ASSOCIAÇÃO VITORIENSE DE EDUCAÇÃO, CIÊNCIA E CULTURA - AVEC
CENTRO UNIVERSITÁRIO FACOL - UNIFACOL
COORDENAÇÃO DO CURSO DE DIREITO – BACHARELADO.

DIEGO VINÍCIUS DE BARROS ALMEIDA

AS VIOLAÇÕES DE DADOS PESSOAIS NAS RELAÇÕES DE CONSUMO PELA INTERNET

VITÓRIA DE SANTO ANTÃO – PE
2024

DIEGO VINÍCIUS DE BARROS ALMEIDA

AS VIOLAÇÕES DE DADOS PESSOAIS NAS RELAÇÕES DE CONSUMO PELA INTERNET

Trabalho de Conclusão de Curso apresentado ao Curso de Direito do Centro Universitário FACOL - UNIFACOL, como requisito parcial para a obtenção do título de Bacharel em Direito
Área de Concentração: Direito do Consumidor

Orientador: Msc. Oberdan Floriano de Lima

VITÓRIA DE SANTO ANTÃO – PE
2024

ASSOCIAÇÃO VITORIENSE DE EDUCAÇÃO CIÊNCIA E CULTURA - AVEC
CENTRO UNIVERSITÁRIO FACOL - UNIFACOL
COORDENAÇÃO DE TCC DO CURSO DE DIREITO
TRABALHO DE CONCLUSÃO DE CURSO

Nome do(a) Acadêmico(a): Diego Vinícius de Barros Almeida

Título do Trabalho de Conclusão de Curso: As violações de dados pessoais nas relações de consumo pela internet

Trabalho de Conclusão de Curso apresentada ao Curso de Direito do Centro Universitário FACOL - UNIFACOL, como requisito parcial para a obtenção do título de Bacharel em Direito.
Área de Concentração: Direito do Consumidor
Orientador(a): Msc. Oberdan Floriano de Lima

A Banca Examinadora composta pelos Professores abaixo, sob a Presidência do primeiro, submeteu o candidato à análise da Monografia em nível de Graduação e a julgou nos seguintes termos:

Professor:

Julgamento – Nota: Assinatura: _____

Professor:

Julgamento – Nota: Assinatura: _____

Professor:

Julgamento – Nota: Assinatura: _____

Nota Final: Situação do Acadêmico:

MENÇÃO GERAL:

_____

_____
Prof. Me. Severino Ramos da Silva
Coordenador de TCC do Curso de Direito

_____
Prof. Me. Maria Paula Latache Ribeiro de Vasconcelos / Prof. Me. Felipe da Costa Lima de Moura
Coordenação do Curso de Direito

Vitória de Santo Antão – PE, ___ de Junho de 2024.

Dedico este trabalho aos meus familiares, em especial a: Janaína Vieira de Barros Almeida e Sergio Ricardo dos Santos Almeida por acreditarem no meu empenho e por terem confiado em toda a minha trajetória ao longo dessa jornada acadêmica.

AGRADECIMENTOS

Agradeço a Deus por ter me iluminado e direcionado a fazer a escolha certa do curso. Á minha família, em especial: Janaína Vieira de Barros Almeida, Sergio Ricardo dos Santos Almeida e Valdemar Lino Chaves Neto; Agradeço aos mestres, professores e amigos que me ajudaram e contribuíram de forma relevante para que eu conseguisse chegar ao final deste curso tão desejado. Sem o apoio, não teria alcançado o meu objetivo de concluir está tão sonhada graduação acadêmica.

“Os efeitos da violação da privacidade ganham dimensões tais que acabam por aumentar a necessidade de se criar um eixo em torno do qual estruturar essa proteção.” (Danilo Doneda – 2017).

RESUMO

A sociedade da informação, como é conhecida a atual sociedade, ganhou este significado em razão da influência sofrida pela informação em tempo real passou a ser um instrumento dos mais eficazes, podendo tanto manipular, quanto distorcer, as informações, dados e tudo aquilo que por ali venha a circular. Assim, objetiva-se demonstrar que a utilização desses dados em plataformas digitais se caracterizam como um instrumento perigoso, considerando que sua finalidade pode ser para uso irregular, diga-se ilegal mesmo. Buscando ainda discutir tudo que envolve a proteção legal aos dados pessoais, e seus princípios norteadores; Tratar dos avanços legais envolvendo a Lei Geral de Proteção de Dados; e ainda, apontar a consequências da proteção inadequada que se dá na atualidade. Assim, as hipóteses aqui apresentadas se voltam no sentido de criação e mecanismos capazes de identificar e punis aqueles que fazem uso desses dados para fins comercias visando obter lucros com a venda e divulgação de informações pessoais de terceiros. E ainda se estabelecer um padrão o qual esses dados não possam ser salvos por plataformas digitais mesmo que com a autorização do cliente, consumidor ou mesmo de alguém que acesse a internet e precise se cadastrar para conseguir um acesso qualquer. Neste contexto, o que se busca com a referida pesquisa é apontar a necessidade de maiores cuidados com as informações pessoais dos usuários das plataformas digitais, visto estar-se em uma era na qual as informações circulam em tempo real.

Palavras-chave: Privacidade do Consumidor; Proteção de Dados Pessoais; Informações sem Consentimento.

ABSTRACT

The information society, as the current society is known, gained this meaning due to the influence suffered by real-time information and became one of the most effective instruments, being able to both manipulate and distort information, data and everything that there come to circulate. Thus, the aim is to demonstrate that the use of this data on digital platforms is characterized as a dangerous instrument, considering that its purpose may be for irregular use, even illegal. Still seeking to discuss everything that involves the legal protection of personal data, and its guiding principles; Deal with legal advances involving the General Data Protection Law; and also, point out the consequences of the current inadequate protection. Thus, the hypotheses presented here aim to create mechanisms capable of identifying and punishing those who use this data for commercial purposes in order to obtain profits from the sale and disclosure of third-party personal information. And even if a standard is established in which this data cannot be saved by digital platforms even with the authorization of the client, consumer or even someone who accesses the internet and needs to register to gain any access. In this context, the aim of this research is to highlight the need for greater care with the personal information of users of digital platforms, given that we are in an era in which information circulates in real time.

Keywords: Consumer Privacy; Protection of Personal Data; Information without Consent.

SUMÁRIO

1 INTRODUÇÃO

A “sociedade da informação”, como é conhecida a atual sociedade, ganhou este significado em razão da influência sofrida pela informação em tempo real passou a ser um instrumento dos mais eficazes, podendo tanto manipular, quanto distorcer, as informações, dados e tudo aquilo que por ali venha a circular.

Os avanços tecnológicos unidos ao melhoramento no tratamento de dados, as informações sobre indivíduos passou a ter uma maior organização, acontecendo uma multiplicação e banco de dados por todo mundo. Isso fazendo com que se dê uma redefiniçao naquilo que evolve direitos e poderes individuais que dizem respeito a própria pessoa.

Assim, tratando desse novo modelo de informações pessoais, é preciso um cuidado bem maior, considerando que o mesmo avança em informações de cunho sigiloso, como os dados pessoais. E isso implica dizer que aqueles que alcançam essas informações de um certo modo passam a ter em mãos um poder maior sobre informações de terceiros.

O que fica evidente com todo esse avanço tecnológico é que a vida do cidadão na atual sociedade tornou-se um mecanismo praticamente público no que corresponde a informações lançadas na rede mundial de computadores, visto que, ali administradores de plataformas captam dados e em alguns casos vendem essas informações para grupos criminosos, os quais fazem uso disso em benefício próprio, causando grandes prejuízos a essas vítimas.

Frente a toda esta nova realidade os cuidados com as informações pessoais e a vida privada devem ser cada vez maiores, considerando que quando esse tipo de conteúdo cai em mãos erradas pode estar se instalando ai um problema bem grande para essa pessoa que tem seus dados divulgados. Passando por inúmeras situações como compras em seu nome, empréstimos, falsificação de documentos, invasão de contas bancárias entre muitas outras coisas, que geram a estas pessoas transtornos e prejuízos.

Assim, diante de toda esta situação que se cria por dados utilizados indevidamente através de plataformas digitais, os quais tendem a gerar problemas e constrangimentos, é que a pesquisa aqui trazida passa a questionar,

Como é possível que o cidadão se sinta protegido na medida em que este passa ter suas informações pessoais compartilhadas de maneira que a propagação das mesmas atinge diretamente, como um ato reflexo, a privacidade dessas pessoas?

Assim, objetiva-se demonstrar que a utilização desses dados em plataformas digitais se caracterizam como um instrumento perigoso, considerando que sua finalidade pode ser para uso irregular, diga-se ilegal mesmo. Buscando ainda discutir tudo que envolve a proteção legal aos dados pessoais, e seus princípios norteadores; Tratar dos avanços legais envolvendo a Lei Geral de Proteção de Dados; e ainda, apontar a consequências da proteção inadequada que se dá na atualidade.

Assim, as hipóteses aqui apresentadas se voltam no sentido de criação e mecanismos capazes de identificar e punis aqueles que fazem uso desses dados para fins comercias visando obter lucros com a venda e divulgação de informações pessoais de terceiros.

E ainda se estabelecer um padrão o qual esses dados não possam ser salvos por plataformas digitais mesmo que com a autorização do cliente, consumidor ou mesmo de alguém que acesse a internet e precise se cadastrar para conseguir um acesso qualquer.

A pesquisa demonstra sua relevância no sentido de que quando o indivíduo tem suas informações pessoais arquivadas em plataformas digitais, estes passam a estar à mercê dessas plataformas, considerando que com aqueles dados podendo ser acessado por alguém, a pessoa a quem as informações pertencem se torna uma possível vítima de golpes das mais variadas espécies.

Diante de tudo isto, o método escolhido para construção desta monografia se volta a uma revisão bibliográfica, de cunho qualitativo, na qual serão utilizados livros, revistas, doutrina, legislação, artigos, periódicos e todo material informativo que se debruce sobre o tema escolhido.

O capítulo dois trata dos dados pessoais de da proteção ao consumidor através do CDC; abordando a busca pela regulamentação da internet das coisas e discutindo o papel do Marco Civil da Internet; analisando então os dados pessoais e seus princípios embasadores.

O capítulo três adentra no ordenamento jurídico brasileiro e os avanços que envolvem a Lei Geral de Proteção de Dados; tratando então da LGPD no Brasil, tratando também da LGPD à luz do ordenamento jurídico brasileiro.

O capítulo quatro discute a LGPD e os dados sensíveis e as consequências da inadequadas proteção que atualmente existe; discutindo então os pressupostos legais e que fundamentam o tratamento dos dados pessoais, por fim tratando do titular do mérito e o resguardo de seus direitos.

2 OS DADOS PESSOAIS E SUA PROTEÇÃO NO CÓDIGO DE DEFESADO CONSUMIDOR

O Código de Defesa do Consumidor (CDC) traz em suas disposições instrumentos que buscam resguardar a segurança e o sigilo dos consumidores, para situações entendidas de risco em meio as relação de consumo. Naquilo que tange à segurança, o artigo 4º, inciso II, alínea d, do CDC determina como objetivo da Política Nacional de Relações de Consumo um ato de governo passível de proteger o consumidor com segurança. “Produtos e serviços com padrões adequados de qualidade, segurança, durabilidade e desempenho”. Isso significa que o governo é obrigado a intervir no propósito de proteger o consumidor (Magrani, 2019, p. 63).

Conforme trata o artigo 6º, inciso II do CDC, “a educação e divulgação sobre o consumo adequado dos produtos e serviços, assegurados a liberdade de escolha e a igualdade nas contratações” deve ser aproveitada pela Internet das Coisas. Sendo imprescindível dispor de informações claras aos consumidores com relação aos riscos oferecidos pelo uso de alguns dispositivos, assim como as informações que são coletadas através destes. Muitos desses dispositivos de IoT (*Internet of Things*), ou sistemas limitados a coleta de dados, conectados à internet os quais dispõem de violação à proteção da vida, saúde e segurança na prevenção de riscos resultantes de práticas na provisão de produtos e serviços entendidos como perigosos ou nocivos, o qual está previsto no inciso I do artigo 6º do CDC (Magrani, 2019, p. 64).

Ainda, o CDC, em seu artigo 43, trata das informações e cadastros de consumidores. O referido artigo descreve em um sentido amplo, indicando a possibilidade de acesso de todos os dados pessoais do consumidor. De forma que, consumidor tem o poder de controlar suas informações pessoais, assim como qualquer tratamento, devendo para isso ser comunicado ao mesmo de modo transparente. Sendo possível monitorar com rigor a distribuição de suas informações pessoais (Bioni, 2019).

Segundo Miragem (2018), o desenvolvimento da IoT provoca uma revisão nos entendimentos já firmados. Naquilo que faz referência a precisa qualificação do fato que provoca deveres e responsabilidade, simultaneamente existe um produto e um fornecedor, a partilha dos regimes de responsabilidade nem sempre fica evidente e, ainda, salienta que:

> Esse estado de coisas resulta na própria reavaliação da extensão do dever de segurança dos produtos e serviços no mercado de consumo. A legislação brasileira é expressa ao limitar o fornecedor, indicando que coloque no mercado apenas produtos cujos riscos sejam normais e previsíveis (artigo 8º do CDC). A pergunta óbvia aqui será: todos os riscos destas novas tecnologias serão normais e previsíveis? Ou mesmo, em vista da cláusula geral de responsabilidade objetiva fundada no risco, prevista no artigo 927, parágrafo único, do Código Civil, de que modo seria identificada "a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem"? As implicações jurídicas da internet das coisas não param, contudo, por aí. Basta imaginar sua repercussão para o sistema de seguros e a avaliação dos riscos segurados, mesmo para permitir a definição de cobertura e de seu custo para o segurado (assim, o seguro de danos de um automóvel sem motorista, ou o seguro de vida de um segurado cujas informações de saúde sejam monitoradas em tempo real) (Miragem, 2018, p. 54).

Destaca-se que os dispositivos da IoT podem apresentar falhas, sendo algo que esperado dos mesmos. De modo que, prefere-se que as falhas ocorram o quanto antes, para que logo possa ser reparado a tempo de se evitar danos em grande escala. Dessa forma, o entendimento do CDC deve ser feito através de uma interpretação extensiva, discriminando os riscos intrínsecos dos que ocorrem excepcionalmente, "pois se um alarde for criado em volta dos produtos conectados online, há o risco sério de inibir inovações e espalhar na sociedade uma onda irracional de receio quanto ao real objetivo técnico destes" (Magrani, 2019, p. 65)

Resumindo, no Código de Defesa do Consumidor os direitos com acesso, retificação e cancelamento e os princípios como transparência, qualidade e limitação temporal, na seara de proteção de dados, abarca o consumidor objetivando a possibilidade de garantir ao consumidor o amplo exercício de controle sobre suas informações pessoais (Bioni, 2019).

2.1 O vazio legal na busca pela regulamentação da internet das coisas e o papel do marco civil da internet

Ainda, como legislação que também trata de regulamentar a IoT, tem-se o Marco Civil da Internet (MCI), Lei número 12.965/2014, que define princípios, garantias, direitos e deveres em torno do uso da internet no Brasil. Em meio aos direitos previstos, o que se visa alcançar é a proteção da privacidade e dos dados pessoais. Antes promulgação da referida lei, se tinha um vazio no ordenamento jurídico no que correspondia aos direitos fundamentais como a liberdade de expressão. Essa lacuna legislativa resultou em inúmeras decisões judiciais conflitantes, nas quais o embasamento se dava através das leis penais, o último remédio direcionador na ordem das condutas sociais (Magrani, 2019, p. 73).

O MCI em seu artigo 7º, descreve como essencial o acesso à internet no sentido do livre exercício da cidadania, trazendo ainda o mesmo artigo direitos aos usuários da internet no Brasil e a efetiva proteção à privacidade nas mais variadas formas.

Enquanto artigo 8º, se preocupa com a liberdade de expressão e com a privacidade como condição para que se exerça do direito de acesso à internet. O inciso I então destaca que, “inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação”; enquanto o inciso II se preocupa com a inviolabilidade e o sigilo de comunicação pela internet; já no inciso III a atenção é com as comunicações privadas armazenadas e o inciso IV excetua ai apenas a ordem judicial (Magrani, 2019, p. 75)

Destaca-se ainda o artigo 10 do MCI, o qual trata de forma mais específica da proteção de dados pessoais, de maneira que, em resumo, aos que possuem meios de comunicação privada e de dados pessoais devem ter um maior cuidado, no sentido de preservar sua intimidade, privacidade, honra e imagem de forma direta ou indireta.

Observa-se que o MCI trata de maneira expressa da necessidade da permissão do titular para a coleta, uso, o armazenamento e o tratamento de seus dados pessoais, da mesma maneira que, uma transferência a terceiros (Bioni, 2019).

Nota-se com isso a necessidade da autorização expressa, livre e informada em torno do tratamento de dados pessoais, o qual se revela ineficaz frente dos termos de usos abusivos (Magrini, 2019, p. 79).

O MCI é o instrumento regulador das tecnologias relacionadas a IoT e inteligência artificial (AI), em razão de que um dos maiores objetivos da Lei é dar o devido apoio às inovações e novas tecnologias, e acordo com o que trata o artigo 4º, inciso III. Mas, ainda assim está não se mostra capaz para proteger o cidadão dos possíveis abusos que venham a acontecer no mundo de IoT e AI. O MCI aplica-se apenas na esfera *on-line*, não sendo utilizável no mundo físico (Magrani, 2019).

Ainda mais, o MCI não discute pontos relevantes no sentido de evitar a coleta, má gestão e monetização de dados. Ou seja, que o texto legal deixa esse vácuo de definições como “dado pessoal” e “dados sensíveis” que mais adiante serão discutidos na Lei Geral de Proteção de Dados (Magrani, 2019, p. 78).

Assim, observando o vazio legal no sentido de resguardar a proteção de dados em meio digital, principalmente, naquilo que tange à relação entre mundo físico e virtual, que são os dispositivos da IoT e AI, é que se deu o complemento, através da entrada em vigor da Lei Geral de Proteção de Dados (LGPD). Deixando claro que, o MCI e CDC devem continuar desempenhado o papel de tutela, dentro daquilo que é de sua abrangência.

Observa-se, portanto, que o Direito brasileiro é completamente atrasado se comparado as mudanças sociais, principalmente no que alude a tecnológica. Visto que, a internet faz parte da vida cotidiana dos indivíduos desde os anos 90, e apenas depois 30 anos passa a vigorar uma Lei que visa regular os dados pessoais dos usuários. De modo que o autor salienta:

> [...] A dogmática jurídica, como esse arcabouço teórico construído desde o passado, tem a pretensão de alcançar soluções para todos os conflitos a partir de valores institucionalizados.
> Daí se nota que o Direito possui sua existência vinculada ao tempo, estando ambos relacionados com a sociedade. O problema está na falta de sincronia entre o tempo e o Direito estatista em face dos acontecimentos de uma sociedade globalizada. O paradigma jurídico moderno não é capaz de atender às inúmeras contingências dessa forma de sociedade (Moreira, 2007, p. 179).

Assim, evidencia-se que o Direito traz em sua bagagem inúmeros desafios para conseguir alcançar sintonia com os avanços sociais. Entretanto, a LGPD significa um salto importante no que se volta a regulação de dispositivos como IoT, devendo-se observar como se dará a efetiva fiscalização e punição dos controladores, de forma

que inúmeras são as possibilidades de atenuar os efeitos do tratamento de dados pessoais sem que a lei seja capaz de identificar.

2.2 Os dados pessoais e seus princípios embasadores

A Lei Geral de Proteção de Dados traz em seu artigo 6º, os princípios que devem se cumprir no período do tratamento dos dados pessoais em juntamente com as bases legais acima apresentadas. Dessa forma, foram firmados 10 princípios legais, em um rol exemplificativo – são levados em conta os princípios do ordenamento jurídico os quais podem ser invocados no caso concreto – devendo estes serem seguidos pelo controlador quando se der o tratamento de dados pessoais.

O princípio da finalidade trazido no inciso I do artigo 6º, trata de definir a "realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades" (Burkart, 2021, p.47). Já o inciso II, do mesmo artigo, o qual observa o princípio da adequação leciona que "compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento" (Brasil, 2018) Assim, esse princípio faz menção à relação lógica da conformidade que se evidencia entre o tratamento e a finalidade objetivada (Burkart, 2021, p.47).

Enquanto o inciso III, do mesmo artigo que trata do princípio da necessidade e determina a "limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados" (Brasil, 2018), no inciso IV tem-se o princípio do livre acesso que traz, a "garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais" (Brasil, 2018), e o inciso V, aponta o princípio da qualidade de dados, e traz que, a "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" (Brasil, 2018).

Destaque-se que, o princípio do livre acesso aos dados pelos titulares, determina que o titular detém o direito de consultar facilmente e de forma integral os

dados a seu respeito que estejam sob o domínio do controlador, sem que tenha que pagar para isso, ou seja, de forma gratuita. O princípio da qualidade dos dados, determina que os dados devem estar sempre atualizados a fim de assegurar a exatidão, a clareza e a relevância destes, sendo observados os princípios da necessidade e finalidade do seu tratamento.

O inciso IV, trata do princípio da transparência, assegurando que, a "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" (Brasil, 2018), discutindo em relação a inobservância do referido princípio em dispositivos IoT, é possível apontar a Alexa, assistente virtual da Amazon, um programa que capta a voz de seus usuários para poder executar comandos.

Conforme destacar Tuohy (2022), em uma de suas publicações na *The Verg,* pesquisas de estudantes da Universidade de Washington, UC Davis, UC Irvine e Universidade de Northestern, foram identificadas algumas inconsistências em meio a política de privacidade do dispositivo. Esses estudos apontam que, a Amazon realiza a coleta as informações através das interações com a assistente virtual, Alexa, em seguida compartilhando estas com as 41 empresas de propagandas que são suas parceiras da Amazon. As informações coletadas por si só se verificam como sensíveis, por isto, devendo estar de acordo com as bases legais de consentimento – expresso e inequívoco – assim como se alinharem aos princípios da finalidade, necessidade, adequação e transparência (Tuohy, 2022).

O inciso VII, cuida do princípio da segurança e determina que, "utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão" (Brasil, 2018). O mesmo cuida da previsibilidade a mitigação de situações de risco envolvendo os dados armazenados, trata-se de medidas que tem relação com procedimentos internos de segurança, sendo possível trazer como exemplo, o impedimento de invasão externa através do uso de bloqueios (Burkart, 2021, p.47).

O inciso VIII, traz o princípio da prevenção o qual, prevê a "adoção de medidas com o objetivo de prevenir a ocorrência de danos em virtude do tratamento de dados pessoais" (Brasil, 2018). O mesmo visa, de modo preventivo, proteger os dados pessoais no sentido de controle de risco e controle de risco dentro da organização.

O inciso IX, traz o princípio da não discriminação, cuida da, “impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos” (Brasil, 2018). Esse princípio tem relação intima com os dados pessoais sensíveis (Bioni, 2019).

Alguns princípios como – segurança, prevenção e da não discriminação – são extrema relevância quando se trata de dispositivos IoT e tratamento de dados sensíveis. Em uma pesquisa realizada pela *Check Point Software Technologies* chegou-se à conclusão que houve um crescimento de 45% em ataques a empresas do segmento de saúde ao redor do mundo (Check Point, 2021, *on-line).* Isso deixa evidente a vulnerabilidade dos dispositivos de Internet das Coisas que cuida do setor de saúde, sendo preciso observar por tais razões, os mencionados princípios, pois a violação dos mesmos não atinge somente o tratamento de dados sensíveis dos pacientes – titulares – mas a saúde como um todo.

Desse modo, a atenção a esses princípios acima trazidos é fundamental no sentido de atenuar os danos que eventualmente venham a ocorrer aos titulares, não somente aos pacientes em leito hospitalar, mas todo sociedade que faz uso de dispositivos IoT.

E finalmente, tem-se o inciso X, que cuida do princípio da responsabilização e prestação de contas. Esse princípio trata sobre a demonstração pelo responsável pelo tratamento – controlador ou operador – através da “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” (Burkart, 2021, p. 48)**.**

3 O ORDENAMENTO JURÍDICO BRASILEIRO E OS AVANÇOS ENVOLVENDO A LEI GERAL DE PROTEÇÃO DE DADOS

Com o surgimento das leis de privacidade e proteção de dados, tem havido um crescimento em torno da consciência no que diz respeito à necessidade de tutela-los, não só pela importância de se proteger a vida privada dos indivíduos, mas ainda pela liberdade destes. Sendo essencial destacar que o passar dos anos, fez com que privacidade, que anteriormente era o "direito de ser deixado só" como interpretaram por Warren e Brandeis (1890), tornou-se o direito de exercer controle sobre as próprias informações.

A privacidade era considerada um direito negativo no período das décadas de 60 e 70, ou seja, era assegurado, de modo que o Estado se abstinha de invadir a esfera individual do cidadão. Porém, com transformações tecnológicas e o tratamento de dados crescente, o conceito de privacidade passa a ter novos contornos, vindo então a sobressair conceitos funcionais que mencionam à possibilidade de o indivíduo conhecer, controlar e até interromper o percurso das informações a ele relacionados. "Assim a privacidade pode ser definida mais precisamente, em uma primeira aproximação, como o direito de manter o controle sobre as próprias informações". (Rodotà, 2008, p. 92).

No ano de 1970, o Estado Alemão de Hesse e a Suécia adicionara à sua lei de privacidade, a proteção de dados, como descreve Rodotà (2008). Este movimento avançou nos anos seguintes, sendo incluso na jurisprudência brasileira.

Conforme, Lugati e Almeida (2020), no Brasil, o controle em torno da proteção de dados foi estabelecido de maneira lenta e descentralizada. Todavia, se pode afirmar que teve seu início, de modo tácito, com a Constituição Federal de 1988. O artigo 5º, que tem o condão de descrever os direitos e garantias fundamentais invioláveis, aponta diversos incisos que servem como base a proteção de dados, a exemplo do inciso X o qual afirma que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito a indenização pelo dano material ou moral decorrente de sua violação" (Brasil, 1988). No mais, o asseguramento da livre expressão, não apenas intelectual, mas artística, a científica e a de comunicação, além da reforçar o acesso à informação, protegidas no artigo 5º, incisos IX e XIV da CF/88.

Nesse sentido, Doneda (2017) alerta no sentido de que a Constituição Federal interpreta que não podem ser invadidos a vida privada e a intimidade, nos termos do artigo 5º, inciso X, principalmente no que refere a interceptação de comunicações telefônicas, telegráficas ou de dados, como trata o artigo 5º, inciso XII, além de ter ser estabelecida a ação de *Habeas Data,* disposta no artigo 5º, inciso LXXII, que almeja a previsão de direito coletivo de acesso e retificação dos dados pessoais.

Inclusive, sustenta que o *Habeas Data* precisa ser analisado com atenção, não apenas por sua importância na formação da democracia ou por ter sido introduzido em muitas das legislações latino-americanas, mas, ainda por tratar-se do primeiro instrumento direcionado à assegurar à pessoa física ou jurídica o acesso ou a promoção de retificação informações a este pertencente e que constam em bancos de dados de órgãos públicos ou instituições similares.

É necessário evidenciar que o referido instituto surgiu como rompimento com o regime militar e tinha, inicialmente, o propósito de garantir ao cidadão o direito ao conhecimento das informações sobre si, e que estava em poder do que o regime militar. O *Habeas Data* "teve o mérito de chamar a atenção do operador e da sociedade para um direito que vinha sendo negligenciado". (Doneda, 2017, p.23)

Com o Código de Defesa do Consumidor (CDC) de 1990, instituto disciplinador a proteção frente a cadastros e bancos de dados. O artigo 43 trata que: "o consumidor, sem prejuízo no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como suas respectivas fontes". Tal artigo traz relação com o *Habeas Data* mencionado, visto que, em meio as proteções descritas, ressalta a exigência que os cadastros e dados dos consumidores devem ser objetivos, claros, verdadeiros, oferecendo a possibilidade de exigência pelo mesmo de sua imediata correção caso não o sejam.

Além disso, destaca-se a importância do parágrafo 2° do artigo 43, do CDC, onde determina este que qualquer abertura de cadastro, ficha, registro e dados pessoais e de consumo deve ser o consumidor comunicado de modo expresso. Sendo assim, é pode-se dizer que o CDC tentou assegurar ao titular dos dados o controle em torno de suas informações, tratando-se isto de um princípio de autodeterminação informativa.

> O artigo 43 estabelece uma série de direitos e garantias para o consumidor em relação às suas informações pessoais presentes em

> “bancos de dados e cadastros”, implementando uma sistemática baseada nos *Fair Information Principles* à matéria de concessão de crédito e possibilitando que parte da doutrina verifique neste texto legal o marco normativo dos princípios de proteção de dados pessoais no direito brasileiro (Doneda, 2011, p.103).

No ano de 2011, é editada a Lei 12.414/2011, chamada de Lei do Cadastro Positivo, está disciplina a respeito dos dados de adimplemento consultados para a formação de histórico de crédito. Sendo a mesma descrita como avanço se comparada à legislação infraconstitucional anterior, visto que, além de apresentar os conceitos de banco de dados, como também das informações que este pode armazenar, acompanha o entendimento de que o compartilhamento de dados só é lícito quando existir o consentimento do cadastrado. De tal modo, estabelece que a "evolução do conceito de autodeterminação informativa no nosso ordenamento”. (Mendes, 2014, p. 146).

A medida em que o Código de Defesa do Consumidor exige somente o comunicado ao titular a respeito da abertura de cadastros e bancos, a Lei de Cadastro Positivo vai mais a diante e exige o consentimento deste. Outrossim, impõe ao controlador a obrigação de não poder fazer uso dos dados fora da finalidade para o qual estão destinados na coleta, proibindo ainda as anotações de informações excessivas. Inovando ainda em seu artigo 17:

> Art. 17. Nas situações em que o cadastrado for consumidor, caracterizado conforme a Lei nº 8.078, de 11 de setembro de 1990 - Código de Proteção e Defesa do Consumidor, aplicam-se as sanções e penas nela previstas e o disposto no § 2º.
> § 1º Nos casos previstos no *caput*, a fiscalização e a aplicação das sanções serão exercidas concorrentemente pelos órgãos de proteção e defesa do consumidor da União, dos Estados, do Distrito Federal e dos Municípios, nas respectivas áreas de atuação administrativa.
> § 2º Sem prejuízo do disposto no *caput* e no § 1º deste artigo, os órgãos de proteção e defesa do consumidor poderão aplicar medidas corretivas e estabelecer aos bancos de dados que descumprirem o previsto nesta Lei a obrigação de excluir do cadastro informações incorretas, no prazo de 10 (dez) dias, bem como de cancelar os cadastros de pessoas que solicitaram o cancelamento, conforme disposto no inciso I do *caput* do art. 5º desta Lei (Brasil, 2011).

De acordo com Mendes (2014), a referida previsão descreve o controle da atividade de processamento por autoridade administrativa, capacitada a aplicar medidas e sanções conjuntamente com um sistema clássico judicial de definição de

lides. Finalmente, o mencionado diploma tem a responsabilidade, segundo Doneda (2006), por analisar de forma mais profunda um modelo de proteção relacionado a dados pessoais, ainda que em uma esfera limitada. Sendo de grande valia no sentido de integrar determinados princípios que correspondem à proteção de dados no ordenamento jurídico vigente.

Em 2011, uma invasão de hackers no computador da atriz Carolina Dieckmann, fez com que sua intimidade fosse violada, e depois de 36 imagens íntimas suas foram divulgadas sem sua permissão nas redes sociais. Em função disto, em menos de um ano, criou-se a Lei 12.737/2012, sendo a mesma conhecida pelo nome Lei Carolina Dieckmann passando a justiça notar que não existia nenhuma legislação específica voltada a especifica penalização dos envolvidos.

A lei tem o propósito assegurar a segurança no ambiente virtual, tornando crime a invasão de dispositivo informático alheio com o fim escuso de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo, como também de obter vantagem ilícita com os dados obtidos. A lei acresceu ao Código Penal os artigos 154-A, 154-B, 266 e 298.

Ainda que, trazendo em suas determinações falhas e de não dispor de meios processuais capazes de assegurar sua eficácia, como descreve Beretta (2014), a Lei Carolina Dieckmann faz parte trajetória da proteção de dados pessoais do Brasil por buscar devolver ao cidadão o controle de seus dados, visto que, novamente se fala de autorização do titular para se conseguir acessar os dados pessoais.

Ainda na linha cronológica brasileira sobre proteção de dados, o Marco Civil da Internet, Lei 12.965 de 23 de abril de 2014, surge como primeiro documento legislativo a dar reconhecimento à internet dentro do contexto de serviço essencial para o exercício da cidadania e, por tal motivo, buscou definir princípios, garantias, deveres para o uso da Internet no Brasil. A referida regulamentação tramitou de modo acelerado nas casas legislativas, quando houve a comprovação de que a espionagem realizada pela Agência de Segurança dos Estados Unidos causou uma grande repercussão em âmbito brasileiro.

A lei inova na busca por garantir o direito à privacidade e a proteção de dados pessoais, entre tantos outros, com o dispõe o artigo 7º e seus incisos:

> Art. 7º- O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
> I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
> II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
> III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;
> IV - não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização;
> V - manutenção da qualidade contratada da conexão à internet;
> VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;
> VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei (Brasil, 2014).

Nota-se então que, por mais que o diploma legal não traga um regramento detalhado, é possível identificar a base dos direitos garantidos aos usuários, os que seriam mais à frente, esclarecidos com a Lei Geral de Proteção de Dados.

> Art. – 7º [...]
> VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
> a) justifiquem sua coleta;
> b) não sejam vedadas pela legislação; e
> c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;
> IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;
> X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei e na que dispõe sobre a proteção de dados pessoais;
> XI - publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet;
> XII - acessibilidade, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, nos termos da lei; e
> XIII - aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet (Brasil, 2014).

O Marco Civil da Internet trata como indispensável a permissão do titular, de maneira livre, expressa e informada, quando necessário o fornecimento de dados pessoais a terceiros. Inclusive, Masso, Abrusio e Florêncio Filho (2014) sustentam, em respeito do adjetivo "livre", que o titular precisaria ter a opção de optar em relação a cláusulas ou contratos de forma parcial, e não apenas pelo todo, para dessa forma ser seguido aquilo que está disposto no inciso VII do artigo 7o, acima supracitado. Sendo informado das possibilidades e consequências de sua escolha.

Nota-se também que o texto já traz em seus dispositivos certos dos princípios presentes em algumas das leis de proteção de dados, dentre os quais, o princípio da finalidade, da adequação e da transparência. Da mesma forma solicita ao titular a possibilidade de solicitar a exclusão de suas informações, quando se finfar da relação entre titular e responsável pela coleta dos dados.

Mesmo que o Marco Civil da internet tenha surgido como um grande avanço, ao ser comparado às tentativas anteriores, as quais s faziam uso, segundo Bioni (2020), de uma técnica prescritiva e restritiva, o Brasil ainda buscava uma legislação mais abrangente. Em especial depois do surgimento do Regulamento Geral sobre a Proteção de Dados da União Europeia (GDPR), onde a afirmação dos 46 se davam em torno de que as transferências de dados entre os responsáveis pelo tratamento só poderiam ocorrer para um terceiro ou organização internacional caso houvesse leis que criassem garantias adequadas. De modo que, a GDPR causou influência na criação da legislação de proteção de dados em diversos países.

Ademais, impostas às restrições estabelecidas pela GDPR, viu-se a necessidade da edição uma lei específica para a tratamento, proteção e sigilo de dados, sendo esta a a Lei Geral de Proteção de Dados (LGPD); trazendo em meio a suas determinações enormes avanços para a proteção da privacidade, assim como segurança dos dados pessoais dos brasileiros, ainda que levantem debates sobre sua revisão e aprimoramento.

3.1 A LGPD no Brasil

De acordo com o que expõe por Bioni (2019), desde 2010 existia uma discussão em relação a uma legislação voltada colocada para consulta no referido ano. Entretanto, foi apenas em 2018 que o Projeto de Lei 53/2018 acabou virando a Lei no 13.709/2018, conhecida como a Lei Geral de Proteção de Dados (LGPD).

A LGPD, então, tendo como base os dispositivos da GDPR, se fundamenta na proteção de dados de um indivíduo natural identificado ou identificável e discute sobre os mecanismos através dos quais entidades públicas e privadas são autorizadas a coletar e tratar tais dados. É uma legislação de extrema técnica que busca garantir, em seu propósito central, os direitos humanos, principalmente os da liberdade, da privacidade e o livre desenvolvimento da personalidade da pessoa natural, como afirma seu primeiro artigo.

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

Conforme Mendes e Doneda (2018), é possível observar cinco linhas principais da LGPD em volta das quais a proteção de dados se desenvolve. A primeira linha se trata da unidade e generalidade da aplicação da Lei, pois se volta na proteção de dados do cidadão, não ficando isso dependente de quem realiza seu tratamento. Os objetivos da LGPD serão direcionados tanto para os setores privados quanto aos públicos, debruçando-se em torno de dados tratados na internet e fora dela.

A segunda linha é a legitimação para o tratamento de dados, que só acontecer quando houver autorização de uma base normativa, sendo feito um exame a respeito de sua legitimidade. "Somente serão legítimos aqueles tratamentos que se enquadrem em ao menos uma das hipóteses previstas no art. 7º ou no art. 23 da LGPD, totalizando11 hipóteses autorizativas para o tratamento de dados pessoais" (Mendes, Doneda, 2018, p. 472).

A terceira linha da LGPD se encontra nos princípios e direitos do titular. A Lei determina uma série de princípios e direitos os quais visam assegurar meios efetivos de controle, através do titular, dos dados utilizados por terceiros, além de possibilitar unidade sistêmica à disciplina de dados pessoais.

Os princípios, tratados no artigo 6º da LGPD, são:

> As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
> IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
> V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento (Brasil, 2018).

A quarta linha da Lei é a determinação de obrigações impostas aos agentes de tratamento. Além dos limites, Traz como previsão uma série de ações que dão reforço a segurança e as garantias dos titulares de dados. É possível citar como exemplo a obrigação, atribuída ao controlador, de definir um encarregado para o tratamento de dados, como determina o artigo 41 da LGPD.

> VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
> VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
> X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a

> observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas (Brasil, 2018).

Na quinta linha, está a responsabilidade dos agentes quando resultarem danos decorrentes do tratamento de dados. A LGPD entende que a natureza da atividade de tratamento de dados traz um si um risco intrínseco e, de tal modo, só precisa compreender os dados estritamente necessários. Desta maneira, como tratado no artigo 42, o legislador adotou um regime de responsabilidade objetiva.

A LGPD se divide em 10 capítulos, possuindo um total de 65 artigos, sendo então, menor e mais enxuta que a Lei que teve como referência (GDPR), a qual traz em seu bojo 11 capítulos e 99 artigos. Dito isto, se pode afirmar que deixou brechas para uma interpretação mais ampla em alguns assuntos, sendo possível citar os prazos como exemplo, "trazendo alguns pontos de insegurança jurídica por permitir espaço para a subjetividade onde deveria ter sido mais assertiva" (Pinheiro, 2020, p.14).

Necessário ainda lembrar que, por tratar-se de um instituto de grande impacto tanto para instituições públicas quanto privadas, estabeleceu-se um período de dezoito meses, a fim de que estas instituições conseguissem se adaptar às novas regras. Depois este período, as penalidades ali previstas poderiam ser aplicadas.

A Lei 13.709/18 cria uma inovação, não apenas em trazer uma legislação própria naquilo que cabe ao tratamento e uso de dados pessoais, mas ao apontar definições mais assertivas sobre titular, tratamento de dados, dados pessoais e consentimento, por exemplo, em face a qualquer legislação surgida anteriormente. Ademais, o instituto do consentimento tornou-se uma das hipóteses de permissão de tratamento, o que na concepção de Bioni (2020) revela que o instituto não apenas deixou de ser a única base legal, como também deixou de ter uma hierarquia superior às demais bases legais apontadas pelos incisos do artigo 7º da LGPD.

Entretanto, isso não quer dizer que o instituto perdeu seu valor. Pois segundo o artigo publicado pelo SERPRO que traz no título "Seu consentimento é lei!”, tem-se essa noção:

> Se a gente fosse eleger a principal palavra da Lei Geral de Proteção de Dados Pessoais (LGPD), a escolhida seria, sem dúvidas, CONSENTIMENTO. É o titular, ou seja, a pessoa a quem se referem

> os dados que deve, se quiser - ao ser questionada, de forma explícita e inequívoca - autorizar que suas informações sejam usadas, por empresas e órgãos públicos, na hora da oferta de produtos e serviços, gratuitos ou não (Serpro, 2024, s.p.).

Finalmente, da mesma maneira que grande parte das leis de proteção de dados, é possível perceber que a LGPD detém dois graus de proteção para estes: uma voltada aos dados pessoais e a outra voltada aos dados pessoais sensíveis. Isto quer dizer que reconhece a diferença dentro de situações que envolvam tratamento e vazamento de dados; ao passo que algumas apenas podem causar pequenos aborrecimento, outras são capazes de provocar uma ameaça contra a integridade física, discriminação, estresse emocional, danos morais e fraude.

3.2 A LGPD à luz do ordenamento jurídico brasileiro

O vocábulo “legislação”, ou “lei”, anota Bittar (2022), aponta, dentre as demais fontes do Direito, para uma fonte estatal, vinculativa, geral, principal e nacional. Designa, assim, normativa jurídica componente de determinado ordenamento jurídico positivo que veicula conteúdos definidores de direitos e deveres. A legislação, nos países filiados ao sistema de civil *law,* como é o caso do Brasil, consiste na mais importante das fontes formais estatais (Diniz, 2006). A sua formulação é obra exclusiva do legislador, contemplando, em certas hipóteses, a iniciativa do projeto de lei a outro Poder da República.

A justificação para esse protagonismo do legislativo reside no fato de que seus membros representam toda a comunidade social e possuem, por conta disso, legitimidade e autoridade para estabelecer normas obrigatórias para todos (Montoro, 1971). Em virtude disso, Montoro (1971, p. 11) assevera que por ser uma vontade jurídica consciente e deliberada, “a lei constitui o grau mais elevado e mais perfeito de formação do Direito Positivo”.

Não obstante, a doutrina contemporânea critica fortemente o excesso de leis que vêm sendo aprovadas pelas Casas Legislativas dos diferentes níveis da federação, gerando um ambiente de notável insegurança jurídica.

Fala-se, conforme registra Ávila (2016, p. 55), “furacão normativo”, “incontinência legislativa”, “aluvião de normas” e “orgia na produção de leis”, tornando o apontamento do caráter instável, efêmero e aleatório do Direito algo banal.

Em uma sociedade hiper acelerada e hiper conectada, na qual convivem pessoas interesses dos mais diversos, crenças não raro conflitantes, ideologias opostas e dentro de um panorama econômico marcado pela velocidade cada vez mais do processo econômico de destruição criativa, o direito naturalmente absorve essas características, mediante uma constante edição de novas leis e outros atos normativos a fim de buscar regular os novos aspectos e relações da vida social.

Como diz Couture (2004), a lei é vida humana objetivada, forma parte dos objetos da cultura, ou seja, representa um objeto ideal vivente, criado quando uma maioria parlamentar, atendendo anseios que identificados na sociedade, quer estatuir novas regras em determinado campo da vida. Como não poderia deixar de ser, as leis sempre terão certo grau de incerteza, de limitação, de provisoriedade e problemáticas, tal como ocorre com a própria vida humana, descabendo idealizar uma consagração absoluta da autoridade e segurança jurídica através dos diplomas legislativos.

Essas observações são fundamentais para que não se caia na ilusão de que todas as respostas para as disputas reais serão encontradas nas leis de proteção de dados pessoais, como o Regulamento Europeu (RGPD) e a Lei nº13.709/2018. Couture (2004) alerta que a arquitetura das leis é sistematicamente perfeita no dia da sua sanção, mas basta uma leve perturbação por parte dos fenômenos da vida social ou econômica para que essa arquitetura se quebre.

No panorama global da proteção de dados pessoais, os primeiros marcos normativos foram leis infraconstitucionais, cabendo mencionar os seguintes: a pioneira Lei do Estado de Hesse, de1970; Lei de Dados da Suécia, de1973; Estatuto de Proteção de Dados do Estado alemão de *Rheinland-Pfalz*, de1974; Lei Federal de Proteção de Dados da Alemanha, de 1977; *Fair Credit Reporting Act*, de1970, dos Estados Unidos; *Privacy Act,* de1974, também norte-americano.

Já na legislação infra constitucional brasileira, que contempla os instrumentos das leis complementares, leis ordinárias, leis delegadas, medidas provisórias, decretos legislativos, resoluções do senado, além das normativas infra legais, tais como decretos regulamentadores, instruções ministeriais, portarias, circulares, ordens de serviço etc., o documento normativo mais relevante sobre privacidade e proteção de dados pessoais é a Lei nº13.709/2018, conhecida como Lei Geral de Proteção de

Dados Pessoais ou LGPD, que dispõe sobre o tratamento de dados pessoais com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Outros marcos legais como o Código de Defesa do Consumidor (arts. 43 e 44), a Lei de Acesso à Informação (Lei nº 12.527/2011–art.31), a Lei do Cadastro Positivo (Lei nº 12.414/2011) e o Marco Civil da Internet (Lei nº 12.965/2014 - artigo 3°, incisos II e III,7° a 17), todos precedentes à LGPD, também albergam princípios e regras concernentes à privacidade e à proteção de dados pessoais.

No âmbito criminal, a Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, que tipificou delitos cibernéticos, e a Lei nº 14.132/2021 (Lei *Stalking*), a qual tipificou o crime de perseguição (*stalking*), oferecem novos e relevantes mecanismos de tutela para as vítimas de delitos que possuem íntima relação com a proteção da privacidade e de dados pessoais. Na esfera infra legal, merecem realce o Decreto nº10.474/2020, que estruturou a Autoridade Nacional de Proteção de Dados (ANPD); a Portaria nº1/2021, que estabeleceu o Regimento Interno da ANPD; a Portaria nº 16/2021, que aprovou o processo de regulamentação no âmbito da ANPD; a Resolução CD/ANPD nº1/2021, que aprovou o Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dados; e a Resolução CD/ANPD nº 2/2022, que aprovou o Regulamento de aplicação da LGPD para agentes de tratamento de pequeno porte.

Os diplomas infra legais que veiculam políticas públicas estratégicas também podem ser citados como instrumentos a serem observados na esfera da proteção de dados pessoais, tais como o Decreto nº 9.319/2018 (Estratégia Brasileira para Transformação Digital, E-Digital), o Decreto nº 9.637/2018 (Política Nacional de Segurança da Informação, PNSI), o Decreto nº 10.222/2020 (Estratégia Nacional de Segurança Cibernética, *E-Ciber*) e a Portaria MCTI nº 4.617/2021 (Estratégia Brasileira de Inteligência Artificial, EBIA). Normativas setoriais igualmente podem versar direta ou indiretamente sobre proteção de dados pessoais e privacidade.

No campo do sistema financeiro, por exemplo, a Resolução BACEN nº 4.658/2018 trata sobre política de segurança cibernética e permite indiretamente que se extraiam ditames aplicáveis à órbita da proteção de dados pessoais. Na área da saúde, uma das mais afetadas pelo direito da proteção de dados pessoais, sobejam instrumentos normativos infra legais, abrangendo Resoluções Normativas da Agência Nacional de Saúde Suplementar - ANS (255/2011,305/2012,389/2015), Súmula Normativa da ANS

(27/2015), Resoluções da Diretoria Colegiada da Agência Nacional de Vigilância Sanitária – ANVISA (9/2015 e 10/2015), Resoluções do Conselho Federal de Medicina - CFM(1605/2000, 1638/2002, 1643/2002, 1821/2007, 1819/2007, 1974/2011, 2107/2014, 2217/2018), Resoluções do Conselho Nacional de Saúde-CNS (251/1997, 466/2012, 506/2016) e Norma Operacional do CNS (01/2013), Portarias do Ministério da Saúde (589/2015, 2022/2017, 467/2020).

Cabe salientar o advento, em 2021, do robusto Código de Boas Práticas de Proteção de Dados para os Prestadores Privados em Saúde, publicado pela Confederação Nacional de Saúde (CNSaúde), que aclara a legislação e sua aplicação para os agentes econômicos desse segmento (Brasil, 2021).

Na área de seguros privados, a Superintendência de Seguros Privados (SUSEP) publicou a Circular SUSEP nº619/2020, versando sobre a política de segurança e sigilo de dados e informações das entidades registradoras credenciadas a prestarem o serviço de registro de operações de seguros, previdência complementar aberta, capitalização é resseguros, e a Circular SUSEP nº638/2021, dispondo sobre segurança cibernética para sociedades seguradoras, entidades abertas de previdência complementar (EAPCs), sociedades de capitalização e resseguradores locais, além de ter emitido o Parecer Eletrônico nº1/2021/DIR4/SUSEP, com extensa abordagem sobre privacidade e proteção de dados no setor.

A Confederação Nacional das Seguradoras (CNseg) lançou, em 2019, o Guia de Boas Práticas do Mercado Segurador Brasileiro sobre Proteção de Dados Pessoais, que não ostenta caráter legislativo ou infra legal, mas orienta as empresas sobre a aplicação da legislação de proteção de dados pessoais neste segmento (CNseg, 2019).

4 LGPD: OS DADOS SENSÍVEIS E AS CONSEQUÊNCIAS DA INADEQUADA PROTEÇÃO DA ATUALIDADE

Nos dizeres de Solow-Niederman (2022), na atual sociedade se vive em uma economia de inferência. Em que está se verifica com a capacidade de dedução, resultado que possui uma base na lógica e ainda na tradução de informações que já se consegue alcançar sobre os indivíduos, sendo detentores disso as empresas e organizações que têm e que, para a autora, trata-se na atualidade do poder legítimo. O que a autora demonstra é que o procedimento de coleta e organização dos dados dos indivíduos não é tão linear quanto se quer crer. Os dados que são recolhidos sobre alguém não são tratados e armazenados somente sob o "arquivo" desta pessoa; podem ser utilizados para fazer inferência sobre outras informações que não foram fornecidas, bem como para fazer inferências sobre outras pessoas.

Sendo assim, não é apenas a pessoa que disponibilizou o controle dos dados que é atingida com a coleta, o tratamento e o compartilhamento dos dados. As consequências podem ocorrer sobre o estado das coisas no presente, mas são capazes de tentar predizer o futuro, o qual acaba por se tornar com um potencial causador de maiores danos pelo fato de não serem verificáveis, como afirma Matsumi (2018). As ocorrências ou inferência como é mais conhecido no meio das redes, também podem se dar por meio de dados não sensíveis a fim de se descobrir os dados sensíveis, de modo que a raça de um indivíduo pode ser inferida através do local em que ela vive, por sua religião, e até mesmo através do padrão de alimentação, de suas crenças filosóficas, e ainda pelos hábitos de leitura ou afiliação política, o que significa a possibilidade de serem inferidas informações de milhares de formas distintas.

Conforme Hinds e Joinson (2018), ao observar 327 pesquisas sobre inferências, eles observaram que as características mais usuais de inferir são gênero, idade, política, localização, ocupação, raça e’ etnia, família e relacionamentos, salário, educação, saúde, orientação sexual.

Neste caso, a LGPD certifica, em seu do artigo 11, que as inferências são tidas como dados sensíveis devendo por tais razões serem tratadas por meio do mesmo regime jurídico, o que é valorável. Contudo, a questão é, que as complicações são maiores do que se é descrito, visto que, as inferências se incluem como dados

sensíveis, de forma que quase a totalidade dos dados pessoais seriam atingidos por tal categoria, fazendo com que se torne nociva a proteção distinta aos dados sensíveis e dados não sensíveis.

Ao se falar em saúde, tem-se o reconhecimento pelo Comitê Europeu para a Proteção de Dados (EDPB), por meio de suas diretrizes a respeito da tomada de decisões individuais automatizadas e também definição de perfis para o fim de regulamentação, que qualquer tipo de dado pode ser usado para se ter conhecimento sobre a condição de saúde atual ou mesmo o risco de saúde de uma pessoa.

Sendo possível trazer como exemplo que, no período da pandemia de Covid-19, diversos países resolveram fazer uso de tecnologias voltadas a monitorar e controlar a propagação do vírus, sendo realizado um mapeamento das pessoas que interagiram com indivíduos infectados, os conhecidos aplicativos de *contact tracing*. Esses aplicativos faziam a coleta de dados como data do diagnóstico, nacionalidade e gênero. Sendo este entretanto, um exemplo pontual. Os estudos de Kosinski (2013) apontam a possibilidade se dar por meio da análise de *likes* no *Facebook*, observar o uso abusivo de substâncias em um número maior que dois terços dos perfis analisados. Sendo ainda possível de perceber a saúde mental de um indivíduo por seus *posts* em redes sociais; e modo que a atividade - ou a falta dela – em meio a essas redes é um direcionamento para os algoritmos.

Desta forma, é possível se chegar a compreensão de que, com dados pessoais aleatórios, como por exemplo uma simples compra em um site, se pode alcançar informações consideradas sensíveis, mesmo que estas, não tenham sido tratadas ou compartilhadas. Vido assim a expor que, a atual proteção de dados sensíveis não corresponde com a atual realidade tecnológica.

4.1 Pressupostos legais fundamentadores aos tratamentos de dados pessoais

O sistema legal desenvolvido para o tratamento de dados no sentido de dispor ao titular ferramenta para administrar suas informações pessoais e assegurar direitos. Assim, deve-se esclarecer que o rol do artigo 7º e do artigo 11 são taxativos, mesmo que demonstrando amplos e com algum grau de subjetividade, como, por exemplo, o

legítimo interesse. Das bases legais tem-se 10, quais sejam: (i) consentimento; (ii) cumprimento de obrigação legal ou regulatória; (iii) execução de políticas públicas; (iv) fins de pesquisa (v) processos judiciais e administrativo; âmbito arbitral; (vi) execução do contrato; (vii) proteção à vida; (viii) tutela da saúde; (viiii) legítimo interesse; (x) proteção ao crédito.

Tem como propósito averiguar os requisitos necessários para o tratamento de dados na LGPD, com destaque nas bases legais apropriadas ao âmbito de IoT e b*ig data*, quais sejam: o consentimento e ao real interesse, além disso, expor as diferenças de tratamento para dados sensíveis. A estrutura legal do consentimento do titular garante ao controlador que o titular dos dados autorizou o tratamento de seus dados para certo fim específico ou pré-determinado. Esta autorização deve ser evidenciada ao titular dos dados de modo claro e transparente, objetivando a ausência de dúvidas pelo do titular (Burkart, 2021).

A autorização fornecida pelo titular, mostra-se como um instrumento essencial no cenário tecnológico moderna, considerando a manipulação em massa de dados pessoais da mesma forma que a comercialização destes. É preciso com isso, que ocorra um entendimento a respeito do consentimento de modo restritivo de maneira que não consiga o agente ampliar a permissão para o tratamento de dados repassando-os a outros meios além dos já acordados, para acontecimento futuro ou de finalidade diversa (Teffé, 2020, p. 6).

Neste aspecto, não se pode levar em conta uma autorização genérica para o tratamento de dados pessoais, devendo esta ser especifica a finalidade. De tal modo, fica possível observar que é neste direcionamento que a LGPD se coloca sobre o consentimento, através de seu artigo 8º, parágrafo 4º:

> Artigo 8º O consentimento previsto no inciso I do artigo 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.
> § 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas (Brasil, 2018).

Levando-se em conta a consequência através da aplicação do princípio da finalidade, pode-se entrelaçar o princípio da informação a ser analisado ao redor do consentimento. A informação remete a uma completa consciência do titular em torno

o do caminho de seus dados pessoais, partindo da ideia do consentimento do tratamento dos dados. De maneira que, o titular tenha a total consciência de: (i) quem o dado se destina; (ii) para qual finalidade será utilizado e por quanto tempo; (iii) quem terá acesso aos dados, e (iv) se eles poderão ser transmitidos a terceiros (Doneda, 2017).

É necessário ressaltar que a exposição de vontade deve ser inquestionável, entretanto, a lei não requer o consentimento de modo expresso. Porém, mesmo não ser necessária a formalidade do consentimento por escrito, o mesmo não pode ser assegurado em função da omissão do titular, mas, de atos positivos que evidenciam a real vontade. Nesse aspecto, a Lei é expressa em determinar ao controlador o ônus da prova, no sentido de que o consentimento foi recebido de acordo com aquilo que dispunha o dispositivo legal, em razão do princípio da responsabilização e prestação de contas (Teffé, 2020, p. 10).

Naquilo que corresponde ao resguardo dos dados sensíveis, a LGPD define ser admissível o tratamento dos dados, de modo que deve existir a expressão do consentimento de maneira específica e com destaque, de modo a indicar as finalidades singulares, conforme o artigo 11, inciso I, da referida Lei. Além disso, segundo Rodotà, a autorização do titular de dados sensíveis define-se pela falta de liberdade, em meio ao exercício da vontade, considerando que se trata de um contratante vulnerável (Rodotà, 2008, p. 90).

Ademais, a LGPD em seu artigo 11, inciso II, também aborda as situações pelas quais é mitigado o fornecimento de consentimento do titular. Tais hipóteses tratam, de forma ampla, a aplicação do interesse público. Nesse caso, há uma ponderação em torno dos interesses públicos frente aos interesses particulares. Tal posicionamento, entretanto, é acaba sofrendo essas críticas considerando o direito crucial para o pleno exercício de direitos como igualdade, liberdade e privacidade. (Mulholland, 2018, p. 168)

Assim, o exercício regular de direitos em processo judicial, administrativo ou arbitral, acaba se tornando uma base legal ampla possibilitando o uso de dados pessoais em meio a processos para produção de provas no processo judicial, e meio a uma parte contra a outra. Segundo a doutrina, em certos casos que entenda que determinados dados podem ser armazenados, de modo que esclarecida a necessidade e para determinado fim específico, neste interim, há formação de provas para o processo judicial. No mais, tem-se ainda que, há a proteção da saúde ou da

integridade física do titular ou de terceiros como razão no processamento de dados pessoais.

4.2 O titular e o mérito no resguardo a seus direitos

É importante frisar e demonstrar os direitos estabelecidos pela LGPD ao titular dos dados. São garantia inerentes ao titular, sendo a este possível solicitar ao controlador de dados, o qual deve responder aos questionamentos de modo célere e preciso. Entretanto, a Lei não determina um prazo para que essas solicitações sejam entregues.

A ratificação de que existe o tratamento, tem como base a possibilidade do titular, sem qualquer justificativa, confirme a existência de tratamento de seus dados pessoais. Esse direito se baseia no princípio da transparência, trazido no artigo 6º da correspondente Lei. Na legislação europeia é tratada, expressamente, nos artigos 13 e 14 da GDPR, a obrigação de dispor das informações dos dados que são recolhidos junto ao titular, como também daqueles que não são coletados (Maldonado; Blum, 2020).

Naquilo que diz respeito ao direito de acesso aos dados, o titular tem o direito de acessar os dados, assim como as informações correspondentes a eles, sendo estas: as finalidades, categorias, destinatários, prazo de conservação, origem dos dados, existências de decisões automatizadas, existência de direitos específicos, procedimento de reclamações e fontes indiretas (Maldonado; Blum, 2020).

É direito do titular ter o conhecimento das finalidades para as quais os seus dados estão sendo processados, devendo ser indicados os tipos de procedimentos que existem, da mesma forma que conhecer as categorias para as quais estão classificando seus dados. E ainda deve ser informado ao titular para quais destinatários o controlador dos dados passou os dados do titular solicitante, nas situações em que o controlador tenha repassado os dados para outras empresas, se faz necessário que se dê o rastreio dos compartilhamentos das informações feitas pelo controlador (Burkart,2021, p. 52).

Em razão do direito do titular, frente a distorção do real propósito da coleta de dados pessoais dos titulares sendo estes utilizados principalmente com o objetivo de

comercialização, é fundamental a garantia desse direito em virtude da excessiva manipulação dos dados. Assim, Sartori e Bahia os autores evidenciam que:

> [...] Se o indivíduo, nos seus mais diversos papeis sociais - como cidadão, contribuinte, trabalhador, consumidor, etc. - tem seus dados pessoais diuturnamente captados, vigiados, processados e transmitidos, tais perfis virtuais passam a fundamentar tomadas de decisões econômicas, políticas e sociais.
> Obviamente que tal realidade é extremamente preocupante, porquanto tem a capacidade de alterar profundamente o modo como as pessoas lidam com as informações. E mais: pode muito bem afetar a capacidade de um indivíduo de se autodeterminar, influenciando não só o seu modo de consumo, mas também sua visão política, social e cultural, isso sem falar na possibilidade de esses “perfis”, formados com base nos dados pessoais, serem utilizados para fins discriminatórios.
> Deve-se considerar, ainda, que isso ocorre de forma invisível à maioria dos usuários, sem seu consentimento, de forma que fica impossível aos indivíduos ter o controle das suas informações pessoais que estão circulando na rede (Sartori; Bahia, 2019, p. 232).

Outrossim, e acordo com o período previsto, este se configura através do período que o controlador reter as informações, da mesma forma que a justificativa da razão pela qual utilizará algum tempo pré-determinada para manipular as informações. A existência em torno dos direitos específicos, por sua vez, caso haja a utilização dos dados resguardados em decorrência de direito específico, como Código de Defesa do Consumidor, o titular dos dados deve ter ciência desse direito (Burkart, 2021, p. 52).

O titular precisa ter o direito de modo simples e rápido, de fazer um registro reclamando, devendo para isso existir um órgão que processe essas reclamações. E ainda, deve ser direito do titular ter o conhecimento se seus dados foram captados por outra fonte. No que alude à existência de tomada de decisão automatizada, o titular precisa ter o direito de conhecer os processos automatizados, e a forma como essas decisões se dão (Burkart, 2021, p. 52).

A proteção da dignidade humana, assim como, os dados pessoais detém uma ligação direta e representam a sua personalidade, reforçando o direito à correção dos dados incompletos, incorretos ou desatualizados. Os direitos mencionados, e a ciência sobre a existência do tratamento e acesso aos dados, são apontados como ações importantes no total uso da correção (Korkmaz, 2021).

A perspectiva em se dar a correção de seus dados pode ser considerada como uma das manifestações da autodeterminação informativa, a qual se encontra em todo ciclo do fluxo informacional. Nesse caso, as correções, a complementação e a atualização dos dados pessoais surgem como instrumento imprescindível para possibilitar que o indivíduo seja retratado de modo real e genuíno. Esse direito, quando realizado da maneira certa, é capaz de evitar que se deem reflexos de um tratamento de dados desatualizado, como no tratamento das decisões automatizadas (Korkmaz, 2021).

A LGPD assegura também ao titular o anonimato, bloqueio ou eliminação de dados desnecessários, aqueles em excesso ou tratados de forma que venha a ferir as determinações legais. Quanto ao anonimato, conforme o artigo 12 da mencionada Lei, os dados em anonimato não serão entendidos como dados pessoais em razão do titular não ser identificado ou identificável de modo permanente e irreversível (Maldonado; Blum, 2020).

Dessa maneira, o titular pode solicitar o anonimato, de maneira que referido dado atravesse um processo que irá desvincula-lo a pessoa com a informação. Sendo possível ainda a retirada da anonimato do dado e, conforme o parágrafo 1º, do artigo 12, “fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios” (Brasil, 2018).

No que corresponde ao bloqueio dos dados, tratado no artigo 5º, inciso XIII, da LGPD, este determina que cabe ao titular solicitar de forma expressa que seus dados sejam suspensos de maneira provisória de qualquer operação de tratamento, armazenamento do dado pessoal ou do banco de dados. No mais, a remoção dos dados desnecessários, em excesso ou processados em afronta à Lei acima citada, é importante ressaltar que em meio a uma sociedade conectada, a coleta de dados atualizados se dá de forma rápida e com facilidade (Korkmaz, 2021).

Em função de outro direito do titular, a portabilidade correspondente às informações do próprio titular passou por alteração através da Lei 13.853/2019, surgindo está através da Medida provisória 869/2018 que transformou em lei ordinária. A mudança ocorreu por meio da transferência da expressão “de acordo com a regulamentação da autoridade nacional” para o centro da formulação, de maneira que através da nova redação é possível compreender que a regulamentação em questão

faz menção ao regramento da própria portabilidade e sua requisição (Maldonado; Blum, 2020, p. 23).

Em resumo, o direito corresponde à obtenção de dados pessoais de modo estruturado de maneira que oportunize o repasse para outro controlador. Esta é relacionada ao próprio titular, sendo mantidos os segredos comercial e industrial. Dessa forma, é possível ao titular, por livre escolha, que detenha parecida contratação em concorrente (Maldonado; Blum, 2020).

A LGPD traz como alternativa a exclusão dos dados desnecessários, excessivos ou tratados em desacordo com a Lei, inciso IV, do artigo 18, aborda a respeito do direito do titular em retirar os dados que não foram cuidados em conformidade com a base legal do consentimento. Desta maneira, o tratamento do dado se seu de forma lícita, contudo, os mesmos teriam de ser eliminados ao fim do tratamento. Destaca-se que ainda que não constando no artigo 5º, da LGPD, trata-se de definitivo o processo de eliminação dos dados. No mais, considerando a base legal do consentimento, o titular pode solicitar a eliminação irreversível de seus dados, a qualquer tempo, quando não mais desejar que seus dados sejam tratados (Korkmaz, 2021).

No que implica o direito de informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados, primeiramente, é necessário recuperar o conceito de uso compartilhado de dados, que tem sua positivação no artigo 5º, inciso XVI, da LGPD, a ver:

> Artigo 5º Para os fins desta Lei, considera-se:
> [...]
> 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 (Brasil, 2018).

Nestes moldes, garante-se ao titular ter conhecimento em torno de seus dados tratados pelas entidades públicas e privadas as quais foram compartilhadas pelo controlador. Estando o referido direito ligado intimamente ao princípio da transparência, da mesma maneira que, ao direito de informação e acesso aos dados.

Ressalta-se que se faz necessário diferenciar o direito à informação do uso compartilhado e portabilidade, de modo que na portabilidade o titular solicita a transmissão dos seus dados pessoais a outro controlador, na medida em que no uso compartilhado, o controlador faz a transmissão desses dados sem que haja a necessidade de solicitação do titular.

Sobre isto, o inciso VIII aborda o direito da informação em torno da possibilidade de não fornecer o consentimento, o resultado negativo do consentimento. Como se sabe, o consentimento integra as bases legais para o tratamento dos dados, apontando que o titular é livre ao compartilhar seus dados aos controladores e, logicamente, este também é detentor do direito de não consentir sobre o tratamento de seus dados (Korkmaz, 2021).

A negação no fornecimento do consentimento pode resultar consequências, devendo estas serem expressas previamente ao tratamento dos dados, de forma que o titular consiga analisar o mais conveniente. Sendo assim, a empresa tem a liberdade de limitar alguns acessos ao titular, em virtude do não fornecimento dos dados essencialmente necessários para o uso, destacando-se a proibição da restrição abusiva por parte de empresas (Maldonado; Blum, 2020).

Finalmente, a LGPD traz a previsão em torno da possibilidade de revogação do consentimento para o tratamento de dados, elencado no artigo 8º, parágrafo 5º. A revogação do consentimento está diretamente relacionada ao livre desenvolvimento da personalidade, considerando que este poder está alinhado ao próprio sentido de autodeterminação no que diz respeito ao consumo (Doneda, 2017)

A anulação do consentimento precisa ser expressa, entretanto, somente a revogação não trará o resultado na cessação do tratamento caso exista outra base legal que possa justificar esse tratamento.

De acordo com a LGPD, a comercialização dos dados biométricos, por intermediação de uma empresa, em que o titular ocupa posição de subordinação, em virtude do vínculo empregatício, pode sim ser questionada. Os dados biométricos, tratam-se de dados sensíveis, devendo por esta razão o titular deve consentir expressamente e inequivocamente sobre seu tratamento. Dentro de uma relação empregatícia o titular pode autorizar para que seu vínculo de emprego seja mantido. Contudo, aqui fica a compreensão, no sentido de que a comercialização de dados, dentro de uma contextualização brasileira, é ilegal.

Em outra esfera, que não seja a seara trabalhista, fica evidente a problematização da comercialização dos dados pessoais sensíveis dos titulares, entretanto, tal prática se mostra cada vez mais presente. Empresas que tem um bancos de dados com números espetaculares como, *Amazon* e *Google*, as quais com bastante frequência são questionadas no que diz respeito a comercialização dos dados de seus usuários.

5 CONSIDERAÇÕES FINAIS

Como visto a atual sociedade está cada vez mais dependente das redes sociais, de maneira que a tecnologia tem avançado com cada vez mais rapidez, fazendo com que a criação de leis voltadas a este segmento acabe ficando defasada de modo tão rápido que, em um piscar de olhos tudo mudou, tudo se transformou e aquilo que antes havia em certo ambiente virtual já não mais tem utilidade.

Neste contexto, é preciso que a sociedade esteja atenta e seja capaz de identificar suas necessidade, direitos e limites. De forma que, informações pessoais devam ser resguardadas e preservadas a todo custo. E isto se dando em função de que, quando essas informações pessoais e sigilosas caem em mãos erradas podem trazer prejuízos inestimáveis.

E esse fato, das informações pessoais estarem em mãos erradas é algo que tem ocorrido com muito mais frequência do que se imagina, quando se leva em consideração aplicativos, mensagens, que os usuários recebem diariamente em suas redes sociais, os quais solicitam sempre uma informação que aparentemente é inofensiva, mas que acaba se tornando perigosa se cair em mãos erradas.

Tudo isso implica dizer que, grande parte das pessoas que fazem uso de redes sociais viaja por caminhos que desconhece e lá acaba deixando rastros que são recolhidos por outros grupos que fazem daquelas informações o que quiserem, já que detém um poder quase ilimitado dentro do mundo virtual.

Atualmente os dados e informações pessoais são a estratégia mais utilizadas pelos grupos criminosos que agem nas sombras das redes sociais em busca de vítimas, isso em função de que é muito comum esses dados ficarem acessíveis em plataformas de compras para esses criminosos.

Quando se fala em Lei Geral de Proteção de Dados (LGPD), isso significa que aquele espaço precisa ser cuidadosamente controlado, por meio de um monitoramento feito por profissionais capacitados e que não coloque em risco a integridade dos usuários das redes. Isso se dando no sentido de que os dados ali agrupados, armazenados afetam diretamente a vida pessoal, profissional e emocional de cada cidadão que tem suas informações ali coletadas e agrupadas.

Atualmente, muitas empresas quando recolhem esses dados acabam deixando os mesmos ali salvos, o que pode gerar um grande prejuízo ao dono dessas

informações. Isso em virtude de que, esses dados são repassados a outras empresas o que acaba causando em diversas ocasiões transtornos graves a essas pessoas.

A LGPD surge com o escopo de resguardar os dados pessoais dos cidadãos, de modo a prevenir abusos e o uso indevido, entretanto isso não quer dizer que tais práticas não continuem ocorrendo. É possível observar isso quando se realiza uma compra em um site qualquer, como por exemplo a Amazon, e lá no final da compra quando o consumidor digita os dados de seu cartão e tem uma opção de salvar o mesmo para as próximas compras. Entretanto existem casos que mesmo o consumidor não aceitando a referida opção as informações permanecem salvas na plataforma, o que tem gerado alguns transtornos, entre eles compras por terceiros não autorizados.

Assim, o que acaba sendo imperativo, é a necessidade de uma efetiva proteção ao indivíduo, tanto em sua informação pessoal como cidadão, quanto dentro do meio virtual como usuário de redes sociais. Não se admite mais em pleno século XXI, que as plataformas digitais estejam tão vulneráveis a ponto de colocar a integridade pessoal de alguém em risco. Pois, quando um consumidor resolve confiar seus dados a um sistema virtual, ele busca confiança e segurança, não sendo possível que aqueles que detém o controle desses sistemas não sejam capazes de oferecer ao usuário estas condições.

É preciso estar à frente da criminalidade quando se trata da segurança de dados e informações dos usuários digitais. Pois em um mundo quase completamente tecnológico não existe espaços para mais erros, o usuário, o consumidor precisam sentir-se seguros e confiantes ao ingressar em qualquer meio digital e colocar lá seus dados pessoais.

Neste contexto, o que se busca com a referida pesquisa é apontar a necessidade de maiores cuidados com as informações pessoais dos usuários das plataformas digitais, visto estar-se em uma era na qual as informações circulam em tempo real.

REFERÊNCIAS

ÁVILA, Humberto. **Teoria da segurança jurídica.** 4 ed. São Paulo: Malheiros, 2016.

BERETTA, Pedro. Sem meios eficazes, Lei Carolina Dieckmann até atrapalha. **Consultor Jurídico**, São Paulo, 10 maio 2014. Disponível em: www.conjur.com.br/2014-mai-10/pedro-beretta-meios-eficazes-lei-carolina-dieckmann-atrapalha. Acesso em 9 mar. 2024.

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

BITTAR, Eduardo Carlos Bianca. Introdução ao Estudo do Direito: humanismo, democracia e justiça. São Paulo: Saraiva,2022.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 10 abr.2024.

BRASIL. **Constituição da República Federativa do Brasil De 1988.** Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 18 mar. 2024.

BRASIL. **Lei nº 12.414, de 9 de junho de 2011.** Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em 27 mar. 2024.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 10 mar. 2024.

BRASIL. CONFEDERAÇÃO NACIONAL DE SAÚDE. **Código de Boas Práticas:** Proteção de Dados para Prestadores Privados em Saúde. Disponível em: https://www.gov.br/ans/pt-br/arquivos/assuntos/noticias/boas-praticas-protecao-dados-prestadores-privados-cnsaude_21.pdf. Acesso em 10 jun. 2024.

BURKART, D.V.V. **Proteção de dados e o estudo da LGPD**. São Paulo: 2021.

CHECK POINT. **Attacks targeting healthcare organizations spike globally as COVID-19 cases rise again**. Disponível em: https://blog.checkpoint.com/2021/01/05/attacks-targeting-healthcare-organizations-spike-globally-as-covid-19-cases-rise-again/. Acesso em 9 mar. 2024.

CONSEG. **Guia de Boas Práticas do Mercado Segurador Brasileiro sobre a Proteção de Dados Pessoais.** 2019.Disponível em:

https://cnseg.org.br/publicacoes/guia-de-boas-praticas-do-mercado-segurador-brasileiro-sobre-a-protecao-de-dados-pessoais.html. Acesso em 10 jun. 2024.

COUTURE, Eduardo. **El arte del derecho y otras meditaciones**. Montevidéu: Fundación de Cultura Universitária, 2004.

DINIZ, M aria Helena. **Compêndio de introdução à ciência do direito**. 18 Ed. São Paulo: Saraiva, 2006**.**

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

DONEDA, Danilo. **A Proteção dos Dados Pessoais como um Direito Fundamental.** Espaço Jurídico. Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011. Disponível em: https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315/658. Acesso em: 26 mar. 2024.

DONEDA, Danilo. **Privacidade e proteção de dados pessoais.** 2017. Disponível em: https://www.gov.br/cgu/pt-br/acesso-a-informacao/institucional/eventos/anos-anteriores/2017/5-anos-da-lei-de-acesso/arquivos/mesa-3-danilo-doneda.pdf. Acesso em 26 mar. 2024.

HINDS, Joanne; JOINSON Adam N. What demographic attributes do our digital footprints reveal? A systematic review. **PLoS ONE,** v. 13, 2018. Disponível em: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0207112. Acesso em 25 mar. 2024.

KORKMAZ, Maria Regina Rigolon, SACRAMENTO, Mariana. Direitos do titular de dados: potencialidade e limites na lei geral de proteção de dados. Rio de Janeiro: **Revista Eletrônica**. 2021. Disponível em: https://revistaeletronica.pge.rj.gov.br/index.php/pge/article/view/234. Acesso em 2 arb. 2024.

KOSINSKI, Michal. Private traits and attributes are predictable from digital records of human behavior. **PNAS,** v. 110, 2013. Disponível em: https://www.pnas.org/doi/epdf/10.1073/pnas.1218772110. Acesso 20 mar.2024.

LUGATI, Lys Nunes; ALMEIDA, Juliana Evangelista de. Da evolução das legislações sobre proteção de dados: a necessidade de reavaliação do papel do consentimento como garantidor da autodeterminação informativa. **Revista de Direito,** Viçosa, v. 12, n. 2, 2020. Disponível em: https://periodicos.ufv.br/revistadir/article/view/10597. Acesso em 25 mar. 2024.

MAGRANI, Eduardo. **Entre dados e robôs:** ética e privacidade na era hiperconectividade. Porto Alegre, RS: Arquipélago, 2019.

MALDONADO, Viviane Nobrega, BLUM, Renato Opice. **LGPD Lei Geral de Proteção de Dados.** 2ª Ed. São Paulo. Revista dos Tribunais, 2020.

MASSO, Fabiano; ABRUSIO, Juliana; FLORÊNCIO FILHO, Marco Aurélio. **Marco Civil da Internet**: Lei 12.965/2014. São Paulo: Editora Revista dos Tribunais, 2014.

MATSUMI, Hideyuki, Predictions and Privacy: Should There Be Rules About Using Personal Data to Forecast the Future?. **Cumberland Law Review**, v. 48, p. 149-210, 2018. Disponível em: https://ssrn.com/abstract=3222217. Acesso 15 mar. 2024.

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

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões Iniciais sobre a Nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor**, v. 120, p.469-483, 2018. Disponível em: https://www.academia.edu/42741127/Reflex%C3%B5es_iniciais_sobre_a_nova_lei_geral_de_prote%C3%A7%C3%A3o_de_dados. Acesso em 10 mar. 2024.

MIRAGEM, Bruno. **Curso de direito do consumidor.** 7. ed. São Paulo: Ed. RT, 2018.

MONTORO, franco. O Problema das Fontes do Direito. Fontes Formais e Materiais. Perspectiva Filosófica, Sociológica e Jurídica. *In*: **Revista de Informação Legislativa,** out./dez. 1971. Disponível em: https://www2.senado.leg.br/bdsf/bitstream/handle/id/180464/000340719.pdf?sequence=1&isAllowed=y. Acesso em 10 jun. 2024.

MOREIRA, N. C. A função simbólica dos direitos fundamentais. **Revista de Direitos e Garantias Fundamentais**, n. 2, p. 163-192, 13 ago., 2007.

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

RODOTÀ, Stefano. **A vida na sociedade de vigilância:** privacidade hoje. Rio de Janeiro: Renovar, 2008.

SARTORI, Ellen Carina Mattias; BAHIA, Cláudio José Amaral. Big Brother is watching you: da distopia orwelliana ao direito fundamental à proteção de dados pessoais. **Revista de Direitos e Garantias Fundamentais**, v. 20, n. 3, p. 225-248, 20 dez. 2019.

SERPRO. **Seu consentimento é lei!**. 2024.Disponível em: https://www.serpro.gov.br/lgpd/cidadao/seu-consentimento-e-lei. Acesso em 20 mar. 2024.

SOLOW-NIEDERMAN, Alicia. Information Privacy and the Inference Economy, **Northwestern University Law Review**, V. 117, n. 2, p. 357-424, 2022. Acesso em: https://scholarlycommons.law.northwestern.edu/nulr/vol117/iss2/1. Acesso 25 mar. 2024.

TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. **Tratamento de dados pessoais na LGPD**: estudo sobre as bases legais. Civilista.com: 2020. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/510. Acesso em 15 abr. 2024

TUOHY, J. P. **Researchers find Amazon uses Alexa voice data to target you with ads**. Disponível em: https://www.theverge.com/2022/4/28/23047026/amazon-alexa-voice-data-targeted-ads-research-report. Acesso em 5 abr.2024.