico para fazer a mudança, podendo realizá-la pela internet ou por telefone celular, bastando acessar o site da prestadora dos serviços.

> Outro ponto de extrema importância presente em ambas as legislações é a segurança da informação. Devido aos escândalos de vazamento de dados e invasões telefônicas, o tema “segurança da informação” está em alta. Mas essa sempre foi uma preocupação. O CDC traz a preocupação com a segurança, visando a proteger a vida e a saúde contra os riscos de produtos e serviços (GONÇALVES; LOTUFO, 2020, p. 1).

Assim, para as autoras,

> Em tempos em que o dado vale mais do que o petróleo, a regulação do ambiente digital se faz necessária. A chegada da LGPD traz o desafio de gestão da conformidade, na qual as empresas terão que se adaptar a uma nova realidade. Estamos chegando a um tempo de revisitar o trabalho feito para desenvolver os canais de atendimento e repensar como tratar os dados pessoais de nossos clientes, sem deixar de ofertar produtos e serviços que resgatem a conexão com o ser humano (GONÇALVES; LOTUFO, 2020, p. 1).

2.4 A LGPD COMO UMA CONSOLIDADORA DO MARCO CIVIL DA INTERNET

Neste presente estudo, não se pode deixar de citar a Lei nº 12.965/2014, denominada de Marco Civil da Internet/MCI, sendo esta, primariamente, uma normativa intrínseca quando se trata das relações dos seres humanos realizadas através da internet.

De acordo com Bioni (2018b, p. 127), o MCI foi uma ação da sociedade civil brasileira tentando evitar que o Poder Legislativo regulamentasse a internet usando leis penais. Nesse contexto, o MCI veio como uma base no que se refere aos direitos e garantias dos cidadãos no mundo virtual.

Compreendeu-se então que o MCI foi desenvolvido como um regulamentador, legalmente falando, das atividades no meio eletrônico. Para o Direito Digital no Brasil, foi um começo, pois, até então, as relações na internet eram tratadas por legislações não específicas. Aplicavam-se as leis do direito penal, do direito autoral e da personalidade, por exemplo.

No entanto, para Bastos (2018), mesmo havendo semelhanças nas correspondências jurídicas virtuais com as que já existiam no ordenamento jurídico brasileiro, não se devia deixar de lado as especificidades de tal âmbito. Mesmo acontecendo uma adequação de certos institutos às mudanças que a sociedade contemporânea trouxe no mundo online, ainda assim existiam algumas incongruências e lacunas, segundo destaca Bastos ao afirmar que

> Necessitava-se, portanto, de maior regulamentação no âmbito do direito digital. Assim, o Marco Civil da Internet se destacou por prever princípios, garantias, direitos e deveres para o uso da Internet no Brasil.
> No entanto, ele próprio deixava uma importante lacuna: a questão dos dados pessoais no direito digital. Reconheceu as relações jurídico-virtuais e os efeitos delas no ordenamento. Dispôs, por exemplo, acerca dos crimes cibernéticos. Mas deixou de abordar como os dados fornecidos pelos usuários poderiam ser utilizados pelas empresas (2018, p. 1).

Ainda, conforme a autora, o MCI deixou uma considerável omissão, quando se trata dos dados pessoais no direito digital brasileiro. Admitiu as relações jurídico-virtuais e os impactos destas no meio. Tratou, também, sobre os crimes cibernéticos. Contudo não abordou como as empresas utilizariam os dados gerados pelos usuários (BASTOS, 2020, p. 1). Daí a importância da LGPD. Diante do exposto, Carvalho e Pedrini afirmam que

> Evidencia-se que, no viés de proteção do usuário perante o ambiente virtual, deve-se considerar os preceitos principiológicos e diretrizes do

> Marco Civil da Internet, uma vez que são verdadeiras conquistas dos internautas frente ao mundo tecnológico. Entretanto, há, ainda, outro comando legislativo que deve ser igualmente observado, trata-se, pois, da LGPD, que trata detalhadamente e especificamente da proteção dos usuários, quando suas informações estão dispostas em banco de dados públicos ou privados (2019, p. 374-375).

3 O PROCESSO DE CRIAÇÃO DA LEI Nº 13.709

Ao iniciar este capítulo, entender o processo que levou à formação da LGPD, anteriormente conhecida como Projeto de Lei da Câmara dos Deputados nº 53/2018, é imprescindível para poder interpretar a lei de uma forma mais adequada, de acordo com a visão dos legisladores.

De acordo com Bioni (2018a), é importante saber que, embora a lei tenha sido aprovada em agosto de 2018, esta não é uma legislação nova, uma vez que já vinha sendo discutida desde 2010, ano em que foi feita uma consulta pública, referente a um anteprojeto de lei, que, acrescente-se, era muito distinto da versão que foi aprovada oito anos depois. Percebe-se que, entre 2010 a 2014, não houve ampla discussão a respeito do tema. No entanto, em julho de 2013, houve escândalos de dimensão mundial quando o americano Eduard Snowden revelou os esquemas de espionagem praticados por determinados países. Snowden revelou que tais governos tinham capacidade de espionar e vigiar toda e qualquer pessoa no planeta, através de comunicação eletrônica, especialmente quando estas usavam plataformas na internet, como o uso dos principais serviços que até hoje as pessoas ainda acessam. Houve declarações de que até mesmo presidentes e chanceleres foram espionados. O Brasil, então, revelou publicamente sua indignação com o que estava acontecendo e afirmou que faria alianças com outras nações para poder reverter a situação ocorrida. Então, no início de 2013 até meados de março de 2014, houve uma aceleração do Projeto de Lei referente ao Marco Civil da Internet, que culminou com sua aprovação. Compreende-se, então, que naquele período foi criado um pequeno sistema no que trata à proteção de dados pessoais na esfera virtual. No entanto, sabe-se que o uso de tais dados, bem como sua proteção, não ocorre somente na internet, então, até 2015, novas discussões foram feitas acerca de uma lei geral que tratasse do tema por completo. Então, foi feita uma segunda consulta pública do anteprojeto e, nesta consulta, houve milhares de contribuições, tanto da iniciativa privada quanto do governo, que, juntas, chegaram a uma conclusão sobre as melhores ideias para este projeto que tinha como título a Lei

Geral de Proteção de Dados. Tal anteprojeto, já no início de 2016, foi enviado para o Congresso Nacional, sendo então um dos últimos atos da então presidente Dilma Roussef. E ao chegar na casa legislativa, foi aglutinado com outros projetos de lei que abordavam o mesmo assunto. Daí, segundo Bioni,

> O resultado foi um texto já bastante maduro que depois viria a ser a base do PLC 53/2018. Nas vésperas do seu afastamento, a presidenta Dilma Rousseff encaminhava o texto do anteprojeto à Câmara dos Deputados que se transformaria no PL 5276/2016, Desde logo, tal iniciativa legislativa contou com o apoio de mais de 40 (quarenta) entidades nacionais e internacionais que já afirmavam ser: "uma redação equilibrada a salvaguardar a inovação e a proteção da privacidade dos cidadãos (2018a, p. 1).

Segundo Moreira (2017), portanto, de 2016 a 2018, discussões foram feitas, havendo várias audiências públicas, para contribuir no debate dos principais temas no que tangia à nova legislação. Essencial salientar que, em 2018, sucederam-se determinadas circunstâncias que culminaram com a aprovação da lei. Pode-se elencar, como exemplo, a entrada em vigor da Regulamentação Europeia de Proteção de Dados Pessoais, que, apesar de ser de outro continente, possuía aplicação extraterritorial, levando muitas empresas brasileiras, mesmo sem presença física na Europa, mas que apresentavam elementos de conexão como o oferecimento de serviços para o bloco europeu, fossem obrigadas a se adequar.

Outro aspecto de grande relevância internacional foi o tumulto envolvendo a empresa britânica *Cambridge Analytica*. Foi exposto que tal organização coletou dados pessoais, por meio das famosas plataformas de redes sociais, utilizando-os para o armazenamento e a análise dos gostos e preferências dos usuários, tais como o personagem favorito em determinado filme, horóscopo, entre outros. Porém, tal companhia, direcionou tais dados, de cerca de 50 milhões de usuários, para envio de publicidade direcionada na Grã-Bretanha, onde suspeita-se que tal armazenamento ajudou a influenciar na votação da saída do Reino Unido da União Europeia. E também nos Estados Unidos, o uso de dados para finalidades políticas, que teriam ajudado na eleição do atual presidente (GOGANI, 2018). Além do mais, a referida empresa já estaria preparada para possivelmente prestar seus serviços no Brasil, durante o último pleito eleitoral para a Presidência da República, tendo tal informação vindo à tona. A partir daí, vários parlamentares das casas legislativas indignaram-se com a situação e pleitearam a necessidade de haver uma lei que

fosse adequada e que protegesse a privacidade dos cidadãos brasileiros, seja no âmbito *online* ou *offline*. (MILHORANCE, 2018).

> Ainda faltava o ingrediente mais quente para eclodir a pauta da proteção de dados pessoais em 2018: o escândalo da Cambridge Analytica escancarou como a desproteção de dados pessoais impacta não só a vida de um cidadão em específico, mas de toda uma coletividade e os alicerces do que se entende por democracia. Logo depois, houve uma sessão temática no Senado para debater, pela primeira vez no plenário em uma das Casas do Congresso Nacional, o tema. E, em maio de 2018, a Câmara dos Deputados realizou também um seminário como decorrência do referido escândalo (BIONI, 2018a, p. 1).

É interessante atentar para as considerações de Azambuja *et al*. que afirmam que

> Em setembro de 2018, o Facebook descobriu um ataque hacker que alcançou 50 milhões de usuários em todo o mundo. Em razão desse fato, vários perfis foram desconectados. Uma nova falha, ocorrida em dezembro, possibilitou a exposição das imagens postadas por 6,8 milhões de usuários. O The New York Times revelou, em dezembro do mesmo ano, que o Facebook forneceu, sem autorização, dados de usuários a empresas como Microsoft, Netflix, Spotify, Amazon e Yahoo. As autorizações davam acesso às mensagens privadas. Segundo a reportagem, as empresas podiam ler, escrever e apagar as mensagens, além de ver todos os participantes em um tópico. A reportagem não detalha como isso era feito. Onde meus dados foram parar? No caso da Cambridge Analytica, 300 mil pessoas foram pagas para participar de um teste de personalidade e fornecer seus dados. Elas, porém, foram usadas para coletar dados de outros. Com isso, foi possível criar um banco de dados com 87 milhões de pessoas, que não tinham ideia de que seriam envolvidas em campanhas políticas e outras atividades (2019, p. 17).

Importante salientar, também, como influência para a promulgação da LGPD, a oportunidade de o Brasil entrar na Organização para a Cooperação e Desenvolvimento Econômico ou Econômico - OCDE, conhecida popularmente como grupo dos países ricos. Tal organização, já em meados dos anos de 1980, possuía orientações acerca da transferência internacional de dados pessoais, bem como de seu uso adequado. Para que uma nação faça parte deste grupo, é necessária uma adequação que inclui dar sua palavra de que seguirá as diretrizes por ela propostas. Assim, na conjetura do Brasil não possuir uma legislação específica no que tange à questão da proteção de dados, dificultaria a entrada deste na referida organização (VENTURA, 2019).

Para Katarivas (2019), ainda outro fator que contribuiu para a aceleração da promulgação da LGPD, repousa sobre a Lei Complementar n° 166, de 8 de abril de 2019, que dispõe sobre os cadastros positivos de crédito. Quando essa lei foi aprovada, determinava que era necessário haver o consentimento expresso do

titular dos dados para que estes pudessem ser alocados em uma determinada base de dados no que tange à sua adimplência, que são as informações de pagamento, bem como o histórico deste e o de crédito. Muitas empresas, chamadas de gestoras, teriam grande interesse em ter acesso a essas informações, porém, a adesão ao cadastro positivo por meio do consentimento era conhecida por ser inferior ao que as instituições financeiras e birôs de crédito pretendiam. Então, houve uma discussão para que não mais houvesse o consentimento prévio, mas que existisse uma adesão automática ao cadastro positivo como direito de oposição. Assim, percebeu-se que tal situação significaria um acesso instantâneo a essas bases de dados que possuem informações de mais de cem milhões de brasileiros economicamente ativos. A Câmara dos Deputados, tendo um debate, envolvendo membros da Sociedade Civil, chegou à conclusão de que, antes de colocar os dados de mais de cem milhões de cidadãos automaticamente em uma base de dados, incluindo todo o histórico de créditos e pegamentos que revelariam muito sobre a vida de cada um, seriam discutidos regras e direitos adequados para esses titulares na esfera de uma lei que versasse sobre estes assuntos. Vê-se, então, que houve o apoio na aprovação de LGDP, para que, após, pudessem ser votadas, também, as alterações na Lei do Cadastro Positivo, que culminaram, então, na Lei Complementar nº 166/2019 (KATARIVAS, 2019).

> Sobre o Cadastro Positivo (Lei nº 12.414/11), após as alterações introduzidas pela Lei Complementar nº 166/2019 será necessária a compatibilização com a LGPD, pois nas operações de consultas aos bancos de dados de pessoas naturais e jurídicas existe corriqueiramente o compartilhamento de diversas informações pessoais reunidas de fontes distintas (dados bancários e creditícios, da Receita Federal, de concessionárias, etc) de forma compulsória (todos os consumidores estão automaticamente no cadastro), a menos que o consumidor expresse o contrário (PEIXOTO, 2020, p. 1).

Diante do exposto, pode-se compreender quais foram as bases da Lei nº 13.709. De acordo com Grossmann (2018), deve-se mencionar que, tirando todos esses anos de discussão e do contexto político, houve uma coalisão multissetorial, envolvendo várias entidades e áreas, e que, com uma manifestação pública, as casas legislativas puderem receber e entender a importância do tema. Tal caminho pôde levar o Brasil junto à países que já possuíam legislação e adequação quanto ao assunto da proteção de dados pessoais.

> De fato, deu-se um casamento inédito de interesses entre a sociedade, liderada por entidades de defesa de direitos civis e do setor privado, como a Coalizão Direitos na Rede e associações como a Abranet, a Brasscom,

> Abes, Assespro e Fenainfo, além de Abert, Movimento Brasil Competitivo, associações comerciais, entre outras. Nesta mesma terça, representantes desse grupo multissetorial foram à presidência do Senado insistir nos pedidos de votação antes do recesso parlamentar. Deu certo (GROSSMANN, 2018, p. 1).

Ainda segundo Bioni (2019), existe também uma perspectiva econômico-social que a nova legislação traz, em especial quando se fala de segurança jurídica, para as entidades, os órgãos públicos, as empresas e sujeitos que querem manipular e tratar os dados pessoais de cidadãos e consumidores. Falar sobre este novo ordenamento é atualizar-se quanto ao novo panorama do qual todos devem ter conhecimento, que é a proteção legal para todos os envolvidos nesse âmbito. Compreende-se que esta lei fomenta o desenvolvimento econômico e tecnológico, assim como preserva a proteção de direitos e liberdades fundamentais. Pode-se compreender o quanto esta legislação foi incentivada. É assim, então, uma forma de segurança quando se trata da questão econômico-social das relações. E, ao analisar que a nova lei possui uma dupla perspectiva, econômica e social, tanto a inciativa provada como a pública podem visualizar novas oportunidades. Não no que tange à ameaça de multas caso haja descumprimento da norma, mas, já que haverá uma mudança, com uma organização no controle dos dados, consegue-se encontrar então *insights* para a nova atividade.

> Ainda é comum se referir à nova Lei Geral brasileira de Proteção de Dados/LGPD, a Lei no 13.709/2018, enquanto um espantalho. Seria mais uma regulação, dentre tantas as outras já existentes, que travaria a economia e a inovação no país. O pessimismo é destilado através do medo. Quem não estiver em conformidade com a nova legislação amargaria prejuízos de até R$ 50 (cinquenta) milhões de reais, uma das suas penalidades previstas. Deveria ser o contrário, empresas e órgãos públicos precisam enxergar na nova regulação de dados uma janela de oportunidade, refletindo sobre o quanto poderão ganhar e se tornarem mais eficientes ao se adequarem à nova lei (BIONI, 2019, p. 1).

Para Vieira (2018), a partir do momento em que a Lei nº 13.708 entrar de fato em vigor, o Brasil estará no mapa global de países que possuem leis gerais de proteção de dados pessoais, sendo um momento importante que proporcionará integração econômica com nações que já têm tais legislações. Isso levaria o país a ser visto como um exemplo adequado no que tange à proteção de dados, o que pode permitir o livre fluxo de informação entre o Brasil e a União Europeia, por exemplo, que se tornará menos burocrático e, portanto, mais fácil. Vislumbra-se, até mesmo, maior competitividade em um cenário global em uma sociedade cada vez mais movida por dados.

Assim, como sugerem Azambuja *et al.*,

> Diante do contexto no qual os direitos à privacidade e proteção de dados foram elevados ao nível dos direitos humanos no cenário internacional, os governos têm dispensado especial atenção para lidar com esses desafios. Nesse cenário, destaca-se o Regulamento Geral sobre a Proteção de Dados (GDPR), publicado em 2018, pela União Europeia (EU), que visa a proporcionar aos usuários maior controle sobre seus dados pessoais e a aumentar as restrições sobre as organizações que tratam e lidam com esses dados. No cenário nacional, por sua vez, o Governo Brasileiro publicou a Lei Geral de Proteção de Dados Pessoais (LGPD), n.º 13.709, de 14 de agosto de 2018, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou 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 (2019, p. 3).

Na Europa, o novo regulamento trouxe muitas mudanças no ordenamento jurídico e, entre as mais destacadas, no que diz respeito ao tratamento de dados dentro do bloco europeu, está a regulamentação no que tange ao uso de maneira íntegra das informações por parte daqueles que tratam os dados, para que haja a garantia de que o princípio da privacidade esteja sendo respeitado, para, então, que a proteção de dados seja consolidada como um direito fundamental (SENA, 2019).

Mudanças na data de entrada vigor da lei em razão do cenário de 2020

De acordo com Tumelero (2020, p. 1), a LGPD foi originalmente publicada com a seguinte redação: “Esta Lei entra em Vigor: II - 24 (vinte e quatro) meses após a data de sua publicação, quanto aos demais artigos.” Com este artigo, que foi revogado, a previsão era pra entrar em vigor no decorrer de agosto de 2020, porém, ao longo do caminho, surgiram alguns projetos de leis para tentar alterar a data da vigência, nenhum estava indo muito para frente até chegar a pandemia.

Finalmente, veio um projeto de lei que veio a tornar-se a Lei nº 14.010/20, que dispõe sobre o Regime Jurídico Emergencial e Transitório das Relações Jurídicas de Direito Privado (RJET), ainda durante o período da pandemia do coronavírus (Covid-19). E foi essa Lei que passou a prever que os artigos 52, 53 e 54 da LGPD - que tratam das sanções - entrariam em vigor em 1º de agosto de 2020.

Assim, na prática, o que essa lei havia previsto é que a LGPD entraria em vigor em 16 de agosto de 2020 e que as sanções previstas na lei passariam a ser aplicáveis a partir de 1º de agosto de 2020.

Ocorre que, durante da tramitação do projeto de lei, que tornou-se a Lei nº 14.010, o Presidente da República publicou a Medida Provisória nº 959 que afirma que a LGPD entra em vigor integralmente, incluindo as sanções, em 3 de maio de 2021. Ora, a Lei nº 14.010 já foi sancionada e está vigente e a Medida Provisória nº 959 também está em vigor. Então, existe uma situação de normas conflitantes que coexistem no cenário atual.

Destaque-se que a Medida Provisória nº 959 tem um prazo de validade, sendo que, para que o seu teor se torne permanente, ela precisa ser convertida em lei pelo Congresso Nacional.

Diante desse contexto, existem alguns cenários possíveis: a) o Congresso analisa e não aprova a Medida Provisória nº 959; b) o Congresso não analisa e a Medida Provisória caduca; ou c) o Congresso aprova a Medida Provisória, convertendo-a em lei.

Nos dois primeiros cenários, a consequência prática seria bem similar: assim que a Medida Provisória caducasse ou não fosse aprovada, em setembro, a LGPD teria vigência retroativa a agosto de 2020 e as sanções só seriam aplicáveis a partir de agosto de 2021. Porém, se o Congresso converter a Medida Provisória em lei, a sociedade teria um cenário em que a Lei entraria em vigor em maio de 2021 e as sanções em agosto de 2021 – ora, esse seria é um cenário de insegurança jurídica.

O que se acredita é que o cenário mais provável é que o Congresso Nacional acabará deixando a Medida Provisória caducar, e, assim a LGPD entrará em vigor em agosto de 2020, contudo, suas sanções só seriam aplicáveis a partir de agosto de 2021.

Vale lembrar que, em relação às sanções, isso não impede eventuais condenações administrativas ou judiciais das empresas por alguma ofensa à LGPD, até porque se percebe que isso acontecendo atualmente, antes mesmo da LGPD entrar em vigor, através das leis consumeristas.

Claro que, ao findar este capítulo e tendo em mente a atual conjectura atual, afetada pela pandemia do coronavírus, mais do que nunca é preciso compreender que

> Modelos de governança de dados mais justos, responsáveis e sustentáveis, que protejam e defendam princípios éticos e regulatórios, ampliam a confiança dos indivíduos e da sociedade na utilização de seus dados para responder a situações de legítimo interesse público. Aspectos relacionados ao direito à privacidade, direito à proteção de dados pessoais e direitos de grupos não inviabilizam o uso de dados pessoais e a possibilidade de seu uso para responder à pandemia. A emergência de saúde pública ocasionada pelo Sars-CoV-2 aponta para a premente necessidade de novas formas de governança de dados pessoais que incluam a sociedade civil para a promoção de benefícios equânimes para toda a sociedade (ALMEIDA *et al*., 2020, p. 2491).

E continuam os autores, afirmando que

> As parcerias entre governos, empresas de tecnologia e universidades são necessárias para viabilizar a extração de conhecimento confiável de grande volume de dados. Os acordos precisam ser claros quanto aos papéis dos envolvidos, resultados pretendidos e alcançados. O estabelecimento de protocolos com princípios orientadores voltados à aplicação ágil e prática de processamento de dados em casos de interesse coletivo, com regras e supervisão nacional e internacional, podem ser uma alternativa, como na atual situação de emergência em saúde (ALMEIDA *et al.,* 2020, p. 2490).

4 OS PRINCIPAIS CONCEITOS E A RESPONSABILIZAÇÃO CIVIL

Dando início a este capítulo, como forma de apresentação, é pertinente compreender que, segundo Doneda,

> A privacidade é componente essencial da formação da pessoa. A sutil definição do que é exposto ou não sobre alguém, do que se quer tornar público ou o que se quer esconder, ou a quem se deseja revelar algo, mais do que meramente uma preferência ou capricho, define propriamente o que é um indivíduo – quais suas fronteiras com os demais, qual seu grau de interação e comunicação com seus conhecidos, seus familiares e todos os demais (2008, p. 1).

Com este pensamento, pode-se assimilar melhor o significado de dados dentro do campo da privacidade. Além disso, é essencial o que Silva e Melo afirmam, quando argumentam que

> O entendimento de privacidade foi sendo alterado ao longo do tempo, tendo havido uma mudança de perspectiva para a tutela da dignidade humana, bem como uma adequação às novas exigências de proteção da esfera privada em um mundo moderno, diante de recentes tecnologias de informação. Assim, a privacidade passou a representar não apenas a proteção de questões existenciais das pessoas, como convicção política, ideologias ou religião, mas também passou a tutelar uma proteção aos dados pessoais. Nesse sentido, privacidade, diante das inovações tecnológicas, é compreendida como direito fundamental à autodeterminação informativa, sendo imperioso compreender que a finalidade da proteção deste direito consiste na proteção da esfera privada, na busca da consagração da dignidade da pessoa humana. Dessa forma, por meio da promulgação da Lei 13.709/2018 o Brasil passou a conferir primazia à autonomia privada no que tange à circulação de seus dados pessoais dos indivíduos. Por meio da recente legislação de proteção de informações pessoais, condicionou-se seu uso e armazenamento à autorização do interessado, de modo a se afirmar que o Brasil pôde, enfim, concretizar a privacidade como um direito à autodeterminação informativa. Assim, o titular do direito à privacidade, observando a autonomia privada que lhe é inerente, pode autorizar e determinar limitações ao próprio direito que lhe assiste. Em um mundo cada vez mais tecnológico, em que todos estão sujeitos a vigilância constante, a privacidade passa a ser reconhecida em seu aspecto positivo de autodeterminação informativa. É o triunfo da autonomia privada que passa a ter aplicação no âmbito das informações pessoais (2019, p. 353-354).

Ao prosseguir pelo presente estudo, deve-se atentar para determinados conceitos e terminologias que são bases da nova lei, pois a implementação das novas regras precisa estar em conformidade com o dispositivo legal, sendo, portanto, imprescindível conhecer as nomenclaturas introduzidas pelo novo regimento. Para compreender melhor o tema, é necessário, antes, compreender o que se define por dados pessoais. Para Doneda (2006), os dados pessoais podem representar determinada característica de alguém que possa ser identificado ou identificável, havendo uma conexão intrínseca com o possuidor deste dado.

Para Roque,

> Os dados pessoais, na sociedade contemporânea, assumem importância estratégica cada vez maior. Podem ser utilizados em inúmeras aplicações, como o direcionamento de propagandas e anúncios específicos para o perfil de determinado consumidor, a partir das páginas que este visita na internet, ou a identificação da preferência ideológica ou mesmo sexual mediante análise dos gastos realizados pelo cartão de crédito, ou a investigação de doenças com maior probabilidade de se manifestarem durante a vida de determinado indivíduo, por meio da análise de seu material genético. Os exemplos são praticamente inesgotáveis e, cada vez mais, presentes no cotidiano – basta lembrar de seu smartphone, que sugere trajetos para o trabalho mesmo nos feriados (2019, p. 2).

É interessante analisar o que diz Pinheiro acerca do assunto:

> Toda informação relacionada a uma pessoa identificada ou identificável, não se limitando, portanto, a nome, sobrenome, apelido, idade, endereço residencial ou eletrônico, podendo incluir dados de localização, placas de automóvel, perfis de compras, número do Internet Protocol (IP), dados acadêmicos, histórico de compras, entre outros. Sempre relacionados a pessoa natural viva (2018, p. 25).

Já em relação a dados pessoais sensíveis, Sander (2019, p. 1) afirma que

> Dado pessoal com maior potencial de ferir direitos humanos básicos. Para a LGPD são considerados dados pessoais sensíveis aqueles relativos a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico.

Na visão de Mulholland (2018), a LGPD, ao regular as atividades no que concerne ao tratamento de dados, por meio de uma maneira diferenciada, faz a categorização e tutelação de dados pessoais e sensíveis. Embora tal legislação traga uma definição ampla acerca dos dois dados acima comentados, tal percepção jurídica já era conhecida desde a entrada em vigor da Lei de Cadastro Positivo – Lei nº 12.414/11 – cujo seu artigo 3º, § 3º, II, não permite registros em bancos de dados com finalidade de análise de crédito, afirmando que “informações sensíveis, assim consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas” (BRASIL, Lei nº 12.414, 2020).

Para Mulholland (2018, p. 166),

> Significa dizer que para fins de análise de concessão de crédito - princípio da finalidade - estão vedadas inclusões nas bases de dados de quaisquer informações de natureza personalíssima e que não se relacione à finalidade almejada com a análise de crédito, com o objetivo de evitar o tratamento discriminatório - princípio da não discriminação.

Compreende-se que o princípio da não discriminação possui enorme relevância no que tange ao tratamento de dados pessoais sensíveis. É aí que surge algo importante a ser ponderado, que é a proteção contra o uso lesivo de tais dados, seja por entes públicos e privados.

Inicialmente, a nova lei é dotada de um relevante aspecto que diz respeito ao consentimento de um titular de dados, concordando acerca do tratamento de dados pessoais. Isso quer dizer que haverá a permissão para tratar dados ao haver demonstração livre, afirmada e evidente de que o dono dos dados esteja em acordo com o tratamento para determinada finalidade, como dispõe o artigo 5°, inciso XII da Lei (BRASIL, LGPD, 2020).

Além do mais, a LGPD determina certos controles em relação ao tratamento de dados sensíveis. Sobre o consentimento, há a determinação de que este seja feito de maneira clara e expressiva, como prevê o art. 11, inciso I. No entanto, deve-se atentar que a LGPD, em certas situações, autoriza o tratamento de dados sensíveis sem a obrigação do usuário titular ter que consentir, como é o caso do tratamento de dados pela Administração Pública, dentre outras leis e regulamentos, como ensina o artigo 11, inciso II, alínea b, da LGPD, tendo a primazia do interesse público.

> No entanto, críticas devem ser feitas a este posicionamento legislativo, especialmente se considerarmos que a proteção do conteúdo dos dados pessoais sensíveis é fundamental para o pleno exercício de Direitos Fundamentais, tais como os da igualdade, liberdade e privacidade. Por isto que a regulação da coleta, uso, tratamento e compartilhamento de dados pela Lei Geral de Proteção de Dados torna-se de suma importância, devendo tais atividades serem realizadas de tal forma a respeitar os princípios previstos na mesma, enfatizando-se, no caso de dados sensíveis, o uso dos mesmos de maneira que atente ao princípio da igualdade e não gere uma discriminação. O princípio da não discriminação deve ser refletido em todas as circunstâncias em que o uso de dados, sejam sensíveis ou não, gere algum tipo de desvalor ou indução a resultados que seriam inequitativos. Esse princípio deve servir como base de sustentação da tutela dos dados sensíveis, especialmente quando estamos diante do exercício democrático e do acesso a direitos sociais, tais como o direito ao trabalho, à saúde e à moradia. (MULHOLLAND, 2018, p. 68).

Quando se trata de dados anonimizados, é importante atentar para o que diz Mendes (2020, p. 1), quando afirma que “um dado anonimizado é um dado pessoal ou sensível que foi tratado para que suas informações não possam ser vinculadas ao seu titular original.” Continuando sobre anonimização, a Lei nº 13.709 afirma que a “utilização de meios técnicos razoáveis e disponíveis no momento do

tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo" (BRASIL, LGPD, 2020).

Almeida *et al.* (2020, p. 2490) afirmam que

> contudo, mesmo sem fazer referência a qualquer indivíduo, podem prejudicar grupos em virtude de informações sobre locais, etnicidade, situações de saúde e condições socioeconômicas, por exemplo requerendo escrutinamento ético sobre os potenciais benefícios gerados por tais evidências.

Por fim, sobre a anonimização, é essencial olhar para o que entende Azambuja *et al.*,

> Vários modelos de anonimização que podem ser utilizados para preservar a privacidade dos usuários são propostos na literatura. O avanço tecnológico não garante uma eficaz segurança da informação, sem uma conscientização do ser humano em relação à segurança. O acesso não autorizado a informações, lugares, objetos, entre outros tipos de dados, na organização, torna a segurança vulnerável, uma vez que as pessoas e as empresas interessadas nesses dados têm acesso indevido a essas informações. As políticas de privacidade dos serviços on-line oferecidos pelas organizações devem estar em conformidade com a LGDP e GDPR. As referidas leis podem aplicar penalidades para as organizações que não se prepararem corretamente para a coleta, a gestão e o uso dos dados privados dos usuários. Estar compliance com a LGDP e GDPR será não só uma oportunidade para melhorar e aumentar o nível de privacidade, segurança e gerenciamento de dados, como um diferencial para os novos modelos de negócio baseados em dados. Em 2018, emerge o conceito de que somos o produto do espaço cibernético. Grande quantidade de informação é publicada no ciberespaço e os sistemas que recebem esses dados ficam cada vez mais inteligentes, ou seja, são capazes de fazer cruzamentos que nem imaginamos. O Big Data é uma realidade. Os efeitos da tecnologia da informação estão no dia a dia das pessoas, dominando as suas vidas de formas que elas não imaginam (2019, p. 26-27).

4.1 A QUESTÃO DO CONSENTIMENTO PELO TITULAR NO QUE SE REFERE AO TRATAMENTO DE DADOS

Uma importante parte do presente estudo baseia-se no consentimento proferido pelo titular. Assim, conforme explica Dhiulia Santos (2019), ao analisar a LGPD, é possível constatar que em relação ao consentimento do usuário, tal tópico tem essencial direção no que tange a esta legislação e a seus efeitos, pois, enquanto no Marco Civil da Internet, tal palavra consta somente 3 (três) vezes, ao longo da nova lei pode-se notar cerca de 35 (trinta e cinco) vezes, algo que revela uma abordagem mais significativa do tema, bem em como os legisladores se preocuparam em sua regulação.

Em relação ao consentimento que o titular de dados tem, pode-se encontrar orientações no MCI, no artigo 7º, incisos VII e IX, o qual ensina que acessar a internet, além de ser um exercício de cidadania, todos têm o direito de não fornecer seus dados pessoais a empresas ou terceiros, ressalvado o consentimento livre, declarado e expressado, bem como no disposto da legislação, e se houver, deve o coletor de forma expressa, anunciar as cláusulas o que se refere ao coletar e tratar das informações fornecidas, assim como deve ser indicado a finalidade que tais dados terão, como direciona o artigos 16, inciso II, do MCI.

Já a Lei nº 13.709/2018, discorrendo sobre o mesmo tema, inicia falando acerca de seu conceito, definindo-o, no art. 5º, inciso XII, como a “manifestação livre, informada, inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade adequada” (BRASIL, LGPD, 2020). Percebe-se então que o consentimento dado pelo titular, no que se refere ao tratamento de dados pessoais, é conceituado como sendo livre, informado e inequívoco, assim como concentrado à uma finalidade acordada. Com a definição da palavra, a própria lei preconiza tal instituto como um pressuposto legitimante no que concerne ao tratamento de dados pessoais. De fato, a possibilidade prevista no art. 7º, inciso I, da referida lei é exclusiva no que tange à possibilidade do titular anuir em relação ao tratamento de dados pessoais, pois os outros pressupostos previstos na legislação não requerem consentimento do cidadão, tratando-se então de tratamento de dados em um modo obrigatório (BRASIL, LGPD, 2020).

Ainda mencionando o artigo 7º, inciso I, da LGPD, acerca do consentimento, sendo este dado por escrito ou por outra maneira que comprove a manifestação tácita do titular dos dados, Dhiulia Santos afirma que

> O consentimento previsto no artigo7º, inciso I, da LGPD deve ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade pelo titular. Nos casos em que o consentimento seja fornecido por escrito, deve haver cláusula destacada das demais cláusulas contratuais. A outorga do consentimento pelo usuário também deve ser precedida de esclarecimentos quanto às finalidades específicas para o tratamento de dados pessoais. Nos casos de autorização genérica ou de informações fornecidas ao titular com conteúdo enganoso ou abusivo ou que não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca, há a nulidade do consentimento para o tratamento de dados pessoais. É vedado expressamente o tratamento de dados pessoais mediante vício de consentimento (2019, p. 10).

Ao analisar o Código Civil, nos artigos 138 a 175, percebe-se que este também traz definições acerca de situações relacionadas ao consentimento. Então,

quando trata-se de dados pessoais, é importante analisar com base no artigo 8°, §4° e artigo 9°, §1° da Lei nº 13.709, que afirmam ser nulo aquele consentimento nas hipóteses de autorizações genéricas e também em situações que as informações dadas ao usuário sejam de origem duvidosa, abusiva ou necessitem de transparência, deixando de estar de forma clara e sem equívocos. Deve ser lembrado que o quando é outorgado o consentimento, este pode ser revogado a qualquer tempo, nos termos do artigo 8°, §5°, da LGPD:

> Art. 8º [...]
> § 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei (BRASIL, LGPD, 2020).

Ao estudar o artigo 5°, inciso X, da Lei nº 13.709, vem à tona a questão da autodeterminação informativa, como figura importante no que concerne a abordagem de consentimento desta nova legislação:

> Art. 5º [...]
> X - Para os fins desta Lei, considera-se: tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (BRASIL, LGPD, 2020).

Dhiulia Santos (2019) explica que a evolução de concepções como autodeterminação informativa, alocação e consentimento do usuário, são formas de legitimar o tratamento de dados pessoais, demonstrando o quão sobremaneira o legislador conferiu a estes destaques, mormente no que se refere à vontade do titular ao tratamento dos dados pessoais. Ainda assim, não se deve deixar de mencionar que mesmo a lei dando aos usuários a escolha de poder determinar o tratamento para seus dados, não existe garantia mesmo assim do direito fundamental, sendo então este o motivo que o consentimento poderá enfrentar problemas para satisfazer o que está disposto no ordenamento jurídico. Não se deve deixar de citar também sobre a questão do consentimento do usuário nas questões que o condicionam a ter acesso a determinados serviços ou produtos. Segundo Doneda (2006), “[...] em tais situações, a pessoa que opta por exercer seu poder de autodeterminação e não revelar seus dados pessoais, no mais das vezes se vê alijado do acesso a determinados bens e serviço [...]” (*apud* SANTOS, 2019, p. 12).

Assim, compreende-se que existe apenas uma simples percepção de que o usuário teve a autodeterminação informativa. Dhiulia Santos afirma ainda que

> Um outro desafio quanto ao consentimento do usuário como instrumento legítimo ao tratamento de dados pessoais, é o fato de que este procedimento, por vezes aparenta-se como inócuo, haja vista que os seus efeitos deste tratamento não são tão nítidos ao titular dos dados pessoais. Ademais, em estudo realizado por pesquisadoras americanas, estima-se que os usuários dispenderiam, pelos menos 201 horas por ano se procedessem à leitura de todos os termos de uso dos websites que são em média acessados por um usuário americano (2019, p. 13).

Sobre o estudo acima, é importante verificar a questão da vontade, pois tem uma função primordial, já que, para Silva e Melo,

> O papel desempenhado pela vontade é de fundamental importância não apenas para o Direito Civil mas para todo o Direito. No entanto, muito embora se reconheça a importância da vontade para o Direito, esta não pode ser analisada fora do contexto social. Do contrário, estar-se-ia aplicando um verdadeiro dogma acerca da vontade. Nessa perspectiva eminentemente individualista, a pessoa se obrigaria tão somente através da declaração de vontade, deixando-se em outro plano a análise de outras circunstâncias nas quais o negócio jurídico deveria ser examinado. Assim, uma vez manifestada a vontade, haveria suficiência, por si só, para gerar consequências jurídicas (2019, p. 369).

No ano de 2020, na situação pandêmica trazida pela Sars-CoV-2, entendemos ser a autodeterminação informativa, evidentemente, uma perspectiva relevante a ser levada em consideração quanto ao exercício dos dados pessoais, paralelamente a garantias tais como transparência, segurança e minimização na utilização dos dados. No entanto, há casos que envolvem urgência e são de interesse público, como por exemplo, a saúde coletiva, sendo que então, mesmo sem o consentimento do usuário, o uso dos dados pessoais pode ser permitido, conquanto sejam respeitados princípios tais como a proporcionalidade ao utilizar as informações dos titulares e, ainda, em relação aos órgãos que têm autorização serem credenciados a processarem tais dados, seguindo o que determina a Lei Geral de Proteção de Dados brasileira e inclusive o Regulamento Geral de Proteção de Dados da União Europeia. Então, vê-se que a LGPD traz muitos aspectos que têm capacidade de simplificar o uso de dados para políticas emergenciais tais como no enfrentamento da COVID-19, os quais podem ser utilizados assim que a lei entrar em vigor (ALMEIDA *et al*., 2020).

Em consonância com o exposto até aqui, no que tange ao campo do consentimento, pode-se entender que este está ligado à função patrimonial que é explicada pelo Direito, como pode se observar nos argumentos de Silva e Melo:

> Dessa forma, o consentimento referente a direitos de personalidade é nitidamente diferente daquele realizado em situações puramente patrimoniais e, como tal, deve ser aferido com uma diferenciada valoração quanto à hierarquia dos valores constitucionais. Assim, a prevalência do valor conferido à pessoa humana pelo nosso ordenamento jurídico constitucional condiciona a interpretação de cada ato ou atividade para que seja realizada à luz da dignidade da pessoa humana (2019, p. 372).

Compreende-se, então, que o simples aceite do titular de dados pessoais dando consentimento para controle de sua informação não é suficiente para a preservação de um direito fundamental em relação à proteção de dados. Assim, a Lei nº 13.709 dispõe de determinados princípios que vão orientar o tratamento de dados, de maneira que, se bem observados, preservarão os direitos fundamentais dos usuários no que concerne ao tema do presente estudo.

4.2 PRINCÍPIOS DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

O artigo 6º da LGPD traz importantes princípios como orientadores no que se refere ao tratamento de dados pessoais:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
> IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
> V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
> VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
> VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
> X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas (BRASIL, LGPD, 2020).

De acordo com Dhiulia Santos (2019), o consentimento do titular dos dados da mesma forma deve ser compreendido de tal forma que sigam os princípios regidos no artigo 6 da LGPD. O uso de princípios na análise de dados tem por finalidade demarcar o manuseio destes dados. Em vista disso, o desenvolvimento dos princípios contidos no artigo 6°, subdivididos de I a X da LGPD não anula o vigor dos princípios da jurisdição brasileira.

O consentimento por parte do titular dos dados da mesma forma deve ser compreendido de tal maneira que sigam os princípios regidos no artigo mencionado acima. O uso de tais princípios na análise de dados têm por finalidade orientar quanto ao uso destes dados. É importante saber que estes pressupostos contidos no artigo 6° da LGPD não anulam o vigor dos princípios que já constam no ordenamento jurídico brasileiro (SANTOS, D., 2019).

O princípio da finalidade tem validade imprescindível para a custódia dos dados pessoais, sendo assim, invalida a aceitação do possuidor destes, caso não supervisionado pelo contratado. Tal princípio é evidenciado pela pelo art. 6º, inciso I, diz que a “realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades”. (BRASIL, LGPD, 2020). Por meio do princípio da finalidade, é proibido aos agentes de tratamento o uso de dados pessoais do usuário que vão além do acordo firmado antes da obtenção dos dados. Também, o mesmo princípio exige uma clarificação direta e restrita da manutenção dos dados do detentor primário, vedando, portanto, o uso destes para outros fins com ressalva de anulação do acordo (SANTOS, D., 2019).

O princípio da adequação contido no art.6º, inciso II, da LGPD, delibera que o trato de dados pessoais precisa ser coadunável com os devidos fins pré-estabelecidos com o contratante, isto é, os dados obtidos pelo contratado necessariamente devem guardar referência com o objetivo definido com o cliente. Desta forma, aos operantes não é permitido de maneira alguma usar de inverdades correspondentes ao objetivo pelo que foi contratado. Por exemplo: imagine-se que um usuário filiou-se, contratando um serviço on-line, para obtenção de informações acerca de torneios esportivos. Sabe-se que seria desnecessária a obtenção de dados pessoais do indivíduo referentes à sua saúde e a seus relacionamentos, considerando que o princípio da adequação dos dados em questão deve corresponder à finalidade coerente e pretendida pelo contratante, descrito no art. 6º,

inciso III, da LGPD, que guarda estrita relação com o princípio da adequação, que dita que o tratamento dos dados pessoais deve limitar-se ao essencial mínimo necessário para realização da finalidade informada ao titular daqueles dados (SANTOS, D., 2019).

Em relação ao princípio da necessidade, Saldanha (2019) explica que, na visão contextual da LGDP, significa que os dados devem ser coletados de modo restrito, assim, observando a forma de tratamento destas informações pessoais, para obedecer o objetivo de permanecerem em sua abordagem de tratamento estrito, devem ser desconsideradas coletas numerosas e abertas.

De acordo com Tumelero (2019, p. 1), compreende-se o princípio da necessidade na visão de “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”.

Sobre o assunto, no aspecto empresarial, Lima (2020, p. 1) argumenta que

> Isso significa que ao fazer o levantamento e a varredura dos dados pessoais armazenados e suas respectivas naturezas, o empresário tem a inédita oportunidade de propor uma revisão da sua estrutura de armazenamento e segurança de informação para que essa seja adequada ao tamanho da sua operação.

O livre acesso corresponde ao quarto princípio descrito no art. 6º da LGPD, através deste é assegurado ao possuidor dos dados a facilitação da consulta sem ônus acerca do período contratado bem como sobre a totalidade de seus dados pessoais obtidos (SANTOS, D., 2019).

Na visão de Lima (2020), no que diz respeito ao princípio da qualidade, sabe-se que de acordo com a LGPD, sua característica é o cumprimento de que os titulares de dados possam conferir, quanto a estes, o que tem relação à sua clareza, exatidão, atualidade, bem como relevância, conforme seja necessário e, também, à garantia de que a finalidade existente esteja sendo obedecida.

Lima (2020, p. 1) destaca ainda que

> Conforme vemos na própria Lei Geral de Proteção de Dados, o titular dos dados tem o direito de correção de dados incompletos, inexatos ou desatualizados e, ainda, informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados e sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa.

O princípio da transparência conforme o art. 6º da LGPD, também denominado de princípio da publicidade, forma-se paralelamente ao princípio da finalidade, um dos mais necessários no que se refere ao trato e ao resguardo dos dados pessoais, pois através deste princípio, penhora aos titulares dos dados a facilidade e a clareza do acesso dos contratados envolvidos nas operações aos mesmos. Então, deve ser de conhecimento público a existência dos dados, conforme elenca o art. 9º, §1º, da Lei nº 13.709/2018. O objetivo deste princípio é guardar o contratado de possíveis abusos por meio de suas informações enganosas. (DHIULIA SANTOS, 2019).

O princípio da segurança, elencado no art. 6º, inciso VII, da LGPD, forma uma das guias claras do direito fundamental ao resguardo dos dados, ao prever a utilização de medidas técnicas e administrativas afim de protegê-los de acessos não autorizados e, ainda, de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão dos mesmos (BRASIL, LGDP, 2020).

O próximo inciso do art. 6º refere-se ao princípio da prevenção, que constitui a extensão direta do direito fundamental à guarda dos dados pessoais, prevendo que os contratados utilizem métodos preventivos afim de evitar ocasionais danos em relação ao cuidado dos dados pessoais.

Ratificando os cuidados contra ocasionais perdas decorrentes do manuseio dos dados pessoais, o art. 6º, inciso IX, da LGPD, indica, ainda, o princípio da não discriminação, que veda a completa utilização dos dados pessoais para objetivos discriminatórios, abusivos e ilícitos (SANTOS, D., 2019). Em relação ao princípio da não discriminação, Lima (2020) acrescenta que pela denominação deste princípio já se reconhece sua essência, assim, é preciso compreender que, quando houver tratamento de dados, este jamais poderá ser efetuado com intuitos e propósitos discriminatórios ou impróprios. Nas palavras de Tumelero (2019, p. 1), trata-se da “impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos”.

Sobre o tema, ainda é importante mencionar que

> Não se pode ter exclusão de titulares de dados pessoais no momento de seu tratamento de dados por determinadas características, sejam elas de origem racial ou étnica, opinião política, religião ou convicções, geolocalização, filiação sindical, estado genético ou de saúde ou orientação sexual. Não é dizer que nunca poderá ter uma setorização de tratamento de dados, porém somente poderá ocorrer tal restrição em condições específicas e previstas em lei, como por exemplo um tratamento de dados de alunos optantes por cotas, perante a Lei de Cotas 12.711/2012, a

> condição de tratamento de dados pessoais será a partir de seu histórico educacional, sendo ele oriundos integralmente do ensino médio público, em cursos regulares ou da educação de jovens e adultos (LIMA, 2020, p. 1).

Já no art. 6º, inciso X, da LGPD, tem-se o princípio da responsabilização e prestação de contas, o qual submete os contratados à obrigatoriedade de realização, de maneira abrangente, todas as condutas de resguardo de dados pessoais e também da serventia dessas medidas. Verifica-se, que estes princípios têm por finalidade assegurar ao proprietário dos dados um amplo controle no que se refere ao cuidado dos dados fornecidos a fim de assegurar a interpelação desta análise (SANTOS, D., 2019). Tumelero (2019, p. 1), por sua vez, acrescenta que tais princípios convergem na "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".

Por fim, afirma Lima que

> Em outras palavras, é dizer que o controlador ou operador tem o dever de prestar contas, ante a sua responsabilização, de demonstrar a autoridade delegante que os objetivos propostos foram cumpridos, sejam elas técnicas e/ou preventivas, e que esses processos guardaram adequação (conformidade) com as regras e princípios estabelecidos, que comprovem a efetividade e a observância da proteção aos dados pessoais (2020, p. 1).

4.3 PROTEÇÃO DE CRIANÇAS E ADOLESCENTES FRENTE A LGDP

As crianças e adolescentes, que não deixam de ser usuários da internet, também foram abrangidos pela nova lei, a qual prevê importantes regras no que tange a tal público, considerado mais vulnerável, nas situações virtuais, em razão de sua idade.

De acordo com Sena (2019), é importante atentar que, em relação a esse público, não se separam os significados de dados pessoais e de dados sensíveis, sendo considerados, os dois, como um só.

O art. 14 da LGPD afirma que "o tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente" (BRASIL, LGPD, 2020). Isso quer dizer que o tratamento de dados pessoais para crianças deverá estar dentro de um consentimento propriamente destacado para tal audiência, o qual é outorgado por seus pais ou pelos responsáveis legais do usuário menor. Tal exigência intenciona o

respeito à integridade da criança, não devendo haver esforços, com todo o aparato tecnológico existente, para que haja a confirmação de consentimento autorizado pelo responsável (SENA, 2019). Além disso, tudo o que for coletado pelos controladores deverá estar condicionado de forma pública, para elucidar quais dados que foram coletados, bem como a maneira de sua utilização e o procedimento adotado no tocante à solicitação apropriada no que concerne a tais dados, conforme diz o artigo 14, § 2°. (BRASIL, LGPD, 2020).

Existem isenções e ressalvas em relação ao consentimento, como na hipótese do § 3° do artigo 14, permitindo a coleta dos dados que serão utilizados uma única vez. *In verbis*:

> Art. 14 [...]
> § 3° Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo (BRASIL, LGPD, 2020).

Percebendo o fato de a internet estar cada vez mais presente na vida de crianças e adolescentes, os autores da Lei Geral de Proteção de Dados estabeleceram dispositivos legais que pudessem estabelecer controles nas atividades em que os mesmos participem e em que ocorre o coleta das informações, ressalvadas as obrigatórias, como consta nos parágrafos 4° e 5° do artigo 14 (BRASIL, LGPD, 2020).

Mesmo que o princípio da transparência faça parte de toda a legislação como um marco obrigatório, considera-se haver necessidade de adaptação do dispositivo legal para incluir a faculdade de construção do entendimento da criança e do adolescente. De acordo com Valente (2018), os legisladores tiveram a preocupação em estabelecer o princípio da transparência no dispositivo legal, tal qual ocorreu na União Europeia, demandando que todas as informações ofertadas terão linguagem clara, acessível e simples acerca do tratamento de dados. Eis o que afirma o autor:

> A Lei Geral de Proteção de Dados exige que empresas envolvidas em algum tipo de tratamento de dados de crianças devem dar transparência a eles. Segundo o texto, “os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos” dos usuários.
> Além disso, a norma prevê que as informações sobre tratamento de dados sejam disponibilizadas “de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e

> mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança (VALENTE, 2018, p. 1).

Por fim, Sena (2019, p. 22) argumenta que

> Considerando que as crianças são sujeitos em desenvolvimento, a instituição de responsabilidade compartilhada do Poder Público e os cuidados dos pais em relação à utilização da tecnologia pelos seus filhos, é razoável notar que com a dispensa do consentimento do responsável do titular, em determinadas situações, a proteção de dados pessoais de crianças poderá sofrer diversos desafios, por se tratar de um ordenamento ambíguo e amplo.

4.4 RESPONSABILIDADE CIVIL E SANÇÕES

É importante iniciar este tópico relembrando acerca do papel que a LGPD representará quando totalmente em vigor. Nesse sentido, Roque afirma que

> A Lei n.º 13.709/2018, mais conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), veio para implementar verdadeira revolução na proteção dos dados pessoais no Brasil. Claramente inspirada na regulação europeia sobre o tema – *General Data Protection Regulation* (GDPR), aprovada pelo Parlamento europeu em 2016 e em vigor desde maio de 2018 –, a LGPD brasileira enuncia, entre suas finalidades, "proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural" (art. 1º) (2019, p. 2).

De acordo com Vieira (2019), quando se fala em responsabilidade civil, entende-se haver uma relevante exigência para consertar um dano causado a terceiro, de forma antijurídica.

Tal instituto pode abarcar duas espécies:

a) **a responsabilidade contratual**: que é aquela decorrente de prejuízos resultantes de inadimplência, do atraso em cumprir cláusulas contratuais, podendo derivar, inclusive da imperícia na execução de uma obra (VIEIRA, 2019);

b) **a responsabilidade civil extracontratual,** concernente ao dever de reparar os danos que são resultantes da quebra de direitos alheios, dos direitos da personalidade, por exemplo, ou seja, é aquela que está estritamente relacionada à quebra de um direito. Então, o sujeito que a este viola e causa dano a um terceiro, terá a obrigação de reparar o dano causado (VIEIRA, 2019).

Assim, o próprio Código Civil fundamenta a responsabilidade em dois conceitos, sendo o primeiro o de ato ilícito, conforme o artigo 186, e o segundo o de abuso de direito, como disposto no artigo 187. *In verbis*:

> Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito.
> Art. 187. Também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes (BRASIL, CC, 2020).

Então, começa-se a entender que quando alguém pratica ato em desacordo com o que a lei diz, causando danos ou lesões a um terceiro, deve, de alguma maneira, reparar pelos estragos causados. E mais de uma pode ser a forma de reparação, como corrobora Vieira (2019, p. 29), ao afirmar que

> O ato ilícito, portanto, é aquele praticado em desacordo com a ordem jurídica que ocasiona a violação de direitos e causa prejuízos a outrem. O ato ilícito pode ser penal, administrativo ou civil bem como pode acarretar dupla ou tripla responsabilidade, por exemplo, um crime ambiental que ofende os particulares (ilícito civil), a sociedade (ilícito penal) e é passível de sanções administrativas. A consequência do ato ilícito civil é a obrigação geral de reparar o dano, disposta no caput do art. 927 do Código Civil de 2002. Além disso, existem situações em que se responde por terceiros, devendo existir uma conexão entre o responsável e o executor do ato. Há também a hipótese de dano causado por coisa da qual se é proprietário. Por outro lado, nos moldes do art. 187 do CC, a noção de ato ilícito foi ampliada, para considerar como ilícito aquele ato que, originalmente é lícito, mas foi exercido fora dos limites impostos pelo seu fim econômico ou social, pela boa-fé objetiva ou pelos bons costumes.

Consequentemente, para que sejam produzidos os efeitos da responsabilidade civil, é essencial a configuração de três determinantes, quais sejam: a conduta, o nexo de causalidade e o dano. Vieira (2019, p. 28) explica que

> A conduta pode ser ação ou inação; comissiva ou omissiva; própria ou de terceiro; lícita ou ilícita; derivada de fato, coisa, produto ou animal. O nexo de causalidade liga a conduta do agente ao dano sofrido pela vítima. Para que surja o dever se indenizar é preciso que o dano verificado seja consequência da ação ou omissão do agente. O dano é a lesão a um bem jurídico.

Compreende-se que a LGPD dá responsabilidade a dois agentes criados durante o processo da legislação em comento: o controlador e o operador, como prevê o artigo 5°, VI e VII, respectivamente. *In verbis*:

> Art. 5º [...]
> VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
> VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador; (BRASIL, LGDP, 2020).

A LGPD, por sua vez, determina a responsabilidade dos agentes de tratamento de dados - operador e controlador - nos danos que acontecerem em virtude da prática da atividade de tratamento, semelhantemente ao modo como o

Código de Defesa do Consumidor. O artigo 43 da LGDP, no entanto, não responsabiliza os agentes quando comprovarem o seguinte:

> Art. 43 Os agentes de tratamento só não serão responsabilizados quando provarem:
> I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;
> II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou
> III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro (BRASIL, LGDP, 2020).

Importante ressaltar que o artigo 42 da mesma lei, ainda no que concerne ao operador e ao controlador, que, se como resultado de suas funções no tratamento de dados, estes causarem danos ou violações, sejam morais ou patrimoniais, serão responsabilizados por isso. O novo dispositivo confere ainda disposição expressa acerca das funções, tendo os dois responsabilidade solidária pelos atos praticados. (BRASIL, LGPD, 2020).

É interessante a análise de Vieira (2019, p. 29), quando afirma que

> A LGPD traz, ainda, previsão expressa de responsabilidade solidária dos operadores e controladores. Nesse sentido, conforme disposição do inciso I do §1º do art. 42. o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da LGPD ou quando não tiver seguido as instruções lícitas do controlador. Já os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados, conforme inciso II do §1º do art. 42 da LGPD, respondem solidariamente. O direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso, é assegurado àquele que reparar o dano ao titular dos dados consoante §4º do art. 42 da LGPD. Nos termos do art. 44 da LGPD, será considerado irregular o tratamento de dados pessoais quando for inobservada a legislação ou quando não for fornecida ao titular a segurança que ele poderia esperar, levando-se em conta as seguintes circunstâncias: o modo pelo qual o tratamento é realizado; o resultado e os riscos que razoavelmente dele se esperam; as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.

Por fim, é essencial mencionar as sanções administrativas trazidas pela nova lei, com aplicação àqueles chamados agentes que fazem o tratamento de dados. Caso estes violem alguma norma preconizada na legislação, terão como responsabilidade o que diz o artigo 52. *In verbis*:

> Art. 52 Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
> I - advertência, com indicação de prazo para adoção de medidas corretivas;
> II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
> III - multa diária, observado o limite total a que se refere o inciso II;

> IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
> V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização; VI - eliminação dos dados pessoais a que se refere a infração" (BRASIL, LGPD, 2020).

Então, tendo em mente este novo caminho, existe a busca de dar maior autoridade e domínio do titular em relação aos seus dados, sob o viés de tentar mesclar o uso da rede mundial de computadores aos elementos intrínsecos no que concerne à proteção dos direitos, especialmente os fundamentais, podendo mencionar, dentre eles, a intimidade e a privacidade.

Isso quer dizer que, ao explorar o ambiente virtual, desde o início de seu uso pela sociedade, tem se mostrado algo em que as pessoas podem exercer liberdades. Claro que se sabe que tal liberdade não é absoluta, assim, não importa se for uma empresa ou, até mesmo, o Estado, estes terão que sofrer responsabilização por quaisquer violações que vierem a cometer em relação a um titular de dados (SILVA; SILVA, 2013).

Ao vislumbrar este cenário e tratando da circunstância atual vivenciada pelos titulares de dados, deve-se atentar para o fato de que

> Com a evolução tecnológica, a proteção jurídica dos dados pessoais, incluído, os dados sensíveis, tornou-se deveras relevante, na medida em que a desproteção dessas informações pode acarretar a vulnerabilidade de direitos e princípios constitucionais, perante, por exemplo, práticas como a apropriação e o repasse no ambiente digital, sem autorização do usuário. No presente artigo científico, observou-se que as cláusulas da Lei n. 12.737/14, conhecida como Marco Civil da Internet, bem como da Lei Geral de Proteção de Dados Pessoais (LGPD) de n. 13.709/18 são promulgadas com o objetivo de proteger os internautas no ambiente digital, tendo por base as premissas do livre desenvolvimento da personalidade da pessoa natural, boa-fé nas relações de tratamento de dados pessoais e cumprimento de princípios da segurança da informação. Nesse viés, o direito à privacidade ganhou novo amparo jurídico específico, na medida em que a reunião desses instrumentos normativos colaborou para tutelar os direitos e garantias de forma mais efetiva no ambiente digital e "online", posto que anteriormente não era regulamentado de forma satisfatória. Entretanto, vislumbra-se que, mesmo após a edição da Medida Provisória nº 869/2018, que instituiu a criação da Autoridade Nacional de Proteção de Dados, a necessidade de complementação da legislação infraconstitucional, pois as disposições nacionais à proteção de dados deixam lacunas na efetividade da segurança informacional do internauta perante seus próprios dados, a exemplo, a previsibilidade de penalidades mais severas quando se descumpre os comandos dispostos na LGPD. Enfatiza-se que o tema acerca da proteção de dados é um assunto imprescindível a ser estudado, analisado e entendido, face a sociedade globalizada, que, constantemente, utiliza, tem acesso e usa informações pessoais nas relações, especialmente, jurídicas, deve-se, dessa forma, garantir relações traçadas na confiabilidade, integridade, com o viés de proporcionar maior segurança jurídica e respeito à autodeterminação informativa, incluindo o dever se proteger o direito à privacidade. E, por fim, sabe-se que, quando se trata de

> meios para se garantir a segurança da informação e a proteção de dados pessoais, é necessário o aperfeiçoamento constante das legislações, dos instrumentos para torná-la aplicável efetivamente, bem como dos modos de conscientização dos usuários/proprietários dos seus próprios dados, sendo, portanto, um trabalho constante, tanto do Poder Público, quanto da Sociedade (CARVALHO; PEDRINI, 2019, p. 379).

Assim, evidente a forma como o ordenamento jurídico deve manter-se atualizado diante das mudanças na sociedade, pois

> Diante dos desafios do mundo moderno é impensável a exploração de atividade econômica sem que haja a utilização de dados pessoais, vivemos na era da informação e numa sociedade digital. Esse ambiente, entretanto, não pode servir como salvo-conduto para revogação tácita de direitos constitucionalmente assegurados, muito pelo contrário, este cenário deve impulsionar o fortalecimento do arranjo institucional que preserve o cidadão, pois quanto maior o avanço tecnológico maior é a possibilidade de obtenção e utilização indevida dos dados pessoais. Assim, plenamente justificada a elaboração da LGPD com previsão de inúmeras obrigações e severas penalizações (SANTOS, A., 2019, p. 21-22).

No que tange à tutela dos dados pessoais, tendo em vista a busca por direitos, percebe-se que, neste campo, tutelas coletivas poderão ser propostas. Trata-se de mais uma garantia no que se refere aos direitos difusos, por isso, Roque argumenta que

> Dessa forma, torna-se absolutamente relevante aprofundar o estudo da tutela coletiva de dados pessoais, o que se buscou realizar mediante o presente estudo, no qual se concluiu que: (i) a proteção de dados pessoais na esfera coletiva pode dar origem a direitos difusos, coletivos em sentido estrito ou individuais homogêneos; (ii) são legitimados coletivos para a proteção de dados pessoais todos aqueles relacionados no art. 5º da Lei n.º 7.347/1985 e no art. 82 do CDC, sem prejuízo da legitimação do indivíduo, em situações excepcionais; e (iii) deve-se admitir a formulação de pedido genérico de reforma estrutural, na forma do art. 324, § 1º do CPC, havendo fundamento legal para a adoção das medidas estruturantes, sobretudo na fase de cumprimento de sentença, nos arts. 139, IV e 536, §1º do CPC (2019, p. 16).

Por fim, consciente das medidas necessárias em relação a uma responsabilização que porventura uma companhia vier a sofrer, é importante desde já atentar para o que diz Pinheiro (2018, p. 36): “Sendo assim, um programa de gestão de dados pessoais bem implementado pode ajudar na redução das penas, na hipótese de ocorrência de um tipo de infração que enseje a aplicação de alguma penalidade”.

Além disso, é importante o que salienta Doneda ao afirmar que

> A responsabilidade civil tem, portanto, função de destaque na disciplina de proteção de dados pessoais, principalmente se houver a definição de casos específicos de responsabilidade objetiva – vide que a imensa dificuldade na demonstração do dano é um dos problemas clássicos enfrentados pela

> consolidação da tutela da privacidade. Assim, uma disciplina de responsabilidade objetiva específica para o setor de tratamento de dados pessoais pode ser um instrumento essencial, tanto para a satisfação de interesses lesados como para fomentar uma determinada cultura de respeito às informações pessoais nas atividades que impliquem no tratamento destas (2008, p. 1).

5 CONCLUSÃO

Uma vez identificado o processo de construção da LGPD, pôde-se compreender que, antes desta legislação ser sancionada, ou até mesmo antes de ela entrar em vigor, já existiam muitas normas no ordenamento jurídico brasileiro acerca da proteção de dados pessoais, como por exemplo o próprio CDC (Lei nº 8.078/1990), a MCI (Lei nº 12.965/2014), a Lei de Acesso à Informação (Lei n° 12.527/2011), entre outras. Ao ver todo esse aparato legal, entendia-se que havia um quebra-cabeças, várias peças espalhadas, que não tinham sintonia, sendo difícil poder agrupá-las. Diante disso, compreende-se que com a promulgação da nova lei, surgiu um impacto positivo, pois antes não era possível estruturar um sistema completo, mesmo havendo grande regulamentação acerca do assunto. Conclui-se que apesar de haver várias leis setoriais de proteção de dados pessoais, elas, na verdade, representavam um grande emaranhado, porque todas essas normas e regras estavam espalhadas, e faltando ainda a maior peça desse quebra-cabeça, que é a LGDP brasileira. A partir de então, tornava-se possível ver todos os conceitos básicos condensados em uma única legislação, o que facilitava o trabalho de todas as entidades e cidadãos que queriam estar em conformidade com as novas regras.

Quando entrar totalmente em vigor a LGPD, o país estará implantando uma nova regulação relacionada aos dados pessoais. Com isto, pretende-se proporcionar mecanismos efetivos e capazes na manutenção de garantias relacionadas à vida privada, com a devida transparência neste processo.

Com o entendimento acerca dos dados pessoais e sensíveis, pôde-se compreender melhor a questão do consentimento, inclusive as penalidades envolvidas no caso de haver desrespeito ao ordenamento no que diz respeito a esse elemento essencial.

Compreendeu-se que a nova lei é regida por princípios que podem instigar a iniciativa pública e privada a transformar a internet em uma esfera mais democrática. Percebe-se que imprecisões, erros ou intrusões podem ocorrer, porém, vislumbra-se que ainda assim, haverá mais proteção jurídica. Assim, no caminho da previsibilidade, a segurança jurídica vem para preservar os direitos.

É evidente o desafio contínuo em relação aos obstáculos que as companhias acabam encontrando para obter coerência com a LGPD,

desenvolvendo e renovando suas políticas de proteção e tratamento, para entrar em consonância com o amparo legal estabelecido, além de sempre atualizar os termos legais que propõem para com as informações de seus clientes-usuários, como parâmetros no que se refere ao uso e ao período de obtenção de dados pessoais, sendo assim, as empresas precisarão adequar-se o mais rápido possível quando a lei de fato entrar integralmente em vigor, pois estarão lidando com direitos fundamentais.

Precisa-se compreender que a nova lei, uma vez implantada integralmente, trará mudanças significativas nas relações entre a empresa e o usuário/consumidor dos serviços e dos produtos. Diante das novas alterações, os usuários precisarão também ter mais conhecimento, daí a importância de haver um maior entendimento do mundo digital, para que todos possam de fato verificar a proteção e a segurança de seus dados pessoais. Isso significa dizer que, ao utilizar a rede e outras tecnologias, os cidadãos precisam ter consciência acerca do consentimento que fornecem, bem como da provável coleta e armazenamento de seus dados.

Vislumbra-se que a presente lei produza a consolidação do uso íntegro, protetivo e legal acerca dos dados pessoais, respeitando os princípios instruídos, para garantir, acima de tudo, ao tratar da proteção da dados pessoais, o respeito ao direito fundamental à privacidade.

Ora, o uso das informações pessoais, excepcionalmente dos dados pessoais, são valiosos para seu titular, desta forma, tendo este, o direito de restringir que estes dados sejam usados de maneira indevida, à proporção que este lhe traga violações, com base no princípio da dignidade humana, é viável confirmar que o manuseio destes dados por pessoas jurídicas de direito púbico e de direito privado fará jus à padronização característica que envolva e determine a participação de controladores e operadores.

Considerando ser o meio online abrangente e extremamente vasto, pode-se considerar complexo e difícil manter o domínio das informações que trafegam pela internet, de modo que em várias situações pode ser que aconteça vazamentos de informações de banco de dados, pois não é possível garantir sempre a integridade dos dados em um mundo virtual, uma vez que que pode haver erros técnicos ou furto de informação.

Desta forma, após a entrada em vigor da Lei Geral de Proteção de Dados (LGPD), torna-se viável examinar o método escolhido pelo legislador a favor da clareza, da autonomia e do cuidado do jurídico em relação aos direitos inerentes à personalidade. Compreende-se que a nova legislação vem para deixar mais transparente a relação dos agentes de tratamento de dados com os titulares, e tal relação deve estar revestida de boa-fé.

A normalização do manuseio de dados coloca o Brasil em igual nível aos demais países do Mercosul que regozijavam de legislação própria, extermina, também, a questão da necessidade de jurisdição em contextos específicos nos quais são requeridos os dados e não concedidos com a justificativa de não obter lei unânime à tal solicitação.

Este é um desenvolvimento significativo para os vínculos não só jurídicos, mas também de interesse comercial em nosso país. Tal lei viabiliza conceder responsabilidade a quem de fato lhe cabe e, em situações de quebra do cumprimento legal, são dadas ordens administrativas e incidem exigências de compensação e reparo em caso de perda. Isso garante uma grande credibilidade jurídica não somente ao titular das informações como também aos agentes de controle.

Por fim, acredita-se também que com a entrada em vigor da Lei Geral de Proteção de Dados no Brasil, em agosto de 2020, que seus mecanismos, sejam eles materiais, processuais ou administrativos, terão a possibilidade, em diversas situações, de serem úteis como incentivo à perpetuação das ordens judiciais de exclusão de conteúdos da internet.

Assim que a LGPD de fato entrar em vigor, espera-se que aqueles que operam os dados pessoais já estejam adequados à legislação, para que seja evitada qualquer violação às informações dos titulares de dados, e para os usuários/consumidores possam estar cientes de todos os direitos que decorrem do direito maior à privacidade.

REFERÊNCIAS

ALMEIDA, Bethania de Araújo *et al*. Preservação da privacidade no enfrentamento da COVID-19: dados pessoais e a pandemia global: dados pessoais e a pandemia global. **Ciência e Saúde Coletiva**, [s.l.], v. 25, n. suppl 1, p. 2487-2492, jun. 2020. DOI https://doi.org/10.1590/1413-81232020256.1.11792020. Disponível em: https://www.scielosp.org/article/csc/2020.v25suppl1/2487-2492/. Acesso em: 18 jun. 2020.

BASTOS, Athena. **Direito digital:** guia da lei geral de proteção de dados pessoais: LGPD**.** 2018. Disponível em: https://blog.sajadv.com.br/direito-digital-lei-de-protecao-de-dados/. Acesso em: 20 maio 2020.

AZAMBUJA, Antonio João Gonçalves de *et al*. A privacidade, a segurança da informação e a proteção de dados no Big Data. **Parc. Estrat.** Brasília-DF, v. 24, n. 48, p. 9-32, jan./jun., 2019. Disponível em: http://seer.cgee.org.br/index.php/parcerias_estrategicas/article/viewFile/914/831. Acesso em: 5 jun. 2020.

BIONI, Ricardo, B. **De 2010 a 2018:** a discussão brasileira sobre uma lei geral de proteção de dados**.** 2018a. Disponível em: https://brunobioni.com.br/blog/2018/07/02/de-2010-a-2018-a-discussao-brasileira-sobre-uma-lei-geral-de-protecao-de-dados/. Acesso em: 5 jun. 2020.

BIONI, Ricardo, B. **Proteção de dados pessoais:** a função e os limites do consentimento. Rio de Janeiro: Forense, 2018b. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530983291/. Acesso em: 20 maio 2020. Acesso restrito.

BIONI, Bruno Ricardo. **Regulação de dados é uma janela de oportunidade**. 2019. Disponível em: https://dataprivacy.com.br/regulacao-de-dados-e-uma-janela-de-oportunidade/. Acesso em: 5 jun. 2020.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Código de defesa do consumidor. **Diário Oficial da União**, Brasília, 11 set. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078.htm/. Acesso em: 20 maio de 2020.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Código Civil. **Diário Oficial da União**, Brasília, 10 jan. 2002. Disponível em: http:// http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm/. Acesso em: 20 maio de 2020.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei geral de proteção de dados. **Diário Oficial da União**, Brasília, 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm/. Acesso em: 20 maio 2020.

BRASIL. Lei nº 12.214, de 09 de junho de 2011. Lei de cadastro positivo. **Diário Oficial da União**, Brasília, 09 jun. 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm/. Acesso em: 20 maio 2020.

BRAUN, Julia. **Na China, atos dos cidadãos valerão pontos e limitarão seus projetos**. 2018. Disponível em: https://veja.abril.com.br/mundo/na-china-atos-dos-cidadaos-valerao-pontos-e-limitarao-seus-projetos/. Acesso em: 5 jun. 2020.

CARVALHO, Gisele Primo; PEDRINI, Tainá Fernanda. Direito à privacidade na lei geral de proteção de dados pessoais. **ESMESC**, Florianópolis, ano 2019, v. 26, n. 32, p. 363-382, 8 ago. 2019. DOI htp://dx.doi.org/10.14295/revistadaesmesc.v26i32.p363. Disponível em: https://revista.esmesc.org.br/re/article/view/217. Acesso em: 5 jun. 2020.

DONEDA, Danilo**. Da privacidade à proteção de dados pessoais.** Rio de Janeiro: Renovar, 2006.

DONEDA, Danilo. **Privacidade, vida privada e intimidade no ordenamento jurídico brasileiro:** da emergência de uma revisão conceitual e da tutela de dados pessoais. 2008. Disponível em: https://ambitojuridico.com.br/cadernos/direito-civil/privacidade-vida-privada-e-intimidade-no-ordenamento-juridico-brasileiro-da-emergencia-de-uma-revisao-conceitual-e-da-tutela-de-dados-pessoais/#_ftn27. Acesso em: 5 jun. 2020.

GODINHO, Adriano Marteleto *et al*. **Responsabilidade civil e novas tecnologias**. Indaiatuba: Foco Jurídico Ltda, 2020. Disponível em: https://books.google.com.br/books?id=drzoDwAAQBAJ&printsec=frontcover&hl=pt-BR#v=onepage&q&f=false. Acesso em: 5 jun. 2020

GOGANI, Ronaldo. **O maior roubo de dados da história do Facebook que ajudou a eleger Donald Trump**. 2018. Disponível em: https://meiobit.com/381701/facebook-cambridge-analytica-roubo-dados-ajudou-campanha-donald-trump-e-brexit/. Acesso em: 5 jun. 2020.

GONÇALVES, Ellen; LOTUFO, Larissa. **O consumidor conectado e a sua relação com o Direito**. 2020. Disponível em: https://www.ecommercebrasil.com.br/artigos/consumidor-conectado-relacao-direito/. Acesso em: 28 maio 2020.

GROSSMANN, Luis Osvaldo. **Senado aprova e lei de proteção de dados pessoais vai à sanção**. 2018. Disponível em: http://www.abranet.org.br/Noticias/Senado-aprova-e-Lei-de-protecao-de-dados-pessoais-vai-a-sancao-1971.html?UserActiveTemplate=site#.XtwAvcBv_IU. Acesso em: 5 jun. 2020

GUIMARÃES, Saulo Pereira. **Conheça quem ganha dinheiro enquanto você navega na internet**. 2015. Disponível em: https://exame.com/tecnologia/conheca-quem-ganha-dinheiro-enquanto-voce-navega-na-internet/. Acesso em: 5 jun. 2020.

KATARIVAS, Nicole. **A lei do cadastro positivo e a lei geral de proteção de dados:** conflito ou sinergia? 2019. Disponível em: https://www.migalhas.com.br/depeso/298656/a-lei-do-cadastro-positivo-e-a-lei-geral-de-protecao-de-dados-conflito-ou-sinergia. Acesso em: 5 jun. 2020.

KRIEGER, Maria Victoria Antunes. **A análise do instituto do consentimento frente à lei geral de proteção de dados do Brasil:** lei nº 13.709/18. 2019. 83 f. TCC (Graduação) - Curso de Direito, Universidade Federal de Santa Catarina,

Florianópolis, 2019. Disponível em: https://repositorio.ufsc.br/bitstream/handle/123456789/203290/TCC.pdf?sequence=1&isAllowed=y. Acesso em: 12 jun. 2020.

LANCHESTER, John. **Você é o produto**: Mark Zuckerberg e a colonização das redes pelo facebook. Mark Zuckerberg e a colonização das redes pelo Facebook. 2017. Disponível em: https://piaui.folha.uol.com.br/materia/voce-e-o-produto/. Acesso em: 05 jun. 2020.

LIMA, Lindamaria. **Os 10 Princípios para tratamento de dados da LGPD**. 2020. Disponível em: https://triplait.com/principios-para-tratamento-de-dados-da-lgpd/. Acesso em: 05 jun. 2020.

MARTINI, Sandra Regina; BERGSTEIN, Laís. Aproximações entre o direito ao esquecimento e a lei geral de proteção de dados pessoais (LGPD). **Disruptiva**, Recife, v. 1, n. 1, p. 160-176, 25 jun. 2019. Disponível em: https://d1wqtxts1xzle7.cloudfront.net/61408339/Artigo_9-_Aproximacoes_entre_o_direito...20191203-19221-4507dt.pdf?1575375701=&response-content-disposition=inline%3B+filename%3DAproximacoes_entre_o_direito_ao_esquecim.pdf&Expires=1591942593&Signature=Tqdwx~U2EScG7ILiwjiMUY8jxs1sXR-4a7k2NmfztXF-r2QWUQJsI0xZHttz9ZmKiq03JcGJ5b3rOctLkuJK5BcV5n7J4W-CjE8IjV8gyFtVQzXli7kYT~EVPsCPzRsZb1pVqaJoJr4IWzDLUO5oDOMkMGe~aIw9EkH00-MNtG3ipRQSDVe8WHN5SW4OmMBUKE4obwgnWh6xUUpS5PHWBqDQWB~v4dNymtbb3FhDtFII2q4vWPVJarpTeMyMk2LYiMf8ORvbH-F18-LEM2M9cFlkiF6xjVI97v0YsFsR9nlw8zqoS1WW0q04KPRC1qo-qtZAm31S~-BXa7WjvnqZRw__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA. Acesso em: 5 jun. 2020.

MENDES, Thomas. **LGPD:** entenda sobre anonimização de dados. Disponível em: https://w3lcome.com/pt/lgpd-dados-anonimizados/. Acesso em: 6 jun. 2020.

MILHORANCE, Flávia. **O que se sabe sobre a atuação da Cambridge Analytica no Brasil**. 2018. Disponível em: https://projetocolabora.com.br/ods8/o-que-se-sabe-sobre-a-atuacao-da-cambridge-analytica-no-brasil/. Acesso em: 5 jun. 2020.

MOREIRA, André de Oliveira Schenini. **A lei de proteção de dados pessoais da União Europeia (GDPR) e sua aplicação extraterritorial às entidades e empresas brasileiras**. 2017. Disponível em: https://www.migalhas.com.br/depeso/267772/a-lei-de-protecao-de-dados-pessoais-da-uniao-europeia-gdpr-e-sua-aplicacao-extraterritorial-as-entidades-e-empresas-brasileiras. Acesso em: 5 jun. 2020.

MULHOLLAND, Caitlin. O direito de não saber como decorrência do direito à intimidade: comentário ao REsp 1.195.995. **Civilistica.com - Revista Eletrônica de Direito Civil**, v. 1, p. 1, 2012. Disponível em: http://civilistica.com/wp-content/uploads/2012/09/Direito-de-nao-saber-civilistica.com-1.-2012.pdf Acesso em: 5 jun. 2020

MULHOLLAND, Caitlin. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (lei 13.709/18). **Revista Dir. Gar. Fund**., Vitória, v. 19, n. 3, p. 167 set./dez. 2018. Disponível em:

http://sisbib.emnuvens.com.br/direitosegarantias/article/view/1603. Acesso em: 5 jun. 2020.

PEIXOTO, Andréa Stefani. **Lei de proteção de dados:** entenda em 13 pontos! 2020. Disponível em: https://www.politize.com.br/lei-de-protecao-de-dados/. Acesso em: 5 jun. 2020.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais comentários à lei n. 13.709/2018:** LGPD**.** São Paulo: Saraiva, 2018. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788553608324/cfi/0!/4/2@100:0.00. Acesso em: 14 maio 2020.

RED CROSS Blood Service admits to personal data breach affecting half a million donors. 2016. Disponível em: https://www.abc.net.au/news/2016-10-28/red-cross-blood-service-admits-to-data-breach/7974036. Acesso em: 5 jun. 2020.

RIBEIRO, Davi. **Qual é a relação entre a LGPD e o CDC?** 2020. Disponível em: https://davirdr.jusbrasil.com.br/artigos/814465325/qual-e-a-relacao-entre-a-lgpd-e-o-cdc?ref=feed. Acesso em: 28 maio 2020.

ROQUE, André. A tutela coletiva dos dados pessoais na lei geral de proteção de dados pessoais: LGPD. **Revista Eletrônica de Direito Processual – REDP**, Rio de Janeiro, v. 20, n. 2, p. 01-19, maio/ago. 2019. Disponível em: https://www.e-publicacoes.uerj.br/index.php/redp/article/view/42138/30270. Acesso em: 5 jun. 2020.

SALDANHA, João. **O princípio da necessidade na LGPD:** a minimização de dados como redutor de custos. 2019. Disponível em: https://triplait.com/o-principio-da-necessidade-na-lgpd/. Acesso em: 5 jun. 2020.

SANDER, Guilherme. **Principais conceitos da LGPD**. 2019. Disponível em: https://sisqualis.com.br/conceitos-lgpd/. Acesso em: 6 jun. 2020.

SANTOS, Alexandre da Silva. **A importância da atuação da auditoria interna na implementação da lei geral de proteção de dados nas empresas públicas**. Orientador: Marco Antonio Carvalho Teixeira. 2019. 23 p. Dissertação (Mestrado em Gestão e Políticas Públicas) - Fundação Getúlio Vargas, São Paulo, 2019. Disponível em: https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/29221/A%20IMPORTANCIA%20DA%20ATUA%c3%87%c3%83O%20DA%20AUDITORIA%20INTERNA%20NA%20IMPLEMENTA%c3%87%c3%83O%20DA%20LGPD%20NAS%20EMPRESAS%20PUBLICAS.pdf?sequence=1&isAllowed=y. Acesso em: 5 jun. 2020.

SANTOS, Dhiulia de Oliveira. **A validade do consentimento do usuário à luz da lei geral de proteção de dados pessoais:** lei n. 13.709/2018. 2019. 50 f. TCC (Graduação) - Curso de Direito, Centro Universitário de Brasília - Uniceub, Brasília, 2019. Disponível em: https://repositorio.uniceub.br/jspui/handle/prefix/13802. Acesso em: 5 jun. 2020.

SILVA, Rosane Leal; SILVA, Letícia Brum. **A proteção jurídica de dados pessoais na internet:** análise comparada do tratamento jurídico do tema na União Europeia e no Brasil. Direito e novas tecnologias. Florianópolis: FUNJAB, 2013. Disponível em:

http://www.publicadireito.com.br/artigos/?cod=e4d8163c7a068b65. Acesso em: 5 jun. 2020.

SILVA, Lucas Gonçalves; MELO, Bricio Luis da Anunciação. A lei geral de proteção de dados como instrumento de concretização da autonomia privada em um mundo cada vez mais tecnológico. **Revista Jurídica Unicuritiba**, Curitiba, ano 2018, v. 3, n. 56, p. 354 - 377, jul./set. 2019. DOI http://dx.doi.org/10.21902/revistajur.2316-753X.v3i56.3581. Disponível em: http://revista.unicuritiba.edu.br/index.php/RevJur/article/view/3581. Acesso em: 5 jun. 2020.

SENA, Sâmara Rodrigues. A proteção de dados pessoais de crianças no ordenamento jurídico brasileiro. **Caderno Virtual**, [s.l.], v. 44, n. 2, p. 1-26, jun. 2019. Disponível em: https://portal.idp.emnuvens.com.br/cadernovirtual/article/view/3854/1673. Acesso em: 5 jun. 2020.

TUMELERO, Thays. **Princípios da LGPD:** terminologia e aplicação prática. 2019. Disponível em: https://ostec.blog/geral/principios-da-lgpd. Acesso em: 5 jun. 2020.

TUMELERO, Thays. **Vigência da LGPD e a insegurança jurídica**. 2020. Disponível em: https://www.nsctotal.com.br/noticias/vigencia-da-lgpd-e-a-inseguranca-juridica. Acesso em: 17 jun. 2020.

VALENTE, Jonas. **Lei de proteção de dados traz mudanças para crianças e adolescentes**. 2018. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2018-09/lei-de-protecao-de-dados-traz-mudancas-para-criancas-e-adolescentes. Acesso em: 5 jun. 2020.

VENTURA, Ivan. **A relação entre a Lei de proteção de dados e o ingresso do Brasil na OCDE**. 2019. Disponível em: https://www.consumidormoderno.com.br/2019/03/20/relacao-lgpd-desejo-brasil-ocde/. Acesso em: 5 jun. 2020.

VERGILI, Gabriela Machado. **Análise comparativa entre direito à privacidade e direito à proteção de dados pessoais e relação com o regime de dados públicos previsto na lei geral de proteção de dados**. 2019. Disponível em: https://dataprivacy.com.br/analise-comparativa-entre-direito-a-privacidade-e-direito-a-protecao-de-dados-pessoais-e-relacao-com-o-regime-de-dados-publicos-previsto-na-lei-geral-de-protecao-de-dados/. Acesso em: 22 maio 2020.

VIEIRA, Ronaldo. **LGPD:** o Brasil também entra no mapa. 2018. Disponível em: https://www.securityreport.com.br/overview/lgpd-o-brasil-tambem-entra-no-mapa/#.XtxGYcBv_IU. Acesso em: 5 jun. 2020.

VIEIRA, Victor Rodrigues Nascimento. **Lei geral de proteção de dados:** uma análise da tutela dos dados pessoais em casos de transferência internacional**.** 2019. 77 f. TCC (Graduação) - Curso de Direito, Universidade Federal de Uberlândia, Uberlândia, 2019. Disponível em: https://repositorio.ufu.br/handle/123456789/26233. Acesso em: 5 jun. 2020.