FACULDADE DE DIREITO DE VITÓRIA
CURSO DE GRADUAÇÃO EM DIREITO

MARIA ALICE FERREIRA CONDE RIOS CAVALCANTI

INTERNET DAS COISAS E *BIG DATA* NA NOVA LEI DE PROTEÇÃO DE DADOS: ANÁLISE DA PROTEÇÃO DOS DADOS SENSÍVEIS

VITÓRIA
2022

MARIA ALICE FERREIRA CONDE RIOS CAVALCANTI

INTERNET DAS COISAS E *BIG DATA* NA NOVA LEI DE PROTEÇÃO DE DADOS: ANÁLISE DA PROTEÇÃO DOS DADOS SENSÍVEIS

Trabalho Científico apresentado ao curso de graduação em direito da Faculdade de Direito de Vitória – FDV, com requisito parcial para a obtenção do grau de Bacharel em Direito, sob a orientação do Prof. Dr. Bruno Costa.

VITÓRIA

2022

MARIA ALICE FERREIRA CONDE RIOS CAVALCANTI

INTERNET DAS COISAS E *BIG DATA* NA NOVA LEI DEPROTEÇÃO DE DADOS: ANÁLISE DA PROTEÇÃO DOSDADOS SENSÍVEIS

Trabalho de Conclusão de Curso apresentado ao curso de Direito da Faculdade de Direito de Vitória, como requisito parcial para obtenção do grau de bacharel em Direito.

Aprovado em _____ de _____ de 2022.

COMISSÃO EXAMINADORA:

_____

Prof. Dr. Bruno Costa

Faculdade de Direito de Vitória – FDV

_____

Examinador

Faculdade de Direito de Vitória - FDV

RESUMO

O presente estudo busca analisar os avanços tecnológicos e a intensa coleta de dados, sobretudo, ao tratar-se da utilização de dispositivos da Internet das Coisas (IoT) e a mineração dos dados pela tecnologia do *big data.* O trabalho teve como objetivo demonstrar os desafios legislativos para regulamentar os direitos dos titulares quanto à proteção dos dados pessoais em meio a tecnologia virtual, especialmente, os dados sensíveis. Além disso, busca analisar a Lei Geral de Proteção de Dados Pessoais (Lei número 13.709 de 2018) que tem como intuito tutelar os dados de forma mais eficaz, o que sofreu demasiada influência do Regulamento Europeu de Proteção de Dados, Regulamento número 2016/679. Assim, diante de uma análise sistemática das legislações que regulamentam os dados pessoais dos usuários da IoT, pode-se concluir que há desafios inerentes à tecnologia, contudo, é possível perceber a importância da LGPD sobre a proteção dos dados pessoais dos titulares, especialmente, a operação da Autoridade Nacional de Proteção de Dados a regulamentação e fiscalização.

Palavras-chave: Internet das coisas; Proteção dos dados pessoais; Lei Geral de Proteção de Dados; Dados pessoais Sensíveis.

SUMÁRIO

INTRODUÇÃO 03

1 INTERNET DAS COISAS..... 06

1.1 *BIG DATA*..... 08

2 AS LEGISLAÇÕES SETORIAIS PARA PROTEÇÃO DOS DADOS PESSOAIS NO ÂMBITO DA INTERNET DAS COISAS..... 12

2.1 A TUTELA DOS DADOS PESSOAIS NO CÓDIGO DE DEFESA DO CONSUMIDOR..... 13

2.2 O MARCO CIVIL DA INTERNET E A LACUNA LEGISLATIVA PARA RRGULAMENTAR A INTERNET DAS COISAS..... 15

3 O TRATAMENTO DE DADOS PESSOAIS NA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E A UTILIZAÇÃO DA INTERNET DAS COISAS..... 18

3.1 PARTES ENVOLVIDAS..... 20

3.2 HIPÓTESES LEGAIS PARA FUNDAMENTAR OS TRATAMENTOS DOS DADOS PESSOAIS..... 21

3.3 PRINCÍPIOS BASILARES PARA O TRATAMENTO DOS DADOS PESSOAIS.. 27

3.4 A IMPORTÂNCIA DA GARANTIA DOS DIREITOS DO TITULAR..... 30

CONSIDERAÇÕES FINAIS..... 36

REFERÊNCIAS..... 37

INTRODUÇÃO

A sociedade enfrentou importantes mudanças, especialmente, a partir de meados do século passado, com o avanço da tecnologia, popularização dos computadores e, posteriormente com a internet, a qual possibilitou a ampliação de todas as formas de comunicação.

A internet fomentou e potencializou a globalização da economia e inseriu a sociedade na era da informação. Desta forma, tornou-se possível o acesso de milhares de pessoas em diversos lugares do mundo de forma veloz e concomitante, bem como a transferência de dados, e-mail e arquivos com as mais variadas extensões, compartilhamento de fotos, vídeos e áudios em tempo real.

Em meio a isso, surgiu a Internet das Coisas, correspondente a sigla do inglês *Internet of Things* (IoT), a qual condiz a objetos físicos, com sensores embutidos que captam informações em seu ambiente, sentem e interagem com o mundo ao seu redor. Maneira inteligente de até mesmo transmitir dados de seus usuários, incluindo dados pessoais, para a *World Wide Web*. (SANTOS, 2019)

Assim, os dados pessoais transmitidos à rede são selecionados por meio de tecnologias de big data ou grandes volumes, com o objetivo de utilizar os dados de forma inteligente.

Junto a várias novas possibilidades e alternativas criadas pela IoT, revelaram-se também novos desafios. Um dos principais desafios abarca sobre as questões de segurança dos dados coletados por estes objetos. Quanto à Segurança da Informação (SI), em vista da privacidade, leis foram editadas ao longo dos últimos anos para promover a proteção dos usuários quanto aos seus dados sensíveis.

Assim, no Brasil foi promulgado uma nova lei regulamentadora em 2018 que entrou em vigor em fevereiro de 2020. Esta lei é a Lei Geral de Proteção de Dados, a qual visa tutelar os dados pessoais dos usuários.

O problema de pesquisa do presente estudo consiste em: quais são os desafios, à luz da Lei Geral de Proteção de Dados, para regulamentar o tratamento de dados pessoais, sobretudo sensíveis, provenientes da utilização da Internet das Coisas*?*

O uso de IoT e big data tornou-se uma ferramenta de possível violação de direitos na sociedade atual, em vista do processamento de dados pessoais sem o consentimento do proprietário. A Lei Geral de Proteção de Dados, promulgada em 2018, regulamenta o tratamento de dados pessoais em meio digital, e visa proteger os direitos fundamentais das pessoas físicas à liberdade, à privacidade e ao livre desenvolvimento da personalidade, mas existem obstáculos causados pela própria tecnologia, que dificultam a implementação deste regulamento Execução eficaz e eficiente.

A base teórica utilizada para o desenvolvimento do presente estudo tem como referência as teses de Bruno Ricardo Bioni (2015, 2018), Eduardo Magrani (2019) e Danilo Doneda (2019) acerca de, respectivamente, proteção de dados pessoais a respeito da função e dos limites do consentimento, ética e privacidade na era da hiperconectividade e a tutela da privacidade.

Para atingir a melhor compreensão sobre a os dados sensíveis, analisou-se a teses de civilistas que irão trazer a base sólida ao que tange o desdobramento do estudo. Tais como Gustavo Tepedino (2019) e Chiara Spadaccini de Teffé (2020).

O método científico aplicado será o hipotético dedutivo para aferição dos resultados, para tanto a pesquisa será composta por três capítulos. Neste primeiro capítulo serão abordadas questões conceituais englobando o conceito de Internet das Coisas e *Big Data*. Serão apresentadas as tecnologias que serão objeto de análise do presente estudo e seus desdobramentos quanto ao tratamento de dados pessoais.

Já no segundo capítulo, serão descritas as legislações setoriais que regulam o tratamento de dados pessoais quanto a utilização da Internet das Coisas e a mineração dos dados na tecnologia *big data*. Este capítulo tem o intuito de demonstrar as fragilidades e lacunas legislativas anteriores à edição da Lei Geral de Proteção de Dados.

E, por fim, o terceiro capítulo tratará do tratamento de dados regulamentado pela Lei Geral de Proteção de Dados que conceitua de forma precisa o que são dados pessoais e suas

subcategorias, como dados sensíveis e dados biométricos – abarcando a diferença no tratamento dos dados pessoais sensíveis. Além disso, aborda das partes envolvidas nos tratamentos desses dados, bem como a necessidade de ter uma base legal para fundamentar o tratamento dos dados pessoais, os princípios que regem todo o procedimento e os direitos que os titulares possuem sobre seus dados.

Durante os capítulos abordaremos casos concretos para visualizar as violações dos direitos dos titulares, bem como os desafios legislativos para regulamentar de forma efetiva tais direitos.

1 INTERNET DAS COISAS

A internet das coisas, – sigla em inglês *internet of things* (loT) – é a capacidade da conectividade e interação entre diversos tipos de objetos do cotidiano com técnica computacional e de comunicação, conectarem-se à Internet. Estes objetos possuem diversos dispositivos e sensores que contêm capacidade de capturar todos aspectos do mundo real. Assim, Santos (2016) estabeleceu que "a conexão com a rede mundial de computadores viabiliza primeiro, controlar remotamente os objetos e, segundo, permitir que os próprios objetos sejam acessados como provedores de serviços".

O termo internet das coisas surge apenas em 2001 no livro branco de Brock, pesquisador do Auto-ID Center. Época em que se falava de uma internet das coisas para alertar aos empresários que tinham coisas que os computadores podiam executar de forma mais eficiente do que as pessoas tendo em vista que estas possuem tempo, atenção e precisão limitadas. (SINGER, 2012)

Segundo Singer, a IoT pode ser definida como "a criação de uma rede global de padronização e identidade dos objetos, é bastante ampla delimitada a IoT pelo o que ela faz: conectar objetos dotados da capacidade de agirem por conta própria, com ou sem supervisão humana". (SINGER, 2012)

O decreto número 9.854/2019 institui o Plano Nacional de Internet das Coisas e dispõe sobre a Câmara de Gestão e Acompanhamento do Desenvolvimento de Sistemas de Comunicação máquina a máquina e Internet das Coisas, em seu artigo 2º traz a conceituação jurídica do termo, a ver:

> [...]
> Artigo 2º Para fins do disposto neste Decreto, considera-se:
>
> I - Internet das Coisas - IoT - a infraestrutura que integra a prestação de serviços de valor adicionado com capacidades de conexão física ou virtual de coisas com dispositivos baseados em tecnologias da informação e comunicação existentes e nas suas evoluções, com interoperabilidade;
> [...]

Assim, a IoT são, em suma, objetos físicos que possuem programação e sensores capazes de captar informações, as quais os tornam cada vez mais personalizados de acordo com os usuários, devido a manipulação automatizada de informações coletadas.

Segundo Magrini (2019, p. 20), a IoT pode ser definida como “computadores, sensores e objetos (artefatos) interagem uns com os outros e processam as informações/dados em um contexto de hiperconectividade”.

O autor aborda a hiperconectividade como a relação entre os indivíduos com objetos físicos, sensores, algoritmos, *big data*, inteligência artificial, entre outros. Segundo o autor, o termo de hiperconectividade está atrelado à relação entre indivíduos, indivíduos e máquinas e entre máquinas. Sendo diferentes formas de comunicação e, nesse contexto, existe corrente de informações e uma intensa produção de dados. (MAGRINI, 2019, p. 20)

A forma pela qual vivemos poderá ser cada vez mais alterada com a integração de objetos inteligentes e *big data.* Em uma pesquisa apresentada pela empresa de consultoria *Gartner*, empresa norte-americana de tecnologia, aponta que o número de objetos inteligentes já superou o número de humanos. Segundo os especialistas, no final de 2018, a estimativa era de 22 bilhões objetos inteligentes espalhados pelo mundo. A estimativa para 2025 é de 38,6 bilhões e para 2030 por volta de 50 bilhões desses dispositivos inteligentes estarão pelo mundo. Ao que tange ao impacto econômico global, estima-se que mais de US$ 11 trilhões em 2025. (GARTNER, 2021, *on-line*)

Devido a tais estimativas de crescimento econômico, a IoT tornou-se mais frequente no setor de investimento na esfera privada e mostra-se como uma tecnologia capaz de solucionar os novos desafios de gestão pública, tendo em vista a sua capacidade de manipulação de dados. (MAGRINI, 2019, p. 25)

Ademais, a IoT pode trazer diversos benefícios aos usuários. Diante da variedade de dispositivos tecnológicos, a IoT pode estar relacionada à saúde, como por exemplo, dispositivos que estão interconectados permitirão monitoramento direto entre paciente e médico, permitindo a avaliação constante da saúde do indivíduo. Poderá, também, estar relacionada a automação residencial que permite que o usuário controle remotamente residência, tais como: a climatização, a abertura de cortinas, desligar alarmes, preparar banho quente, dentre outras funções. (MAGRINI, 2019, p. 25)

Desta forma, à primeira vista é possível se encantar com a tecnologia – facilidade, velocidade e conectividade - contudo, o armazenamento e a manipulação das informações captadas por esses objetos, sem o consentimento do usuário, é um grande desafio para a tutela da privacidade quanto a proteção dos dados.

A título de exemplo, tem-se geladeiras que comunicam sobre os alimentos faltantes para encomendá-los, automaticamente, nos sites de compras dos supermercados, automóveis que gerenciam os dados do deslocamento para melhor traçar rotas de tráfego (BIONI, 2019). Além disso, Airfryers com conexão via-wifi com controle dos preparos a distância, em tempo real, pelo celular ou pelo assistente de voz – tais como Alexa e Google Nest.

Esses dispositivos conectados, gradativamente mais inteligentes e autônomos, estarão interligados ao cotidiano dos indivíduos, irão coletar, transmitir, armazenar e compartilhar dados, sobretudo, sensíveis. Essa manipulação de dados pode gerar riscos ao que tange a tutela da privacidade e segurança dos usuários.

Segundo Marco Aurélio Castro (2009), "atualmente, a geração de robôs vem evoluindo de forma acelerada, produzindo equipamentos semelhantes aos humanos e capazes de ver, ler, falar, aprender e até expressar emoções". Essa afirmação trazida pelo autor Castro (2009), traz a reflexão da complexidade de regular juridicamente dispositivos IoT, diante da capacidade de imitar comportamentos humanos e de outras máquinas. Podem, também, analisar as próprias condutas a ponto de aprender com os erros e demonstrar curiosidade, bem como ter a capacidade de serem criativos. (CASTRO, 2009 *apud* MAGRINI, 2019, p. 26)

Assim, diariamente os objetos se conectam à internet com o poder de, processar, armazenar, compartilhar e analisar grandes quantidades de dados. A quantidade de dados manipulados é diretamente proporcional ao número de dispositivos conectados. Essa relação é o que une o conceito de IoT com o de *big data.* (MAGRANI, 2019, p. 22)

1.1 *BIG DATA*

Existem diversas definições para o *big data.* Segundo o *McKinsey Global Institute, big data* é a utilização em massa de redes sociais online, de aparelhos móveis conectados à internet,

transações e conteúdos digitais, bem como a crescente utilização de computação em nuvem que geram quantidades incalculáveis de dados. (MACKINSEY GLOBAL INSTITUTE, 2011, *on-line*)

O termo *big data* refere-se a banco de dados cujo seu crescimento é dinâmico e seu tamanho está além da capacidade das ferramentas convencionais de captura, gerenciamento e análise de dados.(TAURION, 2013)

Ademais, o instituto Gartner define *big data* como grande volume, grande velocidade e/ou grande variedade de informação que exigem maneiras que requerem baixo investimento e inovadoras de processar informações que permitem *insights* aprimorados, tomadas de decisões e automatização de processos. (GARTNER, 2022, *on-line*)

O *big data* está direcionado em questões de volume de conjunto de dados demasiadamente grandes gerados com inícios de práticas tecnológicas, tais como: tecnologia operacionais, mídia social, acessos à internet e fontes de informações difundidas (TAURION, 2013)

Além dessas definições, Machado apresenta a ideia dos cinco Vs, os cinco pilares do *big data*, quais sejam: volume, velocidade, variedade, veracidade e valor: i) O volume corresponde a quantidade massiva de informações coletadas; (ii) Velocidade é a relação do tratamento dos dados em tempo hábil; (iii) Variedade corresponde a coleta de fontes alteráveis, como as informações dos comércios, inclui-se sensores de objetos inteligentes, dados bancários para relações financeiras, bem como os dados trocados entre máquinas; (iv) Veracidade corresponde na qualidade do dado importando os dados verdadeiros e atualizados; (v) Valor é a classificação dos dados, elencando se são dados úteis ou inúteis. (MACHADO, 2018, p. 514)

Dessa forma, segundo o entendimento de Taurion (2013):

> [...] *big data* pode ser visto como a descoberta do microscópio, que abriu uma nova janela para vermos coisas que já existiam, como bactérias e vírus, mas que não tínhamos conhecimento. O que o microscópio foi para a medicina e a sociedade, o *big data* também será para as empresas e a própria sociedade.

Esse entendimento surge devido à chamada revolução digital, possuímos tecnologia suficiente para analisar um volume inédito de dados digitais, com o *big data*. Dados que antes eram

considerados como *shadow data,* ou dados invisíveis, podem ser coletados, aplicados, organizados e classificados.

Quando se trata de *big data* e de internet das coisas, o potencial dessa união torna-se ilimitado. Isso porque o crescimento da quantidade e qualidade de sensores permite a comunicação entre os dispositivos, o que gera ainda mais interação entre os dados coletados entre eles. (FIGURELLI, 2016)

Em uma pesquisa de medicamentos é possível extrair um exemplo do uso de *big data.* Busca-se cruzar as informações de usuários de diversas drogas, utilizando-se o *big data* para analisar as combinações de remédios que geram efeitos colaterais anteriormente desconhecidos. (TAURION, 2013)

Outro setor onde o *big data* pode interferir é na segurança pública. Dados que podem ser coletados de diversas fontes, que vão de câmeras nas ruas a comentários e posts publicados em mídias sociais, as agências de inteligência e de segurança podem detectar e impedir a prática de atividades ilícitas. Essa tecnologia, pode descobrir tendências comportamentais criminosas, cruzando pedaços de informações que aparentemente não estão correlacionados. (TAURION, 2013)

Para melhor visualização da tecnologia *big data,* tem-se o exemplo da empresa americana Target com o objetivo de identificar consumidoras grávidas. Este público é muito atrativo em vista dos inúmeros objetos a serem adquiridos para a maternidade. Assim, a empresa pode investigar o perfil das consumidoras grávidas que compravam determinados produtos. Logo, os algoritmos dos bancos de dados cruzam as informações e direcionam certos anúncios publicitários a tais perfis. (BIONI, 2019)

Este caso foi emblemático devido a demonstração da eficiência da tecnologia, ao pai ir até a empresa, furioso, acusando a empresa de estimular a filha adolescente a engravidar. Dias depois, ao gerente ligar pedindo desculpas pelo ocorrido, comunicou ao estabelecimento, se desculpando, que a sua filha estava efetivamente grávida. (BIONI, 2019)

Entende-se que a junção dessas tecnologias pode ser um fator preponderante para o crescimento exponencial das empresas, com as informações coletadas pela Internet das Coisas e processadas

pelo *big data*. A utilização desse artifício, pode-se extrair o sentimento dos usuários, por meio das redes sociais, conectadas gera enorme e variada quantidade de dados – texto, imagens, áudios, vídeos, etc. Esses dados são utilizados pelas empresas para conhecer melhor seus clientes e direcioná-los a determinados produtos. (TAURION, 2013)

Note-se, assim, que os dados dos usuários são comercializados, sem o consentimento destes, para alavancar os negócios. Diversos dispositivos possuem a capacidade de captar conversas para entender o que os interesses dos e comercializar essas informações.

A comercialização desses dados pessoais não é o único problema. Os dispositivos IoT podem possuir falhas na segurança que permitem que *hackers* invadam o sistema e acessem todas as informações coletadas por esses aparelhos. Esses dispositivos coletam as informações por meio da ativação de voz, sem que os usuários tenham consciência dessa invasão de privacidade.

Dessa forma, a internet das coisas e o *big data* podem ser aliados à vida cotidiana, ao facilitar diversas tarefas e a potencializar inúmeras outras. Por outro lado, permitem também a ocorrência de violações de direitos, sobretudo, ao que tange ao consentimento da manipulação de dados pessoais.

2 AS LEGISLAÇÕES SETORIAIS PARA PROTEÇÃO DOS DADOS PESSOAIS NO ÂMBITO DA INTERNET DAS COISAS

O contexto de Internet das Coisas (IoT) e a inteligência artificial abarca novos desafios regulatórios ao ordenamento jurídico brasileiro. Tendo em vista a conjuntura de incessante e intensivo armazenamento, tratamento, compartilhamento e monetização dos dados são essenciais para a questão da a privacidade e ética que precisarão ser a meta para os avanços tecnológicos. (MAGRANI, 2019, p. 55)

A Constituição Federal de 1988 abrange o direito à privacidade, incluindo a proteção de dados pessoais, tanto no meio físico quanto no meio digital. É direito fundamental, previsto no artigo 5º, "a inviolabilidade da intimidade e da vida privada". Assim, sobre direito fundamental o autor Adriano Pedra (2017, p. 7) aponta que

> [...]
>
> Os direitos fundamentais podem ser considerados sob diversas perspectivas. Dentre elas, podem ser vistos como direitos inerentes aos seres humanos, independentemente da época ou do lugar, ou podem ser vistos como os direitos mais importantes em um determinado ordenamento constitucional.
> Do ponto de vista substancial, os direitos fundamentais são prerrogativas das pessoas necessárias para assegurar uma vida digna.
>
> [...]

Ainda sobre a Constituição, é importante mencionar, brevemente, sobre o remédio constitucional, *habeas data* (artigo 5º, LXXII). Constitui-se por uma ação constitucional para a) verificar informações relativas à identidade do requerente, constantes de cadastro ou ficha de órgão público ou órgão público; b) para o tratamento de dados, quando não tenha sido escolhido para o fazer através de procedimentos confidenciais, judiciais ou administrativos.

Salienta-se que, em vista das leis infraconstitucionais, tem-se o Código Civil, o Código de Defesa do Consumidor (CDC), o Marco Civil da Internet (MCI) e a Lei Geral de Proteção de Dados (LGPD). (MAGRANI, 2019, p. 56)

É preciso voltar ao mundo do pensamento dos dados, das decisões algorítmicas e do fortalecimento das relações entre os homens e as coisas relacionadas a essa última tendência, principalmente no que diz respeito à privacidade e ao uso de dados sensíveis dos usuários. A

Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/18 foi aprovada em 14 de agosto de 2018 e entrou em vigor em 2020.

Segundo o teórico Danilo Doneda (2019, p. 39), a proteção de dados é como uma garantia de caráter instrumental, a qual deriva da tutela da privacidade, mas não se limitando a isso, que se refere a todas as garantias básicas encontradas no ordenamento jurídico brasileiro. Desta forma, o autor pontua:

> A proteção de dados pessoais é uma maneira indireta de atingir um objetivo último, que é a proteção da pessoa. Ao estabelecer um regime de obrigações para os responsáveis pelo tratamento de dados, bem como de direitos para os titulares destes, não se está meramente regulando um objeto externo à pessoa, porém uma representação da própria pessoa. Os dados pessoais, por definição, representam algum atributo de uma pessoa identificada ou identificável e, portanto, mantêm uma ligação concreta e viva com a pessoa titular destes dados. Os dados pessoais são a pessoa e, portanto, como tal devem ser tratados, justificando o recurso ao instrumental jurídico destinado à tutela da pessoa e afastando a utilização de um regime de livre apropriação e disposição contratual destes dados que não leve em conta seu caráter personalíssimo. Também destas suas características específicas deriva a consideração que, hoje, diversos ordenamentos jurídicos realizam, de que a proteção de dados pessoais é um direito fundamental — uma verdadeira chave para efetivar a liberdade da pessoa nos meandros da Sociedade da Informação. (DONEDA, 2019, p. 39)

Assim, nota-se que os dados pessoais dos indivíduos estão ligados aos direitos da personalidade dos usuários. Para que haja a efetiva tutela desse direito, bem como da dignidade humana, é necessária a garantia da tutela dos dados pessoais.

2.1 A TUTELA DOS DADOS PESSOAIS NO CÓDIGO DE DEFESA DO CONSUMIDOR

O Código de Defesa do Consumidor (CDC) contém disposições que visam garantir a segurança e o sigilo dos consumidores, caso sejam considerados de risco para a relação de consumo. No que se refere à segurança, o artigo 4º, II, d, do CDC estabelece como objetivo da Política Nacional de Relações de Consumo um ato de governo capaz de assegurar o consumidor com segurança. “produtos e serviços com padrões adequados de qualidade, segurança, durabilidade e desempenho”. Isso quer dizer que o governo tem o dever de intervir para proteger o consumidor. (MAGRANI, 2019, p. 63)

Segundo o artigo 6º, II CDC, “a educação e divulgação sobre o consumo adequado dos produtos e serviços, assegurados a liberdade de escolha e a igualdade nas contratações” possui proveito à Internet das Coisas. É necessário trazer informações claras aos consumidores sobre os riscos que o uso de determinado dispositivo e sobre as informações que são coletadas por meio deste. Diversos dispositivos de IoT, os quais são conectados à internet, dispõe de violação à proteção da vida, saúde e segurança contra riscos provocados por práticas no fornecimento de produtos e serviços considerados perigosos ou nocivos”, o qual está previsto no inciso I do artigo 6º do CDC. (MAGRANI, 2019, p. 64)

Além disso, o CDC, em seu artigo 43, contém informações e cadastros de consumidores. Este dispositivo traz um sentido amplo de forma que para acessar todos os dados pessoais do consumidor. O consumidor tem o direito de controlar suas informações pessoais e qualquer tratamento para isso deve ser comunicado ao consumidor de forma transparente. É possível monitorar rigorosamente a distribuição de suas informações pessoais. (BIONI, 2019)

Segundo Bruno Miragem (2017), o desenvolvimento da IoT induz a revisão de entendimentos já consolidados. Ao que tange a exata qualificação do fato que dá causa a deveres e responsabilidade, concomitantemente tem-se um produto e há um fornecedor, a divisão dos regimes de responsabilidade nem sempre se mostra clara 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, 2017)

Frisa-se que os dispositivos da IoT podem falhar e isso é esperável. De tal modo que é preferível que haja a falha o quanto antes com o intuito que seja reparado em tempo para que não haja danos em grande escala. Assim, a interpretação do CDC deve ser realizada por meio de uma interpretação extensiva, distinguindo os riscos intrínsecos daqueles excepcionais, “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)

Em suma, no Código de Defesa do Consumidor os direitos com acesso, retificação e cancelamento e os princípios como transparência, qualidade e limitação temporal, no contexto de proteção de dados, envolvem o consumidor visando a possibilidade de assegurar ao consumidor o pleno exercício de controle sobre suas informações pessoais. (BIONI, 2019)

2.2 O MARCO CIVIL DA INTERNET E A LACUNA LEGISLATIVA PARA REGULAMENTAR A IOT

Além disso, como outra legislação que regulamenta a IoT, tem-se o Marco Civil da Internet (MCI), Lei número 12.965/2014, que abarca princípios, garantias, direitos e deveres para o uso da internet no Brasil. Dentre os direitos previstos, busca-se a proteção da privacidade e dos dados pessoais. Antes da sua promulgação, havia uma lacuna no ordenamento jurídico quando se trava de direitos fundamentais como a liberdade de expressão. Essa ausência legislativa ocasionou em diversas decisões judiciais conflitantes, buscando o embasamento em leis penais, o último remédio para conduzir a ordenação de condutas sociais. (MAGRANI, 2019, p. 73)

O artigo 7º do MCI definiu essencial o acesso à internet para o exercício da cidadania, este mesmo artigo abarca muitos direitos aos usuários da internet no Brasil e proteção à privacidade de diversas formas.

O artigo 8º, por sua vez, trata da liberdade de expressão e privacidade como circunstância para o exercício do direito de acesso à internet. Tem-se que a no inciso I "inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação"; inciso II a inviolabilidade e o sigilo de comunicação pela internet; inciso III das comunicações privadas armazenadas e inciso IV exceto por ordem judicial. (MAGRANI, 2019, p. 75)

Vale destacar também o artigo 10 da referida Lei, dispõe de modo mais específico a proteção de dados pessoais, de modo que, em suma, os detentores dos meios de comunicação privada e de dados pessoais devem cuidar para manter a intimidade, privacidade, honra e imagem das vítimas direta ou indiretamente.

Verifica-se que o MCI dispõe expressamente sobre a indispensabilidade do consentimento do titular para a coleta, uso, o armazenamento e o tratamento de seus dados pessoais, tal como para transferência a terceiros. (BIONI, 2019)

Vê-se, portanto, a necessidade do consentimento expresso, livre e informado sobre o tratamento de dados pessoais, o qual mostra-se ineficaz diante dos termos de usos abusivos. (MAGRINI, 2019, p. 79)

As tecnologias relacionadas a IoT e inteligência artificial (AI) são reguladas pelo MCI, isso porque um dos principais objetivos da Lei é apoiar às inovações e novas tecnologias, conforme o artigo 4º, III. Apesar disso, esta não é suficiente para salvaguardar o cidadão dos possíveis abusos que possam ocorrer no mundo de IoT e AI. O MCI é apenas aplicável no âmbito online, não sendo aplicável no mundo físico. (MAGRANI, 2019, p. 78)

Além disso, o MCI não aborda conceitos importantes para evitar a coleta, má gestão e monetização de dados. De modo que o texto legislativo deixa em aberto definições como “dado pessoal” e “dados sensíveis” que posteriormente serão tratados na Lei Geral de Proteção de Dados. (MAGRANI, 2019, p. 78)

Assim, visando a insuficiência legislativa de tutelar a proteção de dados em meio digital, sobretudo, no tocante à relação entre mundo físico e virtual, que são os dispositivos da IoT e AI, foi completada pela entrada em vigor da Lei Geral de Proteção de Dados. Salienta-se, ademais, que o MCI e CDC permanecerão exercendo o papel de tutela, na medida de sua abrangência.

É possível notar, portanto, que o Direito é demasiadamente atrasado em relação à desenvoltura social, especialmente tecnológica. Ora, a internet está cotidianamente presente na vida dos indivíduos desde os anos 90, e somente após 30 anos entra em vigor uma Lei que efetivamente

regulamenta os dados pessoais dos usuários. Dessa forma, o autor Nelson Camatta Moreiro (2007, p.179) salienta que:

> [...] A dogmá-tica 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.

Assim, mostra-se que o Direito possui inúmeros desafios para ter sincronia com os avanços sociais. Contudo, a LGPD representa como um grande avanço ao que tange a regulamentação de dispositivos como IoT, o que deve-se observar como será feita a efetiva fiscalização e punição dos controladores, uma vez que são inúmeras possibilidades de mitigar os efeitos do tratamento de dados pessoais sem a observância da lei.

3 O TRATAMENTO DE DADOS PESSOAIS NA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E A UTILIZAÇÃO DA INTERNET DAS COISAS

A Lei Geral de Proteção de Dados aborda a percepção de que qualquer dado pessoal tem importância e valor, assim, a Lei institui o conceito amplo de dado pessoal, de igual forma definido no Regulamento europeu, *General Data Protection Regulation* (GDPR), o qual foi estipulado como informação relacionada a pessoa natural identificada ou identificável. (TEFFÉ, 2020, p. 2)

Segundo Danilo Doneda (2019), os dados pessoais possuem referência ao que tange a informação, contudo, esses possuem peculiaridades a serem observadas. O dado pode ser apresentado como informação em estado potencial, ou seja, anterior a transmissão. Dessa forma, o dado estaria correlacionado a uma categoria de "pré-informação", que antecede à interpretação e a um processo de elaboração. A informação, por seu turno, consiste na refinação de conteúdo, mesmo sem aludir ao seu significado, esta carrega um sentido instrumental, de forma que aponta algo além da representação estabelecida no dado.

A informação pode ser classificada em quatro modalidades: (i) as informações relativas às pessoas e seus patrimônios; (ii) as opiniões subjetivas das pessoas; (iii) as obras do espírito e, por fim, (iv) as informações que descrevem fenômenos, coisas e eventos. Quanto ao presente estudo, vamos abordar somente a primeira modalidade. (CALATA, 1983, p.22 *apud* DONEDA, 2019)

O Conselho da Europa, na Convenção de 108, de 1981, estabeleceu que a informação pessoal é "qualquer informação relativa a um indivíduo identificado ou identificável". Note-se que a informação pessoal pode ser caracterizada por fato de estar ligada a uma pessoa, podendo levar ao aspecto objetivo desta. (DONEDA, 2019)

Vale ressaltar que o dado pode ser de uma pessoa indeterminada, dado anônimo. Dado anônimo é aquele incapaz de revelar a identidade de uma pessoa, de modo que não possibilita, de forma objetiva, vincular o dado com determinada pessoa. (BIONI, 2015, p. 25)

Nesse cenário é de suma importância incluir a figura do banco de dados. Os bancos de dados são conjuntos de informações organizadas de acordo com uma determinada lógica. Este possui capacidade de armazenar grande volume de informações, processá-las, instituí-las e combiná-las de diversas formas, em lapsos mínimos de tempo. Ademais, os bancos de dados permitem que informação pessoal possa ser agrupada em subcategorias e vinculadas a certos segmentos da vida de uma pessoa. (DONEDA, 2019)

Assim, a manipulação de dados, sobretudo com o advento da informação, instituiu-se a categoria dos dados sensíveis. Estes são uma espécie de dados pessoais os quais seu conteúdo é passível de discriminação, há preocupação de que certo tratamento poderá haver diferenciação por conta dos conteúdos dos dados, tais como dados que exprimem conteúdo racial, religioso, político, estado de saúde, orientação sexual ou filiação sindical. (BIONI, 2019)

Assim, a LGPD aborda o conceito de dado sensível que é "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" (artigo 5º, II, da LGPD). Vale-se dizer que esse rol é exemplificativo, pode-se incluir outras situações não elencadas.

Os dados sensíveis integram o denominado núcleo duro da privacidade, tendo em vista o conteúdo ser passível a discriminação, eles têm que ser tutelados de forma mais rígida. Constitui-se como dados sensíveis, em vista dos direitos e liberdades fundamentais, podendo colocar em risco tais direitos ao titular. (TEPEDINO, 2019, p. 307)

A instituição da categoria de dados sensíveis se deu devido à percepção da diferença dos efeitos do tratamento desses dados em comparação aos demais. A tutela diferenciada dos dados sensíveis, se faz pela aplicação do princípio da igualdade material. (DONEDA, 2019)

Nesse mesmo sentido, o inciso II, do artigo 5º, da LGPD aborda sobre dados biométricos, estes são dados captados a partir de corpo físico, ou, então, certos comportamentos pessoais. Esses dados abordam informações precisas sobre determinada pessoa de modo que é possível identificá-la rapidamente, em vista de suas características únicas e singulares, tais como: biometria e reconhecimento facial. (MENDES, 2009, p.19)

A prática de tratamento de dados biométricos é demasiadamente difundida pelo país, em diversos setores utilizam-se a tecnologia de reconhecimento facial como meio de segurança tanto para o consumidor ou para o acesso a repartições públicas. (COSTA, 2020)

Em outros casos, os dados biométricos podem ser coletados como forma de captar as emoções dos usuários. A título de exemplo, o aplicativo *TikTok*, em junho de 2021, incluiu, nos termos de privacidade, uma seção que permite ao aplicativo coletar identificadores e informações biométricas dos usuários, os quais inclui expressões faciais e voz. Essa coleta é realizada, sem que o titular tenha consentido de forma expressa, assim como a LGPD determina. Além disso, o aplicativo não deixa claro a finalidade que esses dados são coletados, podendo ser comercializados, sem a devida anuência do usuário.

Dessa forma, frisa-se que LGPD dispõe, como regra geral, que "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 (artigo 1º, da LGPD) que deve ter uma base legal para fundamentar os tratamentos de dados pessoais que operar, bem como a observância dos princípios.

Isso significa que terá que necessariamente ocorrer o encaixe do tratamento formulado em pelo menos uma das hipóteses legais de modo que seja considerado legítimo e lícito, passível de cumulação, assim como a GDPR. Há, contudo, as hipóteses de exclusão previstas no artigo 4º da referida Lei, estas serão regidas por legislações específicas. (TEFFÉ, 2020, p. 3)

3.1 PARTES ENVOLVIDAS

É essencial, para análise da Lei Geral de Proteção de Dados, a identificação correta das partes envolvidas no processo de proteção de dados pessoais, atribuindo-lhes os direitos e deveres de cada um no processo de tratamento de dados pessoais. (BURKART, 2021, p. 42)

Inicialmente, tem-se o titular dos dados que constitui uma pessoa física que fornece seus dados pessoais em uma relação de consumo ou serviço. O controlador, por sua vez, consiste na pessoa

física ou jurídica que recebe os dados pessoais de um titular para executar algum tratamento dos dados fornecidos. Este possui o dever de transparência e de proteger a privacidade dos titulares dos dados.

Existe também o operador que é uma pessoa jurídica ou física contratada pelo controlador para manipular os dados dos titulares, o operador realiza efetivamente o tratamento dos dados sob as ordens do controlador. Além disso, tem-se o encarregado (DPO), também contratado pelo controlador, o qual possui a função de intermediar a comunicação do titular com o controlador. A LGPD determina que o DPO apresente as informações de contato necessárias de forma clara e transparente para que o titular possa entrar em contato quando necessário. (BURKART, 2021, p. 43)

Por fim, a Autoridade Nacional de Processamento de Dados (ANPD) que é o órgão do Governo criado para fiscalizar a de acordo com a LGPD durante o tratamento de dados pessoais. Instituiu-se a responsabilidade de aplicação de multas e pela realização de auditorias, verificando se há a devida observância da LGPD dentro das organizações. É válido salientar que esse órgão ainda está em estruturação, apesar da vigência legislativa.

3.2 HIPÓTESES LEGAIS PARA FUNDAMENTAR OS TRATAMENTOS DOS DADOS PESSOAIS

O sistema legal projetado para o tratamento de dados fornece ao titular ferramenta para gerenciar suas informações pessoais e garantir direitos. Salienta-se que o rol do artigo 7º e do artigo 11 são taxativos, apesar de demonstrar amplos e com certo grau de subjetividade, como, por exemplo, o legítimo interesse. Das bases legais são 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 objetivo analisar os requisitos para o tratamento de dados na LGPD, com ênfase nas bases legais pertinentes ao contexto de IoT e b*ig data*, quais sejam: o consentimento e ao legítimo interesse, além disso, mostrar as diferenças de tratamento para dados sensíveis.

A base legal do consentimento do titular assegura ao controlador que o titular dos dados concedeu o tratamento de seus dados para determinado fim específico ou pré-estabelecido. Tal consentimento deve ser exposto ao titular dos dados de forma clara e transparente, visando a ausência de dúvidas por parte do titular. (BURKART, 2021, p. 47)

O consentimento do titular, mostra-se como uma peça chave no cenário tecnológico atual, tendo em vista a manipulação em massa dos dados pessoais e a comercialização destes. É necessário, portanto, que haja uma interpretação do consentimento de forma restritiva de modo que não pode o agente estender a permissão para o tratamento de dados transferindo-os para outros meios além daqueles já acordados, para momento futuro ou de outra finalidade. (TEFFÉ, 2020, p. 6)

Desta forma, não é possível considerar um consentimento genérico para o tratamento de dados pessoais, apenas com a especificação de sua finalidade. Assim, pode-se observar que é neste sentido que a LGPD se posiciona sobre o consentimento, em seu artigo 8º, §4º, a ver:

> 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**. (Grifou-se)

Em vista da consequência da aplicação do princípio da finalidade, pode-se atrelar ao princípio da informação a ser analisado ao redor do consentimento. A informação aduz a uma inteira consciência do titular sobre o destino de seus dados pessoais, partindo do pressuposto da autorização do tratamento dos dados. Assim, o titular deve ter 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, 2019)

É importante salientar que a manifestação de vontade deve ser inequívoca, contudo, a lei não exige o consentimento escrito. Apesar de não ser necessária a formalidade do consentimento escrito, este não pode ser extraído da omissão do titular, mas sim de atos positivos que demonstram a real vontade. Assim, a Lei é expressa em estabelecer ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o dispositivo legal, em vista do princípio da responsabilização e prestação de contas. (TEFFÉ, 2020, p. 10)

Ao que tange a tutela dos dados sensíveis, a LGPD estabelece que se admite o tratamento dos dados desde que haja a expressão do consentimento de forma específica e destacada, e que indique as finalidades singulares, segundo ao artigo 11, I, da referida Lei. Além disso, segundo Rodotà, o consentimento do titular de dados sensíveis deve ser definido pela ausência de liberdade durante o exercício da vontade, em vista que se trata de um contratante vulnerável. (RODOTÁ, 2008, p. 90)

Ademais, a LGPD em seu artigo 11, 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 dos interesses públicos sobre os interesses particulares. Esse posicionamento, contudo, é fortemente criticado tendo em vista o direito crucial para o pleno exercício de direitos como igualdade, liberdade e privacidade. (MULHOLLAND, 2018, p. 168)

Um caso para se questionar a validade do consentimento em tratamento de dados sensíveis, trata-se dos modelos recentes da Smart TV, da marca Samsung, na política de privacidade da companhia que abarca sobre a captura e transmissão de dados sensíveis para terceiros, caso a função de captura de voz seja ativada. Ainda estabelece que: “por favor, esteja ciente que suas palavras incluírem dados pessoais ou outras informações sensíveis, essa informação estará entre os dados capturados e transmitidos para terceiros pelo uso de reconhecimento de voz”. (O GLOBO, 2015, *on-line)*

Veja que, nesse caso, não há uma expressão de consentimento destacada e específica do titular e a marca não indicou a finalidade singular que justifique o tratamento dos dados sensíveis, além de não se enquadrar na exceção disposta no artigo 11, II da referida Lei, havendo inequívoca inobservância desta.

Além disso, tem-se como outra hipótese legal o legítimo interesse que pretende permitir tratamentos de dados relevantes, que são diretamente ligadas a atividades praticadas pelo controlador e que podem ser fundamentadas. Essa base legal não possui uma finalidade específica, pode variar em cada caso concreto. Portanto, como os dados têm um certo nível de importância, deve-se considerar a finalidade, a necessidade e a proporcionalidade do uso dos dados do uso dos dados, para que um tratamento mais agressivo, inesperado ou abrangente,

reduza as chances de poder processar os dados com base no reconhecimento de interesse legítimo. (TEFFÉ, 2020, p. 14)

Esta hipótese legal seria adotada em situações em que seria (i) desnecessária para obter nova permissão para outros usos dentro de uma relação previamente estabelecida com o proprietário; ou (ii) quando terceiros: não tivessem meios de obter tal tipo de autorização ou esse tipo de interação inviabilizaria o processamento dos dados. (BIONI, 2019)

Esta base legal foi retirada da diretiva GDPR, foi feita uma análise que por ser flexível tornou-se relevante diante da emergência de tecnologias e momento pelo qual a economia se baseia no uso intensivo de dados. O legítimo interesse ganhou um status de "carta coringa regulatória". Contudo, mostrou-se um resultado negativo ao longo de sua vigência por não estabelecer critérios para sua utilização, tais como: (i) a falta de uma aplicação harmônica e consistente e (ii) o risco de o âmbito de inserção das outras bases legais ser defasado, em vista em que esta base legal poderia ser percebida como aquela mais flexível e menos restritiva que as demais. (BIONI, 2019)

Assim, foi-se criado o Grupo de Trabalho do artigo 29 que estabeleceu critérios para sua aplicação, que tinha por objetivo: (i) fornecer previsibilidade e segurança jurídica na aplicação dessa base legal em todo bloco econômico europeu; e (ii) evitar que o legítimo interesse fosse aberto à violação dos direitos e princípios da ordem, principalmente outras hipóteses legais para o tratamento de dados. (BIONI, 2019)

Foi-se popularizado quatro fases para a aplicação do legítimo interesse, interpretação sistemática dos artigos 6º, X, e 10 e 37 da LGPD, quais sejam: a) a verificação da legitimidade do interesse: situação concreta e finalidade legítima (artigo 10, *caput* e I da LGPD); b) necessidade: minimização e outras bases legais (artigo 10, §1º da LGPD); c) Balanceamento: impactos sobre o titular dos dados e legítimas expectativas (artigo 10, II, da LGPD); d) Salvaguardas: transparência e minimização dos riscos ao titular do dado (artigo 10, §§2º e 3º, da LGPD)

Dessa forma, é possível haver o balanceamento entre o direito do titular dos dados e quem faz uso das informações. De forma que é crucial quanto aferir se faz presente um interesse legítimo

é verificar se as legítimas expectativas e dos direitos fundamentais do titular foram garantidos e respeitados. (BIONI, 2019)

É válido salientar que a base legal do legítimo interesse não é aplicada em casos de tratamento de dados sensíveis, como estabelecido no artigo 11, §1º da LGPD. Visto que, como já bem explicado, essa base legal se justifica pela aplicação da proporcionalidade e quanto mais invasivo for o dado menor a chance de aplicação desta. Assim, em casos de tratamento de dados pessoais sensíveis por IoT, deve-se observar a aplicação das demais bases legais trazidas pela LGPD.

Além disso, como já exposto, o artigo 7º da LGPD apresenta 10 bases legais para o tratamento de dados pessoais, não há uma ordem hierárquica entre elas, apenas a utilização destas a cada caso concreto.

Quanto ao cumprimento de obrigação legal ou regulatória, esta base legal o controlador trata os dados para realizar qualquer obrigação legal a que ele esteja sujeito. Assim, esta base legal concede a possibilidade que a LGPD não entre em desacordo com outras leis do ordenamento pátrio. Permite que os dados sejam tratados somente quando a obrigação for indispensável, como por exemplo, obrigações trabalhistas e empresas do mercado financeiro que devem cumprir obrigações que poderão exigir tratamento de dados pessoais de seus clientes. (TEFFÉ, 2020, 22); (BURKART, 2021, 45)

Ao que tange o tratamento de dados pessoais pela administração pública de dados à execução de políticas públicas, esta base a administração pública pode tratar dados pessoais, contudo, são obrigados a aplicarem a transparência, a não ser que este tratamento seja tenha o objetivo de segurança pública, defesa nacional ou outras atividades necessárias no processo de investigação em que o titular do dado seja sujeito. O artigo 23 da A LGPD prevê o tratamento de dados pessoais por pessoas jurídicas de direito público para o exercício de poder legal ou cumprimento de obrigações legais de serviço público. (BURKART,2021, p. 46)

Ademais, o artigo 7º também traz a hipótese de tratamento de dados quando for para realização de estudos por órgão de pesquisa, devendo sempre que possível garantir a anonimização dos dados pessoais, utilizando apenas os conceitos gerais dos dados os quais perdem a possibilidade de relação direta ou indireta com o titular.

Diante desta base legal, analisaremos o caso que ocorreu em São Paulo. Uma loja da Hering foi investigada por coletar dados de clientes sem autorização prévia via tecnologia de reconhecimento facial. A empresa visava coletar os dados biométricos dos clientes para analisar a reação facial diante de roupas, calçados e acessórios vendidos pela marca. Dessa forma, a empresa poderia, a partir desses resultados, promover publicidade. (TECMUNDO, 2019, *on-line)*

A empresa negou a acusação e alegou que "não realiza reconhecimento facial, mas sim detecção facial, por meio da qual estima apenas o gênero, a faixa etária e o humor dos consumidores de forma anônima". E acrescentou que os dados não seriam tratados, armazenados ou compartilhados de modo externo, sendo considerados meramente estatísticos. (TECMUNDO, 2019, *on-line)*

Veja que, nesse caso, mesmo que a empresa não utilize os dados dos clientes para modo externo, os dados coletados constituem como dados sensíveis – há uma discriminação de gênero, faixa etária – e são dados biométricos. Há necessidade de consentimento do usuário para a mera captação deste e, ainda, que sejam respeitados todos os direitos do titular, como por exemplo, ter o acesso a esses dados e ter a confirmação da existência dos dados, bem como sua finalidade.

É possível notar que a empresa demonstra que os dados, apesar de dados sensíveis, constituem dados anonimizados, ou seja, quando há um processo de tratamento nos dados que não é possível a identificação do titular dos dados e utilizaria os dados como meramente estatísticos. Para tanto é necessário que a empresa utilize a base legal de pesquisa e respeite os princípios da transparência e finalidade.

Contudo, é questionável a utilização da base legal de pesquisa, uma vez que se trata de empresa de comércio que poderá desviar tais informações para comercialização destas por meio de publicidade. Deve-se, portanto, ater-se a fiscalização para que a Lei seja observada.

Outra hipótese que permite o tratamento de dados ocorre ocorra se for essencial para a execução do contrato ou processos relacionados ao contrato inicial em que o titular dos dados faz parte, a pedido do titular dos dados. Portanto, é possível, sem o consentimento do proprietário, processar os dados deste que são essenciais para a contratação. Por exemplo: informações

coletadas por instituições financeiras sobre uma determinada pessoa, antes de conceder crédito a essa pessoa. (TEFFÉ, 2020, p.25)

O exercício regular de direitos em processo judicial, administrativo ou arbitral, por sua vez, é a base legal ampla a qual permite o uso de dados pessoais em processos para produção de provas no processo judicial, uma parte contra a outra. Segundo a doutrina, em certos casos que entenda que determinados dados podem ser armazenados, desde que demonstrada necessidade e para determinado fim específico, neste caso, formação de provas para o processo judicial.

Além disso, há a proteção da saúde ou da incolumidade física do titular ou de terceiros como motivo para o processamento de dados pessoais. Esta base legal deve ser aplicada a casos certos e oportunos, e não pode ser considerada em circunstâncias normais. Por exemplo: o tratamento de dados importantes para parar a progressão de epidemias, como o recente incidente de COVID-19.

A hipótese de tratamento para tutela de saúde, por sua vez, permite o tratamento tão somente a profissionais de saúde, autoridade sanitária ou serviços de saúde. Esta base legal deve ter um cuidado devido aos dados dos titulares serem dados sensíveis. Há um grande questionamento se planos de saúde estão autorizados a tratar esses dados e quais riscos ao titular isso pode implicar.

Por último, trata-se de proteção do crédito, esta base legal tem por objetivo facilitar a concessão de crédito, visando aprimorar a análise de risco, bem como aquecer o mercado de consumo. A aplicação dessa base legal será interligada com o Código de Defesa do Consumidor, a Lei do cadastro positivo e as portarias do ministério da Justiça. (TEFFÉ, 2020, p. 27)

3.3 PRINCÍPIOS BASILARES PARA O TRATAMENTO DOS DADOS PESSOAIS

A Lei Geral de Proteção de Dados dispõe, em seu artigo 6º, princípios os quais necessitam ser cumpridos durante o tratamento dos dados pessoais em conjunto com as bases legais acima elencadas. Assim, a lei estabeleceu 10 princípios, em um rol exemplificativo –considera-se

todos princípios do ordenamento jurídico que podem ser invocados no caso concreto – os quais devem ser seguidos pelo controlador durante o tratamento de dados pessoais.

O princípio da finalidade, o qual estabelece que os dados devem ser coletados para determinados fins, específicos e legítimos. Os dados que serão tratados não poderão ter outra destinação para além daquela pré-estabelecida e devidamente informada de maneira clara ao titular dos dados.

O princípio da adequação, por sua vez, está intimamente ligado ao princípio da finalidade, uma vez que deve haver compatibilidade do tratamento com as finalidades informadas ao titular, observando o contexto do tratamento. Assim, esse princípio refere-se à relação lógica da conformidade que se demonstra entre o tratamento e a finalidade objetivada. (BURKART, 2021, p.47)

Ademais, tem-se o princípio da necessidade, o qual estabelece que a coleta de dados deve ser essencial para a devida finalidade estabelecida, de modo que tem que ter a mínima coleta possível com a abrangência, proporcionais e não excessivos em relação às finalidades do tratamento.

Além disso, tem-se o princípio da transparência, este princípio é caro ao que tange o tratamento de dados pessoais pois abarca sobre a necessidade de todas as informações devem ser passadas ao titular de forma clara, precisas e verdadeiras, além de serem facilmente acessíveis sobre a realização do tratamento e respectivos agentes de tratamento, exceto segredos comerciais e industriais.

A título de exemplo na inobservância desses princípios em dispositivos IoT, a assistente virtual da Amazon, Alexa, é programada para captar a voz dos usuários e executar comandos, tais como colocar músicas, falar notícias, clima, dentre outras diversas possibilidades.

Segundo Tuohy (2022), em publicação na The Verge, os estudos de estudantes da Universidade de Washington, UC Davis, UC Irvine e Universidade de Northestern reconheceram diversas inconsistências na política de privacidade do dispositivo. De acordo com esse estudo, a Amazon coleta as informações por meio das interações com a assistente virtual, Alexa, e compartilha com as 41 empresas de propagandas parceiras da Amazon. (TOUHY, 2022) Essas informações

são, em suma, sensíveis e devem estar de acordo com as bases legais de consentimento – expresso e inequívoco – bem como visando os princípios da finalidade, necessidade, adequação e transparência.

Cabe ressaltar, ademais, o princípio do livre acesso aos dados pelos titulares, dispõe que o titular tem o direito de consultar facilmente e integralmente os dados em que o controlador detenha a seu respeito sem que tenha que pagar para tanto, ou seja, se forma gratuita.

O princípio da qualidade dos dados, prevê que os dados devem estar sempre atualizados para a garantia da exatidão, clareza e relevância destes, sendo observados os princípios da necessidade e finalidade do seu tratamento.

Nessa toada, tem-se o princípio da segurança que estabelece que se deve utilizar medidas técnicas e processos administrativos capazes de proteger os dados pessoais de acesso não autorizado e em caso de acidente ou invasão ilegal, perda, conversão, comunicação ou distribuição. Esse princípio prevê a mitigação de situações de risco dos dados armazenados, são medidas relacionadas a procedimentos internos de segurança, como por exemplo, impedir invasão externa por meio de bloqueios. (BURKART, 2021, p.47)

O princípio da prevenção também prevê a adoção de medidas com o objetivo de prevenir a ocorrência de danos decorrentes do tratamento de dados pessoais. Este princípio procura, de forma preventiva, proteger os dados pessoais para efeitos de gestão de risco e gestão de risco dentro da organização.

O princípio da não discriminação, ademais, estabelece que não pode ocorrer a realização do tratamento de dados com a finalidade discriminatório ilícita ou abusiva. Esse princípio está intimamente ligado com os dados pessoais sensíveis. (BIONI, 2019)

Tais princípios – segurança, prevenção e da não discriminação – são de suma importância quando se trata de dispositivos IoT e tratamento de dados sensíveis. Em um estudo realizado pela *Check Point Software Technologies* concluiu-se que aumentou 45% os ataques a empresas do segmento de saúde no mundo (CHECK POINT, 2021, *on-line).* Mostra-se a vulnerabilidade dos dispositivos de Internet das Coisas no setor de saúde, deve-se observar tais princípios pois

a violação destes não afeta apenas o tratamento de dados sensíveis dos pacientes – titulares – mas também a saúde.

Assim, a observância desses princípios acima elencados é essencial para mitigar os danos que eventualmente podem ocorrer aos titulares, não apenas pacientes em leito hospitalar, mas todos os que utilizam dispositivos IoT.

E, por fim, tem-se o princípio da responsabilização disposto no inciso X, do artigo 6º, da LGPD. Esse princípio abarca sobre a demonstração pelo responsável pelo tratamento – controlador ou operador – objetificando a comprovação da observância e cumprimento das normas de proteção dos dados pessoais, bem como a inclusão de medidas eficazes. (BURKART, 2021, p. 48)

3.4 A IMPORTÂNCIA DA GARANTIA DOS DIREITOS DO TITULAR

Salienta-se que é essencial demonstrar os direitos instituídos pela LGPD ao titular dos dados. São garantia que o titular possui e que pode ser solicitado ao controlador de dados devendo atender às indagações de forma célere e precisa, contudo, a Lei não estabelece um prazo para a entrega das solicitações.

A confirmação da existência de tratamento, consiste na possibilidade do titular, sem que haja justificativa, confirmar a existência de tratamento de seus dados pessoais. Esse direito tem como base o princípio da transparência, exposto no artigo 6º da referida Lei. A lei europeia dispõe, de forma expressa, em seu artigo 13 e 14 da GDPR, a obrigatoriedade de apresentar informações dos dados que são recolhidos junto ao titular, além dos que não são coletados. (MALDONADO, 2019)

Quanto ao direito de acesso aos dados, o titular poderá ter acesso aos dados e também as informações referentes a eles, quais sejam: 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, 2019)

O titular possui o direito de saber para qual finalidade os seus dados estão sendo processados, indicando todos os tipos de procedimentos existentes, bem como saber as categorias as quais seus dados estão classificados. Além disso, o titular poderá saber quais destinatários o controlador dos dados enviou os dados do titular solicitante, caso o controlador tenha enviado os dados para outras empresas, é necessário o rastreio dos compartilhamentos de informações feitas pelo controlador. (BURKART,2021, p. 52)

Quanto a este direito do titular, diante da distorção da real finalidade da coleta de dados pessoais dos titulares os quais são usados majoritariamente para fins de comercialização, é imprescindível a garantia desse direito em vista da massiva manipulação dos dados. Assim, Sartori e Bahia (2019, p. 232) salientam:

> [...] 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.

Ademais, quanto ao período previsto, este trata-se do período que o controlador reter as informações, bem como a justificativa do motivo pelo qual utilizará determinado tempo para manipular as informações. A existência de direitos específicos, por sua vez, caso haja a utilização dos dados tutelados por um direito específico, como Código de Defesa do Consumidor, o titular dos dados deve ter ciência desse direito. (BURKART, 2021, p. 52)

O titular deve poder, de forma simples e rápida, registrar uma reclamação e, para isso, deve haver um procedimento de reclamações. Além disso, o titular também deve ter o direito de ter ciência se seus dados foram captados por outra fonte. Quanto à existência de tomada de decisão automatizada, o titular deve ter o direito de saber os processos automatizados e como essas decisões são tomadas. (BURKART,2021, p. 52)

A preservação da dignidade humana e os dados pessoais possuem uma íntima ligação e representam a sua personalidade, comprovando o direito de corrigir os dados incompletos, incorretos ou desatualizados. Os direitos acima referidos, nomeadamente, ter conhecimento sobre a existência do tratamento e acesso aos dados, demostram-se como medida importante no pleno uso da correção. (KORKMAZ, 2021)

A possibilidade de obter a correção de seus dados pode ser observada como uma das expressões da autodeterminação informativa, a qual está presente em todo ciclo do fluxo informacional. Assim, as correções, a complementação e a atualização dos dados pessoais mostram-se como ferramentas imprescindíveis para permitir que o indivíduo seja representado de forma real e fidedigna. Esse direito, quando bem exercido, pode impedir que ocorra reflexos de um tratamento de dados defasado, como no tratamento das decisões automatizadas. (KORKMAZ, 2021)

Ainda, a LGPD garante ao titular a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados de forma que viole os ditames legais. Quanto à anonimização, segundo artigo 12 da referida Lei, os dados anonimizados não serão considerados dados pessoais pelo titular não ser pessoa identificada ou identificável de maneira permanente e irreversível. (MALDONADO, 2019)

Assim, o titular pode solicitar a anonimização, de forma que aquele dado passar por um processo que desvinculará a pessoa com a informação. Sendo possível também a retirada da anonimização do dado e, segundo 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”.

Quanto ao bloqueio dos dados, disposto no artigo 5º, inciso XIII, da LGPD, estabelece que cabe ao titular requerer expressamente que seus dados sejam suspensos provisoriamente de qualquer operação de tratamento, armazenamento do dado pessoal ou do banco de dados. Além disso, a remoção dos dados desnecessários, em excesso ou processados em violação a Lei acima mencionada, é válido destacar que diante de uma sociedade hiperconectada, a coleta de dados atualizados se faz de maneira célere e fácil. (KORKMAZ, 2021)

Como outro direito do titular, a portabilidade relativa às informações do próprio titular sofreu alteração pela Lei 13.853/2019, a qual adveio da Medida provisória 869/2018 que converteu em lei ordinária. A modificação se deu pela transferência da expressão "de acordo com a regulamentação da autoridade nacional" para o centro da formulação, de forma que com a nova redação é possível entender que a regulamentação em questão se refere ao regramento da própria portabilidade e sua requisição. (MALDONADO, 2019)

Em síntese, o direito diz respeito à obtenção dos dados pessoais de forma estruturada de modo que possibilite a transmissão para outro controlador. Esta é relativa ao próprio titular, preservando os segredos comercial e industrial. Assim, cabe ao titular, por livre opção, que possua similar contratação em concorrente. (MALDONADO, 2019)

A LGPD traz como opção a eliminação dos dados desnecessários, excessivos ou tratados em desconformidade com a Lei (inciso IV), como já abordado anteriormente, contudo, o inciso VI, do artigo 18, dispõe sobre o direito do titular em eliminar os dados que foram tratados de acordo com a base legal do consentimento.

Assim, o tratamento do dado se seu de forma lícita, no entanto, estes deveriam ser eliminados ao fim do tratamento. Frisa-se que apesar de não constar no artigo 5º, da LGPD, o processo de eliminação dos dados é definitivo. Além disso, tendo em vista a base legal do consentimento, o titular pode requerer a eliminação irreversível de seus dados, em qualquer momento, quando não quiser mais que seus dados sejam tratados. (KORKMAZ, 2021)

Ao que tange o direito de informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados, inicialmente, é preciso resgatar o conceito de uso compartilhado de dados, que está positivado 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;
>
> [...]

Assim, é assegurado ao titular ter ciência sobre seus dados tratados pelas entidades públicas e privadas com as quais o controlador compartilhou tais dados. Este direito está intimamente ligado ao princípio da transparência, bem como ao direito de informação e acesso aos dados.

Salienta-se que é preciso diferenciar o direito à informação do uso compartilhado e portabilidade, em vista que a portabilidade o titular requer a transmissão dos seus dados pessoais a outro controlador, ao passo que o uso compartilhado, o controlador transmite os dados sem a necessidade de solicitação do titular.

Ademais, o inciso VIII traz o direito da informação sobre a possibilidade de não fornecer o consentimento, as consequências da negativa do consentimento. Como já visto, o consentimento consiste nas bases legais para o tratamento dos dados, demonstrando que o titular é livre ao compartilhar seus dados aos controladores e, por lógica, este também possui o direito de não consentir sobre o tratamento de seus dados. (KORKMAZ, 2021)

A negativa de fornecimento do consentimento acarreta consequências, estas devem estar expressas antes do tratamento dos dados, de modo que o titular possa avaliar o mais conveniente. Nesse caso, a empresa pode restringir determinados acessos ao titular por não fornecer dados estritamente necessários para o uso, frisa-se que é vedado a restrição abusiva por parte de empresas. (MALDONADO, 2019)

Por fim, a LGPD prevê a possibilidade de revogação do consentimento para o tratamento de dados, disposto no artigo 8º, §5º. A revogação do consentimento está intimamente ligada ao livre desenvolvimento da personalidade, tendo em vista que este poder se encontra com próprio sentido de autodeterminação em relação ao consumo. (DONEDA, 2019)

A revogação do consentimento deverá ser expressa, contudo, apenas a revogação não resultará na cessação do tratamento se houver outra base legal para justificar esse tratamento.

Diante dos direitos que o titular possui sobre seus dados, analisaremos os riscos de dispositivos *wearables.* O *smartwatch* (relógio inteligente) é parte da dimensão que são os dispositivos *wearebles* ou, no português, vestível. Esses dispositivos inteligentes são capazes de averiguar os níveis de açúcar no sangue, contagem de passos, localização, frequência cardíaca, dentre outras possibilidades. (THE ONE BRIEF, *on-line)*

Segundo a The One Brief, empresas iniciaram a utilização desses dispositivos em seus funcionários, com o objetivo de melhorar a segurança e aumentar a produtividade destes. (THE ONE BRIEF, *on-line).* Há, portanto, uma preocupação quando à privacidade pois os empregadores podem obrigar seus empregados a aderirem a tecnologia e monitorar os dados sensíveis de seus funcionários. Assim, não seria observado o direito do titular de bloquear o tratamento dos seus dados ou removê-los quando assim entender melhor, por exemplo.

Nesse sentido, há a discussão sobre a legalidade da utilização desses dados em esferas trabalhistas pela possibilidade de o empregador deter os dados dos seus empregados. Por exemplo, a Liga Nacional de Futebol Americano (NFL – *National Football League*) possuem um programa em os melhores atletas podem vender seus dados biométricos para pessoas que buscam aprimorar o condicionamento físico. (THE ONE BRIEF, *on-line)*

Segundo a LGPD, a comercialização dos dados biométricos, intermediados por uma empresa, cujo titular está em posição de subordinação, devido o vínculo empregatício, deve ser questionada. Os dados biométricos, como já visto, são dados sensíveis e o titular deve anuir de forma expressa e inequívoca sobre seu tratamento. Em uma relação empregatícia o titular poderá anuir para que seu vinculo de emprego seja mantido. Portanto, entendo que a comercialização de dados, em um contexto brasileiro, é ilegal.

Em outro contexto, fora da seara trabalhista, é notório a problematização da comercialização dos dados pessoais sensíveis dos titulares, contudo, essa prática esta cada vez mais presente. Empresas que detém bancos de dados em números extraordinários como, Amazon e Google, são frequentemente questionadas sobre a comercialização dos dados de seus usuários.

CONSIDERAÇÕES FINAIS

A tecnologia da Internet das Coisas tem o intuito de melhorar a vida das pessoas por meio da automatização, tendo em vista as facilidades que a tecnologia traz que podem economizar tempo e dinheiro para os usuários, além de serem utilizadas em áreas imprescindíveis para tomadas de decisões.

Contudo, é notório que com a disseminação desses dispositivos tecnológicos, capazes de obter diversas informações em um lapso temporal irrisório e inseridos no nosso cotidiano, atrelado aos usuários - em meio móvel ou inseridos em casa – possuem um potencial de captar de diversas informações, sobretudo, com conteúdo discriminatório.

Dessa forma, a discussão iniciada buscou abarcar a relação entre a tecnologia dos dispositivos da internet das coisas e *big data* e os direitos da privacidade dos usuários, em especial, ao tratar-se da captura dos dados sensíveis.

Ficou demonstrado que a Lei Geral de Proteção de Dados, em conjunto com as demais legislações que tutelam os dados pessoais, busca, de forma significativa, proteger a sociedade contemporânea das violações da privacidade que enfrentamos, principalmente quanto à coleta, armazenamento e transmissão dos dados sensíveis, os quais a Lei determina a necessidade de ter um tratamento diferenciado, diante ao seu potencial lesivo.

Observou-se, por fim, que Internet das coisas e *big data* são tecnologias emergentes que devem estar em consonância LGPD e ter como base uma hipótese legal que justifique o tratamento de dados – rol taxativo – respeitando os direitos do titular e tendo como norte os princípios que regem o tratamento dos dados pessoas – rol exemplificativo.

Dessa forma, neste estudo são apresentados os diversos desafios ao tutelar os direitos com potencial de violação pela tecnologia a IoT e *big data*, principalmente, os desafios éticos, segurança e privacidade, bem como o caminho legislativo que o ordenamento jurídico enfrentou para a tutela desses direitos. É possível concluir que ainda há obstáculos na regulamentação dos dispositivos tecnológicos, especialmente quando se trata de punição, contudo, com a LGPD houve um significativo avanço para o devido controle regulatório.

REFERÊNCIAS

BIONI, Bruno Ricardo. **Xeque-mate**: o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil. São Paulo: GPoPAI/USP, 2015.

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

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

BRASIL. **Constituição da República Federativa do Brasil de 1998**. Brasília: Planalto, 1988 Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 24 maio 2022.

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: 24 maio 2022.

COSTA, R.V. **O uso da tecnologia de reconhecimento facial e a violação a dados biométricos sob a luz da Lei Geral de Proteção de Dados.** 2020.

_____. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências**. Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 11 set. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm.. Acesso em: 24 maio 2022.

_____. Decreto nº 9.854, de 25 de junho de 2019. Institui o Plano Nacional de Internet das Coisas e dispõe sobre a Câmara de Gestão e Acompanhamento do Desenvolvimento de Sistemas de Comunicação Máquina a Máquina e Internet das Coisas**. Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 25 jun. 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D9854.htm. Acesso em: 24 maio 2022.

_____. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 23 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm . Acesso em: 24 maio 2022.

_____. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial [da] República Federativa do Brasil, Brasília**, DF, 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 24 maio 2022.

FIGURELLI, Rogério. **Big Brain**: unindo Big Data e a Internet das Coisas para criar robôs cada vez mais inteligentes. 2 ed. 2016.

FRANCO, Carolina Mendes. **A pessoa humana resumida a um dado corporal**: considerações sobre o tratamento adequado aos dados biométricos. 2009. 121 f. Dissertação (Mestrado em Direito Civil Constitucional; Direito da Cidade; Direito Internacional e Integração Econômica; Direi) - Universidade do Estado do Rio de Janeiro, Rio de janeiro, 2009

INSTITUTE GARTER GROUP. **Big Data**. Disponível em: https://www.gartner.com/en/information-technology/glossary/big-data . Acesso em: 24 maio 2022.

KORKMAZ, M.R., SACRAMENTO, Mariana. DIREITOS DO TITULAR DE DADOS: POTENCIALIDADE E LIMITES NA LEI GERAL DE PROTEÇÃO **DE DADOS**. Rio de Janeiro: Revista Eletrônica. 2021

LEONARDI, Marcel. **Tutela e privacidade na internet**. São Paulo: Saraiva, 2011.

MANYIKA, J. **Big data: The next frontier for innovation, competition, and productivity**. Disponível em: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/big-data-the-next-frontier-for-innovation. Acesso em: 24 maio 2022.

MACHADO, Felipe Nery Rodrigues. **Big data: o futuro dos dados e aplicações.** São Paulo: Érica, 2018.

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

MALDONADO, V.N., BLUM, R. O. **LGPD Lei Geral de Proteção de Dados.** 2ª Ed. São Paulo. Revista dos Tribunais, 2020.

MACKINSEY GLOBAL INSTITUTE. **Big data: the next frontier for innovation, competition, and productivity**. 2011. Disponível em: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/big-data-the-next-frontier-for-innovation. Acesso em: 24 de maio 2022.

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

MULHOLLAND, C S. **Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados** (Lei 13.709/18). *Revista De Direitos E Garantias Fundamentais*, *19*(3), 159-180.

ORNELAS MONTEIRO, G. INSTRUMENTOS DE RECONHECIMENTO FACIAL E OS CONTORNOS DA LEI GERAL DE PROTEÇÃO DE DADOS ANTE A PRIVACIDADE NAS CIDADES (IN)INTELIGENTES. **Revista de Direito e Atualidades**, *[S. l.]*, v. 1, n. 1, 2021. Disponível em: https://www.portaldeperiodicos.idp.edu.br/rda/article/view/5220. Acesso em: 24 maioo 2022.

O GLOBO. **Samsung adverte: Cuidado com o que você diz em frente a sua TV inteligente**. Disponível em: https://oglobo.globo.com/economia/samsung-adverte-cuidado-com-que-voce-diz-em-frente-sua-tv-inteligente-15286181 . Acesso em: 24 maio 2022.

PEDRA, A.S. As diversas perspectivas do Direitos Fundamentais. **Revista de Direitos e Garantias Fundamentais** 2017.

REDAÇÃO DO PORTAL HOSPITAIS BRASIL. **Dispositivos hospitalares também necessitam de cibersegurança**. Disponível em:

https://portalhospitaisbrasil.com.br/dispositivos-hospitalares-tambem-necessitam-de-ciberseguranca>. Acesso em: 24 maio 2022.

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

SANTOS, Bruno P. et al. **Internet das coisas:** da teoria à prática. 2016.

SANTOS, Denise. **Internet das Coisas e *Big data*: a proteção dos dados pessoais sensíveis.** Curitiba, 2019. < Disponível em: https://juristas.com.br/wp-content/uploads/2020/10/ARTIGO-DENISE-DOS-SANTOS-UNIDOMBOSCO.pdf. Acesso em: 24 maio 2022.

SARTORI, E. C. M.; BAHIA, C. J. A. 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.

SINGER, Talyta. Tudo conectado: conceitos e representações da internet das coisas. **Simpósio em tecnologias digitais e sociabilidade**, v. 2, p. 1-15, 2012.

STEWARD, J. **21+ Internet of Things Statistics, Facts & Trends for 2021**. Disponível em: <https://findstack.com/internet-of-things-statistics/>. Acessado em: 24 maio 2022

TAURION, Cezar. **Big Data.** Rio de Janeiro: Brasport. 2013. ePUB.

TECMUNDO. **Hering é investigada por uso de dados de clientes via reconhecimento facial**. 2019. Disponível em: https://www.tecmundo.com.br/seguranca/145544-hering-investigada-uso-dados-clientes-via-reconhecimento-facial.htm. Acesso em: 24 maio 2022.

TEFFÉ, C.S, VIOLA, Mario. **Tratamento de dados pessoais na LGPD**: estudo sobre as bases legais. Civilista.com: 2020.

TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. O consentimento e proteção de dados na LGPD. In: _____. A lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro. São Paulo: Thomson Reuters Brasil, 2019.

THE ONE BRIEF. **Seus Dados na Palma da Mão: As Promessas e Armadilhas dos Dispositivos Wearables**. Disponível em: https://theonebrief.com/latam/portugues/post/seus-dados-na-palma-da-mao-as-promessas-e-armadilhas-dos-dispositivos-werables/. Acesso em: 24 maio 2022.

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: 24 maio 2022.