CENTRO UNIVERSITÁRIO ANTÔNIO EUFRÁSIO DE TOLEDO DE PRESIDENTE PRUDENTE

CURSO DE DIREITO

A INTERNET DAS COISAS E SUA INFLUÊNCIA SOBRE O DIREITO DE PRIVACIDADE

Laiane Santos Vieira

Presidente Prudente/SP

2020

CENTRO UNIVERSITÁRIO ANTÔNIO EUFRÁSIO DE TOLEDO DE PRESIDENTE PRUDENTE

CURSO DE DIREITO

A INTERNET DAS COISAS E SUA INFLUÊNCIA SOBRE O DIREITO DE PRIVACIDADE

Laiane Santos Vieira

Monografia apresentada como requisito parcial de Conclusão de Curso para obtenção do grau de Bacharel em Direito, sob orientação da Prof.ª Dra. Ana Carolina Greco Paes.

Presidente Prudente/SP

2020

A INTERNET DAS COISAS E SUA INFLUÊNCIA SOBRE O DIREITO DE PERSONALIDADE

Monografia aprovada como requisito parcial para obtenção do Grau de Bacharel em Direito.

_____

Prof.ª Dra. Ana Carolina Greco Paes

_____

Prof.ª M.ª Ligia Maria Lario Fructuozo

_____

Prof.ª M.ª Natacha Ferreira Nagáo Pires

Presidente Prudente, 25 de novembro de 2020.

Você tem que agir como se fosse possível transformar radicalmente o mundo. E você tem que fazer isso o tempo todo.

Angela Davis

Dedico esse trabalho ao meu filho amado, Pedro.

AGRADECIMENTOS

Agradeço a minha mãe, por ser meu suporte e minha força, por acreditar nos meus sonhos na mesma proporção que eu acredito, por cuidar com tanto amor de mim e do meu filho, sem ela eu não chegaria a escrever essas linhas, minha vitória só existe porque ela esteve ao meu lado.

Ao meu falecido pai, que jamais será esquecido, por todo apoio e amor incondicionais que recebi durante longos e felizes anos.

A minha irmã Daniele por ser a minha maior incentivadora e motivadora nos estudos, e por ser um ombro amoroso nos momentos em que pensei em desistir.

A minha irmã Lilian por ser inspiração, exemplo de luta e por ser a Dinda do meu pequeno, cuidando do meu filho como se dela fosse.

A minha irmã Elaine, cuja irmandade nasceu através de laços de amor e afeto, por iluminar minha mente e me ajudar em todos os aspectos da criação desse estudo.

A minha madrinha-mãe Dendenha, por cuidar de mim e do Pedro, pelo carinho em forma de bolo de fubá quentinho e pelo colo sempre bem-vindo.

Ao meu filho Pedro por ser tão paciente e amoroso mesmo tão pequeno. Obrigada por ter me escolhido e pela honra de ser sua mãe.

Agradeço a todos os professores, que contribuíram para meu desenvolvimento pessoal e profissional, especialmente à minha professora e orientadora Ana Carolina Greco Paes.

E por fim, a Deus, por ter colocado todas essas pessoas especiais e importantes na minha vida, e por ser sempre meu amigo fiel e refúgio.

RESUMO

A sociedade da informação e o veloz progresso tecnológico, que alteraram a troca de informações entre as pessoas, têm influenciado as relações sociais e o ordenamento jurídico. Neste cenário o direito à privacidade ganhou novos contornos e interpretações. O objetivo dessa pesquisa foi analisar as modificações e implicações causadas pela tecnologia da informação na privacidade dos indivíduos e a partir dessa análise estudar como a massiva utilização de uma nova tecnologia, a Internet das coisas, poderá lesar esse direito constitucionalmente consubstanciado. A metodologia adotada baseou-se em pesquisa bibliográfica envolvendo o estudo da influência da tecnologia nas relações econômicas, sociais e políticas, do direito de privacidade e de legislação pertinente a regulação do uso da tecnologia. A análise bibliográfica permitiu concluir que há certa inovação legislativa visando a proteção do direito de privacidade, mas que há muitos interesses envolvidos, na sociedade, nas organizações tecnológicas e no governo, que tornam a relativização desse direito um fenômeno a ser estudado. Por fim, esse trabalho possibilitou a visualização de um panorama de como a Internet das coisas poderá implicar nos direitos de personalidade.

Palavras-Chave: Privacidade. Direito fundamental. Tecnologia. Internet das Coisas. Sociedade da informação.

ABSTRACT

The information society and rapid technological progress, which has changed the exchange of information between people, have influenced social relations and the legal system. In this scenario, the right to privacy has gained new outlines and interpretations. The objective of this research was to analyze the changes and implications caused by information technology in the privacy of individuals and from this analysis to study how the massive use of a new technology, the Internet of things, could harm this constitutionally enshrined right. The methodology adopted was based on bibliographic research involving the study of the influence of technology on economic, social and political relations, the right to privacy and legislation relevant to the regulation of the use of technology. The bibliographic analysis allowed us to conclude that there is a certain legislative innovation aimed at protecting the right to privacy, but that there are many interests involved, in society, in technological organizations and in the government, which make the relativization of this right a phenomenon to be studied. Finally, this work enabled the visualization of a panorama of how the Internet of things can imply personality rights.

Keywords: Privacy. Fundamental right. Technology. Internet of Things. Information society.

SUMÁRIO

1 INTRODUÇÃO

Quando uma nova tecnologia é desenvolvida se espera que ela traga uma facilidade, uma melhora na qualidade de vida das pessoas e que contribua para o desenvolvimento da sociedade, foi assim com a internet, por exemplo, que reduziu distâncias tornando a comunicação mais rápida e fácil. No entanto, além dessa facilidade - por modificar drasticamente o modo das pessoas se comunicarem e essa modificação afetar toda a sociedade trazendo efeitos em vários âmbitos - o estudo de seus riscos e benesses passou a ser importante para entender o mundo e a dinâmica das relações atuais.

A tecnologia da informação causa na sociedade efeitos sociais, políticos e econômicos. Segundo Bioni (2020 p. 03) “a informação avoca um papel central e adjetivante da sociedade: *sociedade da informação*”.

> A informação é o (novo) elemento estruturante que (re)organiza a sociedade, tal como o fizeram a terra, as máquinas a vapor e a eletricidade, bem como os serviços, respectivamente, nas sociedades agrícola, industrial e pós-industrial. (BIONI, 2020, p.03)

Neste trabalho, buscamos analisar os efeitos de uma nova tecnologia, a internet das coisas, na atual era da sociedade da informação. Em um primeiro momento, demos foco aos efeitos, alterações e mudanças provocadas na privacidade dos indivíduos, quanto a tecnologia da informação em geral. Posteriormente mapeamos as possíveis violações à privacidade com a massificação da Internet das coisas.

A metodologia empregada se constituiu em pesquisa teórica exploratória, partindo de um levantamento bibliográfico que contou com livros e artigos sobre privacidade, transformações sociais trazidas pelo mundo tecnológico e Internet das coisas. Também utilizamos exemplos e fatos do mundo real como ferramenta para estimular a compreensão.

No que diz respeito as vertentes teórico-metodológicas, utilizou-se a linha da tecnologia social científica, “que converte o pensamento jurídico e sua produção em uma tecnologia voltada para questões sociais [...]” (GUSTIN; DIAS, 2013, p. 19) a partir da vertente jurídico-sociológica, através do raciocínio indutivo.

Tornamos o estudo mais específico, focado no direito de privacidade, pois pretendemos demonstrar a importância da discussão sobre a proteção do direito de privacidade e questionar a influência da tecnologia na relativização desse direito fundamental, já que ainda não sabemos quais os limites em que a tecnologia poderá influenciar em nossa vida privada e se os dispositivos que confiamos nossas informações são seguros. Dessa forma, entendemos que o assunto é relevante e influência muito intensamente na vida das pessoas, promovendo na mesma ordem modificações no ordenamento jurídico.

Eduardo Magrani (2019) explica que diante de um cenário onde há carência de regulação adequada do Direito vivenciamos uma autorregulação do próprio mercado, e que a tecnologia tem avançado mais rápido do que nossa habilidade de garantir a tutela dos direitos individuais e coletivos, ainda, segundo o autor:

> Neste contexto, é crucial debatermos as noções de privacidade, segurança e ética que deverão nortear os avanços tecnológicos, refletindo sobre o mundo em que queremos viver e em como nos enxergamos nesse mundo de dados e máquinas relacionado ao novo cenário de IoT e de Inteligência Artificial. (MAGRANI, 2019, p. 27)

Para compreender a relevância dos estudos dos impactos de uma nova tecnologia, entendemos que seria necessário demonstrar quais efeitos as tecnologias antecessoras causaram. Por esse motivo, após a introdução desse estudo o capítulo dois traçou uma linha histórica sobre o implemento e desenvolvimento de uma das tecnologias mais relevantes para o mundo atual, a internet, estudamos as tecnologias que se desenvolveram a partir dela até chegarmos à Internet das Coisas, e encerramos esse capítulo discorrendo sobre os reflexos dessas tecnologias na sociedade.

Em nosso terceiro capítulo passamos a delimitar nosso estudo. Discorremos sobre a privacidade sob a influência da tecnologia. Após demonstrar no capítulo dois que as evoluções tecnológicas impulsionaram modificações sociais, direcionamos nosso estudo para uma implicação específica, a violação da privacidade causada pela tecnologia. Entendemos que essa análise é pertinente já que a privacidade integra o rol de direitos fundamentais, que são pilares Constitucionais de suma importância para o respeito à dignidade da pessoa humana.

Nos tópicos seguintes passamos a entender também quais os dispositivos Constitucionais, leis e regulamentos visam proteger os direitos de privacidade.

No quarto capítulo apontamos as possibilidades de violações do direito de privacidade, dentro de um recorte estabelecido, o da ampla utilização da tecnologia Internet das coisas. Essa análise foi realizada através de exemplos e situações de violações que já ocorrem com o advento tecnológico.

2 EVOLUÇÃO HISTÓRICA DA TECNOLOGIA DA INFORMAÇÃO

A chamada sociedade da informação é uma das mais fortes expressões do mundo contemporâneo. Essa nova sociedade de comunicação traduz o efeito causado pelas mudanças tecnológicas na comunicação, nas estruturas industriais e nas relações sociais.

Toffler (2012), analisando o caminhar da civilização, estabeleceu três grandes ondas que trouxeram mudanças que afetaram drasticamente os caminhos da humanidade. A primeira onda caracterizada pelo implemento da agricultura, a segunda que viabilizou a sociedade industrial e a terceira onda, a da sociedade da informação.

> [...]enquanto o sistema de riqueza da Primeira Onda baseava-se essencialmente em coletar e consumir coisas que crescem na natureza, o da Segunda Onda em produzir coisas por meio de esforço físico e trabalho mecânico, o sistema de riqueza da Terceira Onda – que ganha força entre nós – está muito mais voltado para o pensar, conhecer, saber e experimentar os frutos do conhecimento. (TOFFLER, 2012, p. 40).

Portanto, essa sociedade da informação não traz apenas mudanças na comunicação, mas impacta o direito, que deve tutelar as relações acontecidas na rede mundial de computadores.

Kumar (1997), contestando a ideia de Toffler, afirma que a tecnologia da informação acelerou processos iniciados na era industrial e não há o estabelecimento de um novo princípio de sociedade ou advento de uma “terceira onda”. Como é possível observar em trecho extraído de sua obra:

> Na maioria das áreas, a tecnologia da informação acelerou processos iniciados algum tempo antes, facilitou a implementação de certas estratégias de administração de empresas, mudou a natureza do trabalho no caso de numerosas profissões e apressou certas tendências em lazer e consumo. Mas não produziu mudança radical na maneira como as sociedades industriais são organizadas ou na direção em que evoluem. Os imperativos de lucro, poder e controle parecem ser tão predominantes hoje como sempre foram na história do industrialismo capitalista. (KUMAR, 1997, p.191)

No entanto, o estudioso afirma que ocorreram mudanças significativas de paradigmas na evolução da sociedade industrial para a era digital, já que a

sociedade industrial tinha na mão de obra e na matéria prima seus principais insumos, e a sociedade da informação tem como seu principal insumo a informação:

> A sociedade de informação, segundo seus teóricos, gera mudanças no nível mais fundamental da sociedade. Inicia um novo modo de produção. Muda a própria fonte da criação de riqueza e os fatores determinantes da produção. O trabalho e o capital, as variáveis básicas da sociedade industrial, são substituídos pela informação e pelo conhecimento. A teoria do valor do trabalho, da maneira formulada por uma sucessão de pensadores clássicos, de Locke e Smith a Ricardo e Marx, é obrigada a ceder lugar a uma "teoria do valor do conhecimento". (KUMAR, 1997, p.51)

De similar raciocínio, também entende Pinheiro (2016, p. 70): "A autoestrada da informação está para a economia digital assim como a energia elétrica e as estradas estavam para a economia industrial". Ainda, a autora entende que "[...] informação é poder, como foi um dia a propriedade da terra" (PINHEIRO, 2016, p.70).

Kumar (1997) relata que a informação sempre teve seu monopólio, seja pela Igreja, classes do clero ou pela nobreza, só a partir do século XVII, com a revolução industrial, a pesquisa passou a ser incentivada, e, embora ainda restrita aos detentores de capital, foi um passo inicial para a ampliação do acesso à informação.

Sendo assim, sem nos aprofundarmos no conflito entre os estudiosos se a sociedade da informação causou ou não o impacto de uma revolução, é importante absorvermos do exposto que a informação passou a ser extremamente valiosa, e mais do que isso, acessível a todos, o que é notavelmente algo inédito e nunca vivido na humanidade.

Na era em que vivemos, as tecnologias passaram a ser desenvolvidas para permitir que o homem atuasse sobre a informação e a transformasse em conhecimento.

> A primeira característica do novo paradigma é que a informação é sua matéria-prima: são tecnologias para agir sobre a informação, não apenas informação para agir sobre a tecnologia, como foi o caso das revoluções tecnológicas anteriores. (CASTELLS, 1999, p.78)

A tecnologia passou a ser uma ponte que tornou o conhecimento e sua obtenção possíveis. "Quando a informação é configurada em padrões mais

elaborados e complexos, chegamos ao que se pode chamar de conhecimento[1].” (TOFFLER, 2012, p. 142)

Portanto, estamos vivenciando uma inovação na forma de nos relacionar e construir a informação a fim de buscar maneiras eficientes de otimizar, produzir e alcançar o conhecimento.

E quando falamos sobre a otimização do acesso à informação, um dos adventos tecnológicos mais significativos das últimas décadas, que nos projetou ao patamar evolutivo em que nos encontramos, sem dúvidas foi a internet. A internet construiu o cenário ideal para a propagação da informação.

Desenvolvida primordialmente pelo departamento de defesa dos Estados Unidos em 1969, a internet nasceu no ambiente militar com o desenvolvimento da ARPANET[2] , que tinha como objetivo estimular a pesquisa em computação. “A origem da Internet remonta ao ápice da ‘guerra fria’, em meados dos anos 60, nos Estados Unidos da América do Norte, e foi pensada, originalmente, para fins militares” (PECK, 2016, p.62).

> [...] todos os desenvolvimentos tecnológicos decisivos que levaram à Internet tiveram lugar em torno de instituições governamentais e importantes universidades e centros de pesquisa. A Internet não teve origem no mundo dos negócios. Era uma tecnologia ousada demais, um projeto caro demais, e uma iniciativa arriscada demais para ser assumida por organizações voltadas para o lucro (CASTELLS,1999, p.26)

Na sequência o departamento de defesa norte-americano juntou-se a um centro de pesquisa californiano, a Rand Corporation, para o desenvolvimento de uma rede de comunicação descentralizada. Após avanços no desenvolvimento da tecnologia, em 1975, a ARPANET foi transferida para a agência de defesa e comunicação com o objetivo de tornar a comunicação por computador acessível aos diferentes ramos das forças armadas.

Só em 1990, a ARPANET foi retirada de operação e abriu-se caminho

---

[1] Informação diz respeito a dados que foram processados, por meio eletrônico, mecânico ou manual e que produziu um resultado com significado. O conhecimento é a ampliação da informação pois além de ter um significado tem uma aplicação, conhecimento são informações processadas.

[2] A ARPA foi formada em 1958 pelo Departamento de Defesa dos Estados Unidos com a missão de mobilizar recursos de pesquisa, particularmente do mundo universitário, com o objetivo de alcançar superioridade tecnológica militar em relação à União Soviética na esteira do lançamento do primeiro Sputnik em 1957. A Arpanet não passava de um pequeno programa que surgiu de um dos departamentos da ARPA, o Information Processing Techniques Office (IPTO), fundado em 1962 com base numa unidade preexistente.

para a privatização da internet, que passou a ser denominada INTERNET como atualmente conhecemos, e cresceu rapidamente em uma expansão jamais vista.

> [...] Mas há algo de especial no caso da Internet. Novos usos da tecnologia, bem como as modificações reais nela introduzidas, são transmitidos de volta ao mundo inteiro, em tempo real. Assim, o intervalo entre o processo de aprendizagem pelo uso, e de produção pelo uso, é extraordinariamente abreviado, e o resultado é que nos envolvemos num processo de aprendizagem através da produção, num feedback intenso entre a difusão e o aperfeiçoamento da tecnologia. Foi por isso que a Internet cresceu, e continua crescendo, numa velocidade sem precedentes, não só no número de redes, mas no âmbito de aplicações. (CASTELLS,1999, p.29)

A internet e sua interface arquitetada para que a informação fosse não só recebida, mas modificada e criada, se popularizou em larga escala por proporcionar a qualquer pessoa a possibilidade de domínio da informação.

A partir de 1970, com a chegada do microprocessador[3], tornou possível seu uso na esfera privada, em nossas casas e escritórios. Assim como a internet, o computador também nasceu em ambiente militar[4]. Carvalho e Lorena (2017) explicam que as primeiras aplicações dos computadores serviram para decifrar códigos secretos usados pelos nazistas.

Carvalho e Lorena (2017) relatam que a primeira geração de computadores foi desenvolvida a partir de 1942 e era baseada nas tecnologias de circuitos e válvulas eletrônicas, eram enormes e consumiam muita energia, já na segunda geração (1959-1965) a válvula deu lugar ao transistor, seu tamanho já era 100 vezes menor do que o da primeira geração, tornando mais propício o uso comercial. Na terceira geração (1965-1975) desenvolveu-se os circuitos integrados, foi nesse momento que os chips foram criados e propagou-se a utilização de computadores pessoais, até a chegada da quarta geração de máquinas (1975-1980) caracterizada pelo uso do microprocessador e o surgimento do Personal Computer, o computador pessoal.

A redução de seu tamanho, já que o primeiro computador pesava toneladas e ocupava uma sala inteira, facilitou o processo de introdução de seu uso

---

[3] O microprocessador, minúscula partícula de silício que centraliza o processamento em um computador e onde eram condensadas centenas de transistores, os mesmos elementos que faziam os computadores ocupar grandes espaços foram reduzidos.

[4] O MARK I, foi criado e desenvolvido durante a segunda guerra mundial e foi o primeiro projeto de computador, posteriormente o ENIAC, considerado o primeiro computador eletrônico, pesava 30 toneladas e foi desenvolvido para o cálculo de tabelas balísticas para o exército americano.

no nosso dia a dia, desde então, eles têm se tornado cada vez mais portáteis e acessíveis de qualquer lugar.

De acordo com Carvalho e Lorena (2017) a quinta geração de computadores (1980 até o momento atual) é marcada pelo desenvolvimento da inteligência artificial, a redução de seu tamanho a miniaturas, somados a um maior desempenho e maior capacidade de armazenamento que proporcionaram o ápice de sua popularização.

2.1 Novas Tecnologias de Informação e Comunicação

Em 1989, surge a *world wide web* – www, através de um pequeno projeto de pesquisa concebido pelo físico inglês Tim Bernes Lee[5], criando a rede mundial de computadores que foi o acelerador da globalização da Internet.

E assim, a velocidade dos recursos tecnológicos foi crescendo rapidamente até́ chegarmos à Banda Larga (broadband). Atualmente, tem se tornado cada vez mais comum encontrar pontos de acesso à internet com conexão Wi-fi, e banda larga cada vez mais eficientes e velozes[6], tornando possível nos cercar de Internet onde quer que estejamos.

Ademais, o desenvolvimento do computador e a popularização da internet trouxeram uma gama de novas tecnologias e muitos dispositivos foram criados a fim de facilitar o acesso e tornar eficaz e eficiente a comunicação e troca de informações. O cenário passou a ser caracterizado pelo uso intensivo de softwares, aplicativos e dispositivos. De acordo com Castells (2007, p.119/120) “os produtos das novas indústrias de tecnologia da informação são dispositivos de processamento de informação ou o próprio processamento de informações”.

> Ao transformarem os processos de processamento da informação, as novas tecnologias da informação agem sobre todos os domínios da atividade humana e possibilitam o estabelecimento de conexões infinitas entre

[5] O WWW nasceu em Genebra, criado por Tim Bernes Lee e R. Cailliau e é composto por hipertextos, que são informações textuais combinadas com imagens, sons, organizadas de forma a promover uma leitura (ou navegação) não-linear, baseada em indexações e associações de ideias e conceitos, sob a forma de links.

[6] Países e multinacionais estão correndo para se adaptar a tecnologia 5G que permitirá downloads superiores a 1Gbps (gigabits por segundo), proporcionando inclusive a conversa entre máquinas.

> diferentes domínios, assim como os elementos e agentes de tais atividades. (CASTELLS, 2007 p.120)

Chegamos ao patamar de desenvolvimento tecnológico que nos proporciona o que chamamos hoje de interatividade. A interação em tempo real configura o mais alto valor aplicado a sociedade da informação, além de receber a informação é possível interagir com ela, cria-la, ou seja, participar ativamente.

E é nisso que as novas tecnologias vêm se embasando, em tentar proporcionar o ápice da interatividade, e o foco agora é que o mundo em que nos rodeia também possa ser interativo, os objetos possam se conectar, proporcionando uma interface objeto-pessoa, objeto-objeto, pessoa-pessoa.

Conseguimos perceber a busca pela interface interativa na mudança do conceito de itens comuns do nosso dia a dia. Automóveis possuem computadores de bordo e gps, a telefonia celular alterou sensivelmente sua orientação, não produzindo apenas telefones mas smartphones com acesso à internet, e as televisões que antes não forneciam nenhuma interatividade, o telespectador era apenas receptor, estão conectadas à rede, o que foi uma manobra inteligente pois tenderiam a desaparecer.

Kumar (1997, p.192) afirma que há um movimento em direção à sociedade centrada no lar: “A tecnologia da informação, dirigida por um conjunto inteiro de grandes interesses empresariais, tem sido posta cada vez mais a serviço do consumo baseado no lar”

O entretenimento, a aprendizagem a distância, o teletrabalho, todos facilitados pelo advento da tecnologia da informação têm trazido as pessoas para seus lares e estimulando a utilização de ferramentas tecnológicas que os torne altamente conectados. Dentro dessa abordagem, já tem se desenvolvido cidades e casas inteligentes, espaços altamente inovadores que tem como objetivo principal proporcionar o ápice de interatividade e conectividade.

Sendo assim, diante do panorama narrado uma nova sociedade emerge, a sociedade em rede, e novas maneiras de se comunicar são estabelecidas.

> A sociedade em rede, em termos simples, é uma estrutura social baseada em redes operadas por tecnologias de comunicação e informação fundamentadas na microelectrónica e em redes digitais de computadores que geram, processam e distribuem informação a partir de conhecimento acumulado nos nós dessas redes. (CASTELLS, 2007, p.19).

Esse conceito de sociedade em rede é aplicado em todos os campos,

na economia, no trabalho, na globalização, na comunicação, na mídia, na cultura, ou seja, o mundo tornou-se interligado em redes. Castells (2007) define rede como “um conjunto de nós interconectados” onde todo nó é importante para a rede, independentemente de seu grau de relevância.

Com o novo paradigma de comunicação, jornais e livros impressos são substituídos, já que os meios digitais possibilitam uma interação maior e acesso ilimitado a informação. As redes sociais nascem[7], as mídias digitais crescem cada vez mais, as relações se desenvolvem a partir, e de acordo com o meio tecnológico.

Portanto, pessoas passaram a ser ferramentas importantes no compartilhamento de dados, elas criam as redes sociais e as abastecem com conteúdo o tempo todo. Desse modo, a informação, já anteriormente citada como o insumo mais importante desse milênio, toma novos contornos e seu valor cresce exponencialmente.

De acordo com a revista britânica The Economist[8], o recurso mais valioso do mundo não é mais petróleo, e sim dados. Atualmente, as cinco mais valiosas organizações mundiais são da área de tecnologia e mercado digital, são elas o Google, a Amazon, o Facebook, a Apple e a Microsoft (THE, 2017).

Não se trata apenas de criar um dispositivo, como por exemplo, a Apple, que desenvolveu o i-phone, e sim de torna-lo ferramenta capaz de armazenar, compartilhar e transferir dados. É a possibilidade de tratar os dados que dá o valor ao dispositivo e não o dispositivo em si, como foi outrora.

2.2. A Internet das Coisas

A internet das coisas, ou *Internet of things*, em inglês (utiliza-se a sigla Iot), termo que foi inicialmente apresentado por Kevin Ashton[9] em uma apresentação para a Procter & Gamble em 1999, surge como mais uma forma de utilização da

[7] “No início dos anos 2000, o uso da Internet mudou de um modelo de consumidor para um de interação social entre pares. Inicialmente, a maioria das informações na Internet era fornecida por produtores, organizações como companhias de mídia. Um usuário individual consumia informações, mas não produzia. Por volta do ano 2000, sites como Myspace, Facebook e YouTube determinaram que qualquer usuário poderia criar conteúdo, e um usuário típico passou a carregar mais dados” (COMER, 2016, p.512/513).

[8] A The Economist é uma revista britânica especializada no mercado econômico.

[9] Pesquisador Britânico do Massachusetts Institute of Technology (MIT)

internet, dessa vez tornando os objetos, cotidianos ou industriais, programáveis e capazes de interagir com humanos e outros dispositivos.

Há muitas definições em relação ao termo internet das coisas. Analisando-o sintaticamente, encontramos as palavras: internet e coisas. Conforme já anteriormente explicado o termo “Internet”, se refere a tecnologia aplicada para fins de comunicação e “Coisas”, de acordo com o dicionário Michaelis, trata-se de “Um objeto inanimado em oposição a um ser vivo”.

Atzori, Iera e Morabito (2010, p. 2.788) explicam que a imprecisão em torno do termo é justamente consequência de seu nome e de acordo com os autores, semanticamente, internet das coisas significa uma rede mundial de objetos interconectados com base na comunicação padrão de protocolos. Resumindo, objetos inteligentes e conectados.

A *International Comunication Union*[10] (especificado na recomendação ITU-T Y.4000 / Y.206006/2012) elaborou a seguinte definição: “Uma infraestrutura global para a sociedade da informação, possibilitando serviços avançados interconectando coisas (físicas e virtuais) com base em informações e comunicações interoperáveis existentes e em evolução”.

Sendo assim, a Iot estende a utilização da Internet atual, trazendo uma nova dimensão ao seu uso e aplicação, passando assim a interligar objetos. Essa nova dimensão de uso da internet, o acréscimo de processamento, memória e comunicação dos objetos envolvidos torna-os inteligentes e automatizados, viabilizando seu controle mesmo remoto e permitindo que os próprios objetos sejam acessados e conectados uns com os outros.

Essa nova tecnologia relaciona-se com a evolução denominada Web 3.0[11] que mantêm as características da internet da forma com que a conhecemos mas traz como novidade elementos de inteligência artificial, que além de gerar e armazenar informações, passa também a interpretá-las.

A primeira ideia de Iot que nos vem à mente é o uso das *smart tvs*, cada vez mais populares nos lares brasileiros, mas não se limita ao uso residencial, se aplica a diversos setores da economia, como indústria, agricultura, logística, saúde,

[10] A *International Telecommunication Union* (ITU) é a agência especializada das Nações Unidas na área de telecomunicações, tecnologias de informação e comunicação (TICs).
[11] Termo criado pelo jornalista John Markoff, do jornal *New York Times,* para explicar a evolução da internet que permite além da interação de pessoas o cruzamento de dados.

automação comercial, dentre outros. As máquinas inteligentes utilizarão sistemas capazes de monitorar, coletar, mudar, analisar e integrar dados e informações essenciais e estratégicas, será uma revolução imensa para a indústria.

Quando um cliente solicita um determinado produto, quantidade e características específicas desse produto são transmitidas às máquinas e os dispositivos de Iot comunicar-se-ão entre si em cada etapa do processo, trocando essa informação também com sistemas de gestão, que acompanharão em tempo real toda a produção, atuando com eficiência diante de qualquer problema ou deficiência.

Após concluída a produção, informações sobre quantidade e detalhes do produto já estarão disponíveis para todos os setores, do comercial à logística, que em posse dessas informações tomarão decisões estratégicas com mais precisão e agilidade.

Quanto a aplicação residencial, como anteriormente citado, há uma grande tendência na busca pelo consumo baseado no lar e as casas inteligentes já são uma realidade.

Magrani (2018) explica que com os dispositivos Iot será possível, por exemplo, sinalizar a chegada do morador em casa, destravar o sistema de segurança, ativando o ar condicionado, acendendo luzes, abrindo cortinas, ligando a cafeteira. Os aparelhos se conectarão entre si, e a geladeira, por exemplo, fará a lista de compras da semana, com os itens faltantes e avisará sobre seu consumo de energia ou se apresenta alguma falha ou defeito em seu sistema.

Diante de tantas perspectivas de aplicação da Iot, estima-se, de acordo com pesquisa recente da *Cisco*[12], com o advento da internet das coisas em poucos anos a medida de dados atual – o Gigabyte, que equivale a um trilhão de bytes, dará lugar ao Zettabyte, equivalente a um sextilhão de bytes (CISCO, 2016). É um implemento de proporções astronômicas, que tem gerado muito interesse econômico, já que como anteriormente explanado, dados são muito valiosos.

Em 2017, o BNDES, em parceria com o Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC), apoiou a realização de um estudo para o diagnóstico e a proposição de um plano de ação estratégico para o país para a Iot denominado: “Internet das coisas – um plano de ação para o país.

[12] A Cisco Systems, Inc. é uma companhia transnacional estadunidense sediada em San José, Califórnia, especializada em tecnologia da informação e redes.

Esse estudo foi dividido em etapas, teve seu início em janeiro de 2017 e sua conclusão em março de 2018. O estudo revelou que o impacto que essa tecnologia causaria no país até 2025 em termos econômicos representaria 10% do PIB, e que muitas oportunidades se abririam.

Tal estudo foi o início para tornar o país um lugar propício e seguro para o desenvolvimento da tecnologia Iot e assim atrair investidores do mundo todo.

Sendo assim e por entender que a Internet das Coisas é uma das grandes promessas de inovação tecnológica do futuro, estudaremos suas possíveis implicações sobre os direitos de personalidade.

2.3. A Tecnologia e seus reflexos na sociedade

As relações jurídicas são modificadas e influenciadas por mudanças no âmbito social, econômico e político. A tecnologia promoveu mudanças tão drásticas e decisivas para o avanço da sociedade, conforme demonstraremos, que o estudo e conhecimento dessas mudanças se torna necessário para que possamos entender e lidar com as implicações causadas pela evolução da tecnologia da informação.

Para Paesani (2013), a discussão e a reflexão sobre a sociedade da informação e seus reflexos é de extrema importância para compor as regras que possibilitam a vida em sociedade, conforme trecho extraído de sua obra:

> A sociedade da informação ou do conhecimento demanda uma reflexão sobre a cultura, a justiça e o profundo sentido das regras. Sem o respeito das regras não poderemos conviver em sociedade. Mas, sem uma discussão pública sobre a razão das regras, a vida em sociedade não se projeta em direção ao futuro. É por esse motivo que a discussão sobre as regras inclui o modelo de sociedade em que as regras se inspiram. (PAESANI, 2013, p.23)

Atualmente mede-se a evolução social e econômica de uma nação através do acesso da população à tecnologia. Pinheiro (2016, p.70), assevera que, “globalmente, a presença de tecnologia passa a ser um novo fator de análise de subdesenvolvimento”. Ou seja, a riqueza e desenvolvimento de uma nação passa a ser medida através de sua produção e acesso à tecnologia. Em suas palavras:

> Na Era Digital, o instrumento de poder é a informação, não só recebida mas refletida. A liberdade individual e a soberania do Estado são hoje medidas pela capacidade de acesso à informação. Em vez de empresas, temos organizações moleculares, baseadas no Indivíduo. A mudança é constante e

> os avanços tecnológicos afetam diretamente as relações sociais. (PINHEIRO, 2016, p.74)

Magrani (2014, p.68), afirma que diversos diplomas no Brasil e no mundo têm optado pela urgência do debate pelo reconhecimento de um novo direito fundamental, o direito a inclusão digital, onde a internet estará à disposição de todos. “[...] deve ter seu acesso garantido a todos os cidadãos, sob pena da exclusão digital significar, diretamente, a condição de subcidadania.

A busca pela massificação do acesso à internet, assim como aconteceu com a televisão, o rádio e o telefone, visam tornar a internet democrática, possibilitando que a emissão e recepção de informações estejam ao alcance de todos. Segundo Castells (1999), se espera que a internet seja importante instrumento para a promoção da democracia.

> Esperava-se que a Internet fosse um instrumento ideal para promover a democracia — e ainda se espera. Como dá fácil acesso a informação política, permite aos cidadãos ser quase tão bem-informados quanto seus líderes. Com boa vontade do governo, todos os registros públicos, bem como um amplo espectro de informação não sigilosa, poderia ser disponibilizado on-line. A interatividade torna possível aos cidadãos solicitar informação, expressar opiniões e pedir respostas pessoais a seus representantes. Em vez de o governo vigiar as pessoas, as pessoas poderiam estar vigiando o seu governo — o que é de fato um direito delas, já que teoricamente o povo é o soberano. (CASTELLS, 1999 p. 128)

A ciberdemocracia, expressão impulsionada pelos estudos de Levý (2002), cria um novo paradigma de participação social nas decisões do Estado. Nesse aspecto, a cidadania é exercida de forma digital, exige-se transparência das instituições, acesso à notícias e atualizações governamentais que devem ser facilmente encontradas em portais e sites institucionais do governo, além do mais, a possibilidade de participar mais ativamente da tomada de decisões, propondo ideias, debatendo e articulando discussões.

Outra expressão nascida na era da sociedade em rede, é a Cibercultura[13]. Cibercultura é o maior exemplo de como as mudanças tecnológicas influenciam na sociedade ao ponto de alterar seu alicerce cultural, de engendrar novos

[13]Cibercultura, ou seja, o conjunto tecnocultural emergente do final do século XX, impulsionado pela sociabilidade pós-moderna em sinergia com a microinformática e o aparecimento das redes telemáticas mundiais. Ou uma forma sociocultural que modifica hábitos sociais, práticas de consumo, ritmos de produção e difusão de informação, criando outras formas de relações de trabalho, lazer, sociabilidade e comunicação social (LEMOS; LEVY, 2010, p. 21-22).

costumes e novas formas de socialização.

De acordo com Lemos e Levy (2010) a cibercultura é uma expressão da cultura contemporânea marcada pelas tecnologias digitais que se tornaram parte de nosso dia a dia, como por exemplo o *Internet banking*, celulares e o imposto de renda eletrônico. É a cultura contemporânea sofrendo influência direita da evolução tecnológica.

Quanto a interação social, a internet e seu uso proporcionaram novas formas de socialização, Zygman e Raud (2018, p. 84) acreditam que a tecnologia está causando um distanciamento e individualização do ser humano. Conforme trecho extraído de sua obra “criar e romper vínculos on-line é imensamente mais fácil e menos arriscado do que off-line”.

O que é evidente é que as redes sociais têm garantido o ápice do exercício da liberdade de expressão e manifestação de opinião, já que a internet proporciona um ambiente altamente democrático. É diante desse cenário que os direitos passam a se colidir, passa-se a buscar limites entre a liberdade de expressão e a privacidade, entre a liberdade de expressão e o direito à honra e reputação, por exemplo, evidenciando que além das benesses a rede pode causar dezenas de violações.

Em relação à influência no ordenamento jurídico sabe-se que as relações jurídicas se originam das leis e das relações humanas, e que novas formas de interação social inovam o ordenamento jurídico criando direitos e deveres.

O Direito não é estático, o ordenamento jurídico vive em constante transformação de modo a se adequar às demandas da sociedade, refletindo assim seu desenvolvimento econômico, político, cultural e social.

> [...] o modelo jurídico começa a se transformar para viabilizar o exercício de cidadania digital, seja através de ferramentas de peticionamento ou plebiscito online, ou ainda para garantir o direito de estar conectado à Internet como um novo direito essencial do indivíduo. (PINHEIRO, 2016, p.74)

Isso porque em uma sociedade altamente tecnológica o direito de estar conectado passa a ser fundamental já que aquele que não o está, está a margem. É o que visa garantir a Lei 12.965/14 em seu art. 7°:

> 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;
> 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;
> 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.

De acordo com Paesani (2014) a importância da liberdade informática no desenvolvimento democrático das sociedades contemporâneas está sintetizada de forma positiva na recomendação n° 854, emitida pelo Parlamento Europeu de 1979, onde é enunciado que somente uma sociedade informatizada pode ser uma sociedade democrática.

> Essa afirmação fundamenta-se na consciência de que o processo democrático está profundamente comprometido com a forma de circulação das informações, ou melhor, a disponibilidade de acesso a todos os cidadãos apresenta-se como pré-requisito do processo (PAESANI, 2014, p. 08).

E por fim, outra importante modificação causada pela tecnologia, e uma

das mais pertinentes para o estudo em questão, é a vigilância. Os dispositivos tecnológicos, a internet e as redes sociais propiciam uma maior exposição, visibilidade e possibilidade de acesso a dados pessoais pelas organizações tecnológicas, tornando a vigilância um dos mais importantes debates trazidos pela evolução tecnológica.

Rodotá (2008) explica que vivemos em uma sociedade de vigilância onde as dimensões jurídicas acerca da privacidade foram afrouxadas mundo afora, reduzindo-se as garantias fundamentais. Para o autor depois do atentado de 11 de setembro nos Estados Unidos a privacidade passou a ser um obstáculo para a segurança pública, que se tornou prioridade frente à privacidade. Sobre o assunto, também discorre Fernanda Bruno:

> A expansão da videovigilância, notável nos grandes centros urbanos após os atentados de 11 de setembro de 2001 nos Estados Unidos, reorganiza as relações entre segurança e vigilância. Elas não mais focalizam populações e espaços classificados como perigosos ou suspeitos, mas se dirigem a toda sorte de espaço público, semipúblico e privado. Paralelamente, o fluxo de informações que circula no ciberespaço se torna um foco privilegiado de monitoramento por diversos setores e segundo diferentes propósitos: comercial, publicitário, administrativo, securitário, afetivo, entre outros. Ações e comunicações cotidianas no ciberespaço se tornam cada vez mais sujeitas a coleta, registro e classificação. Colocam-se, de imediato, questões sobre as implicações destes dispositivos para a vigilância, o controle e a formação de saberes específicos sobre desejos, inclinações, condutas e hábitos de indivíduos e populações. (BRUNO, 2013, p.9)

Deveras, nossos computadores e celulares captam nossos dados através de toda e qualquer interação que realizamos, seja através de uma compra online, na utilização de redes sociais ou do *gps*. Esses dados compõem informações muito relevantes sobre nossos hábitos, preferências, lugares que frequentamos e comportamentos, e são eles a matéria prima das empresas de tecnologia.

Sobre o assunto, Bioni (2020, p. 102) explica que os dados pessoais são o ativo que alimenta e movimenta a economia e são a base para sustentação de uma série de modelos de negócios e para a formulação de políticas públicas, e, portanto, a sociedade se torna refém desse fluxo informativo. “Não é à toa que se fala em ‘morte da privacidade’, crise ou erosão da intimidade.

As empresas justificam que o usuário, quando assina os termos e condições de utilização de serviços de tecnologia, autoriza a manipulação de seus dados. No entanto, Rodotá destaca que há uma desigualdade de forças que torna o

usuário vulnerável:

> Raramente o cidadão é capaz de perceber o sentido que a coleta de determinadas informações pode assumir em organizações complexas e dotadas de meios sofisticados para o tratamento de dados, podendo escapar a ele próprio o grau de periculosidade do uso desses dados por parte de tais organizações. Além disso é evidente a enorme defasagem de poder existente entre o indivíduo isolado e as grandes organizações de coleta de dados. (RODOTÁ, 2008, p.37)

Zuboff (2018) revela que há uma nova modalidade de capitalismo, o capitalismo de vigilância, onde as grandes corporações de tecnologia oferecem serviços gratuitos, que automaticamente nos conectam e nos inserem a um mundo de informações, mas ao mesmo tempo monitoram e extraem dados sensíveis sem consentimento do usuário.

> O trabalho da vigilância, ao que parece, não é corroer os direitos de privacidade, mas sim redistribuí-los. Em vez de um grande número de pessoas possuindo alguns direitos de privacidade, esses direitos foram concentrados no interior do regime de vigilância. Os capitalistas de vigilância possuem amplos direitos de privacidade e, portanto, muitas oportunidades para segredos. Estes são cada vez mais utilizados para privar as populações de escolha no que diz respeito a que partes de sua vida desejam manter em sigilo. (ZUBOFF, 2018, p. 48).

Ainda, a autora explica que as leis regulamentadoras e a compreensão pública ficaram defasadas em relação ao rápido desenvolvimento tecnológico e a grande habilidade dessas organizações de vigiar para o lucro. “Como resultado, os direitos à privacidade, uma vez acumulados e afirmados, podem então ser invocados como legitimação para manter a obscuridade das operações de vigilância”. (ZUBOFF, 2018, p. 48).

Sendo assim, a tecnologia promoveu mudanças sociais, políticas e econômicas positivas e negativas que causaram implicações nas relações jurídicas e afetaram direitos e garantias individuais. Essas mudanças tão velozes que vão se modificando a cada inovação tecnológica devem ser estudadas, é importante entender quais direitos foram criados, sopesados ou violados e de que maneira o ordenamento jurídico deve inovar para acompanhar esses avanços.

Por entender que uma das grandes implicações da evolução tecnológica é em relação ao direito de privacidade e por ser o objeto do nosso estudo,

analisaremos a influência da tecnologia sobre os direitos de privacidade no próximo capítulo.

3 A PRIVACIDADE SOB A INFLUÊNCIA DA TECNOLOGIA

Na visão de Gilmar Mendes (2018) a reclusa periódica a vida privada é uma necessidade de todo homem, para a sua própria saúde mental. O jurista entende que sem a privacidade o indivíduo não encontra condições para o desenvolvimento da livre personalidade e que estar submetido a constante observação alheia dificulta o enfrentamento de novos desafios.

Ainda, Mendes (2018) revela que não obstante a importância da privacidade, quando se trata de definir exatamente o que seja o direito à privacidade, doutrina e jurisprudência não são uníssonas. “Mesmo os diplomas legais ou as convenções internacionais não cuidam de precisar o conceito, que tampouco parece encontrar univocidade no acervo de jurisprudência do direito comparado”. (MENDES, 2018, p. 286).

> O direito à privacidade, em sentido mais estrito, conduz à pretensão do indivíduo de não ser foco da observação por terceiros, de não ter os seus assuntos, informações pessoais e características particulares expostas a terceiros ou ao público em geral. (MENDES, 2018, p.288)

O fato é que a privacidade no campo jurídico foi primeiramente entendida como o “direito de estar só”, esse conceito levava o Estado a um não fazer, tratando-se de direitos de primeira geração, direitos negativos em que se impelia o estado a não interferir na vida privada do indivíduo. A primeira vez que a expressão direito de estar só surgiu foi com o artigo *“The Right of Privacy”*[14] de Samuel D. Warren e Louis Brandeis (1890).

> Alegam os autores desse antológico estudo que sua intenção seria perscrutar a eventual existência de um princípio legal que amparasse a pretensão de alguém de proteger sua intimidade e, na hipótese de existir esse amparo legal, definir qual a natureza e o real alcance de tal proteção. Warren e Brandeis utilizam no seu estudo, além da expressão right to privacy, também uma outra para designar o direito à intimidade. Trata-se da locução right to be let alone. (BENTIVEGNA, 2020, p. 148)

[14] Artigo jurídico escrito por Samuel Warren e Louis Brandeis, publicado em 1890 na revista Harvard Law Review e reconhecido como a primeira publicação americana a reconhecer o direito à privacidade.

Posteriormente, o direito à privacidade foi consubstanciado e reconhecido como direito humano na Declaração Universal dos Direitos Humanos de 1948[15], e trazido de forma genérica no texto Constitucional brasileiro, desdobrando-se em direito a intimidade, imagem, dados, informações, domicílio e comunicações.

> A privacidade posta em termos como “um direito de ser deixado só”, que teve seu marco inicial com o ensaio apresentado pelos professores Samuel Warren e Louis Brandeis, datado de 1890 e publicado na Revista de Direito da Universidade de Harvard, nos remetendo ao antigo paradigma de zero-relationship, hoje decai frente ao surgimento de um novo centro gravitacional que leva em conta as contingências sociais: a possibilidade de cada indivíduo controlar o uso de informações que lhe dizem respeito (RODOTÀ, 2008, p. 24).

Conforme a Constituição Federal nos traz, os direitos de personalidade integram o rol de direitos fundamentais, são eles: a intimidade, a vida privada, a honra e a imagem. Conforme art.5°, X.

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

O texto Constitucional cita a intimidade e a vida privada, o que nos leva a entender que são coisas distintas. Bentivegna (2020) explica que há parte da doutrina que se refere a ambos *lato sensu* como direito à privacidade, integrando à privacidade tanto a vida privada quanto a intimidade.

Outros entendem pela teoria dos círculos concêntricos, onde a intimidade seria menos ampla e a vida privada mais ampla. Moraes, P (2019) entende que o direito à privacidade é delimitado por três esferas concêntricas e sobrepostas. A esfera social, que comporta fatos que são suscetíveis do conhecimento de todos, a esfera privada, que compreende fatos que podem ser compartilhados com um número restrito de pessoas e a esfera individual ou íntima, parte reservada a si, onde o

[15] Declaração Universal dos Direitos Humanos de 1948, em seu art. XII: “Ninguém será sujeito a interferências na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataques à sua honra e reputação. Toda pessoa tem direito à proteção da lei contra tais interferências ou ataques”.

indivíduo não compartilha seus fatos. Ainda, no contexto atual da sociedade da informação, o autor insere a “privacidade informacional”:

> O cenário da sociedade da informação, na qual a tecnologia é usada para a coleta, produção, processamento, transmissão e armazenamento de informações, resultou nas definições de “privacidade informacional” ou poder de controle e proteção, na conjuntura da Internet, ao tratamento automatizado de dados pessoais e de “privacidade decisional” ou poder de autodeterminação no tocante a exposição, no contexto dos reality shows, à divulgação de fatos da vida privada (MORAES, P, 2019, p. 197).

De acordo com Moraes (2019) os conceitos constitucionais de intimidade e vida privada embora sejam interligados, podem ser diferenciados, sendo a intimidade relacionada às relações subjetivas e de trato íntimo da pessoa, enquanto a vida privada relacionada com todos os demais relacionamentos humanos, inclusive os objetivos como trabalho e estudo. Assim também entende Gilmar Mendes:

> Embora a jurisprudência e vários autores não distingam, ordinariamente, entre ambas as postulações – de privacidade e de intimidade –, há os que dizem que o direito à intimidade faria parte do direito à privacidade, que seria mais amplo. O direito à privacidade teria por objeto os comportamentos e acontecimentos atinentes aos relacionamentos pessoais em geral, às relações comerciais e profissionais que o indivíduo não deseja que se espalhem ao conhecimento público. O objeto do direito à intimidade seriam as conversações e os episódios ainda mais íntimos, envolvendo relações familiares e amizades mais próximas. (MENDES, 2018, p. 286)

Para Ortiz (2002) quando se fala da privacidade no contexto da sociedade da informação, a discussão sobre intimidade e vida privada se torna irrelevante já que, segundo a autora, com a automação das informações ainda que mecanismos tecnológicos alcancem somente dados da vida privada, através de um cruzamento desses dados pode-se chegar a dados da vida íntima.

Aquém do debate e além do fundamento em texto constitucional, a proteção à vida privada é reforçada no Código Civil, em seu artigo 21:

> Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.

Sobre o instituto, Schreiber (2014) tece algumas críticas, o autor explica que o código Civil brasileiro deu um tratamento inadequado a privacidade dedicando um único artigo a um instituto tão importante e o fazendo de forma genérica sem oferecer parâmetros para solucionar conflitos relacionados à tutela da privacidade.

> Não bastasse isso, empregou a expressão vida privada, revelando certa indiferença à recente evolução do conceito de privacidade, que abandonou uma concepção mais restrita, limitada ao círculo da intimidade da pessoa humana, para abarcar a proteção aos dados e informações pessoais. Sobre esse último aspecto, a codificação não trouxe uma palavra sequer. Não é exagero dizer que o Código Civil ignorou a vasta amplitude do tema, cuja compreensão é essencial para perceber o importante papel reservado à tutela da privacidade no século XXI. (SCHREIBER, 2014 p.136)

Para Paesani (2014, p. 35) o desenvolvimento da informática colocou em crise o conceito de privacidade, “a partir dos anos 80, passamos a ter um novo conceito de privacidade que corresponde ao direito que toda pessoa tem de dispor com exclusividade sobre as próprias informações”

Schreiber (2014) argumenta que atualmente o direito à privacidade alcança também os dados pessoais, sendo mais amplo do que o simples direito a intimidade, transcendendo a esfera doméstica e alcançando qualquer ambiente onde circulem os dados pessoais de seu titular. Ainda, o autor explica o que entende sobre dados pessoais:

> [...] aí incluídos suas características físicas, código genético, estado de saúde, crença religiosa e qualquer outra informação pertinente à pessoa. Nesse sentido, a privacidade pode ser definida sinteticamente como o direito ao controle da coleta e da utilização dos próprios dados pessoais. (SCHREIBER, 2014, p.139)

Rodotá (2008) também entende que o conceito de privacidade evoluiu e como nossas informações nos definem, a privacidade hoje se manifesta essencialmente em ter como controlar a circulação das informações e saber quem as usa significa adquirir, concretamente, um poder sobre si mesmo.

Para Bioni (2020, p.50), “os direitos de personalidade são uma noção ‘inacabada’ que deve ser ‘cultivada’”. Segundo o autor os direitos de personalidade não se limitam às situações previstas no Código Civil, nos artigos 11 ao 21, o que abre o caminho para o reconhecimento da proteção dos dados pessoais como um novo direito de personalidade. Ainda, segundo Doneda:

> A informação pessoal está, quase como ato reflexo, ligada à privacidade por uma equação simples e básica que associa um maior grau de privacidade à menor difusão de informações pessoais e vice-versa. Esta equação nem de longe encerra toda a complexa problemática em torno dessa relação, porém pode servir como ponto de partida para ilustrar como a proteção das

> informações pessoais passou a encontrar guarida em nosso ordenamento jurídico: como um desdobramento da tutela do direito à privacidade. (DONEDA, 2011, p.94)

De acordo com ensinamentos de Mendes (2014, p. 34) a personalidade de uma pessoa pode ser gravemente violada com a inadequada divulgação e utilização de informações armazenadas a seu respeito. “Por se constituírem em uma parcela da personalidade da pessoa, os dados merecem tutela jurídica, de modo a assegurar a sua liberdade e igualdade”.

> A disciplina da proteção de dados pessoais emerge no âmbito da sociedade de informação, como uma possibilidade de tutelar a personalidade do indivíduo, contra os potenciais riscos a serem causados pelo tratamento de dados pessoais. A sua função não é a de proteger os dados per se, mas a pessoa que é titular desses dados. (MENDES, 2014, p.32)

Zuboff (2019, p. 48) explica que os direitos de privacidade na era contemporânea têm relação com a escolha do indivíduo: “Os direitos de privacidade conferem, assim, direitos de decisão; a privacidade permite uma decisão sobre onde se quer estar no espectro entre sigilo e transparência em cada situação”.

Desse modo, ainda que informações de foro íntimo sejam compartilhadas, elas partem de uma decisão do indivíduo em compartilha-las. “Nesse cenário, a privacidade caminhou da sequência ‘pessoa-informação-sigilo’ para ‘pessoa-informação-circulação-controle’” (RODOTÀ, 2008, p. 93). Ou seja, é a possibilidade de o indivíduo controlar o uso de informações que lhe dizem respeito, é uma evolução do direito de estar só.

Sendo assim, esse novo elemento agregado ao conceito de privacidade, o poder do indivíduo de determinar e controlar seus dados pessoais, passou a ser denominado de “autodeterminação informativa”, exigindo uma tutela positiva do estado afim de proteger os dados pessoais.

Sobre o assunto e visando consubstanciar a proteção à privacidade, no que tange aos dados pessoais, a Constituição prevê a inviolabilidade da interceptação de comunicações telefônicas, telegráficas ou de dados (artigo 5º, XII), e a ação de habeas data (art. 5º, LXXII), que possibilita o acesso e retificação de dados.

Em relação a técnica legislativa Constitucional que menciona a inviolabilidade da intimidade e vida privada – proteção à privacidade, em um

dispositivo (art. 5°X) e em outro a inviolabilidade do “sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas” (art. 5º, XII). Danilo Doneda (2011) tece críticas, ele entende que se por um lado a privacidade é encarada como um direito fundamental, por outro as informações pessoais parecem serem protegidas somente em relação a sua comunicação.

> A leitura das garantias constitucionais para os dados somente sob o prisma de sua comunicação e de sua eventual interceptação lastreia-se em uma interpretação que não chega a abranger a complexidade do fenômeno da informação ao qual fizemos referência. Há um hiato que segrega a tutela da privacidade, esta constitucionalmente protegida, da tutela das informações pessoais em si – que, para a corrente mencionada, gozariam de uma proteção mais tênue. E este hiato possibilita a perigosa interpretação que pode eximir o aplicador de considerar os casos nos quais uma pessoa é ofendida em sua privacidade – ou tem outros direitos fundamentais desrespeitados – não de forma direta, porém por meio da utilização abusiva de suas informações pessoais em bancos de dados. (DONEDA, 2011, p.106)

Desse modo, a autodeterminação informativa, por ser entendida como espécie do direito à privacidade, e não ser direito fundamental autonomamente reconhecido, sofria com o questionamento da doutrina e jurisprudência sobre seu alcance e proteção, conforme explicado acima, e esse questionamento permeava em todo mundo, não só no Brasil, conforme explica a jurista espanhola Isabel Ortiz:

> El reconocimiento de que el catálogo de los derechos humanos sea permeable y abierto a la incorporación de nuevos valores no ha sido un principio unánimemente admitido por la docrtina, claro que los avances tecnológicos han reclamado del legislador respuestas a la nuevas pretensiones individuales derivadas de los importantes cambios sociales que aquellos fenómenos introducen. En verdad, el progreso social y el desarrollo tecnológico demandan no sólo protección en la más estricta intimidad del individuo, sino también garantias para asegurar el gobierno de la persona en su relaciones con terceros. Por todo ello, junto a los tradicionales derechos fundamentales, se reconoce el ejercicio de otros, que defienden al individuo en su dimensión social, y que alcanzan significación cuando se tutela a la persona en su condición de ser social16. (ORTIZ, 2003, p. 13)

[16] Tradução livre: O reconhecimento de que o catálogo dos direitos humanos é permeável e aberto à incorporação de novos valores não tem sido um princípio unanimemente admitido pela doutrina, evidentemente, os avanços tecnológicos têm exigido do legislador respostas às novas demandas individuais derivadas de importantes mudanças sociais que esses fenômenos introduzem. Na verdade, o progresso social e o desenvolvimento tecnológico exigem não apenas proteção na mais estrita privacidade do indivíduo, mas também garantias para assegurar suas relações com terceiros. Por tudo isso, a par dos direitos fundamentais tradicionais, é reconhecido o exercício de outros, que defendem o indivíduo na sua dimensão social, e que ganham significado quando a pessoa é protegida na sua condição de ser social. (ORTIZ, 2003, p. 13)

Por entender a importância da proteção jurídica aos dados pessoais, o legislador propôs emenda à Constituição. A PEC, 17/2019, tem como objetivo inserir a proteção de dados pessoais entre os direitos e garantias fundamentais e fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. A PEC segue em trâmite no congresso nacional e se aprovada, a proteção de dados pessoais passará a compor o rol de direitos fundamentais.

Atualmente no pais, além das garantias constitucionais já apresentadas, há normas dispostas em leis esparsas que conferem alguma proteção em alguns aspectos, partindo de um conteúdo geral, como o marco civil da internet e há inovações legislativas buscando um maior aprofundamento e eficácia na proteção de dados, como a lei geral de proteção de dados pessoais, trataremos delas na sequência.

3.1 O Marco Civil da Internet e a lei Geral de Proteção de Dados Pessoais

Em 2014 a lei 12.965, intitulada de marco civil da Internet, veio trazer direitos relacionados ao uso da internet e redes sociais e reforçar garantias constitucionais como as da inviolabilidade da intimidade, privacidade, livre manifestação do pensamento, liberdade de expressão, direito a informação e uma série de outras garantias.

A lei é um marco pois trouxe inovação, iniciou-se a regulamentação sobre o assunto. A lei trouxe metas e direcionamento para os tribunais, para a doutrina e para a criação de novas leis. O legislador percebeu a necessidade de dar diretrizes para os usuários e provedores de internet e elaborou a lei com base em três pilares: neutralidade da rede, liberdade de expressão e privacidade.

Esses limites legais impostos ao uso da internet e das redes sociais não atingem somente o usuário, empresas e organizações devem observar os preceitos de direitos fundamentais e os dispostos na legislação já que tais organizações detêm dados e informações sensíveis de seus usuários e não podem utilizá-los de forma ilegal. Conforme art. 10 da supracitada lei, *in verbis*:

> Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da

> intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas. (grifo nosso)
>
> § 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º .
>
> § 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º.
>
> § 3º O disposto no caput não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.
>
> § 4º As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais.

Em resumo, o marco civil da internet inovou ao disciplinar sobre a proteção aos dados pessoais, além da guarda dos serviços de conexão e dos registros de acesso. No entanto, o debate sobre o alcance da lei e se essa conseguia proteger de forma efetiva os direitos fundamentais se estendeu entre juristas e doutrinadores. O que ensejou o trâmite de muitos projetos de lei no Congresso Nacional para disciplinar novamente a questão.

No contexto mundial entrou em vigor em 2018 na União Europeia a lei que protege dados pessoais, a GDPR – General Data Protection Regulation. Os principais pontos desse regulamento são referentes ao consentimento e utilização de dados privados pelas empresas sem o expresso consentimento do usuário.

No Brasil, foi sancionada pelo presidente Michel Temer a LGPD - Lei Geral de Proteção a Dados Pessoais (Lei n° 13.709/2018), que se inspirou na lei europeia, buscando tornar o país um local livre de incertezas e seguro ao consumidor e às organizações, protegendo os dados coletados dos indivíduos e regulamentando procedimentos de tratamento de dados pessoais.

Bioni (2020) destaca que até a aprovação da LGPD o país contava apenas com leis setoriais de proteção de dados, que segundo o autor não tinha a efetividade de cobrir setores importantes da economia e dentre os cobertos, não havia uniformidade em seu regramento. O autor apresenta os problemas causados por essa

desconformidade:

> Essa assimetria gerava insegurança para: a) que os mais diversos setores produtivos trocassem dados entre si com o objetivo de desenvolver novos modelos de negócios; b) a formulação de políticas públicas e parcerias público-privadas igualmente dependentes desse intercâmbio de dados; e c) o cidadão que não detinha uma proteção integral e universal com relação a todas as atividades do cotidiano em que fornece seus dados, seja para o setor privado ou público. (BIONI,2020, p.102)

Em 2019 o Senado Federal aprovou proposta de emenda à Constituição, a PEC 17/2019, que incluiu no rol das garantias individuais a proteção de dados. Já visando consubstanciar tal garantia a LGPD entrou em vigor em 18 de setembro de 2020, trazendo como objetivo principal regulamentar a política de proteção de dados pessoais e privacidade.

A lei, em seu artigo 5°, inciso I, conceitua dado pessoal como uma informação relacionada a pessoa natural identificada ou identificável. E em seu artigo 7° elenca as hipóteses em que os dados pessoais poderão ser tratados, *in verbis*:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
>
> I - mediante o fornecimento de consentimento pelo titular;
>
> II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
>
> III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
>
> IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
>
> V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
>
> VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
>
> VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
>
> VIII - para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;

> VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019) Vigência
>
> IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
>
> X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

No inciso I do artigo 7° está um dos pontos mais relevantes da norma quanto à proteção à privacidade: o consentimento. O cidadão deve consentir que seus dados pessoais possam ser tratados, além da possibilidade da revogação desse consentimento outrora concedido.

A necessidade de concordar com o tratamento de dados exige na outra ponta a obrigação de informar total e eficientemente junto ao consumidor tudo o que se refere ao tratamento de seus dados. Como por exemplo, qual o tempo em que seus dados estarão armazenados, de que forma serão coletados, com qual finalidade e se serão comercializados ou compartilhados entre empresas parceiras. Passando a ser obrigatório o aceite à política de privacidade.

Dessa forma, todas aquelas pessoas jurídicas de direito público e privado que realizam coleta de dados no país, ou oferte produtos e serviços serão atingidas e deverão se adaptar.

São inúmeras as adequações, primordialmente as empresas devem oferecer um ambiente seguro de proteção aos dados, visando reduzir os riscos de ataques de *hackers* e *malwares*, e ainda assim, caso aconteça, as organizações terão uma série de obrigações a cumprir como comunicar ao órgão ANPD (Autoridade Nacional de Proteção de Dados) sobre o vazamento, os consumidores e tomar providências para amenizar os impactos causados.

Ainda, as empresas deverão elaborar um relatório de impacto à Proteção dos Dados Pessoais (RIPD), este documento terá a finalidade de demonstrar quais dados pessoais serão coletados, como eles serão tratados, usados, compartilhados e quais medidas serão adotadas para reduzir os riscos que possam afetar as liberdades civis e os direitos fundamentais dos titulares desses dados.

Por fim, visando esclarecer melhor como se dará a implantação da LGPD

no governo, este lançou um manual de boas práticas[17] para a implementação na administração pública federal.

Por ser muito recente, ainda não podemos trazer para o mundo dos fatos o impacto trazido com a vigência da lei.

3.2 Projetos de lei sobre a Internet das Coisas

Em 2018, a internet das coisas é citada no decreto 9.319/18 que instituiu o sistema nacional de transformação digital, o menciona em seu anexo I, inciso II, b: "ao reconhecer o potencial transformador das aplicações da internet das coisas, devem ser estabelecidos ações e incentivos destinados à contínua evolução e disseminação dos dispositivos e das tecnologias associadas".

Já em Junho de 2019 instituiu-se o plano nacional da internet das coisas, através do decreto 9.584. Tal decreto estabeleceu um plano nacional com a finalidade de implementar e desenvolver a internet das coisas no pais. Constituindo um grande passo para o desenvolvimento da tecnologia no Brasil.

> Art. 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;
> II - coisas - objetos no mundo físico ou no mundo digital, capazes de serem identificados e integrados pelas redes de comunicação;
> III - dispositivos - equipamentos ou subconjuntos de equipamentos com capacidade mandatória de comunicação e capacidade opcional de sensoriamento, de atuação, de coleta, de armazenamento e de processamento de dados; e
> IV - serviço de valor adicionado - atividade que acrescenta a um serviço de telecomunicações que lhe dá suporte e com o qual não se confunde novas utilidades relacionadas ao acesso, ao armazenamento, à apresentação, à movimentação ou à recuperação de informações, nos termos do disposto no art. 61 da Lei nº 9.472, de 16 de julho de 1997.

Como copiado acima, o decreto em seu artigo 2° define o conceito de internet das coisas, além do conceito de coisas e dispositivo. Além disso, o decreto traça os objetivos que visam fomenta-la no país, como a melhoria da qualidade de vida das pessoas, a capacitação profissional relacionada ao desenvolvimento da tecnologia, o incremento da produtividade, o fomento da competitividade nas

[17] https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-lgpd.pdf

empresas, a busca de parcerias entre o setor público e privado e por fim, a integração do país no cenário internacional.

Também, através do citado decreto, estabeleceu-se um plano de ação destinado a identificar soluções para viabilizar o plano nacional de internet das coisas, dentre os temas propostos destaca-se o de regulação, segurança e privacidade (art. 5°, V, decreto 9.854/19).

No entanto, o texto não entra em maiores detalhes e nada fala sobre a proteção de dados, ou sobre quais entes terão a competência para a regulação da Iot e de que maneira se procederia a regulação.

O decreto foca basicamente na implementação da “Câmara de Gestão e Acompanhamento do Desenvolvimento de Sistemas de Comunicação Máquina a Máquina e Internet das Coisas”, que será presidido pelo Ministério da Ciência, Tecnologia, Inovações e Comunicações, além de outros ministérios e de mais de 60 instituições públicas e privadas, incluindo universidades e centros de pesquisa.

Importante também destacar que no mesmo ano de publicação do decreto e em consequência do plano nacional de internet das coisas a empresa Qualcomm em parceria com o BNDES criou um fundo de investimento de cento e sessenta milhões (KLEINA, 2019). O fundo auxiliará empresas que desenvolvam soluções em Iot, com aplicações que envolvam hardware, software ou análise de dados. São esperadas melhorias em setores como manufatura, smart cities, saúde, agricultura e residencial.

4 VIOLAÇÕES A PRIVACIDADE NO MUNDO FÁTICO

Violações à privacidade de dados através do meio tecnológico podem ocorrer através de crimes atribuídos a hackers[18].

No entanto, são as corporações que detêm a maior gama de dados e informações sobre seus usuários, são elas que nos disponibilizam a tecnologia, criando dispositivos e inovações tecnológicas e por fim, são elas que devem se adequar a regulações e normas vigentes nos países onde mantêm seus negócios. Tais direitos e deveres as tornam responsáveis pela segurança de seus produtos e pelas violações causadas, inclusive por hackers.

Uma das grandes multinacionais de tecnologia, a Samsung, teve que reportar-se aos seus clientes após a repercussão de que seus aparelhos, as *smart tvs*, estariam captando e transmitindo informações de seus usuários (JESUS, 2015). As televisões até então eram aparelhos inofensivos, mas quanto tiveram sua interface tecnológica ampliada e passaram a acessar a internet o questionamento sobre seu acesso remoto através do microfone e câmera passou a ser questionado.

Uma falha no software dos equipamentos de uma empresa americana denominada TrendNet, fez com que o conteúdo captado por suas câmeras de segurança fosse acessado e transmitido por qualquer um, via internet (ALFONSO, 2020). Fato parecido ocorreu com a assistente virtual Alexa da Amazon, que ligou, gravou e enviou a terceiros conversa entre um casal (LEE, 2018).

Por violações como as citadas, o regulamento geral de proteção de dados da união europeia[19] impõe penalidades às empresas que não divulguem suas falhas em 72 horas e passa a exigir que os desenvolvedores de tecnologia tenham a privacidade como parâmetro inicial para a criação de seus produtos.

De acordo com o entendimento de Camara e Rodrigues (2019, p. 74), uma das grandes implicações à privacidade é de que no mundo globalizado organizações tecnológicas internacionais devam se adaptar a regulamentação e normatização de cada país. Esses autores ainda explicam que “economicamente, a

[18] O termo hacker, é originado do inglês hack, que significa cortar alguma coisa de forma grosseira ou irregular. Hackers são pessoas com um conhecimento profundo de informática e computação que trabalham desenvolvendo e modificando softwares e hardwares de computadores.

[19] O GDPR é uma lei aprovada em 2016, que regulamenta a proteção dos dados de pessoas físicas nos 28 países da União Europeia, além da Noruega, Islândia e Liechtenstein (três membros do Espaço Econômico Europeu).

transnacionalidade das regulamentações de proteção de dados pode parecer uma possível barreira de acesso ao mercado interno a uma empresa estrangeira".

> Grandes empresas de tecnologia parecem apresentar um papel duplo, tanto econômico quanto estratégico-político, podendo fornecer o aparato tecnológico necessário para realizar operações ilícitas em território estrangeiro, mas em compliance com as normas de uma nação rival. (CAMARA; RODRIGUES, 2019, p.79)

Para entender melhor o raciocínio apresentado, é importante entender que no processo de elaboração de uma regulamentação visando a proteção da privacidade muitas forças estarão envolvidas. O interesse das multinacionais de tecnologia deve ser considerado por questões econômicas e estratégicas, da mesma forma que o interesse da sociedade na proteção de direitos e garantias fundamentais.

> Numa perspectiva geopolítica, entretanto, devido ao potencial do tratamento de dados em poder influenciar em comportamentos humanos, a aplicação da legislação no tocante a empresas multinacionais de grande porte tem recebido um tratamento diferenciado, deixando evidente a instrumentalização de normas para atender a interesses nacionais. (CAMARA; RODRIGUES, 2019, p. 74)

Bioni (2020) explica que em uma sociedade de vigilância as informações pessoais são a matéria-prima a ser explorada para a geração de riqueza. Por esse motivo as ações regulatórias devem ser criadas considerando esse mercado gerador de negócios e de economia.

> Qualquer perspectiva regulatória para a proteção dos dados pessoais deve levar em consideração o quadro acima descrito, a existência de uma "economia de vigilância". Tal diagnóstico deságua em estratégias regulatórias complementares que são, por um lado, o empoderamento do indivíduo para exercer um controle significativo sobre seus dados pessoais, e, por outro lado, a consideração de que o próprio fluxo das informações pessoais não se deve submeter, tão somente, à lógica desses interesses econômicos em jogo (BIONI,2020, p.42).

Olhando por esse viés, não só as questões atinentes à proteção da privacidade estão em debate, mas também interesses econômicos e políticos. Os governantes passaram a enxergar as multinacionais de tecnologias viáveis tanto para contribuir com o desenvolvimento econômico e tecnológico de suas nações como também para atingir seus interesses de segurança nacional.

Edward Snowden[20] expôs ao mundo que os Estados Unidos utilizavam programas de vigilância para espionar sua população. Um dos pontos principais dessa denúncia era de que esses programas envolviam equipes de inteligência de empresas de tecnologia como a Microsoft, o Facebook e o Google (ENTENDA, 2014).

Na China, em 2019, por exemplo, um novo regulamento dispôs sobre a a necessidade de os cidadãos terem seus rostos digitalizados ao registrar novos serviços de telefonia móvel, essa foi uma alternativa encontrada pelo governo para que as autoridades verificassem a identidade de centenas de milhões de usuários de internet do país (CHINA, 2019) Em maio do mesmo ano, nos Estados Unidos, o corpo administrativo da cidade de São Francisco votou para suspender o uso da tecnologia de reconhecimento facial que seria utilizada pelos órgãos governamentais por razões de segurança e monitoramento (PRATT, 2019).

> Os mecanismos dessa crescente concentração de direitos de privacidade e suas implicações foram minuciosamente examinados por juristas nos Estados Unidos e na Europa, mesmo antes de Edward Snowden acelerar essa discussão. Essa é uma literatura rica e cada vez maior que suscita muitas preocupações substanciais associadas às implicações antidemocráticas da concentração dos direitos de privacidade entre atores de vigilância privada e pública. (ZUBOFF, 2018, p. 49)

Desse modo, como inicialmente apresentado, não só as ações de hackers são um perigo a privacidade. As grandes multinacionais de tecnologia também representam um grande risco com seus interesses no lucro e no fomento de sua atividade, que tem como base irrestritamente os dados pessoais. Além delas, os países e governantes também apresentam grande potencial para violar direitos de privacidade de seus cidadãos, utilizando a tecnologia afim de auxiliar em suas políticas de controle e de segurança.

[20] Edward Snowden prestou serviços como funcionário terceirizado para a NSA, a Agência de Segurança Nacional, principal órgão de inteligência digital dos Estados Unidos e trabalhou para a CIA, a Agência Central de Inteligência americana. Tendo sido responsável pelo vazamento de informações publicadas em junho de 2016 no jornal The Guardian. A reportagem vinculava o governo americano ao desenvolvimento de programas que revelavam informações de pessoas no mundo inteiro.

4.1. Possíveis violações da privacidade com a implantação da Iot

Trazendo a análise da questão da segurança para a internet das coisas. Além das violações à privacidade já apresentadas somam-se a elas o fato de que a tecnologia Iot aumenta a possibilidade de violação de dados pessoais e sensíveis, já que mais coisas estarão conectadas a internet e cada uma delas possui seus protocolos de acesso.

Com a Iot, um único objeto é capaz de captar muitos dados e informações. Um óculos, por exemplo, conectado à internet, poderá captar uma conversa através do microfone, imagens através da câmera, e a localização de alguém através do gps. Ou seja, os meios de coleta e distribuição dos dados são ampliados, aumentando exponencialmente os riscos e as vulnerabilidades.

Utilizando o raciocínio indutivo, a partir das premissas estabelecidas acima, serviços vitais como hospitais, energia elétrica e trânsito em uma cidade inteligente poderão ser vulneráveis. Hackers poderão utilizar pequenas brechas no sistema para evadir o todo, já que os dispositivos estarão conectados, causando danos gigantescos e muitas vezes irreversíveis.

Toda essa perspectiva apresentada, de cidades inteligentes, pode parecer longe de nossa realidade, no entanto, o BNDES já selecionou três municípios para se tornarem as primeiras cidades inteligentes do país, Santa Rita do Sapucai (MG), Caxambu (MG) e Piraí (RJ), onde empresas e prefeituras envolvidas usarão soluções de Iot para iluminação, segurança e rastreamento de veículos (PAYÃO, 2019).

Greengard (2015) explica que a Iot será utilizada de maneiras boas e ruins, que criminosos e terroristas podem usar drones para espionar e lançar ataques. Ainda, segundo o autor, Hackers podem acessar dispositivos contendo câmeras de vídeos e ver o que a pessoa esteja fazendo ou ainda, exibir publicamente seus atos.

O fato é que a tecnologia Iot ainda dá seus primeiros passos tecnológicos. As falhas existentes na segurança podem ainda ser óbvias e detectáveis devido ao reduzido número de dispositivos utilizando a nova tecnologia, e devido ao fato de que os recursos de conectividade são limitados. No entanto, “à medida que o número de dispositivos e recursos da Iot aumentarem, as falhas de segurança se tornarão mais complexas” (MAGRANI, 2018, p.102).

De acordo com Magrani (2018), em relação a segurança dos dados, os próprios desenvolvedores ainda não têm uma noção completa do que é necessário em termos de segurança da Iot e por esse motivo, a fórmula indicada é continuar com a prática de testes de vulnerabilidade em softwares e sistemas, além de conscientizar os usuários da importância de sempre manter seus dispositivos atualizados com as ferramentas de segurança acessíveis. Ainda, segundo o autor:

> Em pouco tempo, provavelmente teremos nosso cotidiano monitorado, em sua grande parte, por meio dos produtos de IoT. Dessa maneira, a privacidade do consumidor é um importante tópico de discussão: caso os dados obtidos não sejam submetidos a um processo de proteção confiável, isso pode causar graves violações à privacidade. (MAGRANI, 2018 p. 102)

Em uma pesquisa rápida através de serviços de busca de informações na internet, encontramos uma série de eventos envolvendo falhas na segurança de dispositivos Iot, como lâmpadas, portas inteligentes, assistente de voz, inclusive uma boneca denominada *My friend Cayla*[21] foi banida da Alemanha através de legislação por ser considerada dispositivo de espionagem (COLLINS, 2017).

Magrani (2018 p. 93) registra que pesquisas recentes realizadas pela *HP Security Research*[22] detectaram que 70% dos dispositivos Iot têm falhas de segurança, e que os principais problemas encontrados foram os de privacidade, autorizações insuficientes, falta de criptografia no transporte de dados, interface web insegura e softwares de proteção inadequados.

De acordo com Greengard (2015) como os dispositivos Iot se comunicarão entre si, mas cada um deles será desenvolvido por uma empresa, com uma interface diferente, algoritmos diferentes e critérios de segurança diferentes, a segurança dos dados nos dispositivos Iot apresentará um grande desafio.

> Moreover, with devices and algorithms communicating with each other— and different standards and quality control criteria applied by different developers and companies—there's a real world risk of building systems that do not deliver a desired level of machine-to-human communication. (GRENNGARD, 2015 p.49)[23]

---

[21] Tradução livre: Minha amiga Cayla.

[22] Hewlett-packard company. Internet of things research study report, jul. 2014.

[23] Tradução livre: Além disso, com dispositivos e algoritmos que se comunicam uns com os outros - e diferentes padrões e critérios de controle de qualidade aplicados por diferentes desenvolvedores e empresas - há um verdadeiro risco mundial de construir sistemas que não entregam o nível desejado de comunicação máquina-para-humano. (GRENNGARD, 2015 p.49)

5 CONSIDERAÇÕES FINAIS

Esse estudo iniciou buscando compreender sobre a sociedade da informação, principalmente, sobre uma das mais importantes e modificadoras inovações tecnológicas do século atual, a internet. Ele prosseguiu em seus capítulos buscando conhecer novas tecnologias vindouras com o implemento da internet, e as modificações sociais, políticas e econômicas trazidas pela evolução tecnológica. Por fim, falamos sobre a mais recente e promissora inovação tecnológica: a Internet das coisas.

Traçar essa linha do tempo nos permitiu enxergar com mais clareza quais os riscos e desafios trazidos com uma nova tecnologia e assim delimitarmos nosso estudo a uma problemática que interessa ao direito, a privacidade.

Frente a uma nova tecnologia, como a Internet das Coisas, que tem potencial de revolução e criação de novos paradigmas, assim como foi a internet, todas as questões relacionadas a essa tecnologia que interessam ao Direito devem ser estudadas e entendidas. Sobre isso, alguns pontos importantes do nosso estudo merecem destaque.

Em primeiro lugar, podemos inferir que não há um único caminho para a proteção da privacidade dos dados. Essa proteção depende de um esforço dos indivíduos, das organizações e do governo, e cada um deles apresenta um interesse diverso, o que torna uma incógnita saber de que forma esse equilíbrio se dará.

Em relação às organizações pesa o fato de que os dados pessoais se tornaram o ativo mais rentável da nossa era, fazendo com que essas empresas coloquem os lucros à frente das questões ligadas a proteção de dados e de privacidade.

Ao governo restam interesses de ordem econômica, de desenvolvimento tecnológico do país e de inserção no mundo globalizado. Entram também questões de segurança nacional em que os direitos de privacidade de seus cidadãos podem ser colocados em segundo plano.

Quanto ao indivíduo, parte mais vulnerável dessa relação, embora o direito de privacidade seja indisponível, não abrir mão de uma fração de sua privacidade pode colocá-lo à margem do mundo tecnológico. E muitas vezes estar

“conectado” na sociedade da informação pode ser mais importante ao indivíduo do que manter em sigilo seus dados pessoais.

Por esse motivo, a inserção da privacidade de dados no rol de direitos fundamentais é importante, ela dá ao indivíduo o poder jurídico de impor a terceiros o dever de se abster de toda intromissão em sua vida privada de forma ampla, podendo controlar seus dados pessoais em qualquer esfera de sua vida, inclusive como usuário de tecnologia.

Também muito importante, são as leis que inovam o ordenamento jurídico dando efetividade a norma constitucional. A LGPD traz mais detalhes de como o direito de privacidade pode ser garantido no mundo dos fatos, impondo limites a atuação das organizações que captam e manipulam dados pessoais.

A Internet das coisas deverá coexistir com os direitos fundamentais. Regulamentações, políticas públicas e o entendimento de toda a sociedade sobre os benefícios e as implicações dessa nova tecnologia deverão ser a base para que esse equilíbrio aconteça. Nesse desafio a Lei Geral de Proteção de Dados desponta como um importante mecanismo, obrigando as organizações tecnológicas a requererem o consentimento de seus usuários entre tantos outros deveres e obrigações.

Dessa forma o estudo nos levou a inferir que a Internet das coisas oferece riscos reais de violação a privacidade. Principalmente porque as organizações não oferecem clareza sobre a forma como captam, mantém e manipulam os dados pessoais de seus usuários.

No entanto, os riscos oferecidos não podem frear o desenvolvimento tecnológico. Os riscos devem objeto de estudo e de criação de políticas públicas, que analisem de maneira profunda quais implicações a tecnologia pode oferecer principalmente no que tange aos direitos e garantias individuais. E ainda, esses estudos devem ser constantes e atualizados com as inovações tecnológicas sob pena de se tornarem obsoletos e atrasados em confronto com a realidade.

REFERÊNCIAS

ALFONSO, Fernando. **Website exposes more than 300 unprotected live webcams.** Daily dot, 02 mar. 2020, Disponível em: https://www.dailydot.com/news/creeper-website-exposes-trendnet-webcams/. Acesso em: 10 ago. 2020.

ATZORI, Luigi; IERA, Antonio; MORABITO, Giacomo. **The Internet of Things: a survey**. Computer Networks, 2010.

BAUMAN, Zygmunt; RAUD, Rein. **A individualidade em uma época de incertezas.** Rio de Janeiro: Jorge Zahar, 2018.

BENTIVEGNA, Carlos Frederico Barbosa. **Liberdade de expressão, honra, imagem e privacidade: os limites entre o lícito e o ilícito.** São Paulo: Manole, 2020

BIONI, Bruno Ricardo**. Proteção de dados pessoais: a função e os limites do consentimento.** 2. ed. Rio de Janeiro: Forense, 2020.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988.** Brasília, DF: Presidência da República [2016]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 10 abr. 2019.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Brasília: Casa Civil, 2003. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/L10406compilada.htm. Acesso em: 20 abr. 2019.

BRASIL**. Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília: Casa Civil, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 20 abr. 2019.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Secretaria-Geral, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 20 abr. 2019.

BRASIL. **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. Brasília: Secretaria-Geral, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D9854.htm. Acesso em: 10 ago. 2020.

BRUNO, Fernanda. **Máquinas de ver, modos de ser: vigilância, tecnologia e subjetividade.** Porto Alegre: Sulina, 2013. 190 p.; Disponível em:

https://comunicacaoeidentidades.files.wordpress.com/2014/07/pg-18-a-51-maquinas-de-ver-modos-de-ser.pdf Acesso em: 05 out. 2020.

CAMARA, Maria Amália Oliveira de; RODRIGUES, Walter de Macedo. **A gestão de dados pessoais por grandes empresas: considerações geopolíticas e jurídicas.** Cadernos Adenauer, Rio de Janeiro, v.20, n. 3, outubro, 2019. Disponível em: https://www.kas.de/documents/265553/265602/Caderno+Adenauer+3+Schutz+von+pers%C3%B6nlichen+Daten.pdf/476709fc-b7dc-8430-12f1-ba21564cde06?version=1.0&t=1571685012573. Acesso em: 30 set. 2020

CARVALHO, André C. P. L. F de; LORENA, Ana Carolina. **Introdução à computação: hardware, software e dados**. 1. ed. - Rio de Janeiro: LTC, 2017.

CASTELLS, Manuel. **A galáxia da Internet.** Rio de Janeiro: Jorge Zahar, 1999.

CASTELLS, Manuel. **A sociedade em rede**. 8. ed. São Paulo: Paz e Terra, 2007.

CISCO Visual Networking Index (VNI) and VNI Service Adoption. Global Forecast update, 2015-2020. **Site Cisco**. 06, jun.2016. Disponível em: https://www.cisco.com/c/dam/global/ko_kr/assets/pdf/2016-VNI-Complete-Forecast-PT.pdf. Acesso em: 05 abr. 2019

COMER, Douglas E. **Redes de computadores e internet**. 6. ed. Porto Alegre: Bookman, 2016.

CHINA due to introduce face scans for mobile users.Site **BBC,** 01, dec. 2019. Disponível em: https://www.bbc.com/news/world-asia-china-50587098. Acesso em: 10 ago. 2020

DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental.** Espaço Jurídico Journal of Law**,** v. 12, n. 2, 2011, p. 91-108. Disponível em: https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em: 18 ago. 2020

GREENGARD, Samuel. **The internet of things**. Cambridge: MIT press essential knowledge series, 2015. Disponível em: https://www.mobt3ath.com/uplode/book/book-61497.pdf. Acesso em: 18 ago.2020

GUSTIN, Miracy Barbosa de Souza; DIAS, Maria Tereza Fonseca. **(Re)pensando a pesquisa jurídica**: teoria e prática. 4ª ed. rev. e atual. Belo Horizonte: Del Rey, 2013.

ENTENDA o caso de Edward Snowden, que revelou espionagem dos EUA. **Site G1**, São Paulo, 14 fev. 2014. Disponível em: http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html. Acesso em: 10 ago. 2020.

JESUS, Aline. **Invasão de privacidade? Smart TVs Samsung podem "escutar" o que você diz.** Techtudo, 09 fev. 2015, Disponível em:

https://www.techtudo.com.br/noticias/noticia/2015/02/invasao-de-privacidade-smart-tvs-samsung-podem-escutar-o-que-voce-diz.html. Acesso em: 10 ago. 2020.

KUMAR, Krishan. **Da Sociedade Pós industrial a Pós moderna.** Rio de Janeiro: Jorge Zahar, 1997.

KLEINA, Nilson. **Brasil terá fundo de US$ 160 milhões da Qualcomm e BNDES para IoT**. Tecmundo, 18 dez. 2019. Disponível em: https://www.tecmundo.com.br/mercado/148681-brasil-tera-fundo-us-160-milhoes-qualcomm-bndes-iot.htm. Acesso em: 20 jul. 2020.

LEE, Dave. **Como a Alexa, a assistente virtual da Amazon, gravou e compartilhou conversa privada de casal.** BBC News, 29 maio. 2018. Disponível em: https://www.bbc.com/portuguese/geral-44280917. Acesso em: 10 ago. 2020.

LEMOS, André; LÉVY, Pierre. **O futuro da internet:** em direção a uma ciberdemocracia. São Paulo: Paulus, 2010.

MAGRANI, Eduardo. **Democracia conectada: a internet como ferramenta de engajamento político-democrático.** Curitiba: Juruá, 2014.

MAGRANI, Eduardo. **Entre dados e robôs: ética e privacidade na era da hiperconectividade.**2. ed. Porto Alegre: Arquipélago Editorial, 2019.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de direito constitucional.** 13. ed. São Paulo: Saraiva Educação, 2018. – (Série IDP)

MORAES, Alexandre de. **Direito constitucional**. 35. ed. São Paulo: Atlas, 2019.

MORAES**,** Guilherme Peña de. **Curso de direito constitucional.** 11. ed. São Paulo: Atlas, 2019.

ORTIZ, Ana Isabel Herrán: **El derecho a la intimidad en la nueva Ley Orgánica de protección de datos personales**. Madrid: Dykinson, 2002.

PAESANI**,** Liliana Minardi**. Direito e Internet:** Liberdade de Informação, Privacidade e Responsabilidade Civil, 7. ed. São Paulo: Atlas S.A, 2014.

PAESANI**,** Liliana Minardi. **O Direito na Sociedade da Informação III:** A evolução do Direito Digital. São Paulo: Atlas, 2013.

PAYÃO, Felipe. **BNDES escolhe três municípios para virarem cidades inteligentes no Brasil.** Tecmundo. 19 mar. 2019. Disponível em: https://www.tecmundo.com.br/mobilidade-urbana-smart-cities/139671-bndes-escolhe-tres-municipios-virarem-cidades-inteligentes-brasil.htm. Acesso em: 12 ago. 2020.

PECK PINHEIRO**,** Patrícia. **Direito Digital.** 6. ed. São Paulo: Saraiva, 2016.

PRATT, Mary K. **Surveillance technology under fire, amid growing societal**

concerns. Tech Target. 21, maio. 2019. Disponível em: https://searchcio.techtarget.com/news/252463774/Surveillance-technology-under-fire-amid-growing-societal-concerns. Acesso em: 12 ago. 2020

THE world´s most valuable resource is no longer oil, but data. **Site The Economist**, 06 maio.2017. Disponível em: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data. Acesso em: 05 jul. 2020.

TOFFLER, Alvin; TOFFLER, Heidi. **O futuro do Capitalismo.** São Paulo: Saraiva, 2012.

ZUBOFF, Shoshana. Big other: capitalismo de vigilância e perspectivas para uma civilização da informação. *In*: BRUNO, Fernanda *et al* (org.). **Tecnopolíticas de vigilância:** perspectivas da margem. São Paulo: Boitempo. 2018. p. 17-68.