

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

**AS MUDANÇAS SOCIAIS E A CRIAÇÃO DA LEI GERAL DE PROTEÇÃO DE
DADOS, LEI Nº 13.709/2018 : UMA ANÁLISE DOS PRINCIPAIS ASPECTOS**

JULIANA PAES LEME SAMPAIO CORREIA

Rio de Janeiro

2022

JULIANA PAES LEME SAMPAIO CORREIA

**AS MUDANÇAS SOCIAIS E A CRIAÇÃO DA LEI GERAL DE PROTEÇÃO DE
DADOS, LEI Nº 13.709/2018 : UMA ANÁLISE DOS PRINCIPAIS ASPECTOS**

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de bacharel em Direito, sob a orientação do **Professor Dr. Guilherme Kronenberg Hartmann**

Rio de Janeiro

2022

CIP - Catalogação na Publicação

P824m Paes Leme Sampaio Correia, Juliana
AS MUDANÇAS SOCIAIS E A CRIAÇÃO DA LEI GERAL DE
PROTEÇÃO DE DADOS, LEI N° 13.709/2018 : UMA ANÁLISE
DOS PRINCIPAIS ASPECTOS / Juliana Paes Leme
Sampaio Correia. -- Rio de Janeiro, 2022.
53 f.

Orientador: Guilherme Kronenberg Hartmann.
Trabalho de conclusão de curso (graduação) -
Universidade Federal do Rio de Janeiro, Faculdade
Nacional de Direito, Bacharel em Direito, 2022.

1. LGPD. I. Kronenberg Hartmann, Guilherme ,
orient. II. Título.

JULINA PAES LEME SAMPAIO CORREIA

**AS MUDANÇAS SOCIAIS E A CRIAÇÃO DA LEI GERAL DE PROTEÇÃO DE
DADOS, LEI Nº 13.709/2018 : UMA ANÁLISE DOS PRINCIPAIS ASPECTOS**

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de bacharel em Direito, sob a orientação do **Professor Dr. Guilherme Kronenberg Hartmann**

Data da Aprovação: __ / __ / ____.

Banca Examinadora:

Orientador

Co-orientador (Opcional)

Membro da Banca

Membro da Banca

**Rio de Janeiro
2022**

AGRADECIMENTOS

Gostaria de agradecer a todos que de alguma forma me auxiliaram nessa jornada acadêmica.
Um agradecimento, em especial, aos meus pais.

RESUMO

O presente trabalho visa analisar e relacionar os pontos principais em relação às mudanças sociais e comportamentais com a criação de uma Lei Geral de Proteção de Dados. Objetivo dessa monografia é destacar os pontos principais das mudanças sociais que ocorreram ao longo dos tempos junto a conjuntura que elevou o papel dos dados pessoais na sociedade como um ativo de grande valor. A partir de uma análise e estudos bibliográficos sobre a temática ficou demonstrado a forma e o porquê dos dados possuírem um enorme valor dentro da sociedade informacional, a sua característica preditiva e a possibilidade de tornar identificar o indivíduos são as principais responsáveis somando a uma sociedade cada vez mais automatizada e conectada. Evidenciou-se, assim, a necessidade e a criação de uma norma regulamentadora que tenha por objetivo proteger os indivíduos e seus dados.

Palavras-chave: Lei Geral de Proteção de Dados, dados pessoais, sociedade informacional, valor dos dados, tecnologia, criação Lei nº 13.709/2018.

ABSTRACT

The present work aims to analyze and relate the main points in relation to social and behavioral changes with the creation of a General Data Protection Law. The purpose of this monograph is to highlight the main points of social changes that have occurred over time along with the situation that has elevated the role of personal data in society as an asset of great value. From an analysis and bibliographical studies on the subject, it was demonstrated how and why data have an enormous value within the informational society, its predictive characteristic and the possibility of identifying individuals are the main responsible adding to a society each increasingly automated and connected. Thus, the need and the creation of a regulatory standard that aims to protect individuals and their data became evident.

Keywords: General Data Protection Law, personal data, informational society, data value, technology, creation of Law n° 13.709/2018.

SUMÁRIO

1 INTRODUÇÃO	2
2. SOCIEDADE CONECTADA	12
2.1 A Quarta Revolução Industrial.	12
2.2 Valor dos dados.	15
2.3 Casos emblemáticos.	17
2.4 Conceito de privacidade na era digital.	19
3. A NECESSIDADE DE UMA LEGISLAÇÃO VOLTADA À PROTEÇÃO DE DADOS.	24
3.1 Classificação das gerações das leis de proteção de dados.	24
3.2 GDPR e a influência na criação da LGPD.	26
3.3 Legislações de dados anteriores a LGPD.	29
4. PRINCIPAIS CARACTERÍSTICAS DA LGPD.	31
4.1 Introdução a LGPD - Lei 13.709/2018.	31
4.2 Conceito e terminologias.	33
4.3 Fundamentos e princípios da proteção de dados.	36
4.4 O consentimento.	45
4.4 As alterações da Lei nº 13.853/2019.	47
CONCLUSÃO	49
BIBLIOGRAFIA	51

1 INTRODUÇÃO

O presente trabalho tem como objetivo relacionar e analisar a relação entre os avanços sociais e a criação da Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, e o seu papel social. Abordaremos a conjuntura histórica que culminou em sua elaboração, os principais princípios norteadores, conceitos e fundamentos da lei.

Para tanto, utilizou-se o método dedutivo, elaborou-se uma pesquisa doutrinária e jurídica para investigar e compreender os principais desenvolvimentos, momentos e conceitos. A fim de elucidar a relevância e pertinência da temática da importância da proteção de dados para a sociedade, destacaremos casos reais emblemáticos, que demonstrarão o valor dos dados pessoais e seus entraves, ao longo do presente trabalho.

O assunto sobre a necessidade de uma legislação de proteção é um debate antigo. O Ministério da Justiça em 2010 lançou a primeira consulta pública sobre o anteprojeto de lei de dados pessoais em uma plataforma online que possibilitaram uma ampla contribuição dos cidadãos e empresas. Ao decorrer dos anos diversos fatores econômicos, sociais e políticos catalisaram a necessidade de criação de uma lei específica. Podemos mencionar casos de espionagem no Brasil que levaram a criação da CPI da Espionagem, a criação do Marco Civil da Internet e a entrada em vigor do Regulamento Geral de Proteção de Dados da União Europeia (RGPD).

Diante desse cenário, no dia 14 de agosto de 2018 foi publicada a Lei 13.7093 - Lei Geral de Proteção de Dados Pessoais - dispoendo sobre o adequado tratamento de dados pessoais e suas sanções. A LGPD teve forte influência da Regulamentação Geral de Proteção de Dados, legislação europeia aprovada em 2016 que aumentou o controle sobre a proteção dos dados pessoais dos cidadãos europeus. A lei brasileira entrou em vigor em 18 de setembro de 2020 e a aplicação de sanções, somente, em 01 de agosto de 2021.

O objetivo da LGPD é proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Com isso, determina padrões e condutas a serem seguidos por qualquer pessoa natural ou jurídica de direito privado ou público que realizem o tratamento de dados pessoais tanto em meios físico quanto digital.

A necessidade de elaboração de uma norma específica sobre tratamentos de dados decorreu dos novos modelos de comportamentos de nossa sociedade junto a função do Estado de preservar a ordem e os limites para a paz. Veremos adiante como a revolução tecnológica junto ao desenvolvimento da informática possibilitou a difusão de informações e, também, da comunicação em níveis exponenciais, rompendo a questão do tempo e espaço devido a fluidez e o dinamismo em que a informação chega de um usuário a outro.

Assim como todas as grandes mudanças na sociedade a revolução atual a era tecnológica, veio acompanhada de enormes desafios para o ordenamento jurídico. O direito tem como objetivo garantir segurança e ordenamento na sociedade para os seus tutelados, diante um novo paradigma necessita acompanhar e se adaptar para cumprir seu papel nesse novo cenário.

A utilização de base de dados, principalmente de forma eletrônica, teve um enorme avanço e expansão nas últimas décadas. A coleta de dados por empresas e pessoas acontece a todo momento. Atualmente, a tecnologia permitiu inúmeras formas de processamento e armazenamentos de dados, como por exemplo a utilização de biometria para entrada em prédios comerciais e o reconhecimento facial utilizado pelo governo. Os dados pessoais tornam o indivíduo identificável e são considerados, atualmente, uma extensão da personalidade.

Os dados pessoais são caracterizados por tornar uma pessoa identificada ou identificável e, em decorrência disso, possuem uma direta ligação entre o titular dos dados. Dessa forma, passaram a ser considerados uma extensão de sua personalidade do titular. Logo, merecem proteção adequada para a garantia de direitos constitucionais como a privacidade e a liberdade.

Nesse sentido, é necessário que haja uma proteção efetiva e apropriada para a proteção de direitos fundamentais. A LGPD surgiu, então, para tutelar os dados pessoais independentes do meio em que se encontram, tanto no físico quanto no digital, porém os dados no meio digital ganham um enfoque maior devido a maior captação e processamento, como veremos a seguir

2. SOCIEDADE CONECTADA

Neste capítulo será realizado uma breve contextualização histórica para que se possa compreender a relação entre os avanços tecnológicos e a necessidade de uma legislação voltada à proteção dos dados nessa nova perspectiva.

2.1 A Quarta Revolução Industrial.

Klaus Schwab, fundador do Fórum Econômico Mundial, em sua obra denominada “Quarta Revolução Industrial” publicada em 2016 trouxe o conceito de Quarta Revolução Industrial, também conhecida como Indústria 4.0, que teve início por volta do ano de 2014 e perdura até a atualidade. Tal revolução é caracterizada, em suma, pelo uso da inteligência artificial, pela forte presença da internet na sociedade e sua ampla utilização nas mais diversas áreas. Klaus preceitua em seu livro:

Atualmente, enfrentamos uma grande diversidade de desafios fascinantes; entre eles, o mais intenso e importante é o entendimento e a modelagem da nova revolução tecnológica, a qual implica nada menos que a transformação de toda a humanidade. Estamos no início de uma revolução que alterará profundamente a maneira como vivemos, trabalhamos e nos relacionamos. Em sua escala, escopo e complexidade, a quarta revolução industrial é algo que considero diferente de tudo aquilo que já foi experimentado pela humanidade. Ainda precisamos compreender de forma mais abrangente a velocidade e a amplitude dessa nova revolução. Imagine as possibilidades ilimitada de bilhões de pessoas conectadas por dispositivos móveis, dando origem a um poder de processamento, recursos de armazenamento e acesso ao conhecimento sem precedentes. Ou imagine a assombrosa profusão de novidades tecnológicas que abrangem numerosas áreas: inteligência artificial (IA), robótica, a internet das coisas (IoT, na sigla em inglês), veículos autônomos, impressão em 3D, nanotecnologia, biotecnologia, ciência dos materiais, armazenamento de energia e computação quântica, para citar apenas algumas. Muitas dessas inovações estão apenas no início, mas já estão chegando a um ponto de inflexão de seu desenvolvimento, pois elas constroem e amplificam umas às outras, fundindo as tecnologias dos mundos físico, digital e biológico.¹

Smartphones, cartão de crédito de bancos digitais, Whatsapp, Google, Facebook, Waze, Uber e diversos outros aplicativos digitais são exemplos de tecnologias as quais estão

¹SCHWAB, Klaus. A quarta revolução industrial. Edipro, 2019, p.15.

intimamente presentes no cotidiano de diversos indivíduos. O advento e popularização da internet possibilitou que inúmeras atividades e situações que antes eram realizadas de forma física e presencial, como checar o extrato do banco ou falar com um amigo, pudessem ser realizadas de maneira virtual e de maneira muito mais rápida e prática.

A internet com o seu dinamismo possibilitou a globalização, uma integração econômica, social, cultural e política entre países. Logo, em um mundo globalizado o fluxo de trocas de informações é intensificado. O processo de globalização foi impulsionado pelo uso de novas tecnologias e, assim, encurtou o distanciamento entre nações e pessoas.

De acordo com filósofo Marshall McLuhan² a internet transformou o mundo em um aldeia global visto que os meios de comunicação quebraram as barreiras geográficas e culturais entre as diversas regiões do mundo. Nos dias de hoje é possível realizar uma conversa em vídeo com pessoas a quilômetros de distância, graças aos avanços tecnológicos.

Nesse conjuntura, ao focarmos no Brasil, devemos mencionar que o mesmo lidera o pódio de segundo colocado no ranking de países em que as pessoas passam mais tempo em redes sociais, os brasileiros gastam em média 219 minutos por dia nas redes digitais, segundo a pesquisas da empresa londrina GlobalWebIndex.³

Em 2019, o Brasil registrou o marco de 82,7% de domicílios conectados à internet. O uso entre os jovens brasileiros com 10 anos de idade ou mais é de 78,3%, segundo o censo do IBGE.⁴ A internet e a conectividade estão cada vez mais presentes entre a população sendo utilizadas para diversos fins, tanto para entretenimento, informação e como importante instrumento de socialização

Nesse cenário online de intensa exposição e compartilhamento de informações, grandes empresas já enxergam um novo segmento mercadológico de um potencial exponencial nesse segmento. As informações e dados fornecidos pelos usuários de sites e

²MCLUHAN, Marshall. Os meios de comunicação: como extensões do homem. Editora Cultrix, 1974.

³BRASIL É O 2º EM RANKING DE PAÍSES QUE PASSAM MAIS TEMPO EM REDES SOCIAIS. Época Negócios. 06 de setembro de 2019. Tecnologia. Disponível em: <<https://epocanegocios.globo.com/Tecnologia/noticia/2019/09/brasil-e-2-em-ranking-de-paises-que-passam-mais-tempo-em-redes-sociais.html>> Acessado em: 15 de out. de 2022.

⁴EDUCA, I. B. G. E. Uso de internet, televisão e celular no Brasil. IBGE Educa. Disponível em: <<https://educa.ibge.gov.br/jovens/materias-especiais/20787-uso-de-internet-televisao-e-celular-no-brasil.html>>. Acessado em 15 de out. de 2022, v. 18, 2019.

aplicativos deu origem ao surgimento de um novo mercado, o mercado de dados na esfera digital. A coleta de dados tem se mostrado como uma mina a ser explorada, pois possuem a capacidade de identificar indivíduos e de prever tendências.

A mudança do físico para o virtual deu origem a uma nova configuração social, onde a troca de informações e de dados é extremamente constante e dinâmica. Apesar dos avanços tecnológicos proporcionam inúmeros benefícios aos usuários, há com ele inúmeras novas problemáticas que devem ser observadas em relação a proteção de direitos fundamentais visto que ao acessar um site o usuário acaba por compartilhar dados pessoais.

Inegavelmente, diante desse novo panorama digital os dados passaram a possuir um enorme valor, por serem captados de maneira extremamente abundante e rápida. Dessa forma, a maneira são coletados, armazenados e utilizados necessitam ser pensada pois, além de serem são dados íntimos e privados havendo carência de regulamentação poderão ser utilizados sem o consentimento do detentor tanto para finalidades positivas quanto negativas e sem uma fiscalização efetiva.

O motivo que inspirou o surgimento de regulamentações de proteção de dados pessoais de forma mais consistente e consolidada a partir dos anos 1990 está diretamente relacionado ao próprio desenvolvimento do modelo de negócios da economia digital, que passou a ter uma dependência muito maior dos fluxos internacionais de bases de dados, especialmente os relacionados às pessoas, viabilizados pelos avanços tecnológicos e pela globalização.

Desse modo, houve a necessidade de resgatar e repactuar o compromisso das instituições com os indivíduos, cidadãos desta atual sociedade digital, no tocante à proteção e à garantia dos direitos humanos fundamentais, como o da privacidade, já celebrados desde a Declaração Universal dos Direitos Humanos (DUDH) de 1948.⁵

Em vista disso, o Estado observando a necessidade de proteger certos direitos fundamentais dos indivíduos como a liberdade, privacidade e livre desenvolvimento da pessoa natural, no tocante a utilização de dados pessoais, criou uma lei geral nacional sobre o tema, a Lei 13.7093 de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais – e, posteriormente a Emenda Constitucional 115 de 2022, que incluiu no rol de garantias

⁵PINHEIRO, Patricia Peck. Proteção de Dados Pessoais: Comentários à Lei n. 13.709/2018-LGPD. Saraiva Educação SA, 2020, pg. 11.

fundamentais a proteção de dados pessoais e fixou competência privativa da União para legislar sobre o tema.

De fato, o Brasil já possuía em sua legislação normas esparsas que versam sobre a proteção de dados pessoais, entretanto o grande destaque dado à Lei Geral de Proteção de Dados é que a mesma surge como um dispositivo geral e unificado sobre o tema, trazendo princípios e normas específicas que serão abordadas ao longo do presente trabalho.

Vale destacar que existe o mercado de dados físicos e que este, também, está tutelado pela LGPD, como veremos nos próximos capítulos. O objeto da tutela protetiva da Lei Geral de Proteção de Dados são os dados pessoais, conceito que será detalhado adiante, independentemente do meio em que este exista, seja físicos quanto digital. Contudo, por o meio digital ser extremamente dinâmico e possibilitar trocas de informações, captação e análise de dados de maneira célere, este acaba sendo mais explorado no presente trabalho.

2.2 Valor dos dados.

Nesta subseção será realizado uma breve contextualização e explicação a fim de elucidar a relevância econômica dos dados no contexto histórico atual.

Clive Humby, especialista em ciência de dados, não ousou ao afirmar que os dados são o novo petróleo⁶. A revolução informacional permitiu o armazenamento, processamento e captação de uma extensa quantidade de dados de uma forma jamais vista antes. Antigamente, as empresas mais valiosas no mercado eram as que lidavam com o petróleo por ser um ativo de grande utilidade. No panorama atual, é possível comprovar que os dados podem ser considerados um novo petróleo visto que as empresas mais valiosas no mercado de capitais são as empresas que lidam diretamente ou indiretamente com dados pessoais, sendo o dado o grande ativo dessa era.

⁶VISVAL, Cristian. Dados são o novo petróleo! O que você tem feito com os seus dados?. Revista Segurança Eletrônica, 2020. Disponível em: <

As informações pessoais e a coleta de dados têm se mostrado como uma mina a ser explorada, pois possuem a capacidade de prever tendências e identificar indivíduos. Inegavelmente, os dados passaram a possuir um enorme valor. Dessa forma, a maneira como os dados são coletados, armazenados e utilizados tem que ser pensada, são dados íntimos e privados podem ser utilizados tanto para finalidades positivas quanto negativas. Segundo o doutrinador Rodrigo Bioni:

Com a inteligência gerada pela ciência mercadológica, especialmente quanto à segmentação dos bens de consumo (marketing) e a sua promoção (publicidade), os dados pessoais dos cidadãos converteram-se em um fator vital para a engrenagem da economia da informação. E, com a possibilidade de organizar tais dados de maneira mais escalável (e.g., Big Data), criou-se um (novo) mercado cuja base de sustentação é a sua extração e comodificação. Há uma “economia de vigilância” que tende a posicionar o cidadão como um mero expectador das suas informações.⁷

Os dados mostram-se de extremo valor para a sociedade atual, pois através deles é possível mapear e identificar as singularidades de cada indivíduo e grupos e, assim, realizar a utilização deles de uma maneira exponencial tanto para o benefício ou malefício do titular. Percebe-se que a característica dos dados como uma extensão da personalidade do titular permite às empresas mapear padrões e com isso, melhorar serviços, direcionar publicidades, abordagem com o cliente, torna mais fácil o processo induzir e cativar o cliente.

Ao analisar as grandes empresas da bolsa de valores percebe-se que na década de 80 as empresas mais valiosas eram as empresas relacionadas à exploração de petróleo, como a Shell e as empresas automotoras. Atualmente, podemos perceber que as empresas que mais valem são as empresas que mexem com dados pessoais, como por exemplo Facebook, Apple, Google e Amazon.⁸

Um exemplo da utilização da análise dos dados pessoais por empresas na internet é a utilização dos cookies, que são arquivos que guardam as informações do usuário. Tendemos a achar que os sites nos fornecem acesso a diversos conteúdos sem nenhum custo monetário.

⁷BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 12/13.

⁸FERRAZ, Marina . Apple, Google e Amazon são as marcas mais valiosas de 2022. 15 de jun. de 2022. Poder360.
<https://www.poder360.com.br/economia/apple-google-e-amazon-sao-as-marcas-mais-valiosas-de-2022/>

Porém, em um mundo de mídias digitais os usuários geram lucros para as empresas pelo simples fato de utilizarem sites. Isso ocorre, porque ao acessar sites disponibilizamos nossos dados na plataforma digital. Há um viés econômico na coleta dos dados dos navegantes, que ocorriam na maior parte dos casos involuntariamente. Os dados depois de coletados passam por tratamento e análises e muitas vezes são vendidos, gerando, assim, receita ao site acessado.

Conforme bem nos exemplifica Rodrigo Boni:

Quando o usuário navega na Internet, há uma série de cliques (clickstream) que revela uma infinidade de informações sobre as suas predileções, possibilitando que a abordagem publicitária as utilize para estar precisamente harmonizada com elas. Desta forma, a publicidade on-line pode ser direcionada com um grau de personalização jamais alcançado pela publicidade of -line. Por isso, a publicidade comportamental on-line reduz os custos da ação publicitária, uma vez que o bem de consumo anunciado é correlacionado cirurgicamente aos interesses do consumidor abordado. A comunicação com o público-alvo daquele produto ou serviço é praticamente certa, ocasionando maior probabilidade de êxito quanto à indução ao consumo.⁹

Surge, então, o dever de uma nova análise sobre a maneira que é realizado o tratamento e o controle dos dados pessoais, visto que se observa cada vez mais o valor delas. Os dados por serem a extensão da personalidade devem ser tutelados para que seja resguardado a privacidade, autonomia e liberdade do titular.

2.3 Casos emblemáticos.

Iremos destacar alguns casos que demonstram a pertinência e relevância da temática da proteção de dados. Os casos a seguir evidenciam a comunicação entre a análise de dados e a privacidade do indivíduo.

Um dos casos emblemáticos sobre a temática de análise de dados e a privacidade é da empresa Target, que no começo dos anos 2000 revolucionou o seu mercado e ganhou muito dinheiro através da utilização de dados pessoais. A Target, uma das maiores empresas

⁹BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, pg. 16.

varejistas dos Estados Unidos, alinhou e organizou com auxílio de métodos matemáticos e programas estatísticos uma numerosa quantidade de dados pessoais oriundos de diferentes fontes, prática hoje chamada de análise comercial de dados. Conseguiram, assim, mapear e identificar padrões de consumos de diferentes nichos sociais, como por exemplo grávidas, pessoas solteiras, donas de casas. O mapeamento ajudava na estratégia de marketing, pois assim evidenciava em seu site produtos que o nicho mais se interessaria.

O caso emblemático se deu pelo fato de que ao notar padrões e reconhecer nichos através da utilização de mapeamento e a utilização de cookie, ferramenta que possibilita ao site acessado reconhecer o histórico de navegação do usuário, a empresa conseguia saber quando uma mulher estava grávida ou era mãe e a parabenizava.

Durante o período de gestação as mulheres consomem um padrão de produtos, assim, essa empresa conseguiu verificar que tal perfil de consumidoras adquire uma determinada lista de produtos. A identificação permitia prever o estágio da gravidez e realizar a sugestão de produtos específicos. Como estratégia de marketing utilizavam essa informação para cativar clientes e oferecer descontos enviando cartas à residência parabenizando e informando que teriam descontos personalizados na loja.

A grande questão se deu que por meio dessa prática, de envio de cartas com base na análise de dados, um pai descobriu a gravidez da filha menor de idade. Gerando, daquele modo, um enorme desconforto familiar e evidenciando, portanto, o poder preditivo da análise de dados e a forte relação dos dados pessoais e a privacidade do indivíduo. Vale mencionar que a empresa não conhecia, de fato, a pessoa grávida e nem sabia de condição de saúde, mas a base de dados captados do usuário e a análises de padrões de pesquisas e comportamentos sugerem para a empresa as potências mães.¹⁰

No Brasil podemos mencionar a CPI da espionagem em 2014 que comprovou a espionagem estrangeira no país. A comissão parlamentar de inquérito foi instaurada após uma série de denúncias de que agências de inteligência dos Estados Unidos estariam acessando informações pessoais, como e-mails, telefonemas e dados digitais, de autoridades e cidadãos

¹⁰ECONÔMICO, TERRAÇO. Big Data: Como a Target descobriu uma gravidez antes da família? 2019. 2020. Disponível em: <<https://www.oguiafinanceiro.com.br/textos/big-data-como-a-target-descobriu-uma-gravidez-antes-da-propria-familia/>> Acessado em: 15 de out. de 2022.

brasileiros. Ao final foi comprovado que de fato houve espionagem e que o Brasil está vulnerável no tocante a proteção de dados pessoais.¹¹

Neste ano, no país, já houveram casos grandes de vazamentos de dados. O Banco Central no Brasil informou que houve um vazamento de dados de 137.285 chaves pix pela empresa Abastece Aí, os dados que foram divulgados foram nome do usuário, CPF, agência do banco, número e tipo da conta. Em 2020, houve o vazamento de dados de 243 milhões de brasileiros cadastrados no Sistema Único de Saúde (SUS) por falhas do Ministério da Saúde.¹²

Nesse sentido, a proteção de nossa privacidade na esfera digital tornou-se uma grande preocupação da atualidade. É evidente que os dados revelam muito sobre a singularidade e características dos indivíduos, e, na mesma medida, colocam em risco seus titulares caso não haja segurança em sua utilização. Ressalta-se, então, o desafio dos legisladores em proteger efetivamente os cidadãos e seus dados, visto que a privacidade é um direito fundamental em nosso ordenamento.

2.4 Conceito de privacidade na era digital.

Será abordado neste subtópico uma breve evolução do conceito de privacidade no ordenamento brasileiro para, então, compreendermos como a revolução informacional e os novos paradigmas remodelaram o conceito de privacidade.

Os direitos fundamentais visam à proteção da dignidade da pessoa humana, ou seja, pretendem garantir o mínimo necessário para que o indivíduo seja capaz de viver e se desenvolver, o mínimo necessário é um reflexo da sociedade e com isso varia conforme suas mudanças. Em virtude da relevância de tais direitos a Carta Magna Brasileira positivou ao longo de seu texto determinados direitos os quais o Estado deve garantir e assegurar. O professor Gilmar Mendes preceitua:

¹¹MENDES, Pricilla. Relatório final da CPI da Espionagem aponta que o Brasil está vulnerável. G1. Seção: Política. 09 abr 2014. Disponível em Acessado em 15 de out. de 2022.

¹²ARAGÃO, Alexandre. 5 grandes vazamentos de dados no Brasil — e suas consequências, São Paulo, 28 de janeiro de 2022. Proteção de dados. Disponível em: <

O catálogo dos direitos fundamentais vem-se avolumando, conforme as exigências específicas de cada momento histórico. (...) Os direitos e garantias fundamentais, em sentido material, são, pois, pretensões que, em cada momento histórico, se descobrem a partir da perspectiva do valor da dignidade humana.¹³

A privacidade tornou-se um direito fundamental, previsto no artigo 5º, incisos X, XI, com a Constituição de 1988, surgindo, então, um dever do Estado de proteger a vida íntima dos seus tutelados.

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

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

XI – a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial;

XII – é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;¹⁴

De fato, no Brasil, a Constituição do Império de 1824 já abordava o direito à privacidade no tocante a carta e a casa, elencada como “Garantias dos Direitos Civis” em seu artigo 179. Entretanto, o que se pretendia proteger era a inviolabilidade do domicílio e das correspondências e não a privacidade em si como entendemos hoje de esfera particular.

Art. 179. A inviolabilidade dos Direitos Civis, e Politicos dos Cidadãos Brasileiros, que tem por base a liberdade, a segurança individual, e a propriedade, é garantida pela Constituição do Imperio, pela maneira seguinte. [...] VII. Todo o Cidadão tem em sua casa um asylo inviolavel. De noite não se poderá entrar nella, senão por seu consentimento, ou para o defender de incendio, ou inundaçãõ; e de dia só será franqueada a sua entrada nos casos, e pela maneira, que a Lei determinar. [...] XXVII. O

¹³MENDES, GILMAR FERREIRA; BRANCO, Paulo Gustavo Gonet. Curso de Direito Constitucional-Séire IDP-16ª Edição 2021. Saraiva Educação SA, 2021, pg. 154.

¹⁴Constituição (1988). Constituição da República Federal do Brasil. Brasília, DF: Senado Federal, 1988.

Segredo das Cartas é inviolável. A Administração do Correio fica rigorosamente responsável por qualquer infração deste Artigo.¹⁵

Historicamente, deve-se mencionar que o direito à privacidade como se entende hoje foi fortemente influenciado por um emblemático artigo chamado “The Right to Privacy” publicado na Harvard Law Review em 1890 por Samuel Warren e Louis Brandeis, dois advogados. O artigo é considerado como a primeira grande manifestação a defender o direito à privacidade não apenas na esfera física, de inviolabilidade de algo material como, por exemplo, uma correspondência mas, na ideia de ser o direito de ser deixado à sós.

O artigo foi escrito tendo como a principal crítica o aborrecimento sofrido pelos indivíduos com as invasões de privacidade social, o caso concreto que destacaram foi a invasão de um jornalista em um casamento. Os autores criticavam as colunas jornalísticas que abordavam assuntos íntimos nos meios de comunicação sem a autorização dos seus titulares, que com os avanços tecnológicos, como a internet e câmeras fotográficas, ficavam cada vez mais assíduas. Remodelando, tendo em vista os novos paradigmas da sociedade, o conceito de privacidade.

Diante de tal cenário, a Declaração Universal dos Direitos Humanos em 1948 consagrou o direito à privacidade como um direito fundamental, demonstrando assim uma necessidade de uma tutela maior aos dados pessoais, o artigo 12º menciona:

Ninguém sofrerá intromissões arbitrárias ou ilegais na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Toda a pessoa tem direitos à proteção da lei contra tais intromissões ou ataques.¹⁶

O conceito e abrangência de privacidade se ressignificam e se moldam de acordo com as necessidades da sociedade. A cultura da informação e os avanços tecnológicos resultam em um novo paradigma de privacidade, a ideia de privacidade não está mais ligada somente à noção de violação de propriedade como nas primeiras constituições do país, hoje o conceito é mais amplo.

¹⁵ BRASIL. Constituição (1824). Lex: Constituição Política do Império do Brazil, de 25 de março de 1824. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao24.htm. Acesso em: 15 de out. de 2022.

¹⁶Declaração Universal dos Direitos Humanos. 1948. Disponível em http://www.planalto.gov.br/ccivil_03/decreto/1930-1949/d19841.htm . Acesso em 27/10/2022.

Doneda preceitua:

A privacidade, nas últimas décadas, passou a se relacionar com uma série de interesses e valores, o que modificou substancialmente o seu perfil. E talvez a mais importante dessas mudanças tenha sido essa apontada por Stefano Rodotà, de que o direito à privacidade não mais se estrutura em torno do eixo “pessoa-informação-segreto”, no paradigma da zero-relationship, mas sim no eixo “pessoa-informação-circulação-controle”. Nessa mudança, a proteção da privacidade identifica-se e acompanha a consolidação da própria teoria dos direitos da personalidade e, em seus mais recentes desenvolvimentos, afasta a leitura segundo a qual sua utilização em nome de um individualismo exacerbado alimentou o medo de que eles se tornassem o “direito dos egoísmos privados”. Algo paradoxalmente, a proteção da privacidade na sociedade da informação, a partir da proteção de dados pessoais, avança sobre terrenos outrora improponíveis e nos induz a pensá-la como um elemento que, mais do que garantir o isolamento ou a tranquilidade, serve a proporcionar ao indivíduo os meios necessários à construção e consolidação de uma esfera privada própria, dentro de um paradigma de vida em relação e sob o signo da solidariedade – isto é, de forma que a tutela da privacidade cumpra um papel positivo para o potencial de comunicação e relacionamentos do indivíduo. Tal função interessa à personalidade como um todo e ganha importância ainda maior quando fatores como a vida em relação e as escolhas pessoais entram em jogo – como ocorre nas relações privadas, na utilização das novas tecnologias, no caso da política e, paradoxalmente, na própria vida pública.¹⁷

Tendo em vista, a noção da privacidade de ser o momento de privacidade essencial para o desenvolvimento psíquico do indivíduo, é na privacidade que podemos ser quem somos sem precisar mostrar-se a alguém, é em suma o direito de não tornar pública alguma informação que diga a respeito a si, caso assim deseje o titular.

Nesse sentido Doneda leciona:

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.¹⁸

Logo, o direito à privacidade garante aos indivíduos a segurança de que sua esfera íntima e particular será resguardada contra intromissões externas. Além disso, garante que a

¹⁷DONEDA, Danilo. Da privacidade à proteção de dados pessoais. 2006 2. ed. São Paulo: Thomson Reuters Brasil, 2020, pg. 39.

¹⁸DONEDA, Danilo. A tutela da privacidade no código civil de 2002. p. 1. Disponível em: . Acesso em 09 out 2014. 23 COSTA JÚNIOR, Paulo José da. O direito de estar só: tutela penal da intimidade. São Paulo: Revista dos Tribunais, 1970. p. 24.

exposição de suas informações, dados, imagem e momentos não acontecerão sem a devida permissão do titular. Conforme ensina Gilmar Mendes:

O direito à privacidade teria por objeto os comportamentos e acontecimentos atinentes aos relacionamentos pessoais em geral, às relações comerciais e profissionais que o indivíduo não deseja que se espalhem ao conhecimento público. O objeto do direito à intimidade seriam as conversações e os episódios ainda mais íntimos, envolvendo relações familiares e amizades mais próximas.¹⁹

Nesse sentido, pode-se afirmar, que o conceito de privacidade mudou ao longo do tempo visto que novos padrões comportamentais surgiram na sociedade. Antigamente, a noção de privacidade relacionava-se com a inviolabilidade da casa e das correspondências. Atualmente o conceito é mais amplo. Podemos afirmar hoje que a privacidade estabelece limites ao acesso de terceiros às informações referentes aos indivíduos, como aos corpos, locais, coisas, comunicações e informações. Desse modo, a legislação de proteção de dados surge, justamente, para garantir essa proteção à privacidade do indivíduo.

¹⁹ MENDES, GILMAR FERREIRA; BRANCO, Paulo Gustavo Gonet. Curso de Direito Constitucional-Séire IDP-16ª Edição 2021. Saraiva Educação SA, 2021, pg. 315.

3. A NECESSIDADE DE UMA LEGISLAÇÃO VOLTADA À PROTEÇÃO DE DADOS.

Tendo em vista o panorama da importância e valor dos dados pessoais no capítulo anterior e o papel fundamental do direito em acompanhar os desdobramentos sociais e dar segurança aos indivíduos e a sociedade, o ordenamento jurídico depara-se com a necessidade de criar normas sobre a temática.

3.1 Classificação das gerações das leis de proteção de dados.

Inicialmente, iremos destacar a classificação proposta pelo doutrinador Viktor Mayer-Schönberger²⁰ das gerações de produções de leis de proteção de dados. A classificação proposta tem como escopo as produções legislativas de todo o mundo e analisar a sua evolução. Apesar do trabalho ter como objeto a legislação brasileira, deve destacar que ela sofreu influência de legislações estrangeiras, como veremos mais detalhadamente nos tópicos adiante. Portanto, a classificação é importante para compreender a evolução da temática no mundo e, conseqüentemente, no Brasil.

Segundo o doutrinador, pode-se dividir em quatro gerações as produções de leis referentes à proteção de dados pessoais. Num momento inicial, a legislação pretendia regular os bancos de dados, sendo assim, as leis versavam, basicamente, sobre concessão de autorização para a criação de bancos de dados e no controle do Estado no uso dessas informações, visto que na época o Estado era o principal destinatário dessa norma. Extrai-se que o objetivo da tutela era voltado à expansão da tecnologia e no processamento de dados e não na de privacidade do cidadão.

Nesse mesmo sentido ensina BONI:

A primeira geração de leis de proteção de dados pessoais decorre, assim, da preocupação com o processamento massivo dos dados pessoais dos cidadãos na conjuntura da formação do Estado Moderno. Naquela época, a saída regulatória foi focar na própria tecnologia que deveria ser domesticada e orientada pelos valores democráticos. Temia-se a emergência da figura orwelliana do Grande Irmão, que poderia sufocar a liberdade do cidadão com

²⁰ MAYER-SCHÖNBERGER, Viktor. Generational development of data protection in Europe. In: AGRE, Philip E.; ROTENBERG, Marc. Technology and privacy: the new landscape. Cambridge: The Mit Press, 2001.

uma vigilância ostensiva. Optou-se, então, por controlar a criação desses bancos de dados por meio da concessão de autorizações para o seu funcionamento.

Em suma, o que marca a primeira geração de proteção dos dados pessoais é o seu foco na esfera governamental, bem como na premissa em se estabelecer normas rígidas que domassem o uso da tecnologia. Todavia, o processamento de dados transcendeu a esfera governamental, o que aumentou a quantidade de atores e, simetricamente, o número de bancos de dados a serem regulados-autorizados. Esse novo cenário exigiu uma nova estrutura normativa.²¹

Como exemplo de lei de primeira geração, podemos citar a lei de Hess, criada nos anos 70. Segundo Laura Schertel:

Em 1970, no Estado Alemão de Hesse, surge a primeira lei mundial de proteção aos dados pessoais, em uma década em que começam a surgir inúmeras legislações de proteção, com o reconhecimento de que os “dados pessoais constituem uma projeção da personalidade do indivíduo e que, portanto, merecem uma tutela forte.”²²

A segunda geração, foi gerada pela necessidade de uma nova ótica sobre a temática, visto que as leis de proteção de dados de primeira geração logo se tornaram ultrapassadas, em virtude da expansão de bancos de processamento de dados que tornou inviável o controle legal com base em um regime de autorização rígido e detalhado. Essa nova geração foi marcada pela preocupação da privacidade de acesso de um terceiro às informações do indivíduo e não mais apenas focada no fenômeno computacional em si como na primeira. Desse modo tratou de oferecer novas formas de controle para que o próprio indivíduo tivesse meios de tutelar seus direitos individuais. Podemos citar como exemplo a legislação europeia chamada Data Protection Convention, conforme o professor Rafael Maciel:

Em 1981 o Conselho da Europa aprovou o Data Protection Convention (Treaty 108), tornando-se o primeiro instrumento legal internacional que visa proteger o indivíduo contra abusos na coleta e no processamento de dados pessoais, regulando o fluxo transfronteiriço.²³

A terceira geração de normas de proteção de dados trouxe o conceito de autodeterminação informativa, ou seja, o indivíduo poderá decidir se deseja ou não

²¹BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, pg. 53.

²²SCHERTEL MENDES, Laura. O Direito Fundamental à proteção de dados pessoais. Revista de Direito do Consumidor, vol. 79/2011. Editora RT.

²³MACIEL, Rafael Fernandes. Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/18). RM Digital Education. 1ª Edição. Goiânia–GO, 2019, pg.8.

compartilhar os seus dados, tal prática visa a garantir uma proteção à privacidade dos dados a partir da necessidade de prévio consentimento do titular para a coleta e tratamento. Podemos citar como exemplo a decisão da Corte Constitucional da Alemanha que admitiu o direito à autodeterminação informacional ao julgar uma norma inconstitucional, criando um marco para a terceira geração, como aponta Laura Schertel:

A sentença da Corte Constitucional, na sua formulação de um direito à autodeterminação da informação, criou o marco para a teoria da proteção de dados pessoais e para as subseqüentes normas nacionais e europeias sobre o tema, ao reconhecer um direito subjetivo fundamental e alçar o indivíduo a protagonista no processo de tratamento de seus dados. Dessa forma, o grande mérito do julgamento reside na consolidação da ideia de que a proteção de dados pessoais baseia-se em um direito subjetivo fundamental, que deve ser concretizado pelo legislador e que não pode ter o seu núcleo fundamental violado. Isso significa uma limitação ao poder legislativo, que passa a estar vinculado à configuração de um direito à autodeterminação da informação.²⁴

Entretanto, apesar dos dispositivos legais já criados era nítido que havia uma disparidade entre a relação entre o titular dos dados e a entidade de coleta, pois de um lado está, geralmente, uma grande empresa que possui experiência e domínio sobre a coleta de dados e de outro lado um indivíduo que, geralmente, não possui todo esse conhecimento.

Nesse sentido, surge a quarta geração de normas de proteção de dados, geração a qual está inserida a Lei Geral de Proteção de Dados. Essa geração visa atenuar a disparidade na relação entre esses indivíduos, o titular e o coletor dos dados, aumentando a proteção de direitos fundamentais através de normas mais específicas e categóricas e determinando o nível de proteção a ser utilizado de acordo com a sensibilidade do dado pessoal que se pretende coletar.

3.2 GDPR e a influência na criação da LGPD.

No cenário internacional devemos mencionar o Regulamento Geral sobre a Proteção de Dados, em inglês General Data Protection Regulation, mais conhecido como GDPR. Iremos, então, destacar alguns pontos para elucidar a relevância dessa legislação para o Brasil.

²⁴SCHERTEL MENDES, Laura. O Direito Fundamental à proteção de dados pessoais. Revista de Direito do Consumidor, vol. 79/2011. Editora RT.

Trata-se de um regulamento europeu sobre proteção de dados pessoais que entrou em vigor em 25 de maio de 2018. A relevância da menção a este dispositivo se dá pelo fato de que o impacto de sua criação não se restringiu ao seu continente, pois atraiu a atenção de diversos países para a importância de uma cultura de proteção de dados. O GDPR serviu como inspiração para a elaboração da Lei Geral de Proteção de Dados brasileira.

Em vista disso, cabe destacar alguns pontos sobre o Regulamento Geral sobre a Proteção de Dados Europeu. A legislação europeia é bem desenvolvida em matéria de proteção de dados, diversos países nos anos 80 criaram normas sobre a temática dos dados, visando proteger a dignidade humana.

No entanto, o emblemático regulamento europeu apesar de ter sido aprovado no ano de 2016, foi em 2011 que o órgão Supervisor de Proteção de Dados Europeu emitiu comunicado indicando a necessidade de edição de uma norma mais abrangente e destinada a padronizar a proteção de dados pessoais na região, visto que as normas existentes não acompanharam as inovações tecnológicas e, assim não tutelavam de maneira eficiente os cidadãos. Somente após intensos debates a lei entrou em vigor nos anos seguintes.

Patricia Peck leciona:

Destaca-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. Foi nisso que a nova legislação inovou, ou seja, padronizou, ou melhor, normalizou, quase como uma norma ISO, o que seriam os atributos qualitativos da proteção dos dados pessoais sem a presença dos quais haveria penalidades. Os efeitos do GDPR são principalmente econômicos, sociais e políticos. Trata-se de apenas uma das muitas regulamentações que vão surgir nessa linha, em que se busca trazer mecanismos de controle para equilibrar as relações em um cenário de negócios digitais sem fronteiras.²⁵

²⁵ PINHEIRO, Patricia Peck. Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD), 2. ed. São Paulo: Saraiva Educação, 2020, p.18.

O regulamento europeu, de um modo geral, traz em seu conteúdo regras e diretrizes mais abrangentes sobre a temática dos dados em comparação com as normas produzidas anteriormente. Ela reforça a proteção do titular dos dados pessoais, pois assegura um maior controle sobre ele trazendo a necessidade do consentimento para a captação e diretrizes que devem ser observadas pelas pessoas físicas ou jurídicas detentoras desses dados. Além de impor novas sanções a serem impostas pelos órgãos nacionais as instituições que operam dados pessoais em caso de desconformidade com a lei.

O Regulamento Geral sobre a Proteção de Dados criou uma influência internacional para que outros países, também, legislassem sobre o assunto. Somado à isso, apesar do regulamento ser aplicado em território europeu a sua abrangência acabou por abarcar outros lugares visto que devem se adequar qualquer empresas ou cidadãos que, mesmo não estando na Europa, ofereçam serviços ao mercado europeu ou monitorem o comportamento de indivíduos que se encontrem na União Europeia, independentemente de sua nacionalidade. Logos as empresas que não se adequassem poderiam sofrer um bloqueio econômico.²⁶

Por Patrícia Peck:

A liderança do debate sobre o tema surgiu na União Europeia (UE), em especial com o partido The Greens, e se consolidou na promulgação do Regulamento Geral de Proteção de Dados Pessoais Europeu n. 679, aprovado em 27 de abril de 2016 (GDPR), com o objetivo de abordar a proteção das pessoas físicas no que diz respeito ao tratamento de dados pessoais e livre circulação desses dados, conhecido pela expressão “free data flow”. O Regulamento trouxe a previsão de dois anos de prazo de adequação, até 25 de maio de 2018, quando se iniciou a aplicação das penalidades. Este, por sua vez, ocasionou um “efeito dominó”, visto que passou a exigir que os demais países e as empresas que buscassem manter relações comerciais com a UE também deveriam ter uma legislação de mesmo nível que o GDPR. Isso porque o Estado que não possuísse lei de mesmo nível passaria a poder sofrer algum tipo de barreira econômica ou dificuldade de fazer negócios com os países da UE. Considerando o contexto econômico atual, esse é um luxo que a maioria das nações, especialmente as da América Latina, não poderia se dar.²⁷

²⁶ LEMOS, Ronaldo. GDPR: a nova legislação de proteção de dados pessoais da Europa. Jornal Jota. 25 de maio de 2018. Dados Pessoais. Disponível em <<https://www.jota.info/opiniao-e-analise/artigos/gdpr-dados-pessoais-europa-25052018>>

²⁷ PINHEIRO, Patricia Peck. Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD), 2. ed. São Paulo: Saraiva Educação, 2020, p.11.

3.3 Legislações de dados anteriores a LGPD.

Essa seção tem como objetivo mencionar dispositivos legais anteriores à criação da Lei Geral de Proteção de Dados que versavam de alguma forma sobre a tutela dos dados pessoais, sem a pretensão de exaurir todos os dispositivos. Assim, destacaremos os principais dispositivos e, adiante, falaremos sobre a criação da LGPD.

Primeiramente, devemos mencionar que mesmo antes da criação de uma lei específica para a proteção de dados o Estado Brasileiro já possuía algumas leis esparsas que versavam sobre a temática, como o Código de Defesa do Consumidor (Lei no 8.078/90), Marco Civil da Internet (Lei nº 12.965), o Decreto sobre Comércio Eletrônico (Decreto nº 7.962/2013), por exemplo. Observa-se que a discussão sobre proteção de dados pessoais é antiga, porém somente em 2018 que o legislador brasileiro criou uma norma geral.

Apesar das leis mencionadas abordarem de algum modo o tema de proteção de dados em seu texto, a tutela que prestavam era sobre um ponto da extensa matéria de dados e processamento, não traziam diretrizes, não estabeleciam padrões de comportamento e nem proteções gerais. Nesse contexto, observava-se uma necessidade de uma lei específica.

Nas palavras de Peck:

Destaca-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 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. Foi nisso que a nova legislação inovou, ou seja, padronizou, ou melhor, normalizou, quase como uma norma ISO, o que seriam os atributos qualitativos da proteção dos dados pessoais sem a presença dos quais haveria penalidades.²⁸

²⁸PINHEIRO, Patricia Peck. Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD), 2. ed. São Paulo: Saraiva Educação, 2020, p.12.

Sendo assim, diante do cenário internacional e a necessidade do Estado de tutelar objetivamente as relações que versassem sobre dados pessoais, o legislador brasileiro criou a LGPD. Nesse sentido, busca-se mencionar adiante uma análise dos principais pontos dessa legislação, e compreender suas inovações.

4. PRINCIPAIS CARACTERÍSTICAS DA LGPD.

Tendo em vista a importância dos dados diante desse novo panorama, a sociedade de economia digital, iremos neste capítulo abordar a da Lei Geral de Proteção de Dados, alguns pontos importantes de sua criação, objetivos e conceitos.

4.1 Introdução a LGPD - Lei 13.709/2018.

A Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018, é uma legislação brasileira que possui o objetivo de disciplinar e garantir segurança ao tratamento de dados pessoais no país, estabelecendo diretrizes e princípios norteadores de maneira unificada, o que não era observado na legislação brasileira antes de sua criação. Além disso, a lei criou a Autoridade Nacional de Proteção de Dados (ANPD), órgão federal responsável por fiscalizar a implementação e aplicação da LGPD.

Segundo Milena Donato:

No Brasil, muito embora já houvesse disciplina sobre a proteção de dados, conforme tratado em tópico anterior, sua setorização e pulverização em leis e decretos esparsos, por certo, obstaculiza a visualização de um sistema. A edição da Lei 15.907/2018, significa, nesse contexto, uma orientação para organização formal desse sistema, a partir da cristalização e reprodução de muitos desses dispositivos esparsos, inclusive com status principiológico em alguns casos.²⁹

Cabe mencionar que a LGPD foi fortemente influenciada pelo Regulamento Geral de Proteção de Dados (GDPR), legislação europeia que versa sobre privacidade e segurança dos dados pessoais dos indivíduos que se encontram em seu território. O regulamento serviu como catalisador para a criação de uma legislação que regula a proteção de dados de forma unificada, visto que a ausência de lei poderia interferir no comércio entre os países, conforme já aprofundado no capítulo anterior.

Nesse viés preceitua o doutrinador Rafael Maciel:

²⁹ TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. São Paulo: Thomson Reuters Brasil, 2019. Pg. 25.

Em 2016, o General Data Protection Regulation (GDPR) foi aprovado e em 2018 ele entrou em vigor. Com sua entrada em vigor, em 25 de maio de 2018, os legisladores brasileiros viram-se pressionados a agilizar a votação de um projeto de lei de dados pessoais, caso contrário as empresas brasileiras teriam enorme dificuldade em realizar negócios com europeus, porquanto o país seria considerado não adequado para tratar dados de cidadãos que estiverem localizados na Europa.³⁰

A lei brasileira desde a sua criação já passou por algumas modificações. A estrutura do corpo do texto da lei ao todo possui 65 artigos divididos entre os seus 10 capítulos aplicáveis a qualquer operação de tratamento de dados pessoais realizada tanto por pessoa natural ou pessoa jurídica de direito público ou privado, independente do meio utilizado, físico ou digital, e do país da sede onde dos dados estejam localizados se: (i) a operação de tratamento for realizada no Brasil, (ii) a atividade do tratamento tiver como finalidade a oferta ou oferecimento tanto de bens quanto serviço no país, (iii) tratamento for de indivíduos localizados no território nacional ou (iv) os dados forem coletados no Brasil, conforme o artigo 1º e 3º da lei:

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.

Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

I - a operação de tratamento seja realizada no território nacional;

II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou

III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.³¹

Sobre a vigência da Lei no 13.709/2018 é importante situar que a mesma foi promulgada em 14 de agosto de 2018 e possuía inicialmente um prazo de 18 meses para a

³⁰ MACIEL, Rafael Fernandes. Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais (Lei n 13.709/18). RM Digital Education. 1a Edição. Goiânia – GO. 2019, pg. 15.

³¹Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2020]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/114020.htm. Acessado em: 15 de out. de 2022.

entrada em vigor, visto que as empresas e pessoas necessitavam adequar-se à nova legislação. Entretanto, o prazo foi alvo de dilação e a lei somente passou a vigorar em agosto de 2020, essa modificação foi trazida pela Lei no 13.853/2019. Destaca-se que as sanções administrativas, sofreram uma dilação maior, entraram em vigor em agosto de 2021, em virtude da modificação trazida pela Lei 14.010/2020.

A discussão legislativa sobre proteção de dados como já vimos ao longo do trabalho não é algo recente, a preocupação em legislar sobre a temática é antiga, porém durante os últimos anos ela foi impulsionada devido ao cenário e contexto social da época, como já explicamos no capítulo anterior.

A Lei Geral de Proteção de Dados dialoga com a constituição na medida que objetiva a proteção de direitos constitucionais fundamentais como a privacidade, segurança, justiça e livre desenvolvimento da personalidade social.

4.2 Conceito e terminologias.

Já é sabido que a Lei nº 13.709/2018 dispõe sobre o tratamento de dados pessoais, nesse contexto para melhor compreendermos faz-se necessário adentrar a certos conceitos e pontuar breves explicações.

O dispositivo legal em questão trouxe em seu artigo 5º conceitos que merecem ser destacados:

Art. 5º Para os fins desta Lei, considera-se:

I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

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;

VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

IX - agentes de tratamento: o controlador e o operador;

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

XI - anonimização: 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;

XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

XIII - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

XV - transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

XVI - uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

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

XVIII - órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que

inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; e

XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.³²

Abordaremos, alguns conceitos do referido artigo adiante. Iniciaremos com o conceito de dado pessoal. De acordo com a legislação dado pessoal é qualquer informação que torne possível o titular do dado identificável ou identificado, como exemplo podemos citar nome, CPF, e-mail, carteiras de identidade, números de Internet Protocol entre outros.

Nota-se que os dados pessoais não necessariamente identificam o indivíduo, mas o tornam identificável, ou seja, sabe-se que o dado é referente a certo indivíduo por mais que não se consiga saber exatamente quem ele é, sabe-se características que podem em algum momento o tornar identificado. Nesse sentido, podemos classificar os dados pessoais em diretos, os que identificam diretamente uma pessoa, ou indiretos, os que permitem a identificação de uma pessoa.

É importante mencionar que os dados pessoais são somente dados de pessoas naturais, os dados de pessoas jurídicas ou dados que não tornem o indivíduo identificável ou identificado não será respaldado pela Lei Geral de Proteção de Dados, uma vez que não se enquadram na definição.

Segundo Rony Vainzof:

Portanto, assim como ocorre no GPDR, a LGPD não se preocupa com quaisquer dados ou informações corporativas em sua essência, sigilosas ou confidenciais, públicas ou privadas, como planejamentos estratégicos, balanços financeiros, sistemas em desenvolvimento, protótipos, fórmulas, outras inovações ou qualquer outro tipo de documento corporativo, os quais, se contiverem dados pessoais, somente estes estarão protegidos pela Lei em estudo.³³

³²Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2020]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/114020.htm. Acessado em: 15 de out. de 2022.

³³ LGPD: Lei Geral de Proteção de Dados comentada [livro eletrônico]/coordenadores Viviane Nóbrega Maldonado e Renato Opice Blum. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

Em seguida, temos a definição legal de dado pessoal sensível, que são os dados relacionados à personalidade e às escolhas de uma pessoa. São por exemplo dados que revelem a origem racial, genética, orientação sexual, religiosa e política. Os dados sensíveis são informações mais íntimas e privadas dos titulares e por essa razão a lei separou hipóteses específicas para que seja possível o tratamento desses dados, as hipóteses estão elencadas no artigo 11º da LGPD.

Já o termo tratamento de dados é qualquer operação realizada com dados pessoais, como a coleta, armazenamento, processamento e distribuição. A definição de consentimento é a manifestação livre do titular de permitir ou não o tratamento dos dados.

Outra conceituação relevante é a figura do controlador, processador e encarregado. O controlador e o processador são agentes de tratamento de dados. O controlador é quem realiza a tomada de decisões, sendo, portanto, o responsável pela proteção dos dados. O processador realiza o tratamento dos dados, o processador. E, por fim, o encarregado é o responsável por realizar a comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados.

Compreender os conceitos é de extrema importância para delimitar a abrangência dos sujeitos e objetos da legislação, conforme Patrícia Peck:

A especificação dos termos utilizados no contexto dos dados pessoais é particularmente importante e visa resolver os problemas de conceituação e até mesmo categorização que as informações coletadas sofriam. A partir da LGPD, passa a ficar claro e apontável o que é ou não dado pessoal, assim como todos os processos, as técnicas ou os procedimentos relativos ao tratamento de dados.³⁴

4.3 Fundamentos e princípios da proteção de dados.

Abordaremos os fundamentos e princípios norteadores trazidos pelos artigos 2º e 6º, respectivamente, da LGPD que deverão ser observados na aplicação e interpretação dos dispositivos da lei.

³⁴PINHEIRO, Patricia Peck. Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD), 2. ed. São Paulo: Saraiva Educação, 2020, p.45

Sobre a importância dos princípios legislativos Celso Antônio Bandeira de Mello
leciona:

Princípio - já averbamos alhures - é, por definição, mandamento nuclear de um sistema, verdadeiro alicerce dele, disposição fundamental que se irradia sobre diferentes normas compondo-lhes o espírito e servindo de critério para sua exata compreensão e inteligência, exatamente por definir a lógica e a racionalização do sistema normativo, no que lhe confere a tônica e lhe dá sentido harmônico. É o conhecimento dos princípios que preside a inteligência das diferentes partes componentes do todo unitário que há por nome sistema jurídico positivo [...]. Violar um princípio é muito mais grave que transgredir uma norma qualquer. A desatenção ao princípio implica ofensa não apenas a um específico mandamento obrigatório, mas a todo o sistema de comandos. É a mais grave forma de ilegalidade ou de inconstitucionalidade, conforme o escalão do princípio atingido, porque representa insurgência contra todo o sistema, subversão de seus valores fundamentais, contumélia irremissível a seu arcabouço lógico e corrosão de sua estrutura mestra. Isto porque, com ofendê-lo, abatem-se as vigas que os sustentam e alui-se toda a estrutura nelas esforçada.³⁵

O artigo 2º expressa os fundamentos da lei, são eles:

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

I - o respeito à privacidade;

II - a autodeterminação informativa;

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

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

V - o desenvolvimento econômico e tecnológico e a inovação;

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

VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.³⁶

Para Patrícia Peck o artigo acima evidencia a íntima relação da lei com a Constituição Federal Brasileira visto ter como fundamento legal a proteção de direitos fundamentais e evidencia, também, a relação de inspiração da lei com o Regulamento Geral

³⁵MELLO, Celso Antônio Bandeira de, Curso de Direito Administrativo. 12ª ed. – São Paulo : Malheiros, 2000, p. 747/748.

³⁶ Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2020]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/114020.htm. Acesso em: 15 de out. de 2022.

de Proteção de Dados Europeu, pois o mesmo é fundamentado em proteções similares, em suas palavras:

A proteção aos direitos fundamentais é bastante evidente no art. 2º da LGPD, que pode ser relacionado ao texto constitucional brasileiro no que concerne ao conteúdo, haja vista que a Constituição Federal Brasileira é pautada na proteção aos direitos fundamentais. Entre os artigos constitucionais destacáveis, pode-se citar: art. 3º, I e II; art. 4º, II; art. 5º, X e XII; art. 7º, XXVII; e art. 219.

Da mesma maneira, o GDPR aponta que o seu documento é pautado nos direitos fundamentais e visa proteger e garantir a privacidade, liberdade, segurança, justiça das pessoas, assim como promover o progresso econômico e social, além de garantir a segurança jurídica dos países: preâmbulo (1), (2), (13); art. 1º (2).³⁷

O artigo 6º versa sobre os fundamentos da lei:

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 integridade 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

³⁷PINHEIRO, Patricia Peck. Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD), 2. ed. São Paulo: Saraiva Educação, 2020, p.47.

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.³⁸

O princípio da finalidade garante ao titular dos dados que os dados coletados serão utilizados apenas para a finalidade legítima informada ao titular no momento anterior à captação. Assim, o titular possui um maior controle sobre a utilização de seus dados, pois o princípio garante que o agente de tratamento de dados apenas usará o dado para a finalidade mencionada no momento do acordo firmado antes da obtenção dos dados.

Diante de tal princípio, se uma empresa de saúde coleta dados de um indivíduo para realizar a análise de exames médicos com o consentimento do titular para essa atividade, a empresa não poderá realizar a análise de dados para outros fins a não ser o já estipulado. Sendo assim, a empresa não poderá utilizar os dados para produzir uma propaganda e marketing direcionado a esse cliente, se caso assim queira deverá requerer um novo consentimento do titular.

Já o princípio da adequação e necessidade complementa o princípio da finalidade, visto que a adequação determina que deve haver a compatibilidade entre o tratamento e a finalidade mencionada. A necessidade, por sua vez, traz a limitação ao tratamento do dado apenas ao mínimo necessário para que possa ser realizada a sua finalidade.

Podemos mencionar a título de exemplificação que o princípio da adequação veda práticas como a de uma empresa do ramo de vestuário que ao realizar o cadastro de um cliente requeira informações que não se adequem ao seu ramo, como por exemplo requerer acesso a dados de saúde ou dados políticos.

³⁸Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2020]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/114020.htm. Acesso em: 15 de out. de 2022

Nos dizeres de Nóbrega e Blum³⁹:

Os três primeiros princípios dispostos na LGPD (finalidade, adequação e necessidade) são umbilicalmente conexos, formando, juntamente com a transparência, o cerne dessa norma jurídica, determinantes para o respeito da proteção dos direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, por meio da tutela dos dados pessoais (...).

O princípio da finalidade conta com grande relevância prática, pois, por meio dele, é garantido ao titular, mediante informação prévia, as fronteiras de

legalidade do tratamento de seus dados, delimitando os propósitos do tratamento, desde que lícitos, e de terceiros que poderão ou não ter acesso aos

dados. Visa mitigar o risco de uso secundário à revelia do titular.

Danilo Doneda considera o princípio da finalidade, provavelmente, como o que carrega de forma mais incisiva os traços característicos da matéria de proteção de dados pessoais, pois o motivo da coleta deve ser compatível com o objetivo final do tratamento dos dados. A sua utilização sempre estará vinculada ao motivo que fundamentou essa coleta, nascendo uma ligação entre a informação e a sua origem, vinculando-a ao fim de sua coleta, de modo que esta deva ser levada em consideração em qualquer tratamento posterior. Como o dado pessoal é expressão direta da personalidade do indivíduo, nunca perde seu elo com este, pois sua utilização pode refletir diretamente para o seu titular.

O princípio da necessidade assegura uma limitação no tratamento de dados, em razão de nortear o tratamento apenas ao mínimo necessário de dados e de tratamento para que se possa atingir a sua finalidade. Assim, o controlador dos dados deverá ponderar entre as coletas e atividades essenciais com o propósito do seu negócio.

Conforme preceitua Rony Vainzof⁴⁰.

No GDPR, o princípio da necessidade é denominado como minimização dos dados e limitação da conservação, de forma que os dados pessoais deverão ser adequados, pertinentes e limitados ao necessário para os propósitos do tratamento. Para isso, é necessário assegurar que o prazo de conservação seja limitado ao mínimo necessário, devendo o controlador fixa-los para descartar os dados ou rever periodicamente a sua necessidade e conformidade. A permissão para o tratamento ocorre quando a finalidade pretendida não puder ser atingida de forma razoável por outros meios.

³⁹NÓBREGA, Viviane Maldonado; BLUM, Renato Opice (org). LGPD : Lei Geral de Proteção de Dados comentada. São Paulo : Thomson Reuters Brasil, 2019.

⁴⁰NÓBREGA, Viviane Maldonado; BLUM, Renato Opice (org). LGPD : Lei Geral de Proteção de Dados comentada. São Paulo : Thomson Reuters Brasil, 2019, pg 114.

Assim, quaisquer políticas empresariais baseadas em “reter tudo” possivelmente serão consideradas ilícitas. Para atingir um certo grau de segurança jurídica, o controlador deverá realizar um teste de razoabilidade e adequação. Se a natureza e a quantidade de dados pessoais forem proporcionais em relação aos objetivos do tratamento, o procedimento possivelmente será lícito.

O princípio do livre acesso pretende assegurar a possibilidade de acesso dos titulares de dados ao tratamento, forma, integralidade e a duração sobre processo de manuseio dos seus dados de forma facilitada e gratuita. Facilitando, assim, um maior controle do titular frente à utilização de seus dados dentro da relação jurídica a qual está inserido.

Para Rafael Maciel⁴¹:

O titular dos dados tem o direito a realizar consulta facilitada e gratuita sobre a forma e a duração do tratamento e sobre a integralidade dos dados pessoais. Os dados devem ter qualidade, ou seja, serem claros, exatos, relevantes e atualizados de acordo com a necessidade e a finalidade do tratamento. Por fim, o dever de transparência implica ao agente o dever de prestar informações claras, precisas e facilmente acessíveis sobre a realização do tratamento, protegido os segredos comercial e industrial.

Vale mencionar que o princípio do livre acesso é reforçado no artigo 9º, que além de reforçar o conteúdo mencionado no princípio destaca algumas informações que deverão ser enquadradas no princípio como: finalidade específica do tratamento, identificação do controlador, informações de contato do controlador, informações acerca do uso compartilhado de dados pelo controlador e a finalidade e responsabilidades dos agentes que realizarão o tratamento.

O artigo 9º traz a seguinte redação:

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;

⁴¹ MACIEL, Rafael Fernandes. Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais (Lei no 13.709/18). Goiás: RM Digital Education, 2019, pg. 24.

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.

§ 1º Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.

§ 2º Na hipótese em que o consentimento é requerido, se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações.

§ 3º Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18 desta Lei.⁴²

No tocante ao princípio da qualidade dos dados endossa o dever do coletor de dados em manter a base de dados pessoais atualizada, verdadeira e alinhada com o propósito do seu negócio, visto que garante aos titulares a exatidão, clareza, relevância e atualização dos dados de acordo com a finalidade pretendida. Aspecto essencial para a proteção de direitos fundamentais.

O princípio da transparência garante aos titulares informações claras, precisas e facilmente acessíveis no que concerne à utilização dos dados pessoais, característica fundamental para que se possa exercer a tutela dos dados, uma vez que se não houvesse transparência o exercício da tutela jurisdicional iria ficar comprometido.

Nesse sentido, Rony Vainzof entende que esse princípio é essencial para que a lei consiga atingir os seus objetivos, visto que é uma legislação voltada a proteger a privacidade e o livre desenvolvimento da personalidade e para que se possa garantir a tutela dos dados é necessário o acesso a eles (2019, p. 115).

Leciona Rafael Maciel:

O titular dos dados tem o direito a realizar consulta facilitada e gratuita sobre a forma e a duração do tratamento e sobre a integralidade dos dados pessoais. Os dados devem ter qualidade, o seja, serem claros, exatos, relevantes e atualizados de acordo com necessidade e a finalidade do tratamento. Por fim, o dever de transparência implica ao agente o dever de

⁴²Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2020]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/114020.htm. Acesso em: 15 de out. de 2022.

prestar informações claras precisas e facilmente acessíveis sobre a realização do tratamento, protegido os segredos comercial e industrial.

Proteção de dados pessoais não é apenas um assunto para a área de tecnologia da informação. Estabelecidas como princípios, a segurança e a prevenção não estão limitadas às medidas técnicas, mas também a medidas administrativas aptas a proteger incidentes, considerados desde o acesso não autorizado até a situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. A prevenção passa por uma implementação da cultura em um programa de governança em privacidade que, a partir da consciência de todos atores sobre o tema, minimiza riscos de incidentes. (MACIEL, Rafael Fernandes, 2019, p.24)⁴³

O princípio da segurança relaciona-se com a adoção de tecnologias e soluções para garantir a proteção dos dados em caso de invasões. Sinaliza a necessidade de utilização de medidas técnicas e administrativas capazes de proteger os dados contra acessos indevidos. Além disso, esse princípio visa proteger, também, a ocorrência de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão de dados pessoais. Tal como o princípio da prevenção determina que deve haver a adoção de medidas para prevenir a ocorrência de danos no manuseio de dados pessoais.

Nóbrega e Blum preceituam:

Indubitavelmente, a violação de dados pessoais (personal data breach) é uma das situações de elevada criticidade no tratamento de dados pessoais, pois colocam em risco ou elevado risco os direitos dos titulares, de forma permanente. São eventos caracterizados por acessos não autorizados e ocorrências acidentais ou propositas de destruição, perda, alteração, comunicação ou difusão de dados pessoais.

Mais do que a própria exposição indevida dos dados pessoais, eventos como os citados culminam também na provável degradação da reputação do controlador e do operador, perante os quais os dados foram confiados e, de alguma forma, falharam em seu dever de proteção. Nessas ocasiões, os agentes também ficam expostos, com maior evidência, às possíveis sanções administrativas 472 e responsabilizações civis 473 . Ou seja, os efeitos são contundentes e prejudiciais a todos, titulares e agentes do tratamento.

Diante de todas essas circunstâncias, a segurança dos dados pessoais apresenta-se na LGPD, de forma certa, como princípio, dispondo que os agentes de tratamento devem utilizar medidas técnicas e administrativas aptas a proteger os dados pessoais de eventuais violações, que, como visto, não envolvem somente eventos dolosos, mas também acidentais.(NÓBREGA, Viviane Maldonado; BLUM, Renato Opice, 2020, p.117).

O princípio da não discriminação determina que não é possível realizar o tratamento de dados para fins discriminatórios, ilícitos ou abusivos. Como vimos, os dados podem ser considerados uma extensão do indivíduo esse princípio surge para inibir a segregação em

⁴³MACIEL, Rafael Fernandes. Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/18). RM Digital Education. 1ª Edição. Goiânia–GO, 2019, pg. 24.

razão dos dados pessoais coletados. Esse princípio reitera a ilegalidade da prática de geoprising, nome dado quando sites mudam o valor de serviços e produtos em razão da localidade em que se é acessado o site, e geoblocking, quando se impede a compra de serviços e produtos em razão da localidade do usuário.

Nos dizeres de Safiya Noble:

(...) é uma forma de discriminação de dados, que usa nossas identidades digitais e atividades para reforçar a desigualdade e a opressão. Muitas vezes, é realizada sem o nosso conhecimento, por meio de nossos engajamentos digitais, que se tornam parte de mecanismos de classificação algorítmicos, automatizados e artificialmente inteligentes que podem nos atingir ou nos excluir. Isto é uma dimensão fundamental de geração, sustentação ou aprofundamento da discriminação racial, étnica e de gênero, e está centralmente ligada à distribuição de bens e serviços na sociedade, como educação, moradia e outros direitos humanos e civis. O redlining está intimamente ligado às práticas comuns, que têm sido consistentemente definidas como ilegais no Estados Unidos, mas que são cada vez mais difíceis de serem avaliadas devido à sua nova faceta digital.⁴⁴

No Brasil, antes mesmo da criação da Lei Geral de Proteção de Dados essa prática já era considerada ilegal, esse princípio reitera esse entendimento. Podemos citar um caso emblemático de geoprising no Brasil. A empresa Decolar.com levou uma multa milionária de R\$2,5 milhões pela a prática de geoprising em 2016, a multa foi aplicada pela Secretaria Nacional do Consumidor. Foi apurado que a empresa privilegia clientes estrangeiros pois, ocultava ou deixava mais alto o valor de acomodações para os consumidores brasileiros.⁴⁵

Por último, temos o princípio da responsabilização e prestação de contas que surge para que o agente coletor dos dados demonstre o seus atos estão em conformidade com as normas de proteção de dados, conforme preceitua Rafael Maciel:

O agente de tratamentos deve não só cumprir com as normas, mas ter capacidade de demonstrar sua conformidade. É o chamado “accountability”, dever de prestar contas, não apenas à Autoridade Nacional de Proteção de Dados (ANPD), mas também aos clientes, público em geral, organizações profissionais e associações, empregados, parceiros comerciais, investidores,

⁴⁴ NOBLE, Safiya Umoja. Algorithms of oppression: how search engines reinforce racism. New York: NYU Press, 2018. Tradução Livre.

⁴⁵MAMONA, Karla. Decolar é multada em R\$ 2,5 mi por oferecer melhores preços a clientes que estão fora do Brasil. Exame, 2022. Disponível em: <<https://exame.com/invest/minhas-financas/decolar-e-multada-em-r-25-mi-por-oferecer-melhores-precos-a-clientes-que-estao-fora-do-brasil/>>

observatórios de proteção à privacidade e imprensa. (MACIEL, Rafael Fernandes, 2019, p.25)

Verifica-se, então, que a importância dos princípios e fundamentos tais se dá pelo fato de que servem como uma base ampla e formam a espinha dorsal da interpretação e aplicação dos dispositivos em matéria de proteção de dados. Logo, é importante destacá-los e compreendê-los para compreender o papel social que a lei pretende exercer.

4.4 O consentimento.

A legislação traz a definição de consentimento como a livre manifestação informada e inequívoca pela qual o titular dispõe sobre a concordância do compartilhamento de seus dados para uma finalidade determinada, conforme o artigo 5º, XII da lei.

Em seguida, o artigo 7º da lei traz as hipóteses e requisitos para que possa realizar o tratamento de dados. Retirando as hipóteses de uso compulsório, a lei prevê que o consentimento é um pressuposto legitimante para o tratamento de dados em seu inciso I.

Observa-se que o consentimento assegura ao indivíduo o poder de escolha e garante a autodeterminação informativa, uma vez que garante a proteção do titular dos dados frente a abusos no tocante ao tratamentos e coleta de dados, pois a coleta deve ser consentida livremente e deve haver o fornecimento das informações sobre a sua finalidade no momento anterior ao consentimento do titular.

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

I - mediante o fornecimento de consentimento pelo titular;

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

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

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

V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados.⁴⁶

O consentimento nos dizeres de Gustavo Tepedino e Chiara Teffé:

O consentimento representa instrumento de manifestação individual no campo dos direitos da personalidade e tem o papel de legitimar que terceiros utilizem, em alguma medida, os dados de seu titular. Ele compreende a liberdade de escolha, sendo meio para a construção e delimitação da esfera privada. Associa-se, portanto, à autodeterminação existencial e informacional do ser humano, mostrando-se imprescindível à proteção do indivíduo e à circulação de informações.

(...)Entende-se que, dentro da cultura das novas normas de proteção de dados, os usuários devem estar em condições de dar seu consentimento de forma livre e informada em relação ao recebimento de publicidade comportamental, independentemente de seu acesso à rede social. Busca-se que, dentro desses moldes, a própria sociedade exija dos setores público e privado boas práticas institucionais e o cumprimento integral da LGPD.⁴⁷

O artigo 8º da lei traz requisitos e formas sobre como o consentimento deve ser expresso. Ele deve ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade pelo titular. Além disso, outro ponto importante está no parágrafo 3º onde é expressado que é nulo o consentimento em que haja algum vício no consentimento, demonstrando assim a importância essencial do consentimento no tratamento de dados.

Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.

§ 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais.

§ 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei.

§ 3º É vedado o tratamento de dados pessoais mediante vício de consentimento.

§ 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.

⁴⁶Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2020]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/114020.htm. Acesso em: 15 de out. de 2022.

⁴⁷TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini. O consentimento na circulação de dados pessoais. Revista Brasileira de Direito Civil. Belo Horizonte, v. 25, p. 83-116, jul./set. 2020.

§ 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.

§ 6º Em caso de alteração de informação referida nos incisos I, II, III ou V do art. 9º desta Lei, o controlador deverá informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração.⁴⁸

Portanto, podemos afirmar que o consentimento é o instrumento pelo qual o indivíduo possibilita ou não o compartilhamento de dados dentro da ótica da proteção de dados. Sendo assim, é possível perceber que é por meio do consentimento que o titular exerce a sua autodeterminação informativa e privacidade, pois, com ela o indivíduo detém o poder de anuir compartilhar ou não. Sendo assim, podemos observar que o consentimento é o tema determinante para que se possa falar em segurança no tratamento de dados.

4.4 As alterações da Lei nº 13.853/2019.

Como já mencionamos anteriormente, a Lei nº 13.709/2018, Lei Geral de Proteção de Dados, sofreu algumas alterações relevantes. Nesse sentido, iremos destacar alguns pontos importantes neste subtópico.

Inicialmente devemos destacar a mudança no tocante a entrada em vigor. A Lei nº 13.709/2018, publicada em 14 de agosto de 2018, possuía a data para a entrada em vigor em fevereiro de 2020. A Lei nº 13.853/2019, antiga Medida Provisória nº 869/2018, alterou para agosto do mesmo ano. Esse aumento da *vacatio legis* é importante para as empresas pois, assim, há um prazo maior para o mercado se adequar.

Outro ponto importante é no tocante a criação da Autoridade Nacional de Proteção de Dados (ANPD) pela Lei nº 13.853/2019. A autoridade é um órgão da administração pública federal que tem o objetivo de promover a proteção e eficácia da aplicação da LGPD, fiscalizando e aplicando sanções. Entretanto, no tocante às sanções administrativas, houve edição da Lei 14.010/2020, antigo PL 1179/2020, que adiou a entrada em vigor das sanções administrativas para agosto de 2021.

⁴⁸ Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2020]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/114020.htm. Acesso em: 15 de out. de 2022

Além disso, a Lei nº 13.853/2019 dispensou a obrigatoriedade de revisão humana de decisões automatizadas, antes o titular dos dados tinha o direito a solicitar a uma pessoa natural a revisão de decisões tomadas, a lei dispensou a obrigatoriedade da pessoa natural, retirando o caráter humanizado. De fato, a lei 13.853/2019 trouxe outras modificações, porém o que se pretende no presente trabalho é abordar as principais mudanças que se relacionam com a sociedade tecnológica e a necessidade uma lei que vise garantir a proteção de dados.

CONCLUSÃO

O presente trabalho teve como objetivo analisar os novos comportamentos sociais e avanços tecnológicos que geraram a necessidade de criação de uma lei geral de proteção de dados no Brasil e, também, realizar uma breve análise dos principais aspectos da Lei Geral de Proteção de Dados e o seu papel social.

Podemos observar, durante este trabalho, como as inovações tecnológicas e os novos modelos de comportamentos, bem como a globalização trouxeram a necessidade de criação de uma legislação que garantisse a proteção da privacidade do cidadão na era dos dados e da internet. Foi possível evidenciar como o conceito de privacidade evoluiu com a sociedade, se tornando mais amplo.

Constatou-se que os dados pessoais possuem, atualmente, um enorme valor econômico, visto que através dele é possível identificar ou tornar identificar o indivíduo e, assim, mapear padrões e comportamentos. E, por isso, merece uma enorme atenção e cuidado em seu manuseio e utilização, o que a Lei Geral de Proteção de Dados visa assegurar.

Mencionou-se como a proteção de dados era abordada de maneira esparsa e incipiente na legislação brasileira momentos antes da criação da Lei nº 13.709/2018, evidenciando a importância e relevância da elaboração de uma norma atual e geral sobre o tema. Diante disso, verificou-se que a criação da Lei Geral de Proteção de Dados trouxe impactos positivos, tendo em vista que concentrou em uma única lei diretrizes, conceitos e princípios básicos sobre o tema, o que proporcionou mecanismos mais efetivos na manutenção de garantias fundamentais relacionadas à vida privada, com a devida transparência neste processo.

Observamos como a criação do Regulamento Geral de Proteção de Dados Europeu influenciou e acelerou a produção legislativa no Brasil. Constatou-se que houve uma evolução no tocante à proteção de dados pessoais no mundo, tendo em vista o panorama de classificação das gerações de produções legislativas vistos os avanços sociais e os novos dilemas criados.

Em relação à Lei Geral de Proteção de Dados foi realizada uma introdução abordando questões relacionadas a sua criação, vigência e explicação de conceitos fundamentais. Foi possível compreender que a referida lei foi elaborada pela necessidade do Estado em tutelar os indivíduos dentro do novo panorama social.

Vislumbra-se que a Lei nº 13.709/2018 é norteada por princípios e fundamentos que pretendem direcionar o manuseio de dados de uma maneira mais democrática entre os agentes da relação, consolidando o uso íntegro e protetivo dos dados pessoais. Pode-se perceber que o consentimento do indivíduo tornou-se o pressuposto essencial para o tratamento de dados, uma vez que a anuência do titular ao tratamento de dados é indispensável, ressalvada as hipóteses de uso compulsório.

Por fim, constata-se que a sociedade caminha para no sentido de requerer cada vez mais a transparência na utilização dos seus dados pessoais. Nesse sentido, é de suma importância que as empresas e pessoas que coletam os dados informem com clareza e aos seus titulares a finalidade da coleta dos dados, além de indicar como serão utilizados, para que então o titular escolha se deseja ou não autorizar a coleta. Nesse contexto, a Lei Geral de Proteção de Dados foi criada para regular essa temática tendo em vista a necessidade social de promover a tutela dos dados, surgindo como uma lei geral e unificada sobre a proteção dos dados, sendo esse então o seu papel social.

BIBLIOGRAFIA

BRASIL. **Constituição (1988). Constituição da República Federativa do Brasil.** Brasília, DF: Senado Federal: Centro Gráfico, 1988.

BRASIL. **Constituição (1824). Lex: Constituição Política do Império do Brazil,** de 25 de março de 1824. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao24.htm. Acesso em: 15 de out. de 2022.

BRASIL. Lei no 13.709, de 14 de agosto de 2018. **Lei geral de proteção de dados.** Diário Oficial da União, Brasília, 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm/. Acesso em: 20 out. 2022.

SCHWAB, Klaus. **A quarta revolução industrial.** Edipro, 2019.

PINHEIRO, Patricia Peck. **Proteção de Dados Pessoais: Comentários à Lei n. 13.709/2018-LGPD.** Saraiva Educação SA, 2020.

MCLUHAN, Marshall. **Os meios de comunicação: como extensões do homem.** Editora Cultrix, 1974.

BRASIL É O 2º EM RANKING DE PAÍSES QUE PASSAM MAIS TEMPO EM REDES SOCIAIS. Época Negócios. 06 de setembro de 2019. Tecnologia. Disponível em: <https://epocanegocios.globo.com/Tecnologia/noticia/2019/09/brasil-e-2-em-ranking-de-paises-que-passam-mais-tempo-em-redes-sociais.html>> Acessado em: 15 de out. de 2022.

EDUCA, I. B. G. E. **Uso de internet, televisão e celular no brasil.** IBGE Educa. Disponível em:< <https://educa.ibge.gov.br/jovens/materias-especiais/20787-uso-de-internet-televisaoe-celular-no-brasil.html>>. Acessado em 15 de out. de 2022, v. 18, 2019.

VISVAL, Cristian. **Dados são o novo petróleo! O que você tem feito com os seus dados?**. Revista Segurança Eletrônica, 2020. Disponível em: <<https://revistasegurancaeletronica.com.br/dados-sao-novo-petroleo/#:~:text=Petr%C3%B3leo%20deve%20ser%20transformado%20em,transformados%20para%20que%20tenham%20valor%E2%80%9D.>> Acesso em: 16 de out. de 2022.

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

FERRAZ, Marina . **Apple, Google e Amazon são as marcas mais valiosas de 2022**. 15 de jun. de 2022. Poder360. <https://www.poder360.com.br/economia/apple-google-e-amazon-sao-as-marcas-mais-valiosas-de-2022/>

ECONÔMICO, TERRAÇO. **Big Data: Como a Target descobriu uma gravidez antes da família?** 2019. 2020. Disponível em: <<https://www.oguiafinanceiro.com.br/textos/big-data-como-a-target-descobriu-uma-gravidez-antes-da-propria-familia/>> Acessado em: 15 de out. de 2022.

MENDES, Pricilla. **Relatório final da CPI da Espionagem aponta que o Brasil está vulnerável**. G1. Seção: Política. 09 abr 2014. Disponível em Acessado em 15 de out. de 2022.

ARAGÃO, Alexandre. **5 grandes vazamentos de dados no Brasil — e suas consequências**, São Paulo, 28 de janeiro de 2022. Proteção de dados. Disponível em: <[https://www.jota.info/tributos-e-empresas/mercado/vazamentos-de-dados-no-brasil-28012022#:~:text=3\)%20Vazamentos%20de%20dados%20no,seguran%C3%A7a%20do%20Minist%C3%A9rio%20da%20Sa%C3%BAde.>](https://www.jota.info/tributos-e-empresas/mercado/vazamentos-de-dados-no-brasil-28012022#:~:text=3)%20Vazamentos%20de%20dados%20no,seguran%C3%A7a%20do%20Minist%C3%A9rio%20da%20Sa%C3%BAde.>) Acessado em: 15 de out. de 2022.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 2006. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

MENDES, GILMAR FERREIRA; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional**. 16ª Edição 2021. Saraiva Educação SA, 2021, pg. 154.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019, p. 12/13.

SCHERTEL MENDES, Laura. **O Direito Fundamental à proteção de dados pessoais**. Revista de Direito do Consumidor, vol. 79/2011. Editora RT.

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

LEMOS, Ronaldo. **GDPR: a nova legislação de proteção de dados pessoais da Europa**. **Jornal Jota**. 25 de maio de 2018. Dados Pessoais. Disponível em <<https://www.jota.info/opiniao-e-analise/artigos/gdpr-dados-pessoais-europa-25052018>>

TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2019. Pg. 25.

NÓBREGA, Viviane Maldonado; BLUM, Renato Opice (org). **LGPD : Lei Geral de Proteção de Dados comentada**. São Paulo : Thomson Reuters Brasil, 2019.

MAMONA, Karla. **Decolar é multada em R\$ 2,5 mi por oferecer melhores preços a clientes que estão fora do Brasil**. Exame, 2022. Disponível em: <<https://exame.com/invest/minhas-financas/decolar-e-multada-em-r-25-mi-por-oferecer-melhores-precos-a-clientes-que-estao-fora-do-brasil/>>

NOBLE, Safiya Umoja. **Algorithms of oppression: how search engines reinforce racism**. New York: NYU Press, 2018. Tradução Livre.

TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini. **O consentimento na circulação de dados pessoais**. Revista Brasileira de Direito Civil. Belo Horizonte, v. 25, p. 83-116, jul./set. 2020.