UNIVERSIDADE FEDERAL DE SANTA CATARINA - UFSC
CENTRO DE CIÊNCIAS JURÍDICAS - CCJ
CURSO DE PÓS-GRADUAÇÃO EM DIREITO
PROGRAMA DE MESTRADO

Ana Carolina Dias dos Santos

VIGIAR E VENDER: A PRIVACIDADE DO USUÁRIO CONSUMIDOR E A INTERNET DAS COISAS

FLORIANÓPOLIS
2023

Ana Carolina Dias dos Santos

VIGIAR E VENDER: A PRIVACIDADE DO USUÁRIO CONSUMIDOR E A INTERNET DAS COISAS

Dissertação submetida ao Programa de Pós-Graduação em Direito (PPGD) da Universidade Federal de Santa Catarina – UFSC, para obtenção do título de mestre em Direito, área de concentração Direito, Estado e Sociedade, da Universidade Federal de Santa Catarina - UFSC.

Orientadora: Carolina Medeiros Bahia

FLORIANÓPOLIS
2023

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

dos Santos, Ana Carolina Dias
Vigiar e vender: a privacidade do usuário consumidor e a Internet das Coisas / Ana Carolina Dias dos Santos ; orientadora, Carolina Medeiros Bahia, 2023.
114 p.

Dissertação (mestrado) - Universidade Federal de Santa Catarina, Centro de Ciências Jurídicas, Programa de Pós Graduação em Direito, Florianópolis, 2023.

Inclui referências.

1. Direito. 2. Direito do consumidor. 3. Internet das Coisas. 4. Privacidade. I. Bahia, Carolina Medeiros . II. Universidade Federal de Santa Catarina. Programa de Pós Graduação em Direito. III. Título.

Ana Carolina Dias dos Santos

VIGIAR E VENDER: A PRIVACIDADE DO USUÁRIO CONSUMIDOR E A INTERNET DAS COISAS

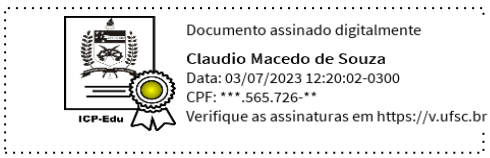
O presente trabalho em nível de Mestrado foi avaliado e aprovado, em 05 de abril de 2023, pela banca examinadora composta pelos seguintes membros:

Prof.(a) Carolina Medeiros Bahia, Dr.(a)
Instituição Universidade Federal de Santa Catarina

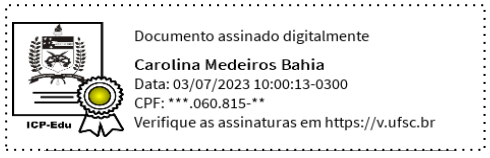
Prof.(a) Liz Beatriz Sass, Dr.(a)
Instituição Universidade Federal de Santa Catarina

Prof. Daniel Deggau Bastos, Dr.
Instituição Universidade Federal de Santa Catarina

Certificamos que esta é a versão original e final do trabalho de conclusão que foi julgado adequado para obtenção do título de Mestra em Direito.



Coordenação do Programa de Pós-Graduação



Prof.(a) Carolina Medeiros Bahia Dr.(a)
Orientador(a)

Florianópolis, 2023.

AGRADECIMENTOS

Nos últimos dias em que escrevia este trabalho, após dois anos de mestrado e algum tempo de pesquisa científica, cheguei à minha melhor compreensão pessoal do que é a pesquisa científica do ponto de vista de uma acadêmica que se encontra exausta.

Fazer uma pesquisa científica é como minerar na busca por uma grande pedra preciosa, que pode ou não existir, sem saber sua localização exata, seu formato e onde começar a escavar. Ao começar a escavação, água começa a minar do chão e quanto mais se escava, mais água surge; e junto à água, surgem outros minérios e preciosidades, aos quais o pesquisador, digo, minerador, não pode se apegar, pois é preciso saber selecionar. E, quando já se escavou o suficiente e parece não mais haver pedra preciosa para localizar, os primeiros indícios de uma luz, um brilho discreto, começam a surgir e a pesquisa começa a fazer sentido. Com isso, as conclusões começam a se formar e a escavação demonstra que valeu a pena.

Ao longo desta jornada, algumas pessoas foram fundamentais para que eu pudesse alcançar a joia rara que hoje chamo de dissertação. Em momentos delicados, de perdas pessoais, de doença, de estresse e, às vezes, de incompreensão, elas estiveram por aqui.

Agradeço primeiramente a Deus, pois a Ele cabe toda gratidão por cada conquista até aqui atingida, e especialmente a realização deste e de outros sonhos.

Agradeço aos meus pais, Suely e Gilson, aos meus irmãos, Thiago, Amanda e André, pois nenhum título acadêmico é tão importante quanto o título de fazer parte dessa família. Agradeço ao Henrique, minha companhia nas horas mais delicadas, meu maior incentivador a ingressar no mestrado e meu amor. Aos meus amigos, que foram suporte emocional, proporcionaram momentos de descontração e, com muita paciência, entenderam cada renúncia até aqui. Obrigada Marco, Anna e Bianca.

Agradeço especialmente à minha professora orientadora, Dra. Carolina Medeiros Bahia, que com maestria é um grande exemplo de docente. Obrigada pela paciência, pela calma, pela atenção e por todo cuidado com a minha pesquisa até aqui.

E agradeço a todos, especialmente aos aqui mencionados, que nem por um instante duvidaram de que seria capaz.

RESUMO

A tecnologia da informação proporcionou inumeráveis avanços na sociedade e diariamente revela novas facetas a serem exploradas na construção de benefícios para a economia, indústria, saúde, comunicação, entre outros setores. A rapidez e aderência das tecnologias pela sociedade foi tamanha que hoje seria difícil – se não impossível – imaginar o desaparecimento de invenções já tão permanentes nesse paradigma, ao ponto que a sociedade se tornou informacional, e todas as suas cadeias produtivas estão intimamente cada vez mais ligadas às tecnologias da informação. A internet das coisas é uma das mais avançadas tecnologias nascidas desse modelo de sociedade informacional e pertence intrinsecamente a uma realidade civil já habituada com a tecnologia a ponto de conviver com objetos inteligentes, ceder-lhe informações íntimas, manter diálogos, planejar a vida e sentir confortavelmente bem com o uso desses equipamentos. Esta pesquisa estuda especificamente a proteção do direito à privacidade do usuário consumidor das tecnologias de internet das coisas perante a legislação consumerista vigente, assim, encarrega-se de explorar o atual contexto da proteção da privacidade e das tecnologias da informação. Para tanto, o estudo se divide em três capítulos, em que primeiramente se contextualiza a sociedade da informação e o capitalismo de vigilância, apresentando conceito das teorias de vigilância e dos modelos econômicos explorados em que se insere o mercado de sensoriamento e IoT. No segundo capítulo, adentra-se especificamente à tecnologia de Internet das Coisas, pormenorizando suas funcionalidades e explorando a problemática que envolve a computação ubíqua promovida pela IoT e a vulnerabilidade do usuário consumidor. Por fim, o último capítulo ocupa-se em discorrer sobre o direito da privacidade, desde o seu surgimento como valor humano a ser preservado até a sua positivação no ordenamento jurídico. Além disso, explana-se sobre a tutela da privacidade sobre o usuário consumidor e sua (in)suficiência protetiva frente à tecnologia da internet das coisas no contexto atual. Por oportuno, a pesquisa abre espaço para possíveis resoluções do ponto de vista normativo e de mecanismos práticos para uma possível extensão da proteção ao consumidor.

Palavras-chave: internet das coisas; privacidade; capitalismo de vigilância.

ABSTRACT

Information technology has provided countless advances in society and daily reveals new facets to be explored in the construction of benefits for the economy, industry, health, communication, among other sectors. The speed and adherence of technologies by society was such that today it would be difficult – if not impossible – to imagine the disappearance of inventions that are already so permanent in this paradigm, to the point that society has become informational, and all its productive chains are intimately more and more linked to information technologies. The internet of things is one of the most advanced technologies born from this model of informational society and intrinsically belongs to a civil reality already used to technology to the point of living with intelligent objects, giving them intimate information, maintaining dialogues, planning life and feeling comfortably well with the use of these devices. This research specifically studies the protection of the right to privacy of the consumer user of internet of things technologies before the current consumerist legislation, thus, it is in charge of exploring the current context of the protection of privacy and information technologies. To this end, the study is divided into three chapters, in which the information society and surveillance capitalism are first contextualized, presenting the concept of surveillance theories and the economic models explored in which the sensing and IoT market is inserted. In the second chapter, the Internet of Things technology is specifically explored, detailing its functionalities and exploring the problem that involves ubiquitous computing promoted by IoT and the vulnerability of the consumer user. Finally, the last chapter is concerned with discussing the right to privacy, from its emergence as a human value to be preserved until its positivization in the legal system. In addition, it explains the protection of privacy of the consumer user and its (in) sufficiency of protection against the technology of the internet of things in the current context. Appropriately, the research makes room for possible resolutions from the normative point of view and practical mechanisms for a possible extension of consumer protection.

Keywords: internet of things; privacy; surveillance capitalism.

ABREVIATURAS

AWS	Amazon Web Services
D2D	Device to device
H2M	Human to machine
IaaS	Infrastructute as a Service
LGPD	Lei Geral de Proteção de Dados
M2M	Machine to machine
MITS	Micro Instrumentation Telemetry Systems
NIST	National Institute of Standards and Technology
P2P	Person to person
PaaS	Platform as a Service
SaaS	(Software as a Service
TPC/IP	Transmission Control Protocol/Internet Protocol

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

Se Marty McFly embarcasse para o futuro até o momento presente, na velha máquina do tempo de Dr. Brown, que grande invenção atrairia sua atenção? Apesar de muitas predições acertadas na viagem De volta para o Futuro, certamente ainda não temos carros voadores sendo comercializados, tênis ajustáveis, máquinas do tempo ou skates voadores – até onde se saiba. No entanto, sem sombra de dúvidas, a capacidade computacional e de predição alcançou possibilidades não imaginadas nem mesmo na ficção científica cinematográfica em 1985, embora que, acertadamente, foram previstas invenções como cinemas em 3D, câmeras compactas, computadores por todos os lugares, sensores e robôs capazes de cumprir tarefas como passear e limpar.

Para além da ficção, no futuro mediato já alcançado, a sociedade avançou consideravelmente na evolução da Tecnologia da Informação, transformando economicamente os meios de produção, os mecanismos políticas, os meios de comunicação e a interação social, ao passo que a informação se tornou a força produtiva e a matéria-prima geracional. A transformação econômica dos meios produtivos escalou até o status de produtividade baseada na coleta de dados e nas predições informacionais, o que será abordado no primeiro capítulo sobre o Capitalismo Informacional e como se tornou um modelo econômico amplamente difundido, em que todos os fatores concomitantes levaram a uma nova economia em rede.

Para tanto, analisam-se os eventos indissociáveis dos caminhos que levaram à difusão econômica de um Capitalismo Informacional, como a criação e popularização da Internet, os avanços sobre componentes tecnológicos como microprocessadores de baixo custo, o computador pessoal e um sistema operacional de baixo custo criado pela Microsoft. Além disso, são elementos importantes da receita ao capitalismo informacional, bem como o estudo sobre os principais modelos econômicos que sustentam a cadeia econômica informacional.

Pouco a pouco, é possível perceber uma guinada do Capitalismo Informacional para o Capitalismo de Vigilância, contexto em que mais do que acessar dados para produzir resultados com valor atribuível, as indústrias da informação estão voltadas para a construção de modelo de vigilância constante de seus usuários, especulando seus hábitos, seus comportamentos e sua preferência para atingir o melhor resultado preditivo e vendável em um grande leilão da informação.

Para entender como esse modelo de, propõe-se uma reflexão utilizando-se da teoria do Hiperconsumo de Gilles Lipovetsky, que permite um pensamento crítico para se perceber mais do que um ambiente de hiperconsumo, um ambiente de hiperconexão que alimenta a cadeia de

uma economia de vigilância. Sugere-se, então, a expansão conceitual sobre teorias de vigilância, tendo como referência os estudos sobre Capitalismo de Vigilância de Shoshana Zuboff, com reflexões sobre as teorias do Panóptico de Jeremy Bentham e Michael Foucault, para uma conclusão acerca do atual estado de vigilância permeado pela sociedade no contexto de tecnologias informacionais.

No segundo capítulo, compreende-se mais detalhadamente o que é a Internet das Coisas e seu funcionamento, adentrando-se em explicações técnicas quanto à capilaridade física de dispositivos inteligentes e capilaridade lógica por meio de códigos, e como essa tecnologia, unida a outros inventos da atualidade, tem formado um "multiverso" tecnológico e virtual.

A tônica da pesquisa envolve especialmente a Internet das Coisas como componente moderno de vigilância em uma simbiose de computação e vigilância que ocorre de forma leve e pouco perceptível por seus usuários consumidores, além de analisar os modelos econômicos que se mantêm com a personalização e predição dos dados coletados via IoT. Retrata-se, ainda, o contexto normativo em que a Internet das Coisas está inserida e como o desconhecimento sobre sua ação pode afetar negativamente o usuário, apresentando-se riscos da vigilância comumente efetuada por dispositivos inteligentes, tais como a vulnerabilidade dos usuários consumidores, os riscos à privacidade, o marketing predatório e o hiperconsumo.

No terceiro capítulo, contextualiza-se o estado jurídico em que se encontra a definição do direito à privacidade, partindo de sua importância axiológica, a positivação e o surgimento da privacidade no universo do direito, os avanços até o reconhecimento como um direito humano e fundamental. Observa-se ainda a positivação do direito à privacidade na Constituição Federal de 1988, bem como a extensão do direito a outros diplomas infraconstitucionais, como o Código Civil, o Código de Defesa do Consumidor e a Lei Geral de Proteção de Dados.

Por fim, debate-se acerca da (in)suficiência dos dispositivos legais existentes em garantir a tutela do direito à privacidade de usuários consumidores de dispositivos com tecnologia IoT, considerando-se especialmente os avanços normativos que preveem uma legislação específica acerca da Internet das Coisas, a busca por um conceito contemporâneo para privacidade e uma suficiência além da norma, mas de mecanismos de aplicação.

A metodologia utilizada ao longo da pesquisa foi exploratória sobre práticas jurídicas a respeito do tema, observando-se, para elucidar o conteúdo, o que diz a doutrina, a jurisprudência, os dados e as informações que o circundam (QUEIROZ; FEFERBAUM, 2019). Ademais, utilizou-se do método indutivo, tendo sido observados dados, casos concretos, pesquisas existentes, posicionamentos jurídicos e informações sobre o tema, como base teórica da pesquisa (DEMO, 1985).

As fontes pesquisadas são predominantemente bibliográficas, com o objetivo de aprofundar-se acerca do desenvolvimento de tecnologias voltadas à promoção do hiperconsumo, na definição de nomenclaturas essenciais ao tema e na análise de bibliografias que retratam o avanço da tecnologia IoT. Além disso, é realizada uma análise bibliográfica das respostas localizadas na doutrina e jurisprudência acerca da proteção da privacidade do consumidor, conforme recorte delimitado para o tema.

Este trabalho, por fim, retrata uma importante discussão no campo jurídico, social e tecnológico, reunindo elementos atualmente essenciais à sociedade, como a tecnologia da informação, o consumo e o direito à privacidade dos consumidores. Nesse sentido, é necessário refletir acerca dos níveis de proteção que se pretende resguardar ao indivíduo, considerando que a junção entre inovação e livre mercado avança, muitas vezes de maneira predatória, sem preocupar-se com os danos deixados para trás.

Retornando ao questionamento original, se Marty McFly embarcasse para o futuro presente, ouso dizer que encontraria robôs não humanoides, mas em geladeiras, tablets, relógios, lâmpadas e maçanetas, bem como descobriria que a vigilância é a força econômica do momento e o reconhecimento facial é uma realidade. Além disso, precisaria buscar amigos no Facebook para ajudar em sua missão, quem sabe para passar de fase em jogo de realidade aumentada, talvez assistir a um vídeo no YouTube para consertar a máquina do tempo e voltar para casa, entender que dinheiro físico é uma raridade e que o vilão da história não viajaria no tempo para se casar com a mocinha, mas faria tudo pela máquina perfeita capaz de predizer as vontades.

2 DO CAPITALISMO INFORMACIONAL AO CAPITALISMO DE VIGILÂNCIA

> "A privacidade, disse, era uma coisa muito valiosa. Todo mundo queria ter um lugar em que pudesse estar a sós de vez em quando. E quando alguém encontrava um lugar assim, não era senão um gesto da mais trivial cordialidade que aqueles que soubessem do fato guardassem a informação para si mesmos." George Orwell, 1984.

Segmentados no mesmo globo terrestre, 3,5 bilhões de pessoas estão conectadas no mesmo universo da internet, de um total de 7,7 bilhões de pessoas. Aquelas conectadas perfazem quase metade da população terrestre (ROSNER *et al.* 2022), que rapidamente se adaptaram às novas formas de comunicação, sociabilidade, economia, trabalho e indústria, impulsionadas pelas transformações tecnológicas do século XX.

Conectados em rede, metade da população global acessa diariamente serviços disponibilizados pela internet, atualiza a cada instante suas redes sociais, cria novas formas trabalho, novos meio produtivos, promove debates e tem acesso a uma infinidade de informações das quais jamais se imaginou ser possível. Com os avanços tecnológicos, hoje em dia não interagimos mais apenas por meio dos aparelhos tradicionais no meio computacional, como computadores e celulares, mas também com os simples equipamentos do dia a dia, como geladeiras, lava-louças, relógios e carros, que estão conectados à internet. Além disso, os meios tradicionais de comunicação competem com o novo mercado grafado pelas plataformas de streaming, o metaverso, as redes sociais e o mercado de criptomoedas, NFTs e Blockchain.

De fato, o mundo não é o mesmo de poucas décadas atrás, e nem o mesmo de um ano atrás. Em tempos de hiperconectividade, a instantaneidade de transformação quebra recordes diários, ao passo que o mundo de um dia atrás pode ser totalmente diferente na manhã seguinte. Porém, não se atinge tal nível de conectividade sem uma completa transformação econômica, na verdade, sublinha-se uma mudança na cadeia produtiva em escala global no último quarto do século XX, como marco de um novo momento de revolução industrial e o surgimento do que o sociólogo Manuel Castells (2018) nomeia de Capitalismo Informacional.

Em um novo modelo econômico, cuja matéria-prima passou a ser a informação, saber gerar, processar e aplicar conhecimentos e dados tornou-se o novo impulsionador do mercado, que também expandiu fronteiras diariamente, e em escala global, conseguiu atingir novos mercados produtivos e de consumo, tudo isso conectado a uma rede global de informações, que alimenta o modelo econômico do Capitalismo Informacional.

A ascensão do capitalismo informacional ocorreu resumidamente nas últimas três décadas. De acordo com Varian (2006), o "boom" tecnológico e a indústria microeletrônica superaram outras cadeias produtivas para atingir seu ápice até então conhecido, A Internet, em

somente alguns anos, revolucionou a indústria da informação, com a “inovação combinatória” de novos produtos e serviços, bem como uma estruturação econômica para que o capitalismo informacional pudesse prosperar.

A prosperidade de qualquer indústria está na capacidade de extrair o máximo do conteúdo bruto que se possui. Quando Castells (2018) teorizou acerca de uma economia baseada na informação, destacou que a humanidade estava diante de uma descontinuidade, pois a informação ganhava um novo papel como produto do processo produtivo, e assim as novas criações da indústria estariam cada vez mais voltadas ao processamento de informações.

No entanto, como é possível obter cada vez mais informação sobre os usuários para manter um modelo econômico próspero e em ascensão? Por meio de uma ordem econômica fundada no conceito de vigilância. É assim que Shoshana Zuboff define outro advento correlato do Capitalismo Informacional, o então Capitalismo de Vigilância, uma nova organização econômica produtiva “que reivindica a experiência humana como matéria-prima” para uma cadeia de processamento de informações e práticas de mercado.

Neste capítulo, se discorrerá sobre a revolução industrial do Capitalismo Informacional, quais seus efeitos no mercado econômico e político, como se estrutura economicamente e o aparato tecnológico por trás da captação da matéria-prima dessa indústria: a informação. Ademais, o Capitalismo de Vigilância será analisado para compreensão desse novo mercado econômico, que se concretiza por meio de redes, internet, aparatos tecnológicos e todo mecanismo capaz de obter dados e traduzi-los de forma rentável.

2.1 CAPITALISMO INFORMACIONAL: A NOVA ECONOMIA

A década de 1960, nos Estados Unidos, é marcada pelos debates sociais acerca da conquista de direitos civis de minorias e movimentos que opunham à Guerra do Vietnã, ao mesmo passo que grifa o avanço tecnológico fortemente incentivado no Vale do Silício. Nos campus universitários da Califórnia, incentivava-se o pensamento cultural de inovação, o empreendedorismo e a liberdade, bem como expandia-se um espírito libertário que daria origem a uma nova economia com incentivos privados e governamentais (CASTELLS, 2018, p. 65).

Para Morozov (2018, p. 14-15), os primórdios da cibercultura em 1960 prometiam uma espécie de democratização e emancipação social por meio de novas tecnologias que poderiam ajudar a promover os debates sociais da década, em uma ideologia utópica que não viria a se concretizar. Por sua vez, as atividades do Vale do Silício apenas promoveriam novas formas de capitalismo às quais a contracultura tentava se impor.

Essa promessa utópica de emancipação social seria então endossada nas entrelinhas como uma artimanha de contenção aos movimentos sociais, construindo-se uma nova narrativa em que as mudanças viriam a partir do desenvolvimento de novas alternativas. Agências e incubadoras teriam então incentivado uma nova forma de capitalismo que encontraria apoio até mesmo na comunidade contracultural (MOROZOV, 2018, p. 17). Em uma visão mais objetiva, a nova economia teria, entre suas finalidades, o desenvolvimento de tecnologias utilizáveis durante a guerra e a criação de novos modelos de produção, que avançariam ao ponto de comercializar equipamentos eletrônicos em valores populares, graças aos avanços da microeletrônica.

Nos primórdios da sociedade da informação, ainda não havia se constatado uma transformação cultural e econômica, pois se interpretavam os fenômenos decorrentes dos avanços da Tecnologia da Informação como uma continuidade de um modelo do Capitalismo Industrial, como uma nova indústria de serviços. A constatação do surgimento de uma nova economia ocorre após perceber-se que os paradigmas do capitalismo industrial eram insuficientes para sustentar os avanços das tecnologias da informação (LOVELUCK, 2018, p. 107).

Para Benjamin Loveluck (2018, p. 111-112), a economia política passou por uma evolução de caráter liberal, em que fatores como a libertação da centralização política - reforçando-se a ideia da revolução informacional em prol de uma emancipação social – sobre o indivíduo, e a renovação das tendências liberais por meio da globalização, uma tendência à desburocratização, são impulsionadores de um novo paradigma que construiria uma nova economia pautada na circulação da informação como “melhor garantia da liberdade individual” e “fonte do desenvolvimento econômico”.

Uma nova economia não surge somente pela mudança na produtividade ou criação de tecnologias, pois os agentes envolvidos em uma nova economia, as empresas e as Nações, não buscam a produtividade pela produtividade ou o avanço tecnológico por objetivos utópicos, uma nova economia surge quando há no horizonte potencialidade de maior lucratividade e maior valor de ação para empresas privadas, bem como maior competitividade econômica para Nações (CASTELLS, 2018, p. 150).

Para implantar uma nova economia ao ponto de torná-la lucrativa, era necessário ampliar o mercado, aumentar a produtividade, acelerar o giro de capital e reduzir custos de produção; Por essa razão, inicialmente, o mercado da tecnologia informacional americana atendeu às demandas militares, até que se conquistasse ampliação suficiente do mercado e houvesse de fato grande produtividade a ponto de atingir lucratividade com investimentos em

inovação tecnológica para todos os setores, conquistando uma fatia maior do mercado (CASTELLS, 2018, p. 151).

A ampliação do mercado para uma economia informacional ensejou mudanças como uma descentralização regional, impulsionando a globalização e quebrando fronteiras do capital, e o aumento da capacidade de obter e processar a informação para a cadeia produtiva. Assim, nos primeiros anos de economia informacional, com a expansão global e ampliação de mercados, as empresas de modo geral aumentaram sua lucratividade na década de 90, iniciando um retorno financeiro feito no investimento em tecnologias da informação. Enquanto isso, empresas diretamente ligadas às tecnologias de informação tiveram grande crescimento de produtividade e lucratividade, gerando uma recapitalização ou novo capitalismo (CASTELLS, 2018, p. 152-154).

Em síntese, o capitalismo informacional não está relacionado somente com uma nova matéria-prima baseada na informação, mas na construção de um novo modelo organizacional produtivo que é interdependente de outros fatores para se concretizar, como a descentralização regional, ampliação de mercados, lucratividade e competitividade, e também é geradora de transformações sociais, culturais e institucionais.

Manuel Castells (2018, p. 154) conclui que toda atividade produtiva requer transformações de ordem social, cultural e institucional, assim a economia é informacional e "não apenas da informação", pois todos "os atributos culturais e institucionais de todo o sistema social devem ser incluídos na implementação e difusão do novo paradigma tecnológico".

De acordo com Freeman *et al.* (1988) *in* Castells (2018), esse novo paradigma tecnológico se dá por um conjunto de inovações técnicas, organizacionais e administrativas, que produzirão, além de sistemas e produtos, a construção de uma nova dinâmica da estrutura de mercado a partir da transformação tecnológica e da informação e como essa transformação age sobre a sociedade.

Manuel Castells (2018) é quem melhor sintetiza as características desse paradigma da Tecnologia da Informação para compreensão do que perfaz a nova economia do Capitalismo Informacional, sendo elas: Informação, Penetrabilidade, Lógica de rede, Flexibilidade e Convergência de tecnologias. Essas características remontam ao Capitalismo Informacional, dentro do contexto único que possibilitaria o surgimento de uma nova economia a partir da informação, mas também todos os fatores concomitantes a uma realidade econômica, social, política e cultural por meio das redes.

Alguns eventos são indissociáveis da compreensão acerca da aderência Capitalismo Informacional na sociedade a partir de 1960, como a criação da Arpanet (*Advanced Research*

Projects Agency Network), antecessora da Internet, que foi uma rede de comunicação horizontal entre redes autônomas, desenvolvida pelo Departamento de Defesa dos Estados Unidos que visava proteger os sistemas de comunicações americanos de um ataque da então União Soviética durante a Guerra Fria, sendo a precursora da rede atual (CASTELLS, 2018, p. 65).

Em 1974, Vinton Gray Cerf e Robert Elliot Kahn trabalharam na construção de um novo protocolo de rede, criando o primeiro protocolo núcleo capaz de ligar a Arpanet a outras redes heterogêneas, esse protocolo era o Transmission Control Protocol (TCP). Mais tarde, foi possível a conexão de um novo protocolo: Internet Protocol (IP), com sua junção formando o protocolo de rede TPC/IP, o mais utilizado até a atualidade (WAZLAWICK, 2016, p. 499-500).

Assim, evoluiu e expandiu-se rapidamente pelos campus universitários, aquecendo uma cultura de liberdade por meio da rede e, futuramente, tornou-se um fator elementar na construção da nova economia e da cultura em rede. Segundo Loveluck (2018), uma nova forma social de caráter essencialmente liberal ganha forma na Internet. Para uma verdadeira difusão da tecnologia da informação, foi necessária uma evolução dos componentes tecnológicos computacionais. Além dos avanços estruturais, o desenvolvimento de circuitos integrados com a capacidade de unificar em uma unidade a central de processamento do computador possibilitou a criação de microprocessadores.

Em 1968, Ted Hoff, trabalhando em projetos da Intel, projetou uma nova tecnologia a partir dos chips de silício, unindo na mesma arquitetura funções de memória estática, memória dinâmica para dados, microprocessador e processador de informações *input* e *output*. Dessa forma, computadores passaram a utilizar esses microprocessadores no lugar das antigas estruturas magnéticas (WAZLAWICK, 2016, p. 420). A criação dos microprocessadores foi importante ao crescimento da tecnologia computacional, afinal, a partir do microprocessador Intel 8080, a história da tecnologia da informação se desdobraria na construção do primeiro computador pessoal.

Em 1975, a MITS (Micro Instrumentation Telemetry Systems) anunciava a criação e comercialização do Altair 8800, o primeiro computador pessoal. A partir de então, o público com acesso e interesse em computação expandiu-se drasticamente, de militares e acadêmicos, os novos interessados eram também amadores curiosos pela nova tecnologia. Esse advento abriria uma nova porta no mercado para as empresas de tecnologia computacional, iniciando-se uma nova base econômica por meio da venda de computadores individuais e de seus aparatos.

Do ponto de vista social, Loveluck (2018, p.68) destaca que a popularização do computador individual era também defendida como base para uma ideologia de libertação do indivíduo pelo computador "*computer liberation* – uma expressão ambígua que designa tanto

uma libertação dos computadores quanto uma libertação (dos indivíduos) pelo computador". Esta ideologia reaquecia os discursos da contracultura vinculados à cibercultura, como respostas à centralização e burocratização, que podiam ser tanto base para reações, como fundamento para o interesse nas tecnologias da informação como forma de libertação.

Sobre o Altair 8800, ele tinha como objetivo ser simples em manuseio mediante comandos e dados visualizados a partir de um painel de luzes, sem uso de monitor ou teclado. De acordo com Wazlawick (2016, p. 498), foi um sucesso ao ser comercializado, principalmente por conta do preço acessível alcançado pela Micro Instrumentation Telemetry Systems (MITS). Foi a partir de um protótipo do Altair 8080, utilizando do chip Intel 8800, que Bill Gates e Paul Allen viram a oportunidade de iniciar um software para esse computador pessoal. Foi então que, em 1975, eles desenvolveram o BASIC para o Altair 8080, (GATES, 1995, p. 33), software o qual consistia em uma linguagem computacional simples e popular, que possibilitou a venda e operação de microcomputadores popularmente.

Inicialmente, a criação rendeu aos inventores um contrato de dez anos com a MITS, sobre os royalties e direitos sobre o BASIC do Altair. Porém, alguns anos antes da conclusão do contrato com o preço elevado do sistema operacional, os casos de pirataria para obter o sistema clandestinamente fizeram com que Bill Gates criasse sua nova empresa com o objetivo de proporcionar a venda do sistema operacional a baixo custo com o intuito de descontinuar a pirataria. Com isso, foi fundada a primeira empresa de software computacional do mundo, a Microsoft (WAZLAWICK, 2016, p. 497-498).

A junção dessas quatro invenções parecem ser o ponto de inflexão necessário para a solidificação do Capitalismo Informacional, pois com computadores individuais, de capacidade operacional simples, com preços acessíveis à grande parte dos consumidores e com uma rede de comunicação como a Internet, os paradigmas da nova economia se expandiram. A descentralização de poderes econômicos e a desburocratização se tornaram realidade por meio das redes, e a criação de novas tecnologias, que passam a atuar em todas as áreas da vida moderna, amplia ainda mais a fatia econômica ocupada pela economia informacional. Dessa forma, a era do compartilhamento de informações se torna uma realidade.

2.2 ESTRUTURA ECONÔMICA E ALGUNS MODELOS DE NEGÓCIOS DO CAPITALISMO INFORMACIONAL - BIG TECHS

Para que uma nova fase do capitalismo, ou uma recapitalização, possa ascender, como ocorreu com o Capitalismo Informacional, é necessário que os ativos em alta também sejam

diversificados, como outrora na fase Industrial. Nas últimas três décadas, a grande aposta e o "novo petróleo" é a informação. A base da nova economia, quando bem explorada, chega a números surpreendentes, como o valor de ações na bolsa das empresas Facebook, Amazon, Alphabet e Microsoft, que em 2017, ultrapassaram o equivalente ao PIB da Noruega. Ou seja, a informação superando um ativo tradicional da indústria (MOROZOV, 2018, p. 170).

Para Morozov (2018, p. 171), assim como o petróleo, as informações são extraídas, mas ao invés de jazidas, os indivíduos ou usuários são as fontes infindáveis das informações que as Big Techs precisam para lapidar modelos de negócios, especialmente voltados à publicidade ou ao *deep learning*, em uma espécie de troca em que as redes proporcionam a distração e o usuário cede dados, mas ao contrário ao petróleo, o usuário parece ser a fonte de matéria-prima infinita.

A troca velada entre usuário, máquina e redes, em uma ciranda em que distrações, entretenimento e significação são proporcionados com simples cliques de distância, de certa forma, não é desconhecida, e que não há "almoço grátis" nas redes também é algo implícito, mas o que não se tem esclarecido aos usuários é de que forma as informações podem se tornar ativos rentáveis e monetizados. A nova realidade é baseada em uma economia estruturada sobre a exploração das informações dos usuários, o uso de inteligências artificiais e tecnologia Big Data, o direcionamento de publicidade e os filtros invisíveis de personalização, tudo depende do plano de negócio estabelecido. Além disso, alguns enredos podem exemplificar melhor a estrutura econômica por trás da economia da informação.

2.2.1 Economia de busca e o maior leilão do mundo

"Como o Google vai fazer dinheiro?", a pergunta foi feita em 1999 por um repórter na coletiva de imprensa do anúncio formal sobre a criação da empresa Google Inc., ocorrida em Stanford, no Gates Building. A resposta evasiva de Sergey Brin era de que o objetivo "é maximizar a experiência do usuário, e não maximizar a receita por busca" (LEVY, 2012, p. 73). Por muito tempo, tornar pública essa resposta não era do interesse do Google, afinal, a receita para lucratividade por meio de um sistema de buscas havia sido encontrada e poderia ser explorada ao máximo sem intervenções. Desde a criação, em 1999, até abrir seu capital ao IPO, Larry Page e Sergey Brin, assim como todos com acesso à rentabilidade da empresa, mantinham a resposta protocolar sobre encontrar lucratividade mediante anúncios, sem que a lucratividade fosse de fato o objetivo da empresa.

A monetização por meio de ferramentas de pesquisa não é propriamente uma inovação do Google, afinal, o método de lançar publicidades em sites de buscas já era utilizado em outros

portais, como Yahoo ou GoTo. Contudo, a publicidade nos moldes tradicionais não agradava aos criadores do Google, que tinham o propósito de monetizar com publicidade sem utilizar os anúncios gritantes e chamativos, que, muitas vezes, mais incomodavam o usuário do que produziam um retorno efetivo ao anunciante. Ou seja, a ideia era obter resultados e manter a pesquisa orgânica sem desagradar o usuário.

Assim criou-se o Google AdWords, um sistema de autosserviço em que o próprio anunciante poderia comprar espaço no resultado das pesquisas realizadas no buscador do Google. De forma extremamente simples, bastaria ao anunciante um cartão de crédito e os dados de seu anúncio, e o sistema então se encarregaria de alocá-lo, orientando-se por um sistema de qualidade do anúncio, número de cliques e possibilidade de pagamento de acréscimos por uma melhor posição no resultado da pesquisa (LEVY, 2012).

Uma readequação matemática levou a uma readaptação do sistema de monetização do Google AdWords Select, adotando o sistema de leilões pelo espaço de anúncio. Dessa maneira, os anunciantes fazem lances acerca de quanto vale o espaço que será ocupado por resultado de busca, ampliando a competitividade entre anunciantes pelo espaço em rede. O sistema de leilões do Google diferencia-se por não obrigar o vencedor do lance a pagar o valor máximo ofertado, mas somente um centavo a mais do que o lance do vice-vencedor (LEVY, 2012). Assim, o vencedor do leilão ocupará espaço de destaque, sem que tenha um grande custo a mais do que seu concorrente, que estará em posição imediatamente próxima na cadeia de anúncios.

Após o lançamento do Google AdWords Select, grandes anunciantes passaram a buscar pela ferramenta, tornando os espaços de anúncio cada vez mais valiosos, com lances determinados pela competitividade entre usuários e o quanto estavam dispostos a pagar por visibilidade. Foi assim que a empresa valorizou a ponto de abrir o capital e ter que expor ao mundo como vinha monetizando por meio de buscas.

A lucratividade por trás dos leilões do Google está na competitividade para ocupar determinados espaços na página de buscas, que também dependerá da concorrência entre as marcas por nicho de produto. Hal Varian, o economista chefe do Google desde 2002 e responsável pela estrutura econômica do sistema de leilões de anúncio (CAMARGO, 2020), explica que a metodologia utilizada pelo Google envolve atingir o menor lance e acirrar a competitividade pela melhor posição disponível, bem como esclarece que a receita só é significativa se houver concorrência (VARIAN, 2006).

É preciso entender que é uma relação que envolve um equilíbrio de atividades entre anunciante, licitante e usuário. A disposição de slots na página é determinada pelo quão valiosa ela é, cujo valor é medido por uma regra qualitativa que estima a qualidade dos anúncios e

quantos cliques eles conseguem atrair. Assim, estimando-se um histórico de alcance dos anúncios, é possível precificar o lance por clique (VARIAN, 2006).

> A classificação dos anúncios é baseada nos lances vezes os efeitos específicos do anúncio: Ba Ea. O lance é em dólares por clique e o efeito específico do anúncio é cliques por impressão. Portanto, Ba Ea é o lance por impressão: quanto o anunciante está disposto a pagar para que seu anúncio seja exibido a um usuário. O anunciante com o maior valor para uma impressão recebe a melhor posição: a posição com maior probabilidade de receber um clique. O anunciante com o segundo maior valor por impressão obtém a próxima melhor posição e assim por diante.[1]

Dessa forma, o que determina o valor de cada lance e posição é a expectativa de alcance e cliques que aquele licitante pode atingir, logo, para obter maior rentabilidade, o licitante também desempenhará o papel de tornar seu espaço atrativo para obter melhor valor de lance, e o anunciante considerará, em seus lances, o custo que deverá assumir para atingir os cliques esperados.

Outro aspecto relevante para que esse modelo de rentabilidade funcione é a utilização do algoritmo de correspondência para exibição dos anúncios e, nesse ponto, entra a participação do usuário. Para Varian (2006, p. 3), o site de buscas faz uma espécie de casamento entre a busca do usuário e aquilo que pode corresponder em possíveis anúncios, "o usuário insere uma "consulta" e o anunciante compra "palavras-chave"". O anunciante então escolhe se o anúncio surgirá como resposta exata às palavras-chave ou se corresponderão ao sentido amplo da pesquisa realizada.

Assim, algoritmos de correspondência são comumente utilizados na união bilateral entre o que é pesquisado e o que pode ser ofertado à título de anúncios. Pensando em um algoritmo mais aprimorado na interpretação da vontade do usuário, o Google então investiu U$ 42 milhões e 1% de suas ações na compra do algoritmo Applied Semantics, que seria adaptado para trabalhar com o Google AdWords e passaria a se chamar Google AdSense (LEVY, 2012).

O AdSense é o algoritmo responsável por analisar o conteúdo de preferência dos usuários e, de certa forma, atribuir um resultado correspondente aos anúncios que se adequariam ao que o usuário buscava. Além de utilizar-se do algoritmo na página de buscas, a empresa investiu em comprar espaço dentro dos sites e blogs; assim, divulgadores vendiam um espaço dentro de suas páginas, um fragmento de código era inserido e o AdSense passava a

[1] Texto original: "The ranking of ads is based on bids times ad-specific effects: baea. The bid is dollars per click and the ad-specific effect is clicks per impression. Hence baea is bid per impression: how much the advertiser is willing to pay for its ad to be shown to a user. The advertiser with the highest value for an impression is given the best position: to position most likely to receive a click. The advertiser with the second highest value per impression gets the next best position, and so on."

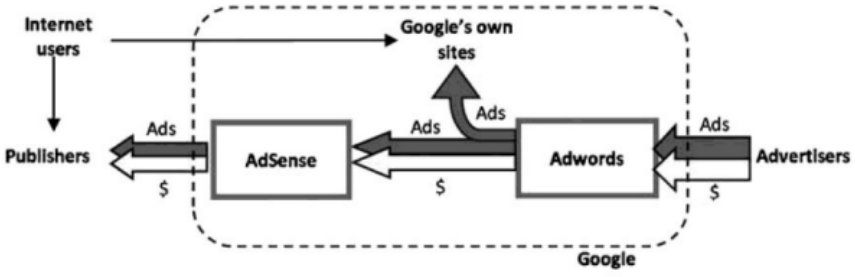
analisar os comportamentos, as pesquisas e os cliques para adotar a melhor estratégia de anúncio a ser utilizada naquele espaço, dinâmica que passou a render cerca de U$ 2 milhões por dia (LEVY, 2012).

O sistema AdSense possibilita uma forma de rentabilidade aos divulgadores, e em contraponto, oferece aos anunciantes resultados personalizados que têm se aprofundado para muito além da correspondência entre palavras-chave. A aferição do AdSense atualmente baseia-se em informações dos usuários como idade, sexo, idioma, localização e interesses. Dessa forma, o Google, utilizando o próprio histórico de buscas do usuário e analisando o comportamento deles dentro das páginas, consegue, por meio do algoritmo, maior acuracidade na personalização do anúncio a ser divulgado pelo AdSense (DESNICA *et al.* 2014).

A sistemática de como essa análise ocorre no Google e como se torna rentável se inicia com a compra do espaço para anúncios pela própria empresa, o que cria a possibilidade de rentabilidade aos sites e blogs. Com o espaço adquirido, a empresa insere códigos *cookies* que armazenam informações sobre as preferências dos usuários ao acessarem ao site. Por conseguinte, o AdSense analisa essas informações para determinar qual o melhor anúncio a ser exibido. À medida que os usuários acessam sites que contenham *cookies* de publicidade, o Google consegue armazenar suas informações para uma análise posterior (DESNICA *et al.* 2014).

Com essa profunda base de dados, os anúncios indicados pelo AdSense tornam-se cada vez mais específicos e precisos às vontades dos usuários. Não é incomum, portanto, a quem está diariamente conectado à internet passar a receber anúncios para uma viagem à praia após uma busca específica pela previsão do tempo de determinada região litorânea. Em uma exemplificação de como atuam Google AdWords e AdSense, Desnica *et al.* 2014 trazem a seguinte ilustração para melhor compreensão:

Figura 1 - Título



Connection between Google's AdWords and AdSense [9]

Fonte: Denisca *et al.* (2014).

As funcionalidades e a monetização mediante anúncios só foram trazidas a público, e com poucos detalhes, após a abertura do capital do Google. A finalidade dessa ocultação de informações não se dá somente pela estrutura econômica por trás do maior site de buscas do mundo, mas pelos debates acerca do uso de dados dos usuários que poderiam surgir e confrontar a política de "maximizar a experiência do usuário e não maximizar o lucro".

Para Gustavo Camargo (2020, p. 50), essa política econômica por meio dos leilões e tratamentos de informações gera um sistema sofisticado de maximização de resultados para publicidade e anúncios, com uma política bem delineada à correspondência bilateral de "o usuário certo sempre na mira do anúncio certo". A economia de busca não é exclusividade do Google, mas é um dos planos de negócios mais lucrativos do capitalismo em rede, e para que ele funcione, é necessário o máximo de informações possíveis dos usuários e de tempo possível de usuários conectados aptos a receberem anúncios.

Camargo (2020) ainda destaca a participação ativa do usuário para que esse modelo de negócio funcione, afinal, é necessário que o usuário esteja conectado para que seus acessos possam ser leiloados instantaneamente e que deixe o máximo de rastros possíveis com seus dados para que os anúncios possam atingir ao alvo. Muito embora seja o usuário um sujeito ativo nesse modelo de negócio, sua participação está restrita a fornecer dados e tempo disponível conectado.

O modelo de economia de busca é uma das principais ferramentas do capitalismo informacional, que não é utilizada somente por uma empresa, mas tornou-se parte da cultura em rede. É um dos métodos de monetização na estrutura econômica atual, em que os agentes principais da cadeia produtiva são aqueles que, em grande parte, estão alheios ao seu grau de participação nessa relação negocial.

Atraídos por serviços gratuitos e facilidades da sociedade em rede, usuários ainda se mostram inconscientes de sua importância para que a cadeia produtiva desse modelo econômico possa avançar ou se manter, ou até mesmo dos riscos aos quais seus dados estão sujeitos em nome da conectividade. Esse debate, embora evitado a princípio pelos criadores da economia de busca, enseja o estudo de mecanismos de proteção, regulatórios ou procedimentais, que possam proteger o protagonista da economia de pesquisa.

2.2.2 Economia do compartilhamento online

Ao entrar na página inicial do Facebook, o usuário logo verá, no canto direito da tela, a proposta da rede: “O Facebook ajuda você a se conectar e compartilhar com as pessoas que fazem parte da sua vida”. Se extrairmos os dois verbos da frase, teremos sinteticamente o modelo econômico seguido pela rede, que é baseado em conectar o maior número de usuários e construir um arquétipo de compartilhamento constante da vida, das experiências, dos entretenimentos, dos debates políticos e de um pouco de publicidade em meio a tudo.

A economia de compartilhamento ganha força especialmente entre os sites e as redes sociais, os quais são espaços online onde usuários sentem-se livres para conectar-se, criar conexões com outros usuários e participar de uma troca de interações e conteúdo. Não há um nicho estabelecido, pois tudo pode ser compartilhado nas redes sociais. Como exemplifica Valente (2017), em cada rede, o usuário pode ter conexões mútuas ou unidirecionadas, nos mais diversos formatos de mídia, como os textos via Twitter, imagens no Instagram, conversas no WhatsApp ou um conjunto de tudo no Facebook.

Para Mucelin (2021), a partir da transição da Web 2.0 para a Web 2.5, a cultura da conectividade e do compartilhamento foi impulsionada, principalmente pelo surgimento das comunidades em rede em que usuários poderiam criar perfis e interagir online. A Web 2.5 é marcada pela conexão móvel ou Mobile Web, momento protagonizado pelo aparelhos móveis, como smartphones e tablets, que ganham conectividade com a internet, permitindo que o usuário possa estar sempre on-line.

A mudança e aderência a uma cultura de compartilhamento não ocorre subitamente. Para Mucelin (2021, p. 40), há três importantes características destacadas por Nicholas John que explicam a aderência ao compartilhamento: “1) a aparência difusa do que é compartilhado; 2) o uso do vocábulo “compartilhar” sem o objeto a ser compartilhado; 3) o uso da palavra para designar novas situações.”

A aparência difusa do que será compartilhado está na ideia geral de não haver um objeto, gênero ou conceito do que será compartilhado, não há nada definido e assim o usuário é quem decide o que irá compartilhar (MUCELIN, 2021). Pode compreender-se, dessa característica, a descentralização de objetos materiais, mas foco na experiência virtual, em que todos podem participar e, teoricamente, compartilharão algo e participando à sua maneira, não estarão sozinhos – teoricamente.

Há ainda, como segunda característica, uma mudança na definição de compartilhar. Nas redes sociais, o compartilhamento é a chancela de pertencimento à nova realidade virtual, aos grupos, às comunidades e aos círculos de interação, sendo necessário compartilhar para participar. Vale destacar as palavras de Mucelin (2021, p. 41) sobre o Facebook: “compartilhar

é a condição para usufruir plenamente das funcionalidades disponibilizadas pelo site. Em algum momento, algo seu também será compartilhado, mesmo que na forma de dados e mesmo que não se tenha ciência".

E por fim, a terceira característica diz respeito a uma nova definição do que é compartilhado, não há limites claros, assim "se compartilha o que antes não era compartilhável", não há um objeto, há apenas comunicação e distribuição, criação de conteúdos virtuais e atualização de status (MUCELIN, 2021). Para fins de definição, Mucelin (2021) considera a economia de compartilhamento como atividade econômica proporcionada pela Internet, pelos sites e pelas redes sociais, e oportunizam um modelo de negócio pautado no compartilhamento pelos usuários, sejam elas pessoas, empresas ou governos realizando atividades públicas ou privadas.

Benjamin Loveluck (2018) categoriza a economia de compartilhamento como uma das dimensões da economia em rede, um dos axiomas. Ele considera que capitalizar a partir do compartilhamento atende à necessidade da estrutura econômica de obter um grande volume de dados. Por essa razão, no centro da economia de compartilhamento, está a captação de informações, e em seu âmago, o uso de redes e serviços gratuitos que atraiam os usuários para interações, compartilhamentos, conteúdos e atuação ativa, ao passo que fornecerão à rede os dados necessários para manter esse modelo de negócio embalado.

Em outra teoria, Lisa Gansky (2010, p. 20) compreende a economia de compartilhamento como uma grande malha – *mesh,* mantendo o termo original, em que o modelo de negócio é compartilhar, em que as características da malha são o "compartilhamento, uso avançado da Web, redes de informações móveis (...) e envolvimento com clientes por meio de redes sociais". Para a autora, o crescimento desse modelo acompanha o crescimento das redes sociais, das redes sem fio e da internet.

De um modo geral, o apanhado de ideias centraliza a economia de compartilhamento como um modelo de negócio, cujo funcionamento se dá por meio dos sites e redes sociais, em uma cultura de compartilhamento, onde os usuários são incentivados a participarem ativamente do compartilhamento de suas vidas, preferências, opiniões ou simplesmente estarem inseridos dentro dessas comunidades de compartilhamento.

Em outro viés mais técnico, vale adaptar o questionamento feito em outrora: "como as redes fazem dinheiro?". A resposta é que as redes também utilizam um sistema de leilões, assim como o Google, mas ainda mais sofisticado, a exemplo de Camargo (2020), que utiliza o Facebook para uma análise das considerações necessárias em seu sistema de leilões. Devida às suas características, o Facebook precisa de um sistema de leilões que observe suas

peculiaridades, como a análise de informações específicas para a finalidade do anúncio, como amigos próximos e publicações do usuário, além de manter o ambiente orgânico do *feed*. Ademais, sua estrutura realiza leilões instantâneos a todo momento, sempre que o usuário entra no feed (CAMARGO, 2020).

Nessa sistemática, as redes sociais fazem uma economia de compartilhamento, e seu material produtivo vem da atuação ativa dos usuários, no compartilhamento de suas preferências, mas também em seus círculos sociais, opiniões e impressões. Na economia de busca, o usuário tornou-se o protagonista da cadeia produtiva informacional, enquanto que, na economia de compartilhamento, o usuário e suas experiências compartilhadas se tornam a própria força motora.

2.2.3 Economia em nuvem

A maior livraria da Terra, assim ficou conhecida a Amazon, o maior site de vendas on-line do mundo, criado por Jeff Bezos em 1994, a princípio, se propunha à venda de livros on-line, mas com a expansão crescente de forma tão rápida fez com que um novo modelo de negócio surgisse no imaginário do fundador (STONE, 2013). ela investiu em um sistema de API (*Application Programming Interface*), que permitiria que desenvolvedores externos pudessem utilizar a página da Amazon na web para publicar produtos, utilizando seu sistema de vendas e pagamentos.

Por meio dessa ferramenta, a Amazon estava abrindo sua página para um novo modelo de negócio e assim formando a *Amazon Web Services* ou AWS (STONE, 2013). Esse modelo construiu um conceito de computação em nuvem, que se trata de negociar com outras empresas a locação de um espaço dentro do sistema de computação da Amazon, assim empresas como Netflix e Pinterest utilizam os servidores da AWS para lançar suas operações na internet, como explica Brad Stone (2013).

Dessa maneira, além de varejista, a Amazon tornou-se uma empresa de infraestrutura computacional baseada em nuvem e uma das principais no ramo. As nuvens computacionais se tornaram um serviço que fornece infraestruturas computacionais, como recursos de armazenamento, computação e serviços para o mercado. Na definição de Soares (2014), é um modelo de infraestrutura com amplo acesso que atende a demandas de recursos computacionais com rapidez e fácil gerenciamento, mediante virtualização, monitoramento e acessibilidade (SOARES, 2019).

A computação em nuvem possui três modelos principais de serviços conforme a NIST *(National Institute of Standards and Technology),* sendo (SOARES, 2019):

a) IaaS *(Infrastructute as a Service)*: os recursos são disponibilizados pelo provedor diretamente e o usuário consegue gerenciar e controlar virtualmente, de maneira independente, sistemas operacionais e aplicações;

b) PaaS *(Platform as a Service)*: o usuário gerencia as aplicações executadas na máquina virtualmente por meio de uma plataforma disponibilizada, e o provedor é quem gerencia a infraestrutura de rede, o armazenamento e os sistemas operacionais;

c) SaaS *(Software as a Service)*: o usuário acessa uma interface, cujos controles estão limitados; sem acesso direto às máquinas, faz uso das aplicações ofertadas pelo provedor.

Com esse modelo de negócio, a Amazon, por meio da AWS, se tornou a maior operação de computação em nuvem do mundo, com serviços de IaaS. De acordo com Camargo (2020), essa oferta de capacidade computacional e serviços digitais especializados facilita a expansão do uso e é uma vantagem ter tantos desenvolvedores trabalhando no mesmo ambiente computacional. Do ponto de vista mercadológico, a Amazon não costuma revelar seus ganhos com AWS, mas em sua rede computacional, há algumas das maiores empresas e Startups em desenvolvimento que alugam esse espaço para criar e geram uma receita significativa.

Compreendendo-se que o Capitalismo Informacional é um fato presente no contexto atual de produção, política e consumo, entender como alguns dos modelos de negócio por trás da estrutura econômica do novo capitalismo funcionam é fundamental para avançar nas discussões sobre seus efeitos na sociedade e no campo jurídico. Os modelos econômicos seguidos pelas maiores empresas de tecnologia da atualidade, como Google, Facebook e Amazon, estão infiltrados no dia a dia da sociedade, constituindo-se em um método de produtividade e economia ensinado e seguido culturalmente, além de afetar outras áreas como reflexos jurídicos a privacidade.

Em contrapartida, o cenário atual de Capitalismo Informacional só poderia ser atingido com construção de uma estrutura econômica para respaldar a lucratividade não só dessas empresas, mas de todos os envolvidos no contexto da sociedade em rede. Atualmente, é difícil imaginar uma atividade lucrativa que não passe por algum mecanismo digital. No campo do consumo, o capitalismo informacional apresenta seus reflexos, desde anúncios direcionados até análise comportamental, e o ato de consumir protagoniza o cerne das tecnologias digitais desenvolvidas, em grande maioria, para entregar conteúdo e opções de consumo. Nesse aspecto, essas interações de consumo podem ser mais bem compreendidas no estudo da Sociedade de Hiperconsumo.

2.3 A SOCIEDADE DE HIPERCONSUMO E MASSA NA ERA DA INFORMAÇÃO

Se toda a cadeia social está constantemente conectada para a manutenção de uma vida social on-line, opinando on-line, iniciando relacionamentos on-line, debatendo on-line, estudando on-line, consumindo on-line, e realizando até as atividades mais corriqueiras pelas redes, estamos diante de uma hiperconexão, que já é realidade e não mais um ideal futurístico. Compreende-se que o Capitalismo Informacional, moldado pela estrutura econômica dos cliques, *likes* e acessos, funciona por meio da conexão contínua de usuários, seja realizando pesquisas e deixando rastros sobre suas preferências de navegação, seja pela autoalimentação das redes pelos próprios usuários, tecendo, em seus feeds, a vida que vivem ou gostariam de viver.

Este cenário hiperconectado, na analogia de Harari (2016, p. 374), se assemelha a uma religião, o "Dataísmo", a religião da sociedade dos dados, em que "o Universo consiste num fluxo de dados e o valor de qualquer fenômeno ou entidade é determinado por sua contribuição ao processamento de dados", organismos e redes podem ser interpretados por bons algoritmos, e toda a sociedade está atrelada a essa entidade de dados.

De forma análoga, não é demasiado afirmar que a sociedade de fato está hiperconectada, e as estruturas econômicas do capitalismo informacional moldaram um cenário predominante de conexão para sustentar a atual formulação econômica. Porém, ainda antes da hiperconexão, Lipovetsky (2007) tecia sua teoria sobre uma Sociedade de Hiperconsumo e Massa, passados diversos estágios da sociedade industrial e da sociedade de consumo, a modernidade então atinge um estado onde democracia, emancipação e representatividade podem enfim estar relacionados com outra atividade comum à civilização humana, ao consumo.

Emancipação social, democracia e representatividade individual já foram temas de um debate por direitos individuais em 1960, e especialmente no Vale do Silício, onde a Tecnologia da Informação era a promissora solução para conquista de espaços pela contracultura. Os vínculos que podem ser constatados entre a Teoria do Hiperconsumo e o Capitalismo Informacional são importantes referências para a percepção social e econômica das atividades de consumo do público hiperconectado.

2.3.1 A democratização no seu carrinho de compras, clique para confirmar

A trajetória até a Sociedade de Hiperconsumo passa por estágios que acompanham as mudanças causadas pelas revoluções industriais nos demais setores da sociedade, especialmente as mudanças em relação ao consumo (LIPOVETSKY, 2007). Para fins de conceituação, Gilles Lipovetsky (2007) descreve em três fases os impactos e as mudanças no consumo que possuem relevância na contextualização conceitual, sendo elas: a) Era do consumo; b) Sociedade de consumo de massa; e c) Sociedade de Hiperconsumo.

A primeira fase, traçada pelo autor como Era de Consumo, consiste no início da Revolução Industrial, com a produção de itens em grande volume e com logística mais barata. O consumo de bens industrializados e produzidos em escala começa a crescer, o marketing de massa ganha espaço no papel de instruir uma identificação entre consumidor e produto. C com mais do que um produto, surgiu um status autenticado pelo poder de compra ainda muito limitado a classes específicas de consumidores, tendo em vista os escassos recursos financeiros das classes em geral (LIPOVETSKY, 2007)

A Sociedade de Consumo, por sua vez, é grafada pelo Fordismo industrial e produtivo, método que impulsionou o crescimento da capacidade das linhas de produção, com efeito direto ao preço de mercado dos itens produzidos em larga escala, dinâmica que proporcionou o maior poder de consumo de modo geral. Outro aspecto da Sociedade de Consumo mencionado pelo autor seria o processo de "democratização" do poder de compra, que se funda no pensamento de que as linhas produtivas fordistas proporcionaram o consumo de ainda mais bens por um grupo ainda maior de indivíduos e classes, em preço ainda mais acessível, condição explorada pelas linhas de montagem e produção de produtos padrão em larga escala (LIPOVETSKY, 2007).

A ênfase na Sociedade de Consumo está na "abundância" de produtos à disposição por preços baixos, uma vez que a economia e o consumo estão consolidados na quantidade produzida e vendida. Nesse contexto de abundância, a sociedade de "desejos" pode imperar, pois o marketing guia os consumidores mediante estímulos lançados pelo mercado, criados pela publicidade, como signos de identificação entre o consumidor e o produto/marca consumido. Há, portanto, um significado por trás do produto de consumo (LIPOVETSKY, 2007).

A Sociedade de Hiperconsumo, proposta por Lipovetsky (2007), desponta em outro sentido. Nessa sociedade, o consumidor não estaria em busca de atender aos desejos estimulados pelas marcas, mas às vontades individuais na busca por uma espécie de democratização de conforto, lazeres, qualidade de vida e saúde. Para o autor, o momento é de consumo voltado às necessidades e não necessariamente na exibição de bens, assim, o

marketing também é voltado à publicidade, que busca entender às necessidades e às sensações e ofertar bens que atendam aos serviços e não necessariamente status.

Na busca de atender às suas necessidades individuais, de acordo com o autor, surge a figura do *Homo consumericus*, o indivíduo moderno que responde sua existência por meio do consumo de bens e serviços, no lugar de selos tradicionais vindos da religião ou da política, a identidade social estaria cada vez mais ligada ao consumo (LIPOVETSKY, 2007). É esse fator identitário que também transforma as ferramentas de *marketing*, antes voltadas à criação da moda simplesmente, transformou-se em "marketing sensorial", que busca atender ao consumo emocional praticado pelo mercado de consumidores (LIPOVETSKY, 2007).

Assim, compreende-se que a teoria do Hiperconsumo de Lipovetsky define que o momento vivido pela modernidade é de um consumo democrático de representatividade, em que os indivíduos podem finalmente ter maior poder de compra e maior expressão de suas identidades individuais mediante bens e serviços à sua disposição. Trata-se de uma espécie de emancipação social por meio do rastreamento das necessidades individuais e da disposição de um grande volume de produtos acessíveis no mercado de consumo moderno.

Nesse sentido, descreve Lipovetsky (2007):

> Não se vende mais um produto, mas uma visão, um "conceito", um estilo de vida associado à marca: daí em diante, a construção da identidade de marca encontra-se no centro do trabalho da comunicação das empresas. Na fase ui, o imperativo de imagem deslocou-se do campo social para a oferta de marketing. Não são mais tanto a imagem social e sua visibilidade que importam, é o imaginário da marca; quanto menos há valor de status no consumo, mais cresce o poder de orientação do valor imaterial das marcas.

Na fase do Hiperconsumo, objetos eletrônicos são consumidos a título de abrir espaço para uma suposta independência pessoal. Lipovetsky (2007, p. 52) entende que é por meio do consumo-comunicação que se busca menos a aprovação alheia e maior soberania individual, como uma "alavanca de potência máxima, vetor de apropriação pessoal do cotidiano". Assim, os estímulos de marketing de representação social não têm o mesmo efeito de outrora, pois o hiperconsumidor não busca representatividade social, mas sim autonomia do indivíduo mediante consumo.

Nesse contexto, extrai-se, como características da sociedade conforme a Teoria do Hiperconsumo, o consumo experiencial voltado para a felicidade privada e experiência individual, a exaltação ao individualismo e o consumo como forma de identificação individual com seus desejos e não mais do grupo social. Com isso, reforça-se a ideia de emancipação das

obrigações sociais e democratização por meio do consumo, isto é, a crença de que o consumidor poder expressar seus anseios individuais em sua forma de consumo.

Paralelamente a essa concepção de Hiperconsumo como movimento de democratização e representatividade, Jean Baudrillard (2014) descreve a organização social humana não só como produtiva, de acordo com a economia e política vivida no momento, mas também organizada pelo consumo e pelos signos que a sociedade de consumo oferta. Por sua vez, Baudrillard (2014) assente com a teoria das necessidades no centro da sociedade de consumo, por meio do que chama de Revolução do Bem-Estar, mas aponta que o movimento de democratização feito pelas mídias transforma as necessidades reais e a igualdade real em uma espécie de igualdade do objeto.

Nesse contexto, a democracia, em termos literais de igualdade e garantias sociais, até pode ser demonstrada pela publicidade como uma necessidade atingida pelo consumo, na igualdade do poder de consumir itens. A crítica feita por Baudrillard (2014) é justamente que esse cenário de consumo abundante revela um cenário oposto à democracia, mas sim de desigualdade social acerca do poder de compra, que nada se assemelha à democracia real e ao alcance de liberdades individuais.

Na economia informacional, vislumbra-se, com mais técnica e sofisticação, alguns meios de impulsionamento do usuário ao consumo. Pariser (2012) desenvolve sua teoria sobre Filtros Invisíveis presentes na internet, que têm a finalidade de criar estímulos personalizados aos usuários para consumirem determinado conteúdo ou produto. A estratégia dos Filtros está intimamente ligada aos modelos de negócios de plataformas on-line, como Google e Facebook. A equação é de que por meio da filtragem de dados dos usuários, essas empresas conseguem aferir maior acuracidade acerca das preferências dos indivíduos por trás da tela, e maior assertividade é sinônimo de maior valor de mercado e maior chance de venda de anúncios que serão milimetricamente personalizados para cada usuário (PARISER, 2012).

Para Pariser (2012), essa personalização pelos filtros vai ainda além da influência sobre o consumo dos usuários com a oferta de propagandas direcionadas. Os feeds de notícia estão cada vez mais moldados para aquilo que o usuário demonstra se interessar, como consumo, lugares, amigos e fonte de informação, ou seja, eles estão programados para delimitar o conteúdo de cada usuário no que o algoritmo compreende como agradável, de forma individual e personalizada.

> O código básico no seio da nova internet é bastante simples. A nova geração de filtros on-line examina aquilo de que aparentemente gostamos – as coisas que fazemos, ou as coisas das quais as pessoas parecidas conosco gostam – e tenta fazer extrapolações.

> São mecanismos de previsão que criam e refinam constantemente uma teoria sobre quem somos e sobre o que vamos fazer ou desejar a seguir. Juntos, esses mecanismos criam um universo de informações exclusivo para cada um de nós – o que passei a chamar de bolha dos filtros – que altera fundamentalmente o modo como nos deparamos com ideias e informações (PARISER, 2012, p. 11)

As previsões de Pariser (2012) é de que cada vez mais as redes serão adaptadas pela personalização para cada usuário; a ideia de redes, sites e plataformas de buscas não adaptados ao usuário será uma ideia estranha. Em contraponto à ideia de "compartilhar e se conectar", os filtros não tendem a aproximar ideias distintas de um debate, apresentar produtos fora da rotina de consumo do usuário ou apresentar no Feed ou sugestão na resposta de busca notícias que não agradem ao usuário, eles tendem a limitar os círculos de amizades, sugestões e notícias às preferências do usuário, unindo pontos de vistas em comum e afastando ideias diferentes a "chance de termos uma relação próxima com pessoas muito diferentes de nós é cada vez menor, na internet ou fora dela – e assim, a chance de entrarmos em contato com pontos de vista diferentes também diminui" (PARISER, 2012, p. 48).

Esse efeito produzido por filtros de personalização, ou simplesmente por algoritmos de inteligência artificial, parece ressaltar os aspectos e as vontades individuais do usuário, que embora esteja inserido em uma comunidade on-line que se propõe a democratizar ou compartilhar e estabelecer conexões, pode na verdade estar se limitando aos grupos e às sugestões que tendem a lhe agradar. Em uma analogia à Teoria do Hiperconsumo, ferramentas como os filtros invisíveis fomentam de certa forma o individualismo moderno dentro das redes, pois mesmo em um modelo de economia compartilhada ou de busca, os algoritmos estão voltados em obter maior acuracidade nas preferências do usuário, o que dificilmente levará a uma exposição a conteúdos diferentes de sua vontade individual.

Assim como a ação dos filtros sobre os anúncios lançados para sugerir opções de consumo, quanto mais personalizado o anúncio conseguir atingir uma possível vontade de consumo do indivíduo, maior valor ele terá no leilão de anúncios, assim, a personalização se assemelha à ideia de consumo individualizado proposta por Lipovestky. Os algoritmos parecem promover, ainda com mais facilidade, o alcance individual a anseios que o usuário talvez nem reconheça ter demonstrado.

No mercado de consumo, Anderson (2006) expõe a teoria acerca da Cauda Longa como um modelo de negócio da atualidade impulsionado pela internet e pelas vendas on-line, em que cultura de nicho ganha espaço nas vendas, isto é, um mercado mais nichado, conforme as vontades captadas pelos rastros deixados pelo consumidor. A Cauda Longa se caracteriza pela oferta abundante de produtos, de todos os tipos e em variedade e acessíveis, funcionando com

o baixo custo de ofertar e estocar todo tipo de item que pode ser consumido por algum nicho de consumidor que está cada vez mais distribuído em nichos espaçados (ANDERSON, 2006).

> Cauda Longa é nada mais que escolha infinita. Distribuição abundante e barata significa variedade farta, acessível e ilimitada — o que, por sua vez, quer dizer que o público tende a distribuir-se de maneira tão dispersa quanto as escolhas. Sob a perspectiva da mídia e da indústria do entretenimento dominantes, essa situação se assemelha a uma batalha entre os meios de comunicação tradicionais e a Internet. Mas o problema e que, quando as pessoas deslocam sua atenção para os veículos on-line, elas não só migram de um meio para outro, mas também simplesmente se dispersam entre inúmeras ofertas. Escolha infinita é o mesmo que fragmentação máxima (p. 160).

Para Anderson (2006, p. 163), o efeito dessa fragmentação dos consumidores em nichos vem das tecnologias digitais que personalizam as ofertas on-line. O efeito prático é de que os consumidores são divididos em correntes individuais em suas bolhas de consumo, isto é, "se romper, a cultura de massa não se transforma em outra massa diferente, mas em milhões de microculturas, que coexistem e interagem umas com as outras de maneira extremamente confusa".

A Cauda Longa possui suas regras para permear, de acordo com Anderson (2006): (1) reduzir custos de estoque é essencial para poder ofertar o maior número de itens possíveis em baixo custo; (2) deixar que os consumidores façam o trabalho através de produção colaborativa, método "*crowdsourcing*", permitir que o consumidor faça gratuitamente avaliações que ajudam na construção dos nichos; (3) desenvolver mais de um modelo de negócio para atender a todos os nichos; (4) segmentar produtos e deixar o consumidor optar pela compra individualizada; (5) precificação variável dos produtos; (6) compartilhar informações úteis que serão relevantes na decisão de compra, como a classificação de itens mais vendidos; (7) oferecer todo produto possível dentro das opções para aquele público; (8) confiar nos filtros colaborativos da Cauda Longa; e (9) entender o poder da oferta de serviços gratuitos.

Nesse sentido, os filtros da Cauda Longa desempenham o papel de encontrar as opções de consumo que se adequam aos interesses do consumidor, pois a cultura é de oferta total, em abundância, mas os filtros selecionam o que pode ser de melhor interesse para o consumidor. A princípio, as tendências dos modelos econômicos do Capitalismo Informacional se preocupam com o consumo experiencial do usuário ao desenvolver tecnologias capazes de prever uma possível vontade de consumo e encaixá-la em um nicho específico. Contudo, acerca da ideia de democratização do indivíduo pelo consumo, algumas reflexões devem ser feitas.

O sociólogo Bauman (2001) contextualiza que a exaltação à individualidade tomou o espaço antes ocupado por ideais de comunidade, passando a figura do indivíduo a ocupar o

espaço central em suas necessidades, decisões e consequências, contando cada vez menos com o senso de comunidade, e assim é a relação da emancipação do indivíduo ao social no novo capitalismo da hipermodernidade. Na modernidade fluida ou leve, a individualidade é o marco central na busca pela liberdade, assim, felicidade e liberdade passam a depender de cada indivíduo em seu próprio espaço e não mais da comunidade em que se insere ou das regras sociais tradicionais da modernidade pesada (BAUMAN, 2001).

Em relação à teoria de Hiperconsumo, a modernidade líquida traz características que reforçam o consumo individualista, agorista e capitalista da liquidez. Assim como Anderson (2006) relata a abundância de nichos e tipos de produtos na Cauda Longa, Bauman (2001, p. 170) descreve como o capitalismo líquido oferece infinitas possibilidades em todos os setores da vida cotidiana, "o mundo se torna uma coleção infinita de possibilidades: um contêiner cheio até a boca com uma quantidade incontável de oportunidades a serem exploradas ou já perdidas". Essa abundância de possibilidades não atrai mais a ideia de posição social ou representatividade, mas sim a própria libertação do indivíduo, ressaltando o querer individual.

Percebe-se que, embora o indivíduo esteja cada vez mais no centro dos meios produtivos e econômicos da sociedade, o que as tecnologias digitais parecem promover é a democratização do poder de consumo, mas não necessariamente uma democratização do indivíduo. De fato, o indivíduo está no cerne das discussões sobre as redes, mas a cultura de filtros, a personalização de consumo e os modelos econômicos pautados na análise de dados tendem a colocá-lo em nichos preferenciais.

A teoria de Pariser (2012) se filia à ideia de que a economia informacional busca rastrear as preferências dos usuários para direcionar anúncios que se encaixem nesses interesses, tato em seu feed de notícias quanto em suas pesquisas. Mesmo desejos não manifestados podem ser indicados pela interpretação feita de seus rastros digitais.

A hiperconectividade produz efeitos positivos no avanço de tecnologias, de descobertas pela humanidade e de facilitação de serviços, mas também traz à tona dúvidas nem sempre esclarecidas sobre direitos dos usuários e consumidores que fazem uso dessas tecnologias simplesmente para atender a certa necessidade, como a busca por um endereço ou para facilitar o dia a dia, como compartilhar uma lista de compras nas notas do celular. Com isso, não fazem ideia de como suas atividades on-line estão sendo meticulosamente rastreadas, armazenadas e interpretadas, fazendo parte de um grande mercado econômico.

Esse contexto fluido da hipermodernidade coloca em risco questões intrínsecas, como a privacidade do indivíduo. Nesse ponto em diante, reflete-se sobre um questionamento feito por

Zeynep Tufekci em sua apresentação no TED TALK em 2017, “estamos criando uma distopia apenas para fazer as pessoas clicarem em anúncios?”.

2.4 O PANÓPTICO DO CONSUMO: VIGIAR E VENDER, RELATIVIZAÇÃO DA PRIVACIDADE EM PROL DO CONSUMO

> “Nesse jardim das delícias, o bem-estar tornou-se Deus, o consumo, seu templo, o corpo, seu livro sagrado.” – Gilles Lipovetsky

Se a economia informacional está voltada para os rastros de dados dos indivíduos como maneira de perpetuar modelos de negócios nutridos pelos próprios usuários, a privacidade entra em pauta por sua afetação no uso de tecnologias digitais. A autora Zuboff (2019) vê os modelos de negócio utilizados pelas grandes empresas de tecnologia como uma estrutura de capitalismo de vigilância como um modelo econômico, que utiliza das experiências humanas e dos dados dos indivíduos para atingir altos índices de lucratividade por um pequeno grupo de empresas que monopolizam o mercado digital com tecnologias como Big Data.

Tratar de uma economia baseada na vigilância envolve explanar e expandir os marcos conceituais sobre teorias de vigilância e sua presença no contexto da sociedade de informação. É necessário concluir que, de fato, estamos inseridos em um modelo econômico baseado em vigiar, entender por qual razão isso ocorre e identificar quais os sujeitos desse cenário.

No livro 1984, o autor George Orwell (2020) retrata uma distopia totalitária, sustentada pela vigilância constante da teletela e forjada sob os artifícios da nova língua ou nova fala. Na ficção, os personagens estão constantemente monitorados pelo Partido do Grande Irmão e até mesmo o pensamento é policiado, retratando um cenário ditador em nome do poder. No entanto, questiona-se o quão distante estaria a sociedade de Hiperconsumo e Capitalismo Informacional de uma distopia de vigilância pelo consumo. O atual modelo econômico só pode ser mantido com a monetização das informações pessoais de usuários, e para captar tantas informações pessoais sem o incômodo dos usuários, inclusive com solícita participação, exploram-se as técnicas de vigilância.

2.4.1 O Panóptico de Bentham

Da ideia de controlar e organizar um grande grupo de indivíduos, com poucos recursos e o mínimo possível de vigilantes, nasce o Panóptico, uma estrutura idealizada por Bentham

(2008), que arquitetava a criação de um estabelecimento que pudesse se adequar, desde a uma penitenciária e um sanatório, até uma escola. A estrutura do Panóptico visa à vigilância constante como método de "inspeção" de pessoas que necessitem deste tratamento, o autor especificava "prisões, casas de indústria, casas de trabalho, casas para pobres, manufaturas, hospícios, lazaretos, hospitais e escolas" (BENTHAM, 2008, p. 15). Chama a atenção os ambientes destinados a tamanha vigilância, mas contextualmente Bentham idealizou o Panóptico em 1785 em meio ao Absolutismo e às vésperas da Revolução Francesa.

A ideia de vigilância constante partia de uma versão humana de onipresença, se assemelharia à onipresença divina de Deus, uma máquina capaz de produzir a imitação d´Ele, em que um grande número de vigiados pudesse ser observado por um mínimo de vigilantes, sem que sua presença pudesse ser notada. Os indivíduos sob a vigilância poderiam ter suas condutas previstas, evitadas e punidas da maneira que o vigilante julgasse adequada (BENTHAM, 2008). De forma quase distópica, assim pretendia Bentham (2008, p. 17):

> Tratava-se de um novo modo de garantir o poder da mente sobre a mente, em um grau nunca antes demonstrado; e em um grau igualmente incomparável, para quem assim o desejar, de garantia contra o exagero. Esse é o mecanismo, esse é o trabalho que pode ser feito com ele.

O poder da mente sobre a mente, nesse caso, seria controlado por aqueles que detivessem o poder. Bentham (2008) destacava as vantagens que um Panóptico teria sobre a sociedade, iniciando-se por espaços confinados como escolas e presídios, chegando a sugerir mecanismos em campos abertos. Para o autor, a onipresença da vigilância evitaria condutas reprováveis, e o número de vigias era favorável do ponto de vista econômico, pois se poupava uma estrutura maior de policiamento. No entanto, vê-se que a ideia de Panóptico se estendia até mesmo aos agentes de vigia, que também estariam sujeitos a uma vigia sobre suas ações sem seu conhecimento, na observância do cumprimento do dever (BENTHAM, 2008, p. 32):

> para aquilo que é chamado de liberdade quanto ele o é para a necessária coerção; tão poderoso como um controle sobre o poder subordinado quanto como uma prevenção da delinqüência; tão eficiente como uma proteção à inocência quanto como um castigo para o culpado.

Nota-se que, a ideia de liberdade é tratada como condição da vigilância, isto é, "liberdade é escravidão", e para se estar livre, os sujeitos deveriam estar submetidos a um sistema de vigilância constante capaz de conferir cada conduta e reprimir aquelas inadequadas. Do Panóptico de Bentham, podemos extrair que inicialmente o projeto não era destinado à

sociedade de modo geral, mas ao longo do texto, parece estender-se para diversos campos da sociedade, como um método a ser seguido pela vigilância.

Como características, destaca-se o ideal de onipresença, ignorância quase ingênua sobre os vigiados, mecanismo economicamente barato em relação a outros métodos de inspeção, a possibilidade de prever comportamentos e reprimi-los, dentro de uma cadeia de processos punitivas que posteriormente poderia ser projetada para demais áreas da sociedade. O aprimoramento do panóptico de Bentham pode levar a uma sociedade de vigilância, que se justificaria pela generalização do poder do panóptico em quantos mais funções pudesse atingir, maximizando a vigilância e assim modulando os sujeitos aos propósitos de quem detém o poder de vigiar. Michael Foucault avança em outra narrativa sobre o Panóptico.

2.4.2 O panóptico de Foucault

A ideia de vigiar por meio de um panóptico é trabalhada por Michel Foucault (1999), em uma visão mais moderna do uso do panóptico em outras áreas da vida, além da estrutura punitiva do Estado. Foucault vê no panóptico um mecanismo também de eficácia do poder disciplinar como uma forma de anatomia política, se desdobrando para os setores produtivos da economia, saúde e educação.

Em um panorama geral, o autor vê distinções entre o panóptico proposto por Bentham e como ele pode ser utilizado na construção de uma estrutura punitiva e hierárquica, o que para o autor, produziria um verdadeiro zoológico com homens substituindo os animais, pois “o Panóptico aparece como jaula cruel e sábia”, contudo, propõe uma visão abstrata ao objeto de uma estrutura física do panóptico e voltada a uma ideia de tecnologia política (FOUCAULT, 1999, p. 228).

Com a generalização das instituições de disciplina em todos os campos possíveis da vida cotidiana, pode construir-se uma sociedade de disciplina, ou melhor dizendo, uma sociedade de vigilância. Por meio da vigilância constante em outros setores, alguns efeitos podem ser alcançados, como a formação de sujeitos mais úteis às suas funções e a vigilância da sociedade além da instituição, situação que é favorável à economia, política e produção (FOUCAULT, 1999).

Em uma linha produtiva, por meio do sistema panóptico, Foucault (1999) propõe que poderia tornar-se mais eficaz e útil o indivíduo então vigiado por seu contratante, maximizando sua produtividade com a possibilidade de corrigir e repreender qualquer erro de conduta. Para ele:

> O dispositivo panóptico não é simplesmente uma charneira, um local de troca entre um mecanismo de poder e uma função; é uma maneira de fazer funcionar relações de poder numa função, e uma função para essas relações de poder. O panoptismo é capaz de reformar a moral, preservar a saúde, revigorar a indústria, difundir a instrução, aliviar os encargos públicos, estabelecer a economia como que sobre um rochedo, desfazer, em vez de cortar, o nó górdio das leis sobre os pobres, tudo isso com uma simples idéia arquitetural (p. 230).

A vigilância constante dos indivíduos para atingir determinados resultados em benefício econômico, político ou social de alguns agentes da sociedade, na busca pela formação de sujeitos mais "úteis" aos objetivos programados. Em primeiro momento, parece a teoria de Foucault ser invasiva, pois o panóptico estará sob poder das instituições e agentes que exerceriam a vigilância independentemente da vontade dos vigiados, ainda que não somente no contexto do cárcere. Ainda assim, a ideia de um panóptico com benefícios para além do controle absoluto do indivíduo, como propôs Bentham, mas justificado pela possibilidade de melhora em desempenhos econômicos, políticos e sociais, como propõe Foucault, parece mais imaginável no contexto da hipermodernidade e além das distopias.

Em 1984 (ORWELL, 2020), a teletela ocupa esse papel, é o panóptico utilizado pelo Grande Irmão para vigiar todos os indivíduos e ter controle absoluto por seus corpos, vontades e pensamentos. Ao mesmo tempo, o objeto é bem-quisto por aqueles que acreditam na ideologia pregada pelo Partido, i sto é, só resiste ao uso da teletela ou a evita aqueles que parecem discordar de sua imposição, enquanto parte da sociedade da distopia narrada por Orwell (2020) está absorta na utilidade do objeto em trazer resultados para a nação, para o Partido e, indiretamente, a outros setores sociais e econômicos. A utilidade parece nebular a imposição e justificar o objeto.

A vigilância constante aplicada nos mais diversos setores da sociedade justificada por uma ideia de utilidade econômica e política é o que se extrai do modelo Panóptico proposto por Foucault (1999, p. 230), que descreve mais do que uma estrutura arquitetônica, mas uma ideia abstrata de vigilância que pode ser aplicada por instituição, cuja vigia pode ser feita por qualquer pessoa. Ou seja, até mesmo os vigias podem ser vigiados, "um edifício transparente onde o exercício do poder é controlável pela sociedade inteira".

2.4.3 O panóptico moderno: vigiar e vender

> "O Panóptico é uma máquina maravilhosa que, a partir dos desejos mais diversos, fabrica efeitos homogêneos de poder." Foucault, 1999.

Saber os desejos mais diversos e proporcionar experiências e sensações do indivíduo fazem parte de uma das dinâmicas do Hiperconsumo, em que conhecer os desejos privados, individuais, "as motivações privadas superam muito as finalidades distintivas" (LIPOVETSKY, 2007, p. 41). O momento narrado é protagonizado pela busca do *Homo consumericus* pela autovalidação e realização pessoal.

Assim, as formas de consumo baseadas na individualidade e realização pessoal transformam os mecanismos de oferta, que precisam saber quais os "desejos mais diversos" a serem atendidos ou simplesmente sugeridos ao consumidor. Essa oferta não se baseará nas técnicas de marketing difundidas em outro momento, mas na interpretação de informações sobre o indivíduo. Considerando que a função do panóptico em ambas as teorias correntes é vigiar, sua diferenciação está em qual a finalidade, isto é, vigiar para quê?

Para Bentham (2008), a vigia se justifica em um momento contextual às vésperas da Revolução Francesa, construindo a teoria de vigilância sob a finalidade de penitência, de previsão e correção do comportamento e controle sob os indivíduos, com caráter punitivista através da máquina do Estado contra o indivíduo.

Para Foucault (1999), a vigia pode ter funções mais abrangentes que simplesmente a punição. Se bem interpretado, o panóptico pode ser uma ideia praticada em qualquer instituição como forma de estabelecer poder e domínio de informações para a produtividade e utilidade dos sujeitos nos setores econômicos e políticos. Vigiar para vender é uma finalidade intrínseca em modelos como a economia de busca ou a economia de compartilhamento, isso porque saber o máximo possível sobre os usuários é necessário para valorizar os lances dos leilões de publicidade.

A vigilância na sociedade atual destoa das técnicas panópticas de Foucault e Bentham, cujas teorias servem de inspiração para a criação do arquétipo. De acordo com Pessoa (2020), a técnica de vigilância moderna é um "superpanóptico", com o biopoder de vigilância por meio dos progressos das tecnologias de informação. Os dados são o objeto central dessa economia, são obtidos em larga escala com tecnologias de Big data, sendo possível coletar, armazenar e manipular um grande volume de informação e extrair melhores interpretações sobre os usuários e suas preferências. São os cinco Vs dessa tecnologia: volume, velocidade, variedade, veracidade e valor, cuja finalidade, de modo geral, do ponto de vista econômico, é agregar valor e melhor desempenho na oferta de serviços pelos agentes econômicos desse setor (PESSOA, 2020).

Esse volume de dados é coletado com o uso de diversos mecanismos tecnológicos que estão inseridos na sociedade em rede e são, em grande parte, desconhecidos do usuário comum,

Pessoa (2020, p. 129) assim destaca a coleta e o armazenamento de dados realizada por meio de "*cookies, web beacons, spywares, tagging e tracking*", mecanismos comumente inseridos em aparelhos muito conhecidos dos usuários, como "celulares, tablets, notebooks, relógios, televisores".

Em exemplificação, Camargo (2020) explica como os *cookies* do Google são inseridos como um simples fragmento de código dentro de uma página na web, e uma vez aceitos, poderão gerar análises estatísticas sobre as preferências deixadas por aquele usuário. Ainda que a página na web não tenha informações pessoais do usuário, o Google sabe quem ele é, e com essa informação, poderá gerar estatísticas com acuracidade suficiente para oferecer propagandas personalizadas ao mesmo usuário. Essa propaganda possui maior valor de lance em leilão se as chances de acerto são maiores, e por essa razão, a acuracidade da ferramenta de análise do site de buscas precisa ser alimentada de informações mais específicas possíveis.

O "superpanóptico", ou simplesmente o panóptico moderno, é alimentado por um modelo de vigilância próprio à atualidade, que nas entrelinhas, forma uma espécie de vigilância consentida por meio do uso das tecnologias da informação. Quantos mais dispositivos, há mais meios de coletar dados e alimentar essa economia informacional, ou seja, a precisão de filtragem depende desse acervo de informações. Para Pariser (2012), a coleta se torna ainda mais fácil quando ampliada para o rastreamento das informações também por meio de objetos inteligentes e da chamada tecnologia IoT.

Além das redes sociais e dos sites, o mercado da tecnologia descobriu que por meio de objetos, a economia da informação pode ser explorada pelo consumo de itens inteligentes. Com um objeto conectado a uma rede, equipado com um chip de identificação e a capacidade de de captar e transmitir informações, as empresas de tecnologia ganharam novos mecanismos para sua filtragem de informações, já que qualquer objeto pode estar conectado e se tornar inteligente com funções práticas. Isso significa que todos os produtos manufaturados, como roupas, carros, eletrodomésticos e até mesmo dinheiro, "terão inteligência, redes de minúsculos sensores e ativadores, aquilo que alguns chamam de 'poeira inteligente'" (PARISER, 2012, p. 135).

A dinâmica da economia vislumbrou maior lucratividade indo além da economia de informação. Percebeu-se que mais do que coletar informação, era necessário um arquétipo de vigilância. Conforme descreve Zuboff (2019, p. 406), a transição para os capitalistas de vigilância não era uma escolha, mas um novo mercado competitivo pela conversão de "superávit comportamental em produtos que preveem com exatidão o futuro". Esse arquétipo não era mais uma opção quando os resultados econômicos já se mostravam vantajosos, pois a

competitividade entre gigantes da tecnologia pela predição comportamental acelerou ainda mais o crescimento desse mercado.

Sobrepujando uma economia baseada em informação, a autora Zuboff (2019) retrata o novo momento da economia global, desencadeado pelos mercados de tecnologia digital e seus meios de lucratividade. O capitalismo de vigilância confirma uma espécie de superpanóptico moderno, em que a finalidade não parece ser o utilitarismo dos indivíduos ou a previsão de condutas para correção punitivista; a finalidade moderna está na capacidade lucrativa que há na predição comportamental baseada na experiência humana, uma matéria-prima infinita, de baixo-custo e fornecida pelo próprio usuário, que se torna consumidor e produto.

Vigiar e vender é o paradigma construído pela nova economia. É uma metodologia que eleva o capitalismo ao estado de vigilância, uma sociedade de vigilância sofisticada pelos recursos tecnológicos e por uma atuação velada nos dispositivos e mecanismos de vigilância. A distopia não parece autoritária, o Grande Irmão não se apresenta como um líder totalitário. Entre as características do Capitalismo de Vigilância, está o papel de passar despercebido e, se percebido, consentido pelo usuário.

2.5 NO CARRINHO DE COMPRAS À EXPERIÊNCIA DO USUÁRIO: CAPITALISMO DE VIGILÂNCIA E REFLEXOS

> "Ele sabe tudo sobre nós, ao passo que suas operações são programadas para não serem conhecidas por nós. Elas acumulam vastos domínios de um conhecimento novo proveniente de nós, mas que não é para nós. Elas predizem nosso futuro a fim de gerar ganhos para os outros, não para nós" Shoshana Zuboff, 2019.

A ideia de uma economia baseada na vigilância é estudada em diversos aspectos, uma economia de predições baseada no comportamento e na experiência humana, é como define a autora Zuboff (2019, p. 283), o capitalismo de vigilância, como um modelo econômico criado pelas grandes empresas de tecnologia, que "reivindica a experiência humana como matéria-prima gratuita para práticas comerciais dissimuladas de extração, previsão e vendas".

A autora apresenta uma versão parasitária da vigilância como modelo econômico, em que as experiências humanas são cada vez mais captadas como matéria-prima de uma cadeia produtiva de bens e serviços e representam um superávit comportamental que serve para interpretação de dados e predição de preferências do usuário, valorizando e monetizando sob previsões comportamentais (ZUBOFF, 2019).

Para Zuboff (2019), o capitalismo de vigilância teve seu ponto de partida com as atividades desenvolvidas pelo Google ao criar suas ferramentas de rastreamento com acesso a informações pessoais dos usuários. Nesse aspecto, a empresa foi pioneira em vender predições do comportamento dos usuários, e o "Google descobriu que nós somos menos valiosos que as apostas alheias no nosso comportamento futuro. Isso mudou tudo." (ZUBOFF, 2019, p. 120).

O excesso de dados coletados pelo Google e a maneira como a empresa criou um sistema de previsões e indicações de propagandas formaram um superávit comportamental de seus usuários, que ao se converterem em leilões de publicidade, criaram o mais eficiente mecanismo de lucratividade do capitalismo de vigilância (ZUBOFF, 2019). Assim, os primeiros "produtos" de previsão são os serviços de publicidade direcionada on-line iniciados pelo Google. A lucratividade da metodologia atraiu outras Bigtechs para explorarem as receitas produzidas pelo imperativo de predição. Para manter esse modelo econômico, é necessário o superávit de informações do usuário constantemente (ZUBOFF, 2019).

A teoria de Zuboff (2019) sobre o capitalismo de vigilância é construída sob o paradigma de uma relação entre Google e usuário, em que os usuários ocupam o papel de fornecedores de matéria-prima de uma economia que depende de um superávit comportamental. Por outro lado, a relação comercial ocorre entre Google e anunciantes dispostos a participarem de seu leilão de informação; assim, por meio da constante vigilância sob os rastros digitais dos usuários, a empresa obtém o excedente informacional que utilizará em suas análises e depois comporá seu acervo de negociação por probabilidade de cliques e compras, que será cada vez mais assertivo e lucrativo.

> Assim, havia aqui uma mistura sem precedentes e lucrativa: superávit comportamental, ciência de dados, infraestrutura material, poder computacional, sistemas de algoritmos e plataformas automatizadas. Essa convergência produzia "relevância" sem precedentes e bilhões de leilões. As taxas de cliques foram às alturas. O trabalho na AdWords e na AdScience tornou-se tão importante quanto o trabalho na busca. Com as taxas de cliques como medida de relevância alcançada pelos consumidores, o superávit comportamental foi institucionalizado como a pedra angular de um novo tipo de comércio que dependia de vigilância on-line em escala (ZUBOFF, 2019, p. 109).

Contudo, Camargo (2020) aponta que a teoria de Zuboff (2019) ignora outros aspectos técnicos que vão além do cenário parasitário apontado pela autora. Isso inclui a complexidade dos ecossistemas construídos nessas plataformas, a interação em tempo real entre usuário, plataforma e anunciantes, bem como toda a cadeia de sistemas digitais que envolve muitos outros serviços. Portanto, esse tema não deve ser estudado de forma simplista, mas sim

considerando todos os aspectos de complexidade e normativos que vão além da criação de um excedente comportamental por um modelo de vigilância digital.

Para Camargo (2020), a concepção sobre capitalismo de vigilância deve envolver a complexidade de todo o ecossistema, pois a economia de vigilância deve ser encarada como um aspecto fundamental de uma teoria mais ampla sobre a economia política. Ela é formada pelos agentes que atuam nesse mercado, criando plataformas e desenvolvendo coleta de dados que também atuam na construção normativa e nos reflexos sobre seus negócios, sem minimizar a importância sobre a economia de vigilância, mas compreendê-la como um fundamento parte de uma estrutura mais ampla.

Sob a ótica apresentada por Camargo (2020), ainda que as descrições do sistema de capitalismo de vigilância dadas por Zuboff (2019) sejam didáticas, resumem o que é um ecossistema informacional muito mais amplo de sistemas, agentes e aparatos tecnológicos, além da vigilância:

> Também não leva em consideração os complexos ecossistemas de aplicações construídos sobre diversas plataformas. Os sistemas digitais que baseiam seu funcionamento em dados pessoais não é monolítico, nem ao se considerar uma única plataforma. Muitas vezes, é formada por emaranhados de serviços, executados por terceiros, a maioria deles submersos, para se chegar a um resultado visível ao usuário. Pensar dois processos paralelos despreza boa parte da imensa complexidade destes modelos de negócio (CAMARGO, 2020, p. 52).

Para Varian (2003), a discussão sobre a nova economia desconsidera a presença de princípios tradicionais já presentes na economia industrial, pois muitos efeitos que impulsionam a economia informacional vêm de um modelo econômico tradicional. Acerca do uso do consumidor como fornecedor de "matéria-prima" para a economia informacional, Varian (2003) identifica que economicamente surge a necessidade de maximização da utilidade do usuário ou consumidor para precificação de produtos e serviços, tendo em vista que a fixação de preço é o que dá flexibilidade para tratar os custos de serviço, isto é, as preferências obtidas em impressões do usuário não servem meramente para vigiá-lo, mas para compor o modelo econômico de preços que terão variação conforme a probabilidade de predição.

Além da precificação de serviços e discriminação de custos, Varian (2003) identifica que a discriminação de preço nesse modelo econômico produz outros efeitos como: a) customização em massa ou personalização de preços por perfil de consumidor, assim as preferências por perfil podem influenciar no modelo de precificação; b) a segmentação de produtos em linhas, conforme a busca dos consumidores, isto é, a possibilidade dos anunciantes exporem os itens em linhas de produtos por segmentação do mercado e consumidor; c) a

discriminação de preço por grupo de interesse, assim, a similitude de preferências por grupo servirão de base para precificação dos serviços.

O autor aponta que tais efeitos intensificam-se na economia informacional, mas estão presentes desde a economia industrial. Em outros setores, o modelo de negócios com base em leilões adotado pelo Google é justificado como a maneira possível da ferramenta de pesquisa precificar o valor dos cliques e das preferências de usuários, sendo este o valor que determinará a sua receita pela exibição de anúncios (VARIAN, 2006).

As considerações de Varian (2001, p. 15) não ignoram a existência de questões afetas à privacidade dos usuários, mas sob seu ponto de vista, o problema da economia de personalização não está em obter informações dos usuários, na privacidade propriamente, mas na confiança dos consumidores com as plataformas. Assim, "os consumidores querem controlar como as informações sobre eles são usadas", isto é, entende que o problema não está em coletar dados, mas em divulgá-los, negociá-los e explorá-los sem o conhecimento do usuário, violando a confiança e não a privacidade do usuário.

Cohen (2017) entende que esse formato é parte de um dos modelos de negócio do capitalismo informacional, ou seja, a coleta e o processamento de dados são parte da cadeia produtiva, por isso a implementação de regulação da privacidade está distante de ser um interesse central. Com isso, a inovação é o objeto central nos discursos dos agentes envolvidos, afastando-se de controles estatais.

Para Cohen (2016, p. 1), a vigilância, enquanto prática de modelo econômico, tomou cada vez mais espaço no campo privado e comercial. Com um mercado digital que adota técnicas organizadas e estratégicas para atrair a participação do usuário de forma "leve, politicamente ágil e relativamente impermeável às restrições regulatórias", essas estratégias são em parte um esforço de afastar dúvidas jurídicas e políticas sobre privacidade e processamento de dados.

Os agentes dessa economia atuam na criação de um discurso de participação do usuário nas ações de vigilância, assim, a participação e mercantilização criam um paradigma entre vigilância e inovação, que no fim tenta manter a regulação estatal distante dessas técnicas (COHEN, 2016, p. 1):

> A ascendência de tais estratégias coincide com uma concertada esforço para mudar o teor dos discursos jurídicos e políticos sobre privacidade e dados em processamento. Os participantes desses discursos posicionam privacidade e inovação como opostos, e alinhar o processamento de dados com o exercício da economia e expressão liberdade. O modelo de vigilância resultante é leve, politicamente ágil e relativamente imune à restrição regulatória. Os comentaristas há muito notaram a existência de um

> vigilância-complexo industrial: uma relação simbiótica entre vigilância estatal e produtores do setor privado de tecnologias de vigilância. O emergente complexo de inovação em vigilância representa uma nova fase politicamente oportunista dessa simbiose, aquele que lança a vigilância sob uma luz inequivocamente progressiva e a reposiciona como um modalidade de inclusão democrática e crescimento econômico. Dentro do complexo de inovação em vigilância, participação e mercantilização estão entrelaçadas como uma questão de economia política. Mas o complexo vigilância-inovação é também uma questão discursiva e formação ideológica. A retórica da participação e da inovação promove o objetivo instrumental de manter o estado regulatório à distância.[2]

Nesse contexto, a visão apresentada por Cohen (2016) coloca o capitalismo de vigilância como parte de um complexo modelo econômico, como uma das técnicas utilizadas na coleta de dados, confirmando que a coleta e o tratamento de dados são essenciais ao capitalismo informacional. Em vista disso, técnicas de vigilância que incluam a participação dos usuários e estratégias que nebulam a sensação de vigilância são desenvolvidas de maneira que a presença do arquétipo e da vigilância se afaste de questões sobre privacidade.

Uma sociedade da classificação é o que o capitalismo de vigilância revela, conforme descreve Rodotá (2008), pois apesar de toda a complexidade dos aparatos digitais, o problema central volta para a criação de perfis individuais ou de grupo baseados em rastros digitais, cuja finalidade é classificar e segmentar a seleção de interesses comerciais. Diferentemente de outras teorias de vigilância, o autor defende que o atual modelo não tem a intenção de corrigir ou impedir comportamentos, o intuito é saber quais são os comportamentos e o quanto eles se repetem, fazendo da vigilância algo natural e fluido das relações de mercado, e do usuário, um "homem de vidro", um sujeito que tem suas informações classificadas e vigiadas (RODOTÁ, 2008).

Para o autor, há de fato uma transformação da sociedade da informação em uma sociedade de vigilância, não sendo a vigilância somente parte do sistema, mas o novo sistema econômico, em que as esferas públicas e privadas estão interessadas na estrutura de classificação dos indivíduos e pouco se dispõem sobre um controle regulamentar ou protetivo

[2] Texto original: "The ascendancy of such strategies coincides with a concerted effort to shift the tenor of legal and policy discourses about privacy and data processing. Participants in those discourses position privacy and innovation as opposites, and align data processing with the exercise of economic and expressive liberty. The resulting model of surveillance is light, politically nimble, and relatively impervious to regulatory constraint. Commentators have long noted the existence of a surveillance-industrial complex: a symbiotic relationship between state surveillance and private-sector producers of surveillance technologies.The emerging surveillance innovation complex represents a new, politically opportunistic phase of this symbiosis, one that casts surveillance in an unambiguously progressive light and repositions it as a modality of democratic inclusion and economic growth. Within the surveillance innovation complex, participation and commodification are entwined as a matter of political economy. But the surveillance-innovation complex is also a discursive and ideological formation. The rhetorics of participation and innovation advance the instrumental goal of holding the regulatory state at arm's length".

a direitos envolvidos como uma cidadania digital, proteção à privacidade ou identidade dos usuários (RODOTÁ, 2008).

Assim, uma certa normalidade se estabelece sobre o uso de informações pessoais para fins econômicos, "uma "normalidade" que tende cada vez mais a coincidir com a conveniência econômica". Rodotá (2008) defende que para se discutir sobre a questão da vigilância, é importante assumir que a mera informação de que os dados poderão ser tratados e utilizados não basta, pois é um conhecimento frustrante que não resulta em medidas efetivas contra condutas de vigilância.

Essa é uma característica do capitalismo de vigilância, uma contradição em que de um lado está a ideia de liberdade, acesso à informação, anonimato e emancipação social, e do outro o potencial em vigiar, controlar e identificar seus usuários (BRUNO, 2013). O ativo do capitalismo de vigilância é a informação do usuário e a ferramenta produtiva é sua participação nesse sistema de capitalismo. Em troca, serviços de produção e comunicação são fornecidos ao usuário para ele concorde em participar dessa capitalização de informações (BRUNO, 2013).

Compreende-se que o capitalismo de vigilância envolve complexos sistemas econômicos e de serviços, que utilizam das preferências e experiências dos usuários para o próprio funcionamento da cadeia produtiva, não se resumindo somente em coletar dados e monetizar publicidade, mas em construir um modelo econômico que se precifica a partir da probabilidade gerada por predições e impressões de usuários e consumidores. Mais do que um modelo econômico, a sociedade de vigilância é uma estrutura de domínio público, atualmente amplamente utilizada além das atividades comerciais, mas também em finalidades políticas e públicas.

Além do imperativo de predição, a economia de vigilância consolidou a necessidade de superávit comportamental ao ponto de criar novas tecnologias que possibilitem mais acesso a dados, mas de forma ainda mais velada, tornando a participação do usuário no jogo mais ativa e o uso de artefatos que de certo modo ocultam sua finalidade na coleta de dados. De acordo com Zuboff (2019), outros artifícios e aparatos surgem para uma economia de ação, uma computação que consegue sumir dos olhos do usuário e ocultar-se na forma de outros artefatos para acomodar economias de escopo e economias de ação. A computação ubíqua revela uma nova onda de produtos e serviços informacionais, utilizando-se das estratégias de vigilância.

Dentro da economia de vigilância, mais de um modelo de negócio pode ser formado. O que se compreende é que a diversificação dos negócios depende dos aparatos tecnológicos que conduzem cada negócio. Além disso, há a percepção de que mais dados precisam ser coletados ou que a profundidade dos dados precisa se estender para as mais variadas possibilidades de

obtenção da informação, das redes sociais e sites a objetos simples do dia a dia. O paradigma do panóptico da vigilância se estende com uma segunda onda de produtos e serviços que cumprem o papel de coletar dados com a opacidade de apetrechos, *cookies* e objetos, por meio da “inevitável” Internet das Coisas.

3 MECANISMOS DE PREDIÇÃO: UM RECORTE SOBRE INTERNET DAS COISAS

> "Podemos sonhar com a época em que a machine à gouvener venha suprir — para o bem ou para o mal — a atual e óbvia insuficiência do cérebro, quando êste se ocupa com a costumeira maquinaria da política." – Père Dubarle. Jornal Le Monde, Paris. 1948.

O jornalista Père Dubarle escreveu, em 1948, uma resenha no jornal Le Monde de Paris intitulada *Machine à gouverner*. O jornalista falava de um equipamento futurístico com capacidades de predição sobre as escolhas humanas a respeito da política e profetizava a criação de uma máquina de governar. A profecia futurística do jornalista foi utilizada em um recorte feito por Norbert Wiener em 1950, quando escrevia sua teoria sobre a Cibernética, em que utilizou o texto como base para demonstrar como as máquinas ainda não possuíam tamanha capacidade interpretativa como necessário para a invenção.

A máquina de governar seria capaz de interpretar os dados do jogo político, e tecer predições sobre a melhor opção e ainda fazê-lo em tempo mais rápido que as instituições humanas por meio de cálculos numéricos e de probabilidade e centralizados no poder do Estado de melhor governar (WIENER, 1950). A resenha jornalística dizia que esse experimento promissor não estaria pronto ainda tão cedo, pois, "afora os seríssimos problemas que o volume de informação a ser coligido e rapidamente processado ainda suscita, os problemas da estabilidade da predição ultrapassam aquilo que possamos seriamente sonhar em controlar", deixando ao final da matéria a dica para que os estudiosos da cibernética se interessassem pelo assunto (WIENER, 1950, p. 177).

Wiener (1950), em seu livro, respondeu ao artigo, revelando os perigos que uma máquina de governar poderia representar sob o controle da humanidade se colocada nas mãos dos líderes políticos errados. Ademais, as máquinas ainda não tinham um milésimo de capacidade de interpretação das intenções humanas, e assegurou:

> A grande fraqueza da máquina – fraqueza que nos salvou até aqui de ser dominados por ela — é a de que ela não pode ainda levar em consideração a vasta faixa de probabilidades que caracteriza a situação humana. A dominação da máquina pressupõe uma sociedade nos últimos estágios de entropia crescente, em que a probabilidade é insignificante e as diferenças estatísticas entre os indivíduos nulas. Felizmente, ainda não alcançamos êsse estado (p. 178).

Em 1948, prever a criação de um dispositivo com capacidade de interpretação dos comportamentos humanos é uma conjectura ousada e não há como se dizer que Dubarle ou Wiener previam que um dispositivo nesse sentido fosse de fato surgir e fazer parte da rotina da

humanidade. Um equipamento portátil ou uma página na web, com memória embutida e capacidade de processamento rápido de dados, é capaz de armazená-los em uma nuvem digital enquanto presta pequenos serviços rotineiros em seu favor, entregando dados justamente para serem filtrados, interpretados, e cujo resultado de predição monetizados, isto é, um dispositivo ou mecanismo comum do século XXI com tecnologia de Internet das Coisas.

A Internet das Coisas é uma das tecnologias que compõem o vasto universo da sociedade informacional, com mecanismos de atuação sob a vigilância comportamental dos usuários. Ou seja, é um dos recursos complexos do capitalismo de vigilância, que adentra uma realidade de ubiquidade, abre portas para novas formas de economia digital, bem como se solidificam com a proporção de usuários que aderem continuamente suas facilidades.

Para compreender os principais aspectos econômicos e normativos acerca da Internet das Coisas e efetuar o recorte científico necessário, este capítulo amplia o marco conceitual sobre a Internet das Coisas, suas funcionalidades, seus mecanismos, sua complexidade, seus aspectos normativos e sua expansão sobre a sociedade da informacional. Além do mais, a contextualização social sobre a dinâmica de utilização de tecnologias de vigilância importa a compreensão da difusão desses dispositivos e qual a relação com os usuários e consumidores na coleta de dados e seu conhecimento sobre o que é feito dessas informações.

O paradigma entre a vigilância ocasionada pela Internet das Coisas e a privacidade produz a reflexão sobre consentimento do usuário. Ainda que não se trate da Máquina de Governar profetizada por Dubarle, a Internet das Coisas demonstra capacidades semelhantes de predição comportamental e aspectos de influência sobre os usuários, que indubitavelmente geram preocupações semelhantes às levantadas por Wiener sobre os danos que uma tecnologia como essa pode representar à sociedade humana como um todo.

3.1 MULTIVERSO DAS COISAS: DO MECANISMOS DAS IOT, MOEDAS DIGITAIS AO METAVERSO

A teoria do multiverso levanta uma hipótese física e quântica sobre a existência de mais de um universo possível, além do universo que habitamos e conhecemos como lar, um conjunto de universos possíveis desconectados (ELLIS, 2011), resultados de outros eventos como o Big Bang. Não se pretende logicamente teorizar acerca de física quântica universal, mas analogamente pormenorizar a eventualidade de um multiverso digital, vários universos produzidos pela dinâmica da hiperconectividade e dos diversos aparatos digitais.

Enquanto o multiverso é compreendido como um conjunto de universos como um efeito físico resultado do mesmo evento originário, a hiperconetividade representa um estado do indivíduo com um conjunto de conexões de comunicação constantes entre o objeto/coisa, usuário, internet, redes sociais, sensores digitais, algoritmos, e demais elementos da rede (MAGRANI, 2019). A disponibilidade do usuário para estar sempre conectado é a característica central da hiperconetividade, pela conexão entre usuários por redes de comunicação ou as relações entre usuários e máquinas, ou simplesmente entre máquinas e máquinas (MAGRANI, 2019).

De acordo com Magrani (2019), a conjectura da hiperconectividade depende do aumento de dispositivos disponíveis para estabelecer os vários conjuntos de conexão, enviando e recebendo informações, ou seja, quanto mais dispositivos conectados, mais dados podem ser produzidos, e os efeitos são de modo geral um fluxo contínuo de informações e a massiva produção de dados. Além disso, ele reúne alguns dos principais desdobramentos da hiperconectividade:

> o estado em que as pessoas estão conectadas a todo momento *(always-on*); a possibilidade de estar prontamente acessível (*readily accessible*); a riqueza de informações; a interatividade; o armazenamento ininterrupto de dados (*always recording*).9 O termo hiperconectividade está hoje atrelado às comunicações entre indivíduos (*person-to-person*, P2P), indivíduos e máquina (*human-to-machine*, H2M) e entre máquinas (*machine-to-machine*, M2M) valendo-se, para tanto, de diferentes meios de comunicação (MAGRANI, 2019, p. 20).

Podemos extrair alguns universos da comunicação forjados pela hiperconectividade e mantidos por complexos mecanismos de conexão: a) P2P – *Person to person*: a comunicação entre usuários dentro de Redes Sociais e Sites e outros dispositivos de comunicação; b) H2M – *Human to machine*: a comunicação entre usuário humano e máquina, conexão formada pelo usuário com dispositivos conectados a rede; c) M2M – *Machine to machine*: diferentes dispositivos conectados à rede, coletando e trocando dados.

Nesse contexto, a conexão constante de diversos conjuntos é prioridade da hiperconectividade. Zuboff (2018) narra que uma reconfiguração para o crescimento das empresas de tecnologia foi tratada como inevitável rumo ao desenvolvimento das tecnologias de Internet das Coisas, isto é, o "inevitabilismo" seria o discurso das grandes empresas do Vale do Silício para garantir a continuidade de crescimento do setor. Um recorte conceitual e o retorno aos fundamentos são importantes para delinear do que se trata a tecnologia de Internet das Coisas e como podem ser categorizadas as tecnologias de vigilância.

O termo Internet das Coisas (*Internet of Things*), comumente representado pela sigla IoT, foi proposto por Kevin Ashton em 1999, que acreditava na possibilidade de conexão entre pessoas e a rede por meio da internet, pelas mais variadas opções de objetos rotineiros, facilitações da vida moderna (MAGRANI, 2019). Em 1990, o fundador da Sun Microsystems, Bill Joy, já refletia sobre o surgimento de tecnologias de conexão de dispositivo para dispositivo, que na época denominou como D2D – *device to device* – trabalhando com a ideia de conexão de várias redes (MAGRANI, 2019).

Contudo, o termo *Internet of Things* prevaleceu e a teoria formulada por Ashton se amolda perfeitamente à realidade dos objetos inteligentes que podem se conectar literalmente a qualquer coisa ou rede, podendo armazenar dados sobre o usuário e transmiti-lo de maneira inteligente para tornar mais úteis áreas como a economia, saúde, facilidades pessoais e consumo (MAGRANI, 2019). Em definição técnica, a Internet das Coisas é uma extensão da internet comum, porém conectada a objetos do dia a dia, desde que haja capacidade computacional, comunicação e conexão com a rede de internet. Assim, a "conexão com a rede mundial de computadores viabilizará, primeiro, controlar remotamente os objetos e, segundo, permitir que os próprios objetos sejam acessados como provedores de serviços" (SANTOS *et al.* 2016, p. 2).

Os dispositivos de Internet das Coisas funcionam com uma estrutura própria e flexível para sua adequação, composta por a) uma camada de aplicação; b) uma camada de rede; e c) uma camada de percepção. Essa estrutura é essencial para a composição de um mecanismo básico de Internet das Coisas (SANTOS *et al.* 2016). Conceitualmente, Camargo (2020) acrescenta ainda uma camada de disponibilização ou interface, cuja função é o acesso aos dados e a criação de rotinas de processamento por meio de interfaces.

Com as respectivas distinções conceituais, podem definir-se as seguintes camadas (SANTOS, 2016; CAMARGO, 2020):

a) Camada de aplicação ou armazenamento: é onde de fato ocorrem os serviços prometidos aos usuários, responsável pelo processamento e armazenamento de dados;

b) Camada de rede ou transporte: é onde se realizam os serviços de gerenciamento, roteamento e identificação;

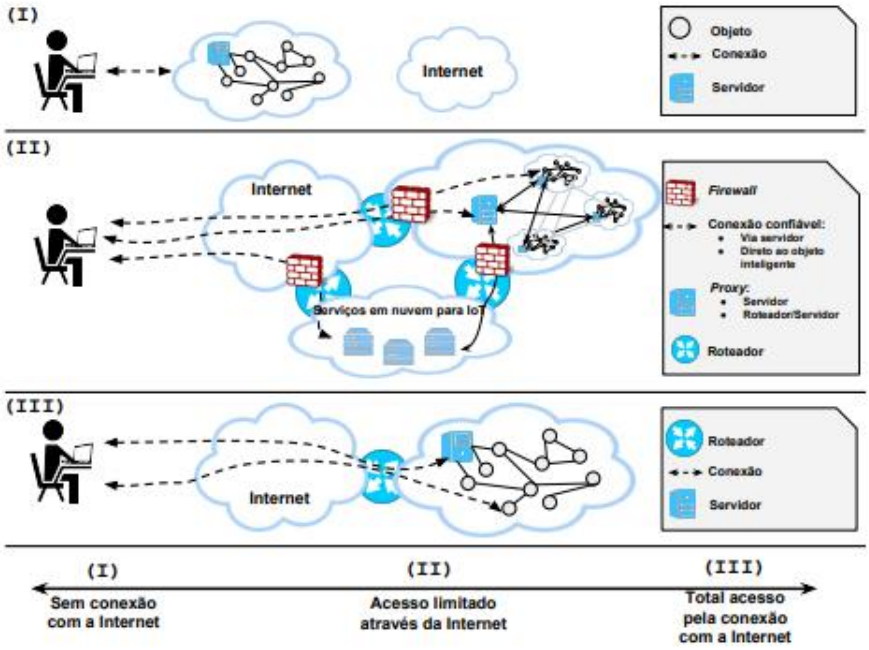
c) Camada de percepção ou detecção: se encontram os objetos que farão de fato a captação e processamento de informações como sensores de inteligência;

d) Camada de disponibilização ou interface: onde é possível acessar os dados e a criação de rotinas de processamento através de interfaces.

Essa tecnologia possui três modelos de redes aos quais pode objetos inteligentes podem se conectar: a rede autônoma de objetos inteligentes que funciona sem a intervenção externa de internet, com os objetos se comunicando diferentemente em uma rede interna; a rede de internet estendida, que se encontra parcial ou totalmente vinculada ao uso de internet das coisas com objetos inteligentes da rede conectando-se à Internet , e por último a rede de Internet das Coisas, em que os objetos inteligentes estão totalmente conectados à internet e permitem sua conexão integral com a internet diretamente, sem precisar de um servidor de intermediação (SANTOS *et al.* 2016, p. 16-17).

Os modelos de conexão são demonstrados na imagem abaixo por Santos *et al.* (2016), para elucidação dos diferentes conjuntos de conexões que podem ser utilizados pela Internet das Coisas:

Figura 2 - Título



Fonte: Santos *et al.* 2016.

Esses modelos de conexão podem atuar nos mais diversos objetos com IoT, outros aparatos fazem com que a estrutura da Internet das Coisas funcione; sensores, transitores e códigos executam as camadas de estruturação e formam os diferentes modelos de conexão de cada dinâmica. Por meio do uso de Internet das Coisas, a indústria 4.0 pode elaborar projetos inteligentes capazes de produzir resultados precisos de predição, assim, um objeto simples como um relógio pode captar informações que "são geradas, coletadas, processadas e distribuídas a qualquer momento e em qualquer lugar, realizando comunicações entre pessoas,

entre pessoas e ‘coisas’ e somente entre ‘coisas’” (BACCARIN *in* BARBOSA *et al.* 2018, p. 89).

Contudo, nem todo objeto pode comportar de fato a tecnologia IoT. O que caracteriza esse equipamento como tal são as funcionalidades de processamento, endereçamento, identificação, comunicação, cooperação, detecção de estímulos, atuação e interface, elementos que acumulados ou não conseguem produzir um grande volume de informações de forma rápida sobre seu usuário (BARBOSA *et al.* 2018).

Atualmente, com a abundância de dispositivos com IoT disponíveis para consumo, o próprio mercado tem delimitado o que seria Internet das Coisas Úteis, como tecnologias voltadas a cidades, saúde e educação e Internet das Coisas Inúteis, que seriam os objetos simples que não têm grande ganho produtivo em possuir tecnologia *high tech*, exercendo a mesma função e em preço mais barato no formato manual (MAGRANI, 2018).

Para Cohen (2019), os investimentos que rumaram à expansão dos objetos inteligentes por meio da Internet das Coisas criaram uma expansão radical da capacidade de vigilância, com uma rede sensorial com dispositivos móveis constantemente ativos e sensores sempre integrados à rede, coletando e transmitindo dados sobre o comportamento dos usuários para diversas plataformas conectadas. Contudo, essas estruturas sensoriais são projetadas para funcionarem de forma opaca aos olhos do usuário, de maneira que a coleta de dados e atuação dos sensores ocorra de forma invisível e automática, sintonizando-se “as condições ambientais e comportamentais” (COHEN, 2019, p. 69).

A opacidade é também apontada por Zuboff (2018), ao mencionar a citação do cientista da computação Mark Weiser, afirmando que “As tecnologias mais profundas são aquelas que desaparecem. Elas se entrelaçam no tecido da vida cotidiana até que sejam indistinguíveis desta”. Isto é, uma característica da Internet das Coisas é fazer com que suas atividades sensoriais passem despercebidas do usuário de modo que a figura de uma força computacional seja afastada das percepções do usuário.

Além dos aparatos tecnológicos que fomentam o funcionamento da Internet das Coisas, a opacidade de uma realidade constantemente conectada faz surgir outras tecnologias para um universo além da realidade física e totalmente digitalizada. Um exemplo do universo alternativo que a rede sensorial pode produzir é o Metaverso, uma rede cuja proposta é ir além do universo virtual até então estabelecido. De acordo com Mystakidis (2022), trata-se de um universo pós-realidade, que mescla a realidade virtual e física com a convergência de tecnologias multissensoriais com ambientes virtuais, objetos inteligentes e pessoas.

Assim, a rede do Metaverso é formada por um conjunto de objetos inteligentes com múltiplos sensores conectados que convergem para a realidade física e virtual (MYSTAKIDIS, 2022, p. 487):

> O Metaverso é baseado em tecnologias que permitem interações multissensoriais com ambientes virtuais, objetos digitais e pessoas. A fidelidade representacional do sistema XR é possibilitada por exibições estereoscópicas que são capazes de transmitir a percepção de profundidade [11]. Isso é possível com exibições separadas e ligeiramente diferentes para cada olho que replicam a visão em ambientes físicos [11]. Os monitores XR com altas resoluções ativam um amplo campo de visão do usuário que pode abranger de 90 a 180 graus. Os sistemas XR também oferecem experiências auditivas superiores em comparação com os sistemas 2D. O áudio 3D, espacial ou binaural permite a construção de paisagens sonoras que melhoram decisivamente a imersão em AR e VR [12]. (...) Ele funde espacialmente o mundo físico com o virtual [8]. O resultado final é uma camada projetada espacialmente de artefatos digitais mediados por dispositivos, por exemplo, smartphones, tablets, óculos, lentes de contato ou outras superfícies transparentes [9]. Além disso, o AR também pode ser implementado em headsets VR com capacidade de modo de passagem, exibindo entrada de sensores de câmera integrados.

A rede sensorial que possibilita o Metaverso vem do contexto de aparatos tecnológicos produzidos para garantir a existência do universo da Internet das Coisas; na verdade, a IoT é uma das tecnologias habilitadoras do Metaverso, pois com outras tecnologias como Big Data e Inteligência Artificial, seus sensores e "convergências aceleram a conexão da rede e integração dos espaços virtuais" (PEREIRA *et al.*, 2022, p. 5).

Desse modo, a realidade de múltiplos sensores espalhados em dispositivos inteligentes caminha para ser uma das bases de um novo universo tecnológico como a rede do Metaverso. A nova rede é uma evolução a partir da união de outras tecnologias como Internet das Coisas, produzindo um universo pós-realidade que une realidade aumentada e realidade física. A grande rede sensorial da Internet das Coisas, consequentemente, produz um grande volume de dados, que de fato é a sua finalidade, e também gera múltiplas transações que podem apresentar riscos de segurança e necessidade de intermediações financeiras.

Eis que o *blockchain* surge como alternativa para a desmaterialização financeira e sistema de autenticação de segurança sobre diversas transações de dados e ativos financeiros. Julie Cohen (2019) descreve o *blockchain* como um protocolo de autenticação e segurança das transações e ferramenta promissora na garantia de segurança do ambiente virtual. Além da segurança, ele pode ser utilizado como moeda de troca nas transações negociais dentro dos modelos de negócio que envolvem o grande volume de dados entre corporações, afastando-se de intermediações tradicionais ou monopolizadas por agentes financeiros tradicionais e

permitindo o uso de criptomoedas e a construção de um capital financeiro dentro do ambiente virtual (COHEN, 2019).

De acordo com Schwab (2016), o uso generalizado da Internet das Coisas está criando uma revolução em diversas abordagens. Para o autor, o *blockchain* pode revolucionar até mesmo métodos tradicionais de certificação e autenticação, como registros civis, diplomas, contratos, atestados médicos entre outros, ou seja, qualquer transação pode ser transformada em código, revolucionando modelos de autenticação para outras demandas da economia virtual.

Constrói-se uma estrutura em que a Internet das Coisas é sedimentada no campo virtual e físico, por meio de ferramentas que promovem uma turbidez entre objeto e mecanismos de computação, ou seja, o usuário vê uma ferramenta de facilitação do dia a dia, uma IoT Útil ou Inútil e raramente consegue perceber as camadas de inteligência atuando na coleta de seus dados. A Internet das Coisas é uma das portas de entrada para a nova rede de conexão do Metaverso e justifica a necessidade de outras tecnologias que transformam o ambiente virtual, sensorial em um ambiente seguro, como o *blockchain*, além de tantos outros mecanismos que derivam da IoT.

Ainda assim, a Internet das Coisas segue sendo um modelo tecnológico de captação de dados representado pela vigilância por meio das redes de sensores e dispositivos inteligentes. Por isso, é importante considerar a extensão conceitual da estrutura em que se insere, os reflexos normativos e os paradigmas que surgem de sua relação com os usuários.

3.1.1 Computação ubíqua e atuação

Uma das críticas de Zuboff (2019) ao Capitalismo de Vigilância é o "determinismo tecnológico" da transição para uma computação ubíqua, termo que define como uma realidade computacional de sensores por todas as partes, em que tudo estará “conectado, será sabível e acionável”. Sua crítica é que essa nova realidade parece ser imposta pelos agentes do mercado tecnológico e não uma opção natural da comunidade civilizada, havendo pouco debate sobre ser inevitável em uma realidade em que a computação possa estar em toda parte da vivência humana.

Para a autora, a ideia de que a maximização da computação ubíqua é inevitável é uma construção que partiu dos líderes do capitalismo de vigilância. Grandes empresas como o Google definiram, em seus próprios termos, a inevitabilidade da realidade ubíqua, e esse é o aparato que sustenta e consagra uma política maquiavélica do capitalismo de vigilância (ZUBOFF, 2019).

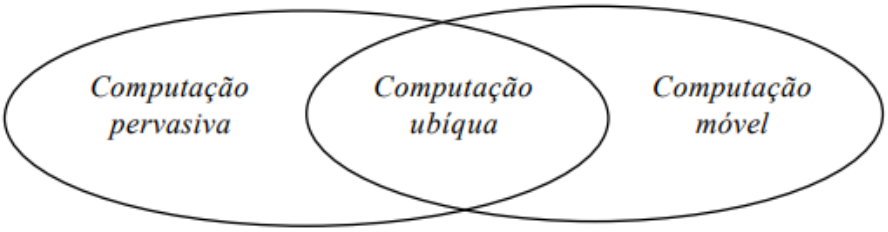
Voltando ao princípio conceitual, para entender a ubiquidade, outras definições são necessárias. Mark Weiser foi responsável pela ideia de uma computação que pudesse estar em todos os lugares, que computadores poderiam estar presentes nos mais simples objetos, sua previsão era de um futuro de convivência com computadores e não apenas interação (ARAUJO, 2003). Porém, só a computação ubíqua não é responsável por proporcionar os mecanismos digitais inteligentes por toda a parte, pois a complexidade tecnológica é resumida por Zuboff (2019), excluindo-se a dinâmica que há entre outros aparatos além da ubiquidade. É necessária, portanto, uma junção de Computação Pervasiva e Computação Móvel para que seja possível ampliar a Computação Ubíqua (SILVA *et al.* 2015).

Computação Pervasiva é o que define a invisibilidade do computador no ambiente para o usuário. Dessa forma, a inteligência computacional consegue obter informação do ambiente e utilizá-la na formação de modelos computacionais, sem que o usuário esteja consciencioso do desempenho dessas funções, como configurações e aplicações adaptadas pela máquina ou detecção de outros dispositivos para interações entre máquinas, sensores e serviços computacionais. Essa interação é o que faz da máquina "inteligente" (ARAUJO, 2003).

A Computação Móvel é a capacidade de mobilidade dos serviços computacionais, isto é, a possibilidade computacional de deslocar-se com uso de dispositivos, e assim, o usuário sempre pode estar conectado a uma rede computacional independentemente de sua localização (ARAUJO, 2003). A Computação ubíqua é a junção das funcionalidades dos dois modelos anteriores, a convergência de mobilidade computacional e com invisibilidade da construção de modelos computacionais em dispositivos, que dinamicamente pode obter informações e adaptar-se às necessidades do usuário, assim como pode conectar-se a outras redes e interagir de maneira inteligente (ARAUJO, 2003).

Como na figura 3, assim ocorre a relação entre computação móvel e pervasiva e ubíqua:

Figura 3 - Título



Fonte: Araújo (2003).

Da dinâmica computacional da ubiquidade, podem se extrair as características de invisibilidade, descentralização, pró-atividade, sensibilidade ao contexto e interfaces naturais, que funcionam da seguinte maneira (SILVA *et al.* 2015):

> Invisibilidade: Quanto mais presente uma tecnologia estiver, menos perceptível ela deve ser. O computador torna-se fundamental nas atividades cotidianas, mas dilui-se no mundo físico, tornando-se onipresente e imperceptível. A tecnologia não deve exigir mais que atenção periférica dos usuários.
>
> Pró-atividade: O sistema deve ser capaz de se antecipar a intenção do usuário.
>
> Sensibilidade ao Contexto: O sistema deve possuir mecanismos que permitam a aquisição de informações do meio. Estas informações são o cerne para todo o processamento do ambiente ubíquo.
>
> Interfaces Naturais: Uma das propostas da Computação Ubíqua é a comunicação natural entre pessoas e sistemas computacionais. Diante disso, surge a necessidade de se buscar técnicas para que os recursos de comunicação utilizados dia a dia de uma sociedade, como gestos, voz e mesmo olhares, possam ser utilizados na interação entre homem e a máquina.
>
> Descentralização: O computador pessoal é um dispositivo de propósito geral que atende muitas necessidades do usuário, tais como: edição de texto, contabilidade, navegação na web, produção de apresentações, entretenimento, etc. Nos dispositivos ubíquos, entretanto, a limitação de espaço físico impõe a limitação de recursos computacionais que, por sua vez, produz o objetivo de focalizar poucas necessidades específicas. Em um cenário ubíquo, as necessidades gerais passam a ser supridas através da colaboração mútua entre várias entidades computacionais.

Nesse sentido, a ideia inicial de uma realidade ubíqua vai além da construção proposital de uma cultura de computação por todas as partes. A ubiquidade ocorre com o conjunto de invisibilidade e mobilidade, descentralizando-se de objetos padrões de computação e tornando-se opaca aos olhos do usuário comum e inteligente na conexão com diversos dispositivos.

A junção dessas modalidades computacionais produz solo fértil para as tecnologias de Internet das Coisas; assim, é possível que as pessoas se comuniquem naturalmente com aparelhos virtuais, como pedir uma música para a Alexa, compartilhar a agenda de trabalho com a Siri, contar os passos, batimentos cardíacos e a quantidade de calorias ingeridas no relógio de pulso, e saber quais itens estão em falta na geladeira de casa. Com todo esse aparato técnico, constrói-se uma computação ubíqua, onipresente em todos os setores da vida cotidiana; em contraponto, os equipamentos também contam com a estrutura de análise comportamental tanto de si mesmo quanto de seu usuário, para estabelecer suas interpretações e seus padrões de uso. Nesse sentido, descrevem Santaella *et al.* (2013, p. 30):

> Objetos computacionais implementados em objetos com hardwares em sua arquitetura, como sensores, controladores e atuadores, e conectados em redes centralizadas, descentralizadas ou distribuídas poderão ter também comportamento sistêmico e coletivo. Podem atuar como enxames, por exemplo, seguindo padrões em seus modos de agir coletivo e se assemelhar a comportamentos de animais que vivem em grupos. Ou possibilitarão a observação da dinâmica comportamental de si mesmos

> e de seus agentes cooperativos, dinâmica que usualmente não teria como ser monitorada e, a partir dessa observação, extrair novos padrões coletivos dos modos de agir desses sistemas.

Logicamente, a coleta de todos esses dados pela Internet das Coisas terá finalidade de atender às necessidades dos usuários, mas também estará sujeita a outras funções desconhecidas pelo público comum, preenchendo o requisito de invisibilidade a interação da IoT com outros dispositivos, rede e sensores ocorre despercebida. A maximização da computação ubíqua é um evento presente e consagra a evolução tecnológica, então conhecida para a Internet das Coisas. O "inevitabilismo" apontado por Zuboff de fato é real, e a convivência com a computação inteligente desponta outros modelos econômicos possíveis por meio da IoT e da sua grande capacidade de coleta de dados e transações entre pessoas, máquinas e redes.

3.1.2 Modelos econômicos: escopo, ação e personalização

O campo das tecnologias de Internet das Coisas explora outras modalidades de economia na produção de bens e serviços. Pode-se compreender que a realidade de computação ubíqua impõe um universo de dispositivos sempre conectados e aptos à captação de dados para atender serviços aos usuários. Dessa forma, é necessariamente lógico que o desenvolvimento e a venda de produtos inteligentes são fundamentais para a maximização da ubiquidade por meio da IoT. Julie Cohen (2016) identifica, como um dos modelos econômicos adotados no complexo de inovação da vigilância, a participação voluntária do usuário dentro atividades que a tecnologia propõe. A estratégia da participação envolve um automonitoramento provocado pelo próprio usuário e seus constantes feedbacks, que servirão para criar uma base de dados.

A técnica envolve criar um ambiente de incentivos ao usuário para interagir com a tecnologia, e como exemplo, pode-se citar a dinâmica de notas e recomendações da Amazon dentro de seu site, espaço onde o usuário é incentivado a expor livremente suas impressões sobre os produtos vendidos. Em outros modelos, a dinâmica envolve incentivar o usuário a convidar mais pessoas para a interação (COHEN, 2016). O que essa dinâmica não revela ao usuário comum é que esta breve interação está ocorrendo entre pessoa e máquina, e as impressões ali registradas são dados que construirão um perfil de nicho com a cooperação do usuário.

Por sua vez, Zuboff (2019) acredita que a competitividade pelo excedente comportamental dos usuários trouxe para o campo das tecnologias digitais a modalidade de

economia por escopo, e para acomodar ainda mais dados, as estruturas de captação precisariam adotar novos métodos por escopo e por ação. Nesse sentido, Zuboff (2019, p. 406):

> A necessidade de escala levou a uma busca incansável por novos suprimentos, em grande volume, de superávit comportamental e produziu uma dinâmica competitiva que visa controlar esses suprimentos de matéria prima e buscar espaços indefesos e sem legislação nos quais processar os inesperados e mal compreendidos atos de despossessão. O tempo todo os capitalistas de vigilância nos habituaram, de modo furtivo, mas resoluto, a suas reivindicações. No processo, nosso acesso à informação e aos serviços necessários tornou-se refém de suas operações, nossos meios de participação social foram fundidos com seus interesses. Produtos de predição lucrativos dependem de superávit comportamental, e a competição levou os desafios de suprimento a um novo nível, expresso no imperativo de predição. Produtos de predição mais poderosos requeriam economias de escopo, bem como de escala, diversidade, assim como volume. Essa diversidade ocorre em dois níveis. O primeiro é a extensão através de uma ampla gama de atividades; o segundo é a profundidade de detalhe preditivo dentro de cada atividade.

Expandir a coleta de dados, nesse ponto de atuação das tecnologias de vigilância, envolve adotar novas estratégias. A economia de escopo é o método que propõe acesso a um vasto e variado volume de informações, com extensões para fora do mundo virtual, e envolve captar padrões íntimos, de personalidade e emoção, nas vastas áreas de vivência do usuário. Por isso, o modelo de escopo usa da inserção de coisas presentes no campo externo ao mundo virtual, como objetos simples (ZUBOFF, 2019). A economia de ação envolve uma atuação ativa da tecnologia de vigilância, com métodos que incentivem a participação do usuário em servir dados. É também um mecanismo voltado a personalizar e reconfigurar informações para o usuário, de forma a prever as possíveis escolhas do usuário com mais certeza (ZUBOFF, 2019).

Pariser (2012) resume esses modelos econômicos praticados pelos dispositivos inteligentes em um sistema de filtragem e personalização ainda mais avançado, em que muitas facilidades e inovações são produzidas, mas “a personalização sempre envolve uma troca: ganhamos conveniência, mas cedemos à máquina um pouco de privacidade e controle”. Compreende-se que a economia de personalização seja intensificada à expansão com base nos resultados positivos que os acertos de previsão podem trazer aos anunciantes e para as plataformas; assim, a expansão de dispositivos para criar filtros de personalização sobre os usuários faz parte de um modelo ultra personalização muitas vezes “turvo” para o usuário (PARISER, 2012).

A princípio, os formatos econômicos operados pelas tecnologias de Internet das Coisas se assemelham à formatação de uma realidade de expansão das maneiras de se coletar dados, classificá-los em profundidade, criar incentivos para a participação ativa do usuário e até atuar ativamente em influências para uma predição mais certeira. Estruturalmente, a tecnologia de

Internet das Coisas não se trata somente de objetos inteligentes, mas de um aparato tecnológico subdividido que forma a sua capacidade de computação inteligente e concretiza uma realidade ubíqua da computação em estar presente em todos os espaços de formas diversificadas.

3.1.3 Capilaridade lógica e física: cookies e sensores

O contexto da ubiquidade impõe uma hiperconexão em redes sociais e sites comumente disseminados no dia a dia, que além de uma comunidade virtual, fornecem ferramentas cuja gratuidade costuma ser acompanhada da condição de fornecimento de dados pessoais (PESSOA, 2020). A realidade ubíqua não está inserida somente nas redes sociais e sites, nem tampouco somente em objetos inteligentes. Camargo (2020) distingue um caráter duplo da Internet das Coisas, formado por capilaridade lógica e capilaridade física.

Conceitualmente a capilaridade lógica é um formato de Internet das Coisas utilizado em aplicações como *cookies*, enquanto a capilaridade física diz respeito aos aparelhos e sensores físicos conectados à internet (CAMARGO, 2020). As redes e sites normalmente se utilizam dos *cookies,* uma tecnologia via código cujas informações ficam registradas ao primeiro acesso em uma página. E então, nas próximas visitas ao site, o navegador informará ao servidor as informações da última visita, o que importará na lembrança de hábitos, comportamentos, opções e informações do usuário (PESSOA, 2020).

Por definição, *cookies* são conceituados como "cadeias de números e letras geradas aleatoriamente que podem ser enviadas de um site para o navegador do usuário, onde são armazenadas em um subdiretório no computador durante uma sessão e retornadas inalteradas ao site"[3] (FROW, 2019, p. 208). A função deles é basicamente de criar um registro de identificação e memorizar o computador utilizado em determinado acesso ou serviço para, posteriormente, dar continuidade aos registros em próximas visitas e transações feitas naquele mesmo site. Em virtude disso, trata-se de uma tecnologia voltada a registrar preferências do usuário e criar um perfil. Esses registros, portanto, poderão ser acessados no espaço e tempo para outras operações entre anunciantes e envio de propagandas personalizadas (FROW, 2019).

Esse formato de operacionalização não é exclusividade dos cookies, tecnologias como rastreamento de login universal, rastreamento de cookie HTML, identificador gerado por

[3] Texto original: "randomly generated strings of numbers and letters that can be sent from a website to the user's browser, where they are stored in a subdirectory on the computer during a session and returned unchanged to the website."

cliente ou dispositivo, Web beacons, são operações de registro desenvolvidas com a mesma finalidade (FROW, 2019). Nesse sentido (CAMARGO, 2020, p. 34):

> Com esse mecanismo de persistência de estado, passou a ser possível não apenas reaproveitar informações para reutilização no ciclo de navegação seguinte, mas também manter agrupados vários dados de um usuário mesmo antes de saber quem ele é. A navegação em um e-commerce é um bom exemplo. O usuário entra na loja e navega. Não tenta fazer uma compra, nem dá seus dados de identificação. Mas com os cookies, o servidor consegue rastrear todos os seus passos pelo site até que, em um determinado momento, ele decide fazer a compra. Identifica-se, portanto. Então, aquela aplicação não passa a conhecer o usuário a partir desse momento. Ela já o conhece desde a primeira vez que ele a acessou. Agora, ela apenas sabe o seu nome.

Essas tecnologias baseadas em cadeias de códigos perfazem as de IoT, de capilaridade lógica, em que um fragmento de código está inserido na página acessada, e enquanto estiver ativo, poderá registrar os rastros do usuário dentro do ambiente virtual e identificar o dispositivo para dar continuidade futura. Em contrapartida. as tecnologias IoT de capilaridade física são aquelas que utilizam objetos físicos para atuação por meio de dispositivos e sensores conectados à internet.

As tecnologias de capilaridade física estão espalhadas em sensores e computadores inseridos em objetos, com conectividade, realizando camadas de interação, como a descrição feita no tópico 2.1. Para Magrani (2019), as tecnologias de ambiente físico criam um ecossistema de computação onipresente, computação ubíqua em que computador, sensores e objetos interagem com usuários e uns com os outros no processamento e na troca de informações.

Cohen (2019) descreve que esses sensores compõem uma rede que antes era de comunicação e se torna uma rede sensorial, organizadas com sensores sempre ativos que transmitem um grande fluxo de dados, variados e altamente granular. Essa vastidão e variação dos dados é possível com a inserção de sensores em ambientes diversos, captando todo tipo de informação.

Os dispositivos móveis sensoriais captam informações de geolocalização e coletam e transmitem dados mensagens entre máquinas, como pesquisas na internet, compartilhamentos em redes sociais (COHEN, 2019), interações aplicativos diversos, como aplicativos que monitoram atividades físicas, e se comunicam com equipamentos de pulso, que monitoram a mobilidade diária, aplicativos que acompanham o trânsito e se comunicam com aparelhos GPS, entre muitos outros.

A rede sensorial forma um espécie de sistema nervoso autônomo do usuário, pois como uma espécie de espelho sensorial, reflete atividades, funções fisiológicas, emoções, sentimentos

do usuário e todo tipo de informação que for capaz de captar sensorialmente. Essa rede, portanto, é construída para operar na invisibilidade, como um canal sintonizado ao ambiente e às condições locais (COHEN, 2019). Essa invisibilidade ou não percepção das operações dos dispositivos inteligentes é característica própria da projeção do objeto, voltando-se ao conceito de Weiser sobre computação ubíqua, uma tecnologia que é capaz de fazer a computação desaparecer do pano de fundo, ou seja, "máquinas que se encaixam no ambiente humano em vez de forçar humanos a entrar no ambiente delas farão do uso do computador algo tão revigorante quanto um passeio no bosque" (ZUBOFF, 2019, p. 244).

Assim, quando em 2015 o Google anunciava o "fim da internet" como a conhecíamos até então, no Fórum Econômico Mundial, o discurso anunciava uma internet moldada pela rede sensorial que já era operante, liberta dos equipamentos tradicionais de computação, computadores pessoais e smartphones. Isto é, livre para operar em simples objetos do dia a dia, sem que o usuário perceba diretamente essa atuação (ZUBOFF, 2019).

A expansão da Internet das Coisas no âmbito físico ou lógico traz preocupações no campo da proteção da privacidade devido ao desconhecimento dos mecanismos de trocas de dados e sua monetização, bem como ao aumento de dados captados para processamento, baseados em dados pessoais (CAMARGO, 2021). O desconhecimento do usuário sobre a finalidade das operações comerciais realizadas pelas IoT abre espaço para a desconfiança em relação à rede sensorial e à proteção do usuário no uso de equipamentos inteligentes (MAGRANI, 2019).

Ademais, Pariser (2012) aponta ainda o risco do desconhecimento sobre como os dados captados podem ser convertidos em ações de atuação sobre o usuário, e não só "como ocorre", mas o desconhecimento se isso está ocorrendo ou não quando o usuário utiliza um objeto que apenas deveria atender ao serviço solicitado. Conhecimento e consentimento emergem em águas turvas do ambiente codificado (COHEN, 2019). Assim os riscos das operações aos direitos dos usuários também são obscurecidos pelos artifícios que os objetos tecnológicos representam ao usuário, ou seja, é uma questão de detecção e submissão do consentimento. Este estudo aborda a Internet das Coisas operada por objetos inteligentes de capilaridade física, que constituem o atual cenário de computação ubíqua.

Do uso indiscriminado desses objetos no dia a dia, surgem alguns paradigmas a serem analisados, como a normatividade e as possíveis regulações para proteção do usuário e a problemática acerca do direito à privacidade do usuário, que se estende a outros conceitos comuns no âmbito da tecnologia ubíqua, como termos de consentimento e relatividade da privacidade.

3.2 ASPECTOS NORMATIVOS DA INTERNET DAS COISAS

> "Parafraseando Stan Lee, o criador do Homem-Aranha, grande poder traz grandes responsabilidades, mas os programadores que nos trouxeram a internet e, agora, a bolha dos filtros nem sempre estão a fim de assumir essas responsabilidades." Eli Pariser, 2012.

Compreendidos os modelos negociais da Internet das Coisas e como seus aparatos são atuantes na vigilância de usuários, questões principiológicas se tornam importantes, como a possível regulação desse mercado e a identificação de quem são os interessados em uma construção normativa. Dois aspectos dividem uma possível regulação da Internet das Coisas: de um lado, o interesse econômico em atividades mais livres e desregulamentas nas redes; e de outro, o interesse normativo em construir mecanismos de proteção do usuário.

A construção de uma regulação ou a priorização dos ganhos econômicos esbarram mutuamente em suas próprias justificativas, pois se cria um limbo procedimental de ganhos e riscos: ganhos para quem sabe aproveitar esses espaços não regulados no meio tecnológico, e riscos para os usuários consumidores de tecnologias cujos dados estão no cerne da discussão.

3.2.1 Interesse normativo e o consumo de vigilância

No debate de construção de políticas regulatórias sobre Internet das Coisas e proteção do usuário quanto à privacidade, esbarra-se sempre em um conceito imposto de "tudo ou nada". Para avançar inovando com tecnologias digitais de vigilância, é necessário renunciar a garantias fundamentais como privacidade (MAGRANI, 2018).

No cenário global, o tema é tratado muitas vezes de forma polarizada. Como descreve Magrani (2018, p. 176), uma "falácia do tudo ou nada" que serve no fundo para distorcer o foco dos debates sem chegar em avanços concretos. Para ele, é "preciso assegurar a proteção dos usuários da Internet das Coisas, mas deixar espaço aberto para que a tecnologia possa continuar a ser aperfeiçoada", encontrar uma mediação entre os aspectos gerais de políticas públicas de segurança, privacidade e compreender a importância da continuidade da inovação tecnológica. Nesse sentido, Magrani (2018, p. 176):

> Nesse cenário, para evitar a perspectiva falaciosa do tudo ou nada e sua influência sobre o próprio processo de elaboração de políticas públicas, é necessário realizar pesquisas para compreender os modelos regulatórios que têm se desenvolvido para subsidiar a evolução da IoT. A pesquisa no âmbito do eixo horizontal privacidade e

> segurança deverá ser baseada em um mapeamento compreensivo e uma análise das iniciativas comparadas, contextualizando-os no panorama regulatório brasileiro. Essa análise deve ter por base estudos das seguintes dimensões: (1) análise da dimensão legal (políticas para a IoT, boas práticas, instrumentos regulatórios em vigência, práticas contratuais, lacunas regulatórias e outros pontos relevantes) e propostas regulatórias para fazer frente a necessidades nacionais específicas; (2) análise da dimensão de governança (boas práticas, de transparência, participação e abertura nos processos decisórios referentes às políticas adotadas) e propostas de modelos de governança participativa.

A proposta é um eixo horizontal de mediação entre interesses de ambos os lados, em que a importância e os benefícios da Internet das Coisas ao contexto moderno são reconhecidos, mas que políticas de respeito à direitos fundamentais como a privacidade sejam também construídas. A visão apresentada por Cohen (2019) revela outros fatores que devem ser considerados para entender os conflitos de interesse quanto às regulamentações na Internet das Coisas. Ele descreve que, junto com essas tecnologias, o mercado criou uma espécie de domínio público biopolítico sobre processamento de dados, de maneira que a fonte de matérias-primas está disponível para ser tomada e convertida em insumos da cadeia produtiva.

Assim, descreve Cohen (2019, p. 7):

> As matérias-primas consistem em dados que identificam ou se relacionam com pessoas, e o domínio público formado por esses materiais é biopolítico – ao invés de, digamos, pessoal ou informacional – porque as atividades produtivas que ele enquadra como desejáveis são atividades que envolvem a descrição, processamento, e gestão de populações, com consequências produtivas, distributivas e epistemológicas.

O domínio público da informação é uma zona privilegiada aos agentes de atuação, pois configura um modelo ao qual o usuário não pode se opor, e legitimam-se os padrões de apropriação de informações e ocultam-se as políticas distributivas, ou seja, é uma ideia de privilégios de extração e apropriação de dados livremente (COHEN, 2019). Esse conceito de operação baseado em um domínio público biopolítico sobre a informação foi construído sob pressão das grandes indústrias de tecnologia na tentativa de frear ou afastar agentes reguladores de suas atividades. Cohen (2019) entende que mais do que os discursos de impedimento à inovação, há uma atuação ativa da indústria tecnológica junto às instituições políticas para evitar uma regulação.

Essa ausência de regulação deixa o campo aberto para o semear da autorregulação como um modelo de legitimação de apropriação e processamento de dados dos usuários; assim, a praxe tornou-se o aviso de termos de uso e consentimento inserido como uma autorização dominante do uso das técnicas de processamento de dados por todas as empresas de tecnologia. Um termo com políticas de privacidade turvas, em um longo e incompreensível texto, foi o

modelo de autorregulação criado pelas plataformas (COHEN, 2019). Modelos autorregulatórios não funcionam com agentes predatórios e inescrupulosos.

Defende O'Neil (2020) que uma série de medidas regulatórias e procedimentais precisam ser adotadas para frear técnicas predatórias de apropriação de dados sobre as experiências humanas. Além de uma atuação ativa dos agentes do Estado e da construção de normas reguladoras, ele entende ser necessário reprogramar toda a interpretação dada pela tecnologia, que muitas vezes tem extrapolado limites de privacidade e promovido comportamentos de desigualdade. Por isso, além de regulação, O'Neil (2020) defende a criação de mecanismos de auditoria das interpretações, fiscalização dos algoritmos e participação de pessoas na conclusão da predição que também entendam o ecossistema e não somente assumam o resultado final de uma operação matemática comportamental apresentado pela máquina.

Zuboff (2019) vislumbra um "desprezo" dos agentes do capitalismo de vigilância pelas tentativas de regulação do mercado. Ele cita as falas do CEO do Google Eric Schmidt como exemplo, ao afirmar que a tecnologia avança de forma tão rápida que sua regulação é desnecessária e seus problemas podem ser resolvidos pela autorregulação, explicando que "nós avançaremos mais rápido que qualquer governo". Para a autora, o capitalismo de vigilância colocou em xeque o direito à privacidade como uma excludente necessária para os avanços da inovação tecnológica, como um "tudo ou nada", ou seja, a privacidade teria sido relativizada pelo viés de neoliberalismo para não impor limites às práticas corporativas de vigilância (ZUBOFF, 2019).

Vale observar que a ótica apresentada por Cohen (2019) não é tão simplista, pois mais do que afastar as instituições reguladoras, a autora entende que os agentes do capitalismo de vigilância atuam para serem os próprios reguladores, não desprezando eventual necessidade de regulação, mas uma conclusão de que se houver de se regular, que seja a regulação feita pelos próprios agentes utilizando termos de consentimento e autorização tácita do usuário com o uso de suas informações.

Pariser (2012) identifica que o atual formato cria uma ilusão de responsabilidade do usuário ao possibilitar que ele concorde ou não com o processamento de suas informações pelas tecnologias de vigilância, mas essa não é uma medida adequada na proteção da privacidade do usuário, pois "dizer que para entender as opções basta passar um bom tempo lendo o manual não é uma resposta satisfatória". Nesse contexto, a Internet das Coisas é uma realidade presente de inteligência computacional que já produz efeitos contemporâneos na privacidade dos usuários, mas poucas normativas regulatórias surgem em seu encalço, por desinteresse, pela

construção de um modelo de autorregulação e também pela névoa de desconhecimento que envolve o usuário da Internet das Coisas.

Embora as políticas de autorregulação criadas pelos agentes do capitalismo de vigilância sejam comumente fundadas em um terminologia de consentimento do usuário, o usuário comum desconhece os efeitos dessa concordância para inserir-se no contexto de economia e produção construído pelos mecanismos de computação ubíqua. Os poucos aspectos normativos e o desconhecimento do usuário certamente desencadeiam problemas de privacidade do usuário e abrem espaço para práticas predatórias com danos concretos.

3.2.2 Marketing predatório e privacidade: algoritmos de destruição em massa e hiperconsumo

As externalidades que podem ser causadas pelas tecnologias de Internet das Coisas são muitas, mas fundamentalmente uma economia baseada no avanço contínuo de técnicas de vigilância implica externalidades sobre a privacidade dos usuários. A privacidade é, neste estudo, o objeto sob o qual mecanismos de proteção e regulação são questionados.

A pesquisadora O'Neil (2020) é uma matemática que atuou no desenvolvimento de cálculos estatísticas para operação de tecnologias digitais de interpretação e desenvolveu seu próprio estudo sobre técnicas predatórias de vigilância em massa, que são utilizadas no mercado de processamento de dados, intitulado Algoritmos de Destruição em Massa, ou simplesmente ADM, como simplifica a autora. Além disso, ela descreve como cálculos matemáticos somados ao uso de algoritmos de aprendizagem estão promovendo a desigualdade em diversas áreas da sociedade e afetando negativamente até mesmo a disposição da democracia (O'NEIL, 2020).

No campo do consumo, vale destacar uma prática de capitalismo ou simplesmente marketing predatório, que converge para a criação de perfis pessoais baseados em sentimentos íntimos e extremamente pessoais em propagandas massivas, predatórias e direcionadas para a influência no comportamento de compra do alvo pretendido e que mais assustadoramente funcionam (O'NEIL, 2020). O exemplo dado pela autora explica como as faculdades nos Estados Unidos com pouco prestígio acadêmico e mensalidades em valores monumentais trabalhavam seu marketing predatório direcionado a alguns grupos sociais.

As universidades com fins lucrativos e nem sempre prestigiadas na busca por mais alunos que se enquadrem no financiamento governamental adotam todo tipo de campanha para atingir o respectivo grupo e angariar os novos financiamentos (O'NEIL, 2020). Contudo, torna-se essa campanha preocupante quando as mesmas universidades passam a utilizar sistemas de

publicidade com palavras-chave, que demonstram, de forma clarividente, a abusividade pretendida e a violação da privacidade. Foi o caso da universidade Cotinthian College, que foi denunciada por campanha predatória cujos termos de publicidade envolviam lançar propagandas massivas a usuários pudessem ser identificados pelas palavras-chave “isolados;” “impacientes;” “empacados;” “poucas pessoas na vida que se importam com eles” (O’NEIL, 2020).

Ainda mais predatório era o direcionamento de propaganda para vagas de emprego da Vatterott College, que direcionava campanhas de recrutamento para usuárias que se enquadrassem nas palavras-chave “mãe no seguro-desemprego com filhos”; “moças grávidas”; “recém-divorciada”; “baixa-autoestima”; “emprego de baixa-renda”; “passou por perda recente na família”; “tenha sofrido maus tratos físicos ou psicológicos”, entre outros termos que envolvem a experiência da vida pessoal negativamente.

Esses dois casos são demonstrações de um marketing predatório e invasivo da vida pessoal, afetando diretamente a privacidade dos usuários que, em algum momento, buscaram por essas terminologias ou que simplesmente uma IoT foi capaz de identificar um ambiente que configura esse contexto específico sobre o usuário. O’Neil (2020) revela que, nesses casos específicos, a finalidade do marketing predatório é apropriar-se das vulnerabilidades pessoais, pois conhecendo as vulnerabilidades do usuário que se pretende atingir ou do grupo direcionado, é possível lançar campanhas publicitárias massivas direcionadas a ele, prometendo uma rápida e drástica mudança de vida e oferecendo um recomeço ou uma oportunidade para pessoas que estão vulneráveis e buscando por soluções.

De modo geral, esse tipo de campanha acaba por ocasionar um volume de grandes dívidas, financiamentos universitários para pagamento futuro e diplomas com pouco prestígio no mercado de trabalho, que acabam por não garantir a oportunidade apresentada de início (O’NEIL, 2020). A técnica algorítmica, nesses casos, é uma abordagem de classificação em uma análise Bayesiana, em que se classificam as variáveis de maior impacto para obter o resultado desejado. O’NEIL (2020) segmenta o público-alvo dentro de plataformas como Google e Facebook, e desse ponto em diante, a capacidade preditiva dessas plataformas em entregar os anúncios agregará valor ao anúncio.

Por essa razão, a expansão das tecnologias e IoT é o marco importante em expandir as informações dos usuários a fim de identificar com ainda mais profundidade experiências, sentimentos, emoções, saúde e momentos extremamente pessoais. Essa predação mercadológica criadora de filtros e perfis pessoais age de maneira despercebida sobre informações que podem ter cunho extremamente privado, das quais o usuário não publicou em

rede e não tem a intenção de tornar pública, mas a realidade ubíqua possibilita que meras impressões sejam captadas e já transformadas em informação.

Este tipo de tecnologia voltada ao consumo possui perigos que acerca do desconhecimento do usuário sob suas finalidades e como o processamento da informação poderá retornar em uma ação direta de influência sob o próprio usuário. Com isso, Pariser (2012, p. 145) explicita:

> Além disso, como as transformações aplicadas aos dados muitas vezes são bastante turvas, nem sempre sabemos ao certo que decisões estão sendo tomadas a nosso respeito, por quem ou para quê. E isso já é bastante sério quando estamos falando de fluxos de informações, mas a questão se torna ainda mais grave quando esse poder afeta o nosso próprio aparato sensorial.

Outro aspecto relevante é a maneira como a influência de economias de ação agem na criação dos filtros que o usuário receberá como recomendação de acesso e, consequentemente, no que ele irá consumir. A bolha de filtros tende a indicar o que o conjunto de experiências registradas sobre o usuário indica que ele deve gostar de consumir e não necessariamente o que precisa ou até mesmo itens e ideias diferentes daquelas com as quais se está acostumado a consumir (PARISER, 2012).

O efeito desse tipo de conclusão é usar de conclusões filtradas na criação de identidades que tendem a se comunicar com identidades semelhantes, consumir produtos que seu perfil virtual costuma consumir, ler e assistir aquilo que o perfil filtrado costumaria assistir, formando assim uma bolha identitária fechada para informações diversas e não democráticas (PARISER, 2012).

Ademais, sobre o poder de influência dos filtros de publicidade direcionada e predatória, Pariser (2012) faz uma importante conceituação sobre a atual cultura de consumo, pois houve um momento em que o consumo era ditado pela necessidade, mas atualmente o consumo é ditado pela autoexpressão, e até o que é necessário para a autorrealização ou autoexpressão do consumidor é uma insígnia indicada pela classificação das informações.

Observando extensivamente todo o dilema da participação dos usuários na concessão de seus dados em rede ou nas interações com objetos inteligentes, percebem-se reflexos da sociedade de hiperconsumo proposta por Lipovetsky. O ritmo de consumo voltado às experiências, às sensações e ao bem-estar é disseminado pela rede sensorial, que consegue captar as possíveis vontades, desejos e sentimentos de seus consumidores. Nesse sentido, o consumo emocional pode facilmente ser sedimentado.

> O sensitivo e o emocional tornaram-se objetos de pesquisa de marketing destinados, de um lado, a diferenciar as marcas no interior de um universo hiperconcorrente, do outro lado, a prometer uma "aventura sensitiva e emocional" ao hiperconsumidor em busca de sensações variadas e de maior bem-estar sensível (LIPOVETSKY, 2007, p. 47).

A busca pelo bem-estar individual é mais bem perpetrada se acompanhada de dispositivos sensoriais e de comunicação entre sensações e redes que podem promover o acesso à vontade que se tem. No hiperconsumo, o consumo emocional estabelece um vínculo do indivíduo com o objeto de consumo, ou seja, uma significação individual é estabelecida (LIPOVETSKY, 2007).

Em outro aspecto, o hiperconsumo indica tendências ao consumo mais individualizado, em que a aparência social não é mais tão importante quanto atender à autoexpressão e à representatividade individual. O fetichismo volta-se à justificação do objeto de consumo para o indivíduo, "a mania pelas marcas alimenta-se do desejo narcísico de gozar do sentimento íntimo de ser uma "pessoas de qualidade", de se comparar vantajosamente com outros, de ser diferente da massa" (LIPOVETSKY, 2007, p. 50).

Essa relação ao consumo individualizado para atender vontades íntimas enseja mecanismos que possam perceber essas experiências e conhecer com profundidade as possíveis vontades do consumidor, tarefa que a realidade ubíqua e a Internet das Coisas facilitam com a captação de ambiente e de dados do usuário. O modelo de hiperconsumo explica em parte a aderência dos usuários a tecnologias que atendam a algumas de suas sensações e vontades mais íntimas, ainda que na maioria se desconheça essa esta operação ocorre e quais reflexos aos seus direitos podem ser causados.

O contexto da hiperconexão por meio da Internet das Coisas e a realidade ubíqua pode também ser analisado sob o enfoque das teorias de Bauman (2001) em seus estudos sobre a Modernidade Líquida, quando contextualiza de que modo a exaltação à individualidade tomou espaço antes ocupado por ideais de comunidade, passando a figura do indivíduo a ocupar espaço central em suas necessidades, decisões e consequências, contando cada vez menos com o senso de comunidade O cenário retratado é de uma modernidade leve e fluida, em que a individualidade é o marco central para a liberdade tão almejada, assim, felicidade e liberdade passam a depender de cada indivíduo em seu próprio espaço e não mais da comunidade em que se insere ou das regras sociais tradicionais da modernidade pesada (BAUMAN, 2001).

A modernidade líquida se configura cada vez mais latente com a realidade tecnológica na promoção de técnicas de consumo e processamento de dados; o "fetichismo subjetivo" e o "agorismo" nunca estiveram tão fluídos como então. A ideia de uma sociedade "agosrista" é

retratada por Bauman (2001) como uma configuração da sociedade em todos os setores hodiernos da vida voltados à instantaneidade e ao imediatismo, e com a mesma urgência, descarta-se por um novo artefato que lhe identifique ainda mais com o conceito de felicidade terrena que se busca atingir constantemente.

> Sim, é verdade que na vida "agorista" dos cidadãos da era consumista o motivo da pressa é, em parte, o impulso de adquirir e juntar. Mas o motivo mais premente que torna a pressa de fato imperativa é a necessidade de descartar e substituir. Estar sobrecarregado com uma bagagem pesada, em particular o tipo de bagagem pesada que se hesita em abandonar por apego sentimental ou um imprudente juramento de lealdade, reduziria a zero as chances de sucesso (BAUMAN, 2001, p. 38)

Enquanto o "fetichismo da subjetividade" se concretiza na sociedade de consumidores como uma ilusão acerca da realidade do consumo, consome-se em nome de uma ideia, um símbolo, que nada mais representa do uma simulação que não existe (BAUMAN, 2001). Assim, tem se configurado em alguns pontos a sociedade disseminadora de sensores e computação ubíqua, convivendo-se com as constantes recomendações daquilo que parece ser sua vontade, sua necessidade como forma de perpetuação de uma estrutura em que o mais importante é manter usuários conectados ou sob alcance de sensores de classificação.

A centralização do indivíduo na sociedade de consumo, ainda que em teorias distintas, demonstra aspectos predominantes do hiperconsumo da sociedade fluida em relação à generalização da Internet das Coisas e todos os aparatos que estruturam seu sistema mercadológico. As externalidades que as condutas predatórias de maximização do consumo mediante iniciativas de marketing direcionado e hiperfiltrado objetivamente esbarram na privacidade do usuário, sendo esse um dilema da sociedade hiperconectada e do capitalismo de vigilância.

3.3 PARADIGMA DA INTERNET DAS COISAS E A PRIVACIDADE

Todo o aparato tecnológico da Internet das Coisas traz reflexos na sociedade os quais tem se explorado muito pouco sob soluções, e muitas vezes, garantias fundamentais são colocadas sob o viés do inevitável ou "tudo ou nada", isto é, para inovar nesse cenário, é necessário renunciar a alguns direitos. A economia de vigilância que coloca a experiência humana como insumo essencial de seu modelo produtivo faz imprescindível que meios de coleta de informações estejam a postos para coletar e processar dados.

Contudo, mesmo um modelo econômico já consolidado deve respeitar limites intrínsecos à organização e configuração social, pois ainda que a relativização da privacidade pareça estar em oferta, mecanismos devem garantir sua proteção. No contexto da computação ubíqua, a autorregulação por parte das indústrias de processamento de dados tem trabalhado há anos sob uma máxima de aceitação do usuário acerca de seus termos de uso e consentimento, colocando esse artifício como uma ferramenta regulatória e contratual entre as partes. Assim, a relativização do consentimento produz sequelas na garantia da privacidade e recursos legais e mecanismos objetivos precisam ser analisados para proteção da tutela da privacidade.

3.3.1 Relativização do consentimento e hipervulnerabilidade: uma análise prévia à privacidade

No cerne dessa discussão, está a privacidade do usuário. No Capítulo 3, a privacidade será abordada como todo seu conceito axiológico e normativo, e qual a tutela desempenhada no campo legal para proteção do direito à privacidade na configuração social do usuário da Internet das Coisas. O contexto econômico até então abordado demonstra uma vulnerabilidade do usuário consumidor sob o domínio de suas informações em rede e sobre como elas são processadas por tecnologias que estão cada vez mais inseridas em seu dia a dia, especificamente em relação aos dispositivos compostos por Internet das Coisas. Com isso, a característica de invisibilidade da computação torna essa vulnerabilidade de percepção ainda mais grifada.

Nesse sentido, retrata Pariser (2012, p. 162) sobre a economia de personalização que "se baseia numa transação econômica na qual os consumidores se encontram numa situação de desvantagem inerente: enquanto o Google sabe o valor da informação sobre a cor da sua pele, você não sabe". O mercado oferece serviços gratuitos ou facilidades com objetos inteligentes, e o preço pago pelo usuário são alguns dados, mas se tratados como propriedade ou garantia fundamental, a troca parece ser injusta (PARISER, 2012).

Contudo, essa configuração é a norma da sociedade em rede, uma condição para inserção e acesso na sociedade hiperconectada é dispor de alguns dados para alimentar a rede de informações (PESSOA, 2020). E ainda que se tente excluir essa realidade virtualizada nas redes, é quase impossível fugir da personalização, uma vez que a configuração da sociedade hiperconectada envolve realizar até mesmo tarefas simples com algum dispositivo tecnológico conectado à rede. Além disso, mesmo com o uso de redes não rastreáveis. há o risco de os serviços não serem prestados adequadamente.

A predominância da economia de vigilância reivindica o domínio público dos dados que possuem valor de mercado, e entendendo que esse ativo parte das pessoas, dos usuários da rede, por que então não se discutem os direitos fundamentais envolvidos nessas operações? Para Pessoa (2020, p. 56), é essencial que a discussão da atual configuração social seja debatida sob o enfoque das garantias humanas e fundamentais:

> Numa sociedade em rede, por sua própria arquitetura informacional, o processamento de dados produzidos nos processos comunicativos torna-se o novo ouro do século XXI, de forma que, num Estado geral de vigilância, faz-se necessário analisar essa nova arquitetura social, sob o prisma dos direitos e garantias humanas e fundamentais dos indivíduos, especialmente do direito à privacidade.

A ausência de clareza sobre o tratamento de dados e coleta de informações pessoais gera minimamente uma desconfiança do usuário devido ao desconhecimento sobre os processamentos dos dados. Isso abala a confiança, mas ainda assim não faz com que usuários deixem de utilizar tecnologias de vigilância (MAGRANI, 2019).

Para Pariser (2012), há uma explicação bastante simples para esse dilema. Além do desconhecimento técnico sobre tecnologia digital de modo generalizado, a razão pela qual não se deixa de utilizar tecnologias de vigilância é a atenção limitada para o problema, pois, resumidamente, "somos ocupados" e normalmente "confiamos que, se todo mundo está fazendo a mesma coisa, não haverá problema". Essa confiança sem fundamento deixa espaço para a atuação cada vez mais ativa de tecnologias de vigilância, tanto na captação da informação quanto na economia de ação e influência; assim, redes aproveitam-se para modificar termos de privacidade e pouca atenção lhes é designada, até porque se todos estão aderindo, que mal há? (PARISER, 2012).

Do ponto de vista dos agentes da tecnologia de vigilância, o subterfúgio mais óbvio é o consentimento do usuário com suas políticas de privacidade. Criam-se termos documentados, extensas páginas com informações que a maioria dos usuários não parece compreender, e com sua aceitação, uma espécie de legitimação é formada entre as partes, com contratos de adesão sem margem para discussão ou modificação (PESSOA, 2020).

Julie Cohen (2019), entende que a técnica cria uma espécie de legitimação do consentimento dentro da rede, uma sublimação contratual do termo usual para um modelo em rede de adesão; por meio dessa forma de consentimento, os agentes das redes definem suas zonas de apropriação livre e produtiva. Assim, um conceito sobre consentimento em rede é modulado (COHEN, 2019):

> A concepção de consentimento que emerge dessa condição padrão não tem precedentes no direito dos contratos ou em qualquer outro corpo de direito. O consentimento para a extração de dados está sendo sublimado no ambiente codificado e, ao longo do caminho, está sendo efetivamente redefinido. No mercado em rede contemporâneo, o consentimento flui do status, não da conduta, e se vincula no momento da entrada no mercado. Nessas circunstâncias, a ênfase jurídica em coisas como divulgação, painéis de privacidade e competição por termos se torna uma forma de teatro Kabuki que distrai usuários e reguladores do que realmente está acontecendo (p. 69).

Nos estudos de Bruno Bioni (2019), se destaca o protagonismo do consentimento no contexto tecnológico e também normativo. O autor demonstra que em todas as gerações de leis que tentaram tutelar a proteção de dados, a figura do usuário e seu consentimento foram pontos centrais na determinação dos tratamentos de dados. O consentimento no contexto normativo é adjetivado e abordado quase como um sinônimo de autodeterminação informacional, destacando-se que a "proteção dos dados pessoais assinala, destarte, um percurso no qual o consentimento emerge, é questionado e se reafirma como sendo o seu vetor central" (BIONI, 2019, p. 173).

Entretanto, esse protagonismo do consentimento do usuário parte de algumas premissas no campo normativo que não se vislumbram da realidade, ou seja, um conceito de irredutível protagonismo do usuário que é confrontado com os poderes que o usuário possui para discutir ativamente frente ao controle de seus dados pessoais (BIONI, 2019, p. 188).

> O saldo desse percurso é apostar no indivíduo como um ser capaz, racional e hábil para controlar as suas informações pessoais. Temse, assim, um quadro regulatório encapsulado por uma compreensão reducionista do conteúdo a que se deve referir autodeterminação informacional que, passadas mais de duas décadas, não mais se ajusta ao contexto subjacente dos dados pessoais como ativo econômico em constante circulação (Capítulo 1) e que modula o livre desenvolvimento da personalidade dos cidadãos (Capítulo 2 supra).

A proposta de Bioni é uma rediscussão sobre o protagonismo do consentimento do usuário nos modelos regulatórios que parecem ignorar que, no campo fático, a atuação do usuário é resumida na aceitação ou não de um contrato de adesão nebuloso e formatado em rede. A realidade fática é de pouco conhecimento sobre tecnologias digitais e até mesmo interpretação de modo geral sobre direitos e garantias fundamentais por parte dos usuários, sendo seu papel de consentimento definidor da legitimidade não adequado sem que mecanismos tornem esse conhecimento acessível ou mais objetivo.

Como possível solução, Pariser (2012) defende que as opções precisam se tornar mais claras e objetivas, e alguma alfabetização algorítmica se faz necessária. Além disso, é

necessário haver a conscientização sobre valores como justiça, liberdade e privacidade, que precisam se tornar populares e acessíveis.

O paradigma que se forma é da privacidade confrontada às tecnologias de Internet das Coisas; os aspectos normativos demonstram pouco interesse em regulação tradicional e fiscalização nos ambientes de computação ubíqua, tendo esses mercados buscado se autorregular e evitar a atuação estatal. Contudo, essa autorregulação não demonstra efetividade em garantir que preceitos fundamentais da sociedade civil, como a privacidade, estejam bem resguardados, pois de modo geral, o capitalismo de vigilância se consolidou ainda mais com a realidade ubíqua e com a Internet das Coisas.

A conclusão é de que cada vez mais a sociedade estará sujeita às inspeções das redes sensoriais, principalmente quando projetadas para influenciar opções de consumo, apropriando-se de experiências pessoais e privadas com a mera percepção comportamental e de ambiência. Essas atividades geram externalidades à privacidade dos usuários de várias dimensões, fazendo-se necessária alguma forma de tutela jurídica sobre a privacidade no uso de Internet das Coisas, tanto do ponto de vista da regulação quanto da formação de mecanismos alternativos.

4 CONTEXTUALIZAÇÃO JURÍDICA DO DIREITO À PRIVACIDADE

4.1. O DIREITO DE ESTAR SÓ: SÍNTESE CONCEITUAL DA PRIVACIDADE

> "A man is entitled to be protected in the exclusive use and enjoyment of that which is exclusively his" – Lord Cottenham

O valor da solidão, do estar só ou de permanecer em paz com aquilo que é exclusivamente seu, sob a sombra que protege aquilo que não se deseja expor ou que não deve ser exposto, é simplesmente a sombra da privacidade tornando-se um valor a ser protegido pela sociedade moderna. As ramificações entre esferas púbicas e privadas modificaram-se acentuadamente com a formação da sociedade. Em seu estudo sobre a condição humana, Arendt (2007) descreve que a sociedade moderna aos poucos descobriu a riqueza por meio de atividades anteriormente reservadas à privatividade, e aos poucos as riquezas da comunidade, que antes eram em benefício de um bem comum, passam a ter mais valor social quando a comunidade se preocupa com suas riquezas individualmente.

Para Arendt (2007), a esfera privada tornou-se a única preocupação comum entre indivíduos, sendo propriamente a esfera social desde então; assim, a intimidade, então protegida pela esfera privada, fundiu-se com a esfera social e tomou novos contornos e sentidos de proteção para o homem. Isto ocorre porque, embora intimamente os indivíduos sempre estiveram cientes das características das atividades que eram próprias da vida privativa, não necessariamente buscava-se dar a devida proteção ao tema, uma vez que ainda não era um valor incutido e valorizado atualmente. Afinal, a vida pública e em comunidade era o objetivo maior do que os valores individuais, a exposição da intimidade à esfera social trouxe essa mudança (ARENDT, 2007).

Do ponto de vista histórico, na análise de Cancelier (2017, p. 41), as esferas pública e privada nasceram na antiguidade clássica, pois "havia a esfera da *pólis* e a esfera do *oikos*, sendo aquela comum aos cidadãos livres e está particularizada aos indivíduos". A vida pública era determinada pela posição do cidadão no *oikos*, isto é, a posição política e de sua família definiria se ocuparia um espaço na vida pública, e ao ingressar na esfera pública, o cidadão assumia uma vida política.

Intensificam-se, na Idade Média, hábitos de isolamento sob atividades que envolvem o corpo, o ato sexual e as necessidades fisiológicas, ainda sem um conceito próprio de individualidade, ou seja, poder tornar privado alguns hábitos da vida cotidiana aos poucos passaram a ser um "*status*" dos mais abastados (CANCELIER, 2017). Contudo, um conceito

de privacidade nasce como um valor da sociedade na ascensão da burguesia sobre o regime da sociedade feudal. Para Rodotà (2008), a possibilidade de isolar-se era um privilégio ainda restrito à classe burguesa, que de fato tinha a seu favor a propriedade para exercer o privilégio de isolar-se em "seu espaço".

Na síntese apresentada por Rodotà (2008, p. 27), o nascimento da privacidade não está atrelado a uma realização individual que ocorreu de forma natural, mas sim à "aquisição de um privilégio por parte de um grupo" que percebeu o proveito da própria intimidade e passou a exercê-lo, exigi-lo e apropriar-se de seu espaço de isolamento. Isso tudo de maneira não linear para com outras classes sociais, que caracteristicamente não atendiam ao âmago do privilégio exigido e da tutela para exigi-lo, a propriedade.

Assim, a estrutura jurídica de tutela da privacidade era então tratada nos moldes da proteção à propriedade, e sem aplicabilidade pela classe operária que não atenderia à questão central da propriedade (RODOTÀ, 2008). Na sociedade moderna, a privacidade passa a ser uma reivindicação de todas as classes, pois as possibilidades que a intimidade e a vida privada podem oferecer são conhecidas, e os questionamentos sob uma tutela geral para a privacidade surgem.

Propõe Rodotà (2008), para a compreensão da privacidade, que é necessário conhecer as funções culturais atribuídas a cada momento vivido e em cada grupo a fim de entender a proposta de privacidade então vivenciada, isto é, o conceito de privacidade traduz-se de diversas maneiras, a depender da cultura e do sentido a que se atribuiu. Embora já houvesse uma consciência humana sobre atos íntimos, que deveriam ser reservados da esfera pública, juridicamente, uma discussão sobre a tutela a respeito da privacidade só entrou em cena em 1890, em um artigo publicado por Samuel Warren e Louis Brandeis na Harvard Law Review.

A princípio, os autores constatam que a proteção do indivíduo por meio da proteção da propriedade era parte dos princípios da lei comum até então sedimentada como um princípio geral não tutelado (WARREN; BRANDEIS, 1890). Contudo, de tempos em tempos, a sociedade declina-se a acompanhar mudanças políticas, sociais e econômicas, que fazem valer o reconhecimento de novos direitos, o que produz uma passagem acerca dos direitos que devem ser tutelados com base nos valores e fatores relevantes a serem considerados. Dessa forma, em um primeiro momento, a sociedade protegeu direitos como a vida, para proteção física dos indivíduos, e a propriedade, como via de proteção do patrimônio (WARREN; BRANDEIS, 1890).

Para Warren e Brandeis (1890, p. 1), uma evolução no reconhecimento de direitos conduziu à confirmação de direitos espirituais do homem, ao intelecto e aos seus sentimentos, "o escopo desses direitos legais se ampliou; e agora o direito à vida passou a significar o direito

de gozar a vida, - o direito de ser deixado em paz;". Assim, a ampliação da gama de direitos protegidos pela sociedade e para o indivíduo, transcendendo ao direito à integridade física ou à propriedade, para direitos de cunho personalíssimo e que vão além do mínimo para sobreviver, traze à tona direitos que consideram o sentimento e as emoções humanas, tal como o "direito de ser deixado em paz", ou simplesmente à preservação da vida privada.

Essa mudança está justamente relacionada ao desfazimento de valores da comunidade para dar espaço a valores individuais que se acentuam durante a modernidade, especialmente após a emancipação das classes operárias e das mulheres, em que as revoluções reivindicaram também direitos de ordem individual (ARENDT, 2007).

Warren e Brandeis (1890) iniciam seu debate sobre a privacidade a partir da evolução dos meios de comunicação no século XX e como se cunhavam na exposição da vida privada de alguns indivíduos normalmente "famosos". O objetivo do debate era justamente questionar a legislação vigente à época acerca da existência de princípios de proteção da privacidade, qual a sua natureza e até onde protegiam o indivíduo. A crítica que se inicia sobre as então fofocas de revistas sobre celebridades e a pouca privacidade que lhes era resguardada serve de base para compreender a natureza do direito à privacidade naquele contexto histórico.

Sintetiza Mendes (2008) que o estudo de Warren e Brandeis é justificado pela busca de reconhecimento do direito à privacidade diante da vida moderna e complexa; valores como a sensibilidade humana à publicidade, a preservação de sua solidão e intimidade tornaram-se essenciais, e a intromissão na vida privada passa a ser repudiada.

Warren e Brandeis (1890) fazem então distinções importantes sobre o direito a não violação da vida privada, ou simplesmente de ser deixado em paz, não categorizando como um direito oriundo do direito à propriedade do indivíduo, mas como um direito à privacidade, e é esse o princípio que deve justificar a proteção extensiva da vida pessoal de violações. Para essa distinção, eles constroem a narrativa exemplificada por julgados e doutrinas que confrontam a existência de um princípio da privacidade na proteção pessoal e intelectual frente a um direito de propriedade.

O debate delimitava um direito de característica individualista e natureza negativa, partindo do princípio do direito de ser deixado só. De acordo com Mendes (2008), é um direito originalmente considerado burguês, devido à natureza de direito negativo, que consiste na abstenção do Estado em agir na seara privada do indivíduo. Para Doneda (2020, p. 32), o direito à privacidade originalmente foi inserido em um contexto jurídico patrimonialista, como debatido por Warren e Brandeis, mas destaca ainda que o perfil garantista à privacidade estava

voltado à preservação de direitos que só atendiam ao substrato individualista da sociedade, “uma prerrogativa reservada a extratos sociais bem determinados”.

Com a guinada do modelo de Estado liberal para um Estado de bem-estar social, junto aos movimentos que visavam maior garantia de direitos sociais, proporcionou-se uma conversão do direito à privacidade garantido a certos grupos sociais para um direito amplo e vinculado a garantias de personalidade e da realização pessoal (DONEDA, 2020).

Por sua vez, Cohen (2013, p. 1905) apresenta uma concepção de privacidade como um instituto dinâmico oriundo das políticas liberais, que pode modificar seus princípios de forma autônoma e ser exercido na forma de um direito abstrato dentro das liberdades individuais, isto é, “o eu liberal possui direitos abstratos de liberdade e capacidade de deliberação e escolha racionais e é capaz de exercer suas capacidades de maneiras não influenciadas pelo contexto cultural”.

Para a autora, tentar entender a privacidade somente baseando-se na sua essência para o indivíduo e em princípios fundamentais é insuficiente se comparada com a percepção real que cada indivíduo tem sobre o que é privacidade e qual o seu valor individual. Cohen (2013) defende que os conceitos sobre privacidade como uma construção consecutiva da cultura geral frustram a percepção de que a privacidade não tem uma condição fixa, que sua relação entre indivíduos, sociedade e culturas é dinâmica, e por isso é um valor abstrato de liberdade.

A definição de privacidade e os termos como vida privada e intimidade no campo jurídico passaram a ser utilizadas a partir do artigo publicado por Brandeis e Warren em 1890, sendo marco desses fundamentos a justificativa utilitarista de políticas de privacidade, além de um imaginário a visão utilitária da privacidade justificava o porquê de criar-se uma tutela legal como solução para conflitos morais (BRANCO, 2018).

Como sintetiza Doneda (2020), os fenômenos vinculados à privacidade não eram uma novidade para o direito, mas um tratamento específico para direitos com respaldo na privacidade era um novo cenário jurídico. Em um contexto mais atualizado, Doneda (2020) defende que a privacidade não deve mais ser tratada nos moldes aos quais foi compreendida e no que representou para a sociedade em outros momentos históricos; o fluxo de informações e tratamento de dados nas circunstâncias atuais exigem uma roupagem própria para um conceito atual de privacidade.

A noção de privacidade como o “direito de estar só”, baseado no que significou estar só em outrora, pode se revelar um conceito ultrapassado diante dos avanços tecnológicos do uso e compartilhamento de informações. Como defende Rodotà (2008), na sociedade da informação, definições genéricas sobre um “direito de ser deixado só” não corresponde especificamente com

os valores do momento vivido, pois o conceito geral sobre "estar só" ainda é intrínseco a um aspecto geral da privacidade, mas especificamente "tendem a prevalecer definições funcionais da privacidade que, de diversas formas, fazem referência à possibilidade de um sujeito conhecer, controlar, endereçar, interromper o fluxo das informações" sobre ele (RODOTÀ, 2008, p. 92).

Por essa inadequação de uma conclusão genérica, Rodotà (2008, p. 109) apresenta seu próprio conceito para a privacidade na sociedade da informação como o direito de poder controlar as próprias informações, como um poder negativo, sendo o "direito de manter o controle sobre as próprias informações e de determinar as modalidades de construção da própria esfera privada".

Esse breve apanhado histórico com considerações axiológicas constroem uma compreensão geral acerca da privacidade como um valor nascido na sociedade e que sofreu desdobramentos e transformações quanto à sua definição e natureza até a chegada de conceitos mais específicos que enfrentam a realidade da sociedade da informação. No campo do Direito, a privacidade tornou-se um importante instituto jurídico com base nas raízes até aqui estudadas e, consequentemente, gerou uma base para outros direitos do campo dos Direitos Fundamentais ao Direito Privado.

4.2 DIREITO À PRIVACIDADE COMO UM DIREITO FUNDAMENTAL

> "Em outras palavras, de forma bem direta: vivemos na era das escolhas de Sofia automatizadas. Independente do acerto ou desacerto dessas decisões automatizadas, é inequívoco que a proteção dos valores estruturante da nossa democracia constitucional requer que o Direito atribua elementos de transparência e controle que preservem o exercício da cidadania" – Gilmar Mendes (2020).

Apesar de comumente estudar-se a privacidade a partir do artigo *The right to privacy*, publicado por Warren e Brandeis em 1890, como um marco do reconhecimento da privacidade na esfera jurídica, foi Thomas Cooley, em 1879, que mencionou, em uma de suas decisões na Suprema Corte americana, o direito de ser deixado sozinho *the right to be let alone* (TAVARES, 2019). A proposta de direito mencionada por Cooley, contudo, era conceituada como uma limitação dos poderes do Estado e entes públicos perante o indivíduo na esfera privada, que ainda assim gerou repercussão suficiente até a chegada de um estudo mais elaborado como proposto por Warren e Brandeis (TAVARES, 2019).

A princípio, ao tratar de um direito à privacidade, Warren e Brandeis descreveram um direito de estar só, cunhado especialmente na proteção dos indivíduos na esfera privada de

sofrer exposições involuntárias de suas vidas íntimas, sendo uma tendência crescente na época, por meio da imprensa, a divulgação de questões íntimas (TAVARES, 2019). Para os autores, a exposição da vida privada de terceiros estava assumindo uma forma de barganha, pois a comercialização de intimidades de determinados indivíduos para vender mais manchetes era impulsionada pela chegada de tecnologias inovadoras na época, como câmeras, novos meios de comunicação e aparelhos tecnológicos (CANCELIER, 2017).

O avanço das tecnológicas de informação com maior capacidade de processamentos e novas finalidades foi importante para a construção de um marco legal sobre a privacidade. De acordo com Cancelier (2017), o desenvolvimento de tecnologias da informação, ampliando a circulação de informações, a coleta e o sensoriamento de dados, somado às mudanças sociais de esfera pública para privada e a acentuação do individualismo, promoveram a "democratização do interesse pela tutela da privacidade".

Aos poucos, a privacidade vai ganhando espaço nos ordenamentos jurídicos como gênero digno de proteção, cujos conceitos foram modulados conforme conceitos culturais sobre a vida privada, e que características merecem a tutela, demonstrando o caráter abstrato desse direito e sua aplicabilidade. Uma definição do direito à privacidade contemporâneo é necessária para lidar com os desafios experimentados na sociedade hiperconectada, pois como visto até aqui, assim como em outros momentos históricos, a sociedade vem conhecendo cada vez mais mecanismos tecnológicos cujas funcionalidades estão baseadas na coleta de informações.

Assim, os estudos sobre privacidade estão cada vez mais ligados à proteção de dados e informação (DONEDA, 2020). Isso ocorre porque os desdobramentos atuais da sociedade demandam atenção ao uso e controle de informações pessoais de forma correlata a um gênero mais abrangente de direitos, que é a privacidade. Por conseguinte, o reconhecimento do direito à privacidade no ordenamento jurídico é fundamental para o avanço da pesquisa sobre privacidade e a chegada a um acordo semântico acerca do conceito contemporâneo de privacidade.

4.2.1 Tutela jurídica da privacidade e a CRFB/1988

O direito à privacidade, em suas primeiras aparições jurídicas, confirmava que o gênero, de modo geral, aparentava um direito destinado somente a um substrato de indivíduos (DONEDA, 2020), especificamente sujeitos de notoriedade pública cujas vidas eram interessantes aos olhos da sociedade. Ou seja, eram os indivíduos que se importavam com ter alguma proteção quanto a sua vida.

A imagem de um direito “para poucos” surge do contexto fático de suas manifestações em seu surgimento. Como discorre Mendes (2014), os primeiros casos judiciais a debaterem o direito à privacidade foram especificamente de pessoas com notoriedade pública, como da atriz Elisa Rachel Félix na França, em 1858, que após seu falecimento, o Tribunal de Séné reconheceu o direito da família de impedir a publicação de imagens da atriz em seu mortuário (CANCELIER, 2017).

Como já observado, após a publicação, em 1890, de *The right to privacy* (BRANDEIS; WARREN, 1890), um conceito geral sobre vida privada passou a ser debatido. Ainda que não se possa considerar como texto definidor de um conceito, o artigo foi importante para criar característica sobre a privacidade e afastar as teorias tradicionais de um direito patrimonial, relacionando a privacidade à inviolabilidade da personalidade do indivíduo (MENDES, 2014).

Conforme Doneda (2020), a privacidade passou a ser uma preocupação da sociedade de modo geral com os avanços nas coletas de informações e a criação de bancos de dados, como o *National Data Center* na década de 1960, que chamava a atenção da sociedade aflita por não saber o que poderia estar sendo feito com suas informações. O resultado da tentativa de criação estatal de um banco de dados pelo governo americano foi uma conclusão de que poderia sim incorrer violação à privacidade dos indivíduos, mas o debate teve reflexos para a criação de outros institutos normativos, como *Fair Credit Reporting Act* de 1970, que visava justamente a criação de bancos de dados de consumidores, e *Privacy Act,* em 1974 (DONEDA, 2020).

Contudo, desde 1948, a privacidade já estava prevista em um texto normativo internacional, a Declaração Universal de Direitos Humanos, que prevê a inviolabilidade da vida privada do indivíduo, sua família, seu domicílio e sua correspondência (MENDES, 2014). Mendes (2014) pontua que o reconhecimento do direito à privacidade também foi seguido pelos outros institutos jurídicos internacionais, como a Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais, o Pacto Internacional de Direitos Civis e Políticos e a Convenção Americana sobre Direitos Humanos.

No contexto normativo nacional, Cancelier (2017) destaca a presença de um direito à inviolabilidade do domicílio desde a Constituição de 1824, ou em sentido literal, “todo o Cidadão tem em sua casa um asylo inviolavel. De noite não se poderá entrar nella, senão por seu consentimento, ou para o defender de incendio, ou inundação; e de dia só será franqueada a sua entrada nos casos, e pela maneira, que a Lei determinar” (BRASIL, 1824).

Denota-se que a inviolabilidade ao domicílio e à correspondência está presente em todas as Constituições seguintes no Brasil e serve de contexto histórico sobre a evolução do direito à privacidade neste âmbito como um direito originalmente compreendido como propriedade

(DONEDA, 2020). Contudo, a comparação de um direito à privacidade com origem na propriedade serve somente como fundamento de estudo histórico, pois como estudado, há uma ruptura entre a fundamentação do direito baseado na propriedade e o efetivo reconhecimento de um direito à privacidade ou de estar só (DONEDA, 2020).

No direito brasileiro, a Constituição Federal de 1988 ocupou-se de tutelar "a intimidade, a vida privada, a honra e a imagem das pessoas" no inciso X do artigo 5º, grifando com inviolabilidade desses direitos uma limitação à "liberdade de comunicação", prevista expressamente no art. 220 da CRFB/1988, de acordo com Mendes e Branco (2017). De modo geral, Mendes e Branco (2017) fazem pouca distinção entre as terminologias de "vida privada" e "intimidade", mas analisam que algumas correntes jurídicas defendem a intimidade como parte do direito à privacidade, ou seja, a privacidade seria um direito mais amplo. Em toda relação que envolva uma questão de direito à intimidade, está presente uma questão de privacidade, mas em nem toda questão de privacidade está presente um direito à intimidade.

Essa definição é defendida por Bulos (2014, p. 571), que ressalva que, embora haja uma distinção tênue entre os dois conceitos, "amiúde, a ideia de vida privada é mais ampla do que a de intimidade". Nessa concepção, a intimidade está ligada à princípios muito pessoais do indivíduo, enquanto a vida privada diz respeito a todas as relações sociais do indivíduo. Em sintetização, cita-se a definição de Cancelier (2017, p. 78) para essas propostas de diferenciação entre as terminologias:

> Algo secreto, sigiloso ou íntimo pode ser relacionado ao mesmo aspecto que se deseja manter em segredo. O privado pode ser íntimo, o íntimo pode ser secreto, o secreto pode ser privado. Ao mesmo tempo, cada um deles poderá assumir – de forma bastante subjetiva – a depender do sujeito da fala, um significado específico. Assim, nem sempre o íntimo será secreto ou o assunto sigiloso será privado. O que se quer dizer é que o significado do discurso irá variar conforme quem o profere, possibilitando cada um dos termos aqui apresentados usos variados.

Desse modo, a privacidade deve protagonizar uma necessidade humana, intrínseca ao sujeito e sua essência (CANCELIER, 2017), abrangendo outras demandas, como a intimidade, e como descreve Doneda (2020), é também um aspecto derivado da dignidade da pessoa humana. Como uma tutela da pessoa, a privacidade pode abranger tanto uma finalidade protetiva à informação fornecida ou recebida, quanto seguir sendo medida de proteção de questões em que o objeto central é a privacidade ou não, ampliando o campo de atuação dessa tutela protetiva (DONEDA, 2020).

Não obstante as definições distintivas entre a vida privada, a intimidade e seus derivados, para a presente pesquisa, basta a compreensão de que o direito à privacidade abrange

a proteção à vida íntima, privada e das informações do indivíduo, optando-se simplesmente pelo uso da terminologia "privacidade". Assim, a partir da Constituição Federal de 1988, a privacidade surge como um Direito Fundamental no cenário jurídico brasileiro, e por conseguinte, reflete na previsão do direito estampado no Código Civil de 2002 com o direito à inviolabilidade da vida privada (BRASIL, 2002).

No direito privado, a tutela da privacidade lhe garantiu espaço como um direito de personalidade descrito no artigo 21 da Lei nº 10.406/2002, e nesse sentido, cabe brevemente a conceituação desse gênero. Tartuce (2018, p. 188) afirma que os direitos de personalidade têm por objeto de proteção os atributos inerentes à pessoa e à sua dignidade; seguindo o fundamento constitucional, a tutela dos direitos de personalidade visa o "modo de ser, físicos ou morais do indivíduo".

Em outra análise, Tepedino *et al.* (2013) pontua que a previsão dos direitos de personalidade no Código Civil ratifica garantias já consolidadas no texto constituição mediante direitos individuais abordados de maneira subjetiva, e em que a dignidade da pessoa humana é reiterada como prioridade do ordenamento jurídico. Em geral, observa-se que o direito à privacidade passou por uma ruptura conceitual, desvinculando-se do conceito de direito oriundo da propriedade e criando natureza jurídica própria a partir das atribuições de garantir a dignidade da pessoa humana no tocante a preservar aquilo que o indivíduo preza como íntimo e privado.

Todavia, a conceituação tradicional sobre a privacidade passa por transformações, pois como aponta Stefano Rodotà (2008), a noção de um direito meramente fundado em poder "estar só" serve de pano de fundo genérico para um novo conceito necessário sobre o direito à privacidade. Atualmente, interessa ao titular do direito, além do direito de isolar-se ou preservar sua vida íntima, o poder de controlar suas informações pessoais, mudança oriunda dos avanços tecnológicos e também das mudanças na esfera privada de modo geral (RODOTÀ, 2008).

Como exemplo, pode-se citar o voto do Ministro Gilmar Mendes em sessão do Supremo Tribunal Federal, que julgou a Ação Direta de Inconstitucionalidade nº 6.387. A ação proposta visava barrar os efeitos da Medida Provisória nº 954/2020, que resumidamente obrigava que operadoras telefônicas fornecessem dados pessoais de todos os titulares no prazo de sete dias a partir da publicação do ato (BRASIL, 2020). Dentre os pontos que merecem destaque no voto, é o reconhecimento pleno e justificado de que o conceito tradicional utilizado para interpretação jurídica da privacidade passou por uma reconfiguração para a afirmação garantidora de outros direitos, como a autodeterminação informacional e a proteção de dados (BRASIL, 2020).

O Ministro é enfático ao reforçar a autodeterminação informacional e o controle da informação pelo indivíduo propriamente dito como a regra e não a exceção na garantia de direitos aos quais está implicitamente vinculada como a privacidade (BRASIL, 2020). Assim como defende Cohen (2013), o dinamismo do direito à privacidade necessita de uma interpretação pós-liberal, que considere além do individualismo acentuado pelo liberalismo, as questões inerentes à autodeterminação da informação como um aspecto inerente à formação da subjetividade do indivíduo.

O direito à privacidade passa por mudanças ensejadas pelo contexto dinâmico das tecnologias e do formato social, mas também pelo reconhecimento de outras necessidades à personalidade do indivíduo, como o controle de suas informações e um papel atuante. Para além de uma garantia de natureza negativa quanto à atuação de terceiros sobre a esfera privada, o debate traz à tona a formação conceitual de uma privacidade garantidora de atuação por meio do conhecimento e controle das informações pessoais.

4.2.2 Direito Fundamental à Proteção de Dados e Informação

A metamorfose que sucede o direito à privacidade evolui para adequar-se às transformações sociais e à tecnologia, sendo uma questão correlata a outra. De acordo com Mendes (2014), o nascimento da disciplina de proteção de dados pessoais deriva da transformação do direito à privacidade, que enseja uma tutela especifica sobre o tratamento de informações.

O resultado é a proteção da privacidade com agregados, por assim dizer, os ordenamentos jurídicos em diversos países estão sendo adaptados para envolver à privacidade os desdobramentos de proteção sobre dados, por entender que “constituem uma projeção da personalidade do indivíduo, merecendo inclusive tutela constitucional” (MENDES, 2014, p. 11). Historicamente, a postulação de um direito à proteção de dados foi originalmente construída em 1970 com a Lei de Hesse na Alemanha, sendo o primeiro texto normativo acerca do tema (DONEDA, 2020).

De acordo com Doneda (2020), a preocupação com uma legislação para tutelar a proteção de dados ganhou espaço quando o processamento de dados passou a ser um risco para o indivíduo; assim, a proteção de dados é proveniente da tutela da privacidade e do fortalecimento de direitos individuais.

Os riscos da sociedade da informação sobre o tratamento de dados ensejam que os indivíduos cada vez mais se preocupem com quem está obtendo acesso às suas informações, o

que está sendo feito e quais direitos podem ser acionados se houver algum prejuízo. O conceito informacional faz parte do desdobramento contemporâneo da privacidade, em que a informação pessoal também é objeto da tutela da privacidade, não como um direito negativo do qual pode se exigir inércia de terceiros, mas um direito positivo do qual pode o indivíduo exigir o controle de suas informações.

Cabe conceituar que, ao se falar de proteção de dados e informação, uma distinção categórica entre os institutos deve estar em mente, visto que os dados e a informação estão em momentos diferentes na cadeia produtiva informacional, o "dado, assim, estaria associado a uma espécie de "pré-informação" anterior à interpretação e a um processo de elaboração", enquanto "informação" já "pressupõe a depuração de seu conteúdo – daí que a informação carrega em si também um sentido instrumental, no sentido da redução de um estado de incerteza" (DONEDA, 2020, p. 139).

Neste estudo, analisa-se o direito de proteção de dados e a informação, fazendo-se a distinção entre os institutos, porém considerando que a doutrina costuma tratar essas terminologias sem distinções como o direito à proteção de dados (DONEDA, 2020). A tutela sobre a informação já existia em alguns institutos normativos com conceitos diversos do que representa na proteção da privacidade. Nessa seara, importa a informação referente ao indivíduo, suas características e seus comportamentos, como, por exemplo, nome civil, endereço, padrões comportamentais e histórico de compras, que são informações com relevância para proteção dos dados de privacidade (DONEDA, 2020).

No entanto, além de um direito ramificado em outro direito – a privacidade – o direito à proteção de dados possui status simultâneo como um direito humano e um direito fundamental, salientando-se que esses dois gêneros jurídicos não são a mesma coisa (SARLET, 2021). Como ensina Sarlet (2021), resumidamente, um direito humano deve estar positivado em algum texto normativo dos tratados internacionais, fazendo universalmente sujeitos de direito todas as pessoas em todos os lugares, enquanto um direito fundamental é aquele contido no texto constitucional, podendo ser um direito humano ou não.

No tocante ao direito à proteção de dados, destaca-se que sua tutela no âmbito de direitos humanos tem sido defendida como um direito derivado do direito à privacidade expressamente contido nos tratados e nas convenções internacionais, ganhando força de proteção como um dos direitos humanos universais (SARLET, 2021). O reconhecimento da proteção de dados como um direito fundamental, por sua vez, pode ocorrer de forma expressa pela positivação na carta constitucional, ou de maneira implícita, como um direito "deduzido interpretativamente" a partir de outros direitos (SARLET, 2021).

No campo dos direitos fundamentais, essa interpretação depende da classificação material e formal do direito pretendido para com o regime jurídico constitucional. Do ponto de vista formal, “um direito é tido como fundamental de acordo com o nível de robustez das garantias estabelecidas pelo constituinte”, isto é, o regime jurídico-constitucional pré-existente determinará se o direito pretendido corresponde à posição jurídica adotada (SARLET in DONEDA, 2021, p. 66).

Do ponto de vista material, o direito pretendido possui “relevância do conteúdo das posições subjetivas atribuídas pela ordem jurídica a determinado sujeito de direitos”, servindo como derivação de outros princípios e direitos fundamentais já protegidos constitucionalmente (SARLET in DONEDA, 2021, p. 66). Fazendo-se essa interpretação do regime jurídico-constitucional brasileiro, Sarlet (2021) considera que o direito à proteção de dados formalmente é abarcado pela hierarquia normativa constitucional, assim como materialmente é englobado por princípios e direitos fundamentais celebrados na Constituição Federal, fazendo deste um direito fundamental em nosso ordenamento jurídico.

Desse modo, o Supremo Tribunal Federal fundamentou, em diversas decisões, até o efetivo reconhecimento da proteção de dados como um direito fundamental a partir do julgamento da ADI 6.387 (BRASIL, 2020). Tão logo filia-se ao entendimento apresentado por Mendes (2014), o direito a proteção de dados é garantido constitucionalmente, derivando do direito à privacidade, com ação dúbia de caráter negativo, como garantia de não atuação do Estado contra a proteção de dados e como garantia positiva do direito à proteção e ao controle dos dados pelo indivíduo.

Antes de um reconhecimento ao direito à proteção de dados como direito fundamental, como observou o Ministro Gilmar Mendes em seu voto na ADI 6.387, já se ensaiava a garantia plena de um direito desta natureza mediante outros institutos infraconstitucionais, como no Código de Defesa do Consumidor, na Lei do Cadastro Positivo, no Marco Civil da Internet e, por fim, na promulgação da Lei Geral de Proteção de Dados (BRASIL, 2020). No tocante às vulnerabilidades já apontadas, algumas considerações jurídicas do âmbito infraconstitucional já buscavam de certa maneira proteger os sujeitos de direito no direito privado, como se demonstra adiante.

4.3 PRIVACIDADE CONECTADA: DO CÓDIGO DE DEFESA DO CONSUMIDOR À LGPD

A expansão do universo digital nas relações privadas, consequentemente, impactou as atividades de consumo. Os produtos inteligentes capazes de tornar a vida do consumidor mais fácil com IoT são, por um lado, atraentes aos olhos de quem busca automação de tarefas cotidianas e a incessante busca de ganho de tempo, mas por outro lado, trazem consigo desafios quanto à segurança das informações de seus usuários e consumidores.

De acordo com Magrani (2018), o avanço das tecnologias, sobretudo o ritmo acelerado de crescimento no uso da IoT, impacta profundamente as relações entre "consumidores, máquinas e empresas" sem que haja efetiva garantia de segurança da privacidade do consumidor por parte das empresas, no mesmo ritmo em que cria novos dispositivos IoT. Contudo, antes de adentrar em uma possível aplicabilidade em defesa do consumidor da IoT, é necessário realizar uma análise das normas infraconstitucionais, na qual nota-se a proteção da privacidade do consumidor antes mesmo de uma análise de reconhecimento como direito fundamental.

No Código de Defesa do Consumidor, a privacidade é tutelada na forma do direito à informação sobre dados inseridos em bancos cadastrais previsto no art. 43, sendo a criação de bancos de dados autorizada pelo art. 6º (MIRAGEM, 2016), sendo preditivo uma interpretação do direito à informação como controle da informação inerente à privacidade.

Em 2018, foi sancionada a Lei nº 13.709, passando a regulamentar as políticas de proteção de dados pessoais, em vigor desde agosto de 2020, conhecida como Lei Geral de Proteção de Dados, é o marco regulatório de direitos individuais dos usuários em relação a seus dados pessoais e de obrigações civis daqueles que operam as ferramentas digitais de armazenamento de dados (BRASIL, 2018). Assim, aos poucos, avançou-se para uma proteção de direitos, inclusive do direito à privacidade do usuário enquanto consumidor, tutela que merece maiores considerações para se alcançar uma aplicabilidade sobre as tecnologias IoT e seus consumidores.

4.3.1 Direito à privacidade e as normas infraconstitucionais

No âmbito jurídico brasileiro, o Código de Defesa do Consumidor, promulgado na forma da Lei nº 8.078/1990, é o ordenamento jurídico que respalda os princípios das relações de consumo, dos direitos e das garantias para proteção do consumidor (BRASIL, 1990). Localiza-se o direito à privacidade em relação ao consumidor, primeiramente, no tratamento dado à criação de bancos de dados com informações do consumidor, especialmente a inscrição

negativa como mau pagador, já que o artigo 43 é autorizador dessa prática, desde que respeitados os limites impostos previstos no artigo 4º do referido *Códex* (CARVALHO, 2018).

Dispõe o artigo 43 do CDC que o consumidor terá absoluto direito de acesso às informações sobre si, em cadastros, fichas, registros e dados pessoais. Dessa forma, há autorização legal para a criação de bancos de dados de proteção ao crédito, e uma vez respeitados os limites legais, haverá somente exercício regular do direito (BENJAMIN *et al.* 2021). A criação de cadastros e bancos de dados sobre o consumidor recebeu permissão legal no CDC, a fim de permitir a criação de vínculo histórico entre consumidor e fornecedor de crédito, de modo que haja maior segurança na liberação de crédito aos consumidores, reforçando o valor que a concessão de crédito representa ao sistema econômico (BENJAMIN *et al.* 2021).

Contudo, como lecionam Benjamin, Marques e Bessa (2021), a previsão contida no artigo 43 é resultado de uma ponderação de valores, como a privacidade, honra, informação e crédito, frente ao princípio da proporcionalidade, criando-se uma exceção que permite a coleta, o armazenamento e a divulgação de informações pessoais. Logicamente, a permissão é limitada em respeito à proteção aos direitos de personalidade, não sendo permitida a violação à honra e à privacidade do consumidor, que se consubstancia nos direitos previstos no art. 4 do CDC (BENJAMIN *et al.* 2021).

Em outro aspecto ao direito à privacidade contido no Código de Defesa do Consumidor, Miragem (2016) aponta as questões acerca do controle da informação pelo consumidor como direito inerente à privacidade, isto é, se há consentimento e ciência do consumidor sobre a colheita de suas informações e sobre sua concordância no uso dessas informações pelo fornecedor de serviços. Nesse sentido, destaca-se Miragem (2016, p. 347):

> E a questão, justamente, é saber em que medida o acesso, coleta e transmissão destas informações constituem ou não uma interferência na privacidade do consumidor. Ou de outro modo, se existiriam dados específicos que só pertencem ao espaço protegido pela privacidade do indivíduo, ou está se trata de um conceito flexível, moldando seus limites de acordo com o caso concreto.

Embora haja autorização legal como a prevista no art. 43 do CDC, a autonomia do indivíduo garantirá seu direito à autonomia da vida privada, e por assim dizer, sua autodeterminação individual (MIRAGEM, 2016), de forma que a permissão legal para coleta de dados do consumidor está limitada também pela autodeterminação do indivíduo sobre suas informações.

Além do CDC, outros institutos normativos buscaram proteger, de certa maneira, os dados inerentes ao direito de personalidade do consumidor, como a Lei de Cadastro Positivo sob Lei nº 12.527/2011 (BRASIL, 2011), uma normativa composta de conceitos protetivos como "dados sensíveis e outros, bem como de alguns dos princípios mais importantes de proteção de dados, entre os quais os da finalidade, transparência, minimização e segurança" (DONEDA, 2021, p. 43).

Em 2009, deu-se início ao debate para um Marco Civil da Internet, mediante um processo pela plataforma digital com a possibilidade de participação direta de usuários da internet na construção de um texto base a ser utilizado na confecção do Projeto de Lei que se tornaria a Lei nº 12.965/2014, conhecida como Marco Civil da Internet (MAGRANI, 2014), que estabeleceu um regime geral de direitos sobre usuários sem a aspiração de preencher uma lacuna por uma legislação específica sobre a proteção de dados. Como explica Doneda (2021), a Lei nº 12.965/2014 sinalizava. em seu artigo 3º, III, a proteção de dados como um de seus princípios a ser considerado na forma de uma lei própria, ensejando que em dado momento a positivação à proteção de dados especificamente era necessária.

O anseio por uma regulamentação geral sobre proteção de dados tornou-se frequente com menção em dispositivos normativos, sendo a demanda por uma tutela protetiva acentuada com os avanços tecnológicos; por conseguinte, dando origem aos debates para a criação de um texto base para a lei de proteção de dados. A proteção da privacidade do consumidor na sociedade da informação enseja uma concepção específica aos riscos dos novos consumos; porém, como destaca Magrani (2018), ainda não há uma legislação específica sobre algumas tecnologias como Internet das Coisas ou Inteligência Artificial que resguardem especificamente o direito à privacidade dos consumidores.

Na ausência de uma norma própria, é necessário analisar a aplicabilidade de outros diplomas legais, como o Código de Defesa do Consumidor e q Lei Geral de Proteção de Dados, quanto à relação entre consumidor e a Internet das Coisas (MAGRANI, 2018). Por questão de ordem, analisar-se-á, primeiramente, a possível aplicabilidade da Lei nº 8.078/1990, o Código de Defesa do Consumidor, na proteção do direito à privacidade do consumidor e outros direitos, sendo posteriormente abordada a Lei Geral de Proteção de Dados e sua aplicabilidade.

4.3.1.1. A especificidade da lei consumerista aplicada à Internet das Coisas

Considerando-se a inexistência de um regulamento específico de proteção do consumidor usuário de dispositivos com tecnologia da Internet das Coisas, Eduardo Magrani

(2018) propõe uma extensão de direitos do Código de Defesa do Consumidor, considerando a especificidade do tema em uma interpretação extensiva da Lei nº 8.078/1990 em relação à IoT. Ao pensar em uma interpretação extensiva, devemos ter em mente que nem toda norma aplicada no CDC sobre produtos e serviços comuns terá a mesma efetividade sobre a Internet das Coisas.

Como exemplo, Miragem (2021) cita o artigo 8º do CDC, que prevê precisamente que produtos e serviços não podem ser colocados em mercado se oferecem risco à segurança dos consumidores, impõe a obrigatoriedade de os fornecedores informarem sobre os riscos, bem como questiona "todos os riscos destas novas tecnologias serão normais e previsíveis?". Por isso, Magrani (2018) propõe que a interpretação do CDC, nesse caso, diferencie "riscos "inerentes" daqueles completamente inesperados", evitando criar impedimentos à inovação, que também não é o propósito da normativa.

Ao tratar de problemas de privacidade do consumidor, como a publicidade direcionada de forma abusiva ou predatória, do ponto de vista jurídico, o CDC possui como remédio o artigo 6º, IV, que prevê o direito básico à proteção do consumidor contra publicidade enganosa e abusiva, e o artigo 39, III, que veda o envio sem solicitação de qualquer produto ou serviço (MAGRANI, 2018).

Uma visão preliminar da aplicação desses institutos, simplesmente para coibir a atividade abusiva dos criadores de dispositivos IoT ou da criação de perfis com as informações captadas por esses dispositivos, parece um método desanimador se não consideradas as especificidades na relação entre o consumidor, a máquina e os dados. Devemos imaginar, em um caso concreto, a aplicabilidade das normas dentro de uma realidade processual. Por exemplo, como poderia o consumidor fazer valer tais direitos em uma cadeia probatória ao tentar comprovar que seu relógio de pulso com Internet das Coisas tem armazenado informações sobre seus horários para refeições e, coincidentemente, diariamente, uma notificação de um aplicativo de *delivery* lhe oferece um cupom de descontos?

Certamente o relógio de pulso não foi adquirido para armazenar suas informações alimentares, não mais do que o consumidor pretendia registrar somente para si, sem expor para terceiros ou para uma Inteligência Artificial. Mas, do termo "coincidência" até uma efetiva "prova" dentro da cadeia processual, há um longo caminho a ser percorrido, e notoriamente o consumidor nem sempre é conhecedor de mecanismos legais para tomar conhecimento sobre as atividades que seu dispositivo faz além do pretendido.

Porém, voltando-se à interpretação de Magrani (2018), a continuidade de seu raciocínio demonstra a previsão de uma considerável redução da privacidade e segurança dos usuários para garantir a continuidade da inovação tecnológica. Conclui sua análise da seguinte maneira:

> determinados aspectos e cenários ligados ao desenvolvimento tecnológico devem ser deixados em aberto para que haja espaço para a inovação. Porém há casos, conforme exploraremos a seguir, em que a lei deve ter aplicabilidade para fins de coibir abusos e reparar danos ao consumidor (MAGRANI, 2018, p. 27

Nesse aspecto, filia-se à ponderação de Miragem (2016) a mera aplicação do CDC pode não garantir essa proteção, sobretudo pelo desconhecimento dos consumidores acerca das inúmeras transações que podem ser feitas com suas informações entre sistemas, máquinas e empresas, sobre a complexidade na utilização de seus dados e simplesmente por desconhecer da possibilidade de uso das suas informações. Uma normativa própria sobre a Internet das Coisas pode prever mais detalhadamente as nuances dessa tecnologia na garantia de direitos dos consumidores, é o que defende Magrani (2018).

Em outro aspecto, Doneda (2020) também defende uma interpretação expansiva do Código de Defesa do Consumidor na identificação de princípios em comum que possam efetivamente proteger o consumidor. A título de exemplo, cita o princípio da finalidade "por intermédio da aplicação da cláusula da boa-fé objetiva e da própria garantia constitucional da privacidade, pelo qual os dados fornecidos pelo consumidor deverão ser utilizados somente para os fins que motivaram a sua coleta", o que pode ser uma medida de vedação da coleta de dados sensíveis e comercialização de bancos de dados (DONEDA, 2020, p. 271).

Porém, Doneda (2020) aponta que mesmo esta tutela é de certa forma limitada, tanto em sua incidência sobre essas tecnologias, como em suas disposições. De modo geral, entende-se que o Código de Defesa do Consumidor pode contribuir com princípios gerais que devem ser protegidos para o consumidor. Mendes (2008), por sua vez, também defende que os princípios fundamentais do Código de Defesa do Consumidor devem assumir papel norteador na proteção de dados do consumidor, tanto reconhecimento da vulnerabilidade do consumidor de maneira técnica por possuir menos informações que o fornecedor, como fática por possuir menos recursos intelectuais e econômicos de acesso à proteção de dados.

Para Mendes (2008), o Código de Defesa do Consumidor permite uma interpretação na proteção de dados que considere o consumidor como sujeito de direitos e não somente considere as relações de mercado, uma tutela da personalidade do consumidor. Além disso, ele apresenta como solução à problemática do acesso aos dados pelo usuário consumidor, a impetração de *habeas data*, o instituto jurídico garantidor do acesso a toda informação de caráter público, considerando-se que os cadastros e bancos de dados do consumidor devem ser públicos.

Ainda assim, a autora considera que além de uma norma própria, a complexidade de proteção ao consumidor nesse âmbito enseja "uma ampla e variada estrutura jurídica e administrativa", que "é capaz de oferecer os mecanismos necessários para fazer valer os direitos fundamentais do cidadão à privacidade, liberdade e igualdade" (MENDES, 2008, p. 43).

Tão logo pode-se concluir que, ao figurar uma relação de consumo, ainda que entre pessoa, máquina e computador, o Código de Defesa do Consumidor pode ser um norteador de princípios e direitos garantidos na proteção do consumidor, pois de modo geral a norma pode ser utilizada na proteção do direito à privacidade do consumidor. Porém, em respeito à complexidade das relações entre usuário e Internet das Coisas, ou simplesmente usuário e tecnologia informacional, o Código de Defesa do Consumidor não será suficiente para garantir amplamente a privacidade do usuário consumidor. Compete, ainda, analisar a Lei Geral de Proteção de Dados e sua possível aplicabilidade como tutela de proteção do direito à privacidade no uso da Internet das Coisas.

4.3.2 Direito à Privacidade na Lei Geral de Proteção de Dados e aplicabilidade à Internet das Coisas

Como acompanhou-se até aqui, a evolução normativa acerca da tutela protetiva da privacidade que caminhou até a criação de uma lei específica para a proteção de dados no Brasil é ainda muito recente, sendo objetivamente a Lei nº 13.709/2018, cuja necessidade já era anunciada em outros textos normativos que a antecederam, como no Marco Civil da Internet (DONEDA, 2021).

A LGPD não se limitou a repetir princípios já previstos no ordenamento jurídico, ela trouxe na verdade novos elementos de proteção, institutos próprios e princípios específicos de direitos aos usuários, a figura de um agente regulador e uma previsão de responsabilidade civil própria (DONEDA, 2021). O direito à privacidade foi elencado pela LGPD como um dos fundamentos contidos no artigo 2º da lei, sendo especificamente:

> I. o respeito à privacidade; II. a autodeterminação informativa; III. a liberdade de expressão, de informação, de comunicação e de opinião; IV. a inviolabilidade da intimidade, da honra e da imagem; V. o desenvolvimento econômico e tecnológico e a inovação; VI. a livre iniciativa, a livre concorrência e a defesa do consumidor; VII. os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Como destaca Miragem (2019), o direito à privacidade é uma das justificativas de proteção dos dados pessoais. Ademais, ele defende que além de uma expectativa objetiva de proteção de suas informações, de maneira subjetiva por meio da proteção de dados, o usuário exerce a tutela da privacidade pela esfera do consentimento e da autodeterminação da informação.

De acordo com Doneda (2020, p. 270), um regime de reconhecimento da proteção de dados pessoais destaca de modo geral a defesa dos direitos de personalidade, não se limitando somente à tutela da privacidade, de modo que "a proteção de dados pessoais é uma garantia de caráter instrumental, derivada da tutela da privacidade, porém, não limitada por esta". Na verdade, o que se percebe é uma "ambivalência" na utilização do direito à privacidade e à proteção de dados como uma continuidade histórica de direitos postulados até a chegada da LGPD (DONEDA, 2021). Por essa razão, a maioria dos temas relacionados à proteção de dados no Brasil envolvem de alguma maneira uma ramificação da privacidade.

O direito à privacidade, como fundamento da LGPD (art. 2º, I), traz duas perspectivas de atuação como mecanismo garantidor de direitos individuais: primeiramente, como uma liberdade negativa do titular em poder exigir uma atuação inibitória sobre o tratamento de dados que não concorde; e em segundo, como uma liberdade positiva de ter o controle sobre seus próprios dados (QUEIROZ, 2021).

Além do direito à privacidade, merecem atenção os demais fundamentos da LGPD, como a autodeterminação informativa (art. 2º, II), que se trata do "direito de cada indivíduo poder controlar e determinar", do acesso e do uso de seus dados pessoais (DONEDA *et al.* 2021, p. 64). A liberdade de expressão de informação, comunicação e opinião (art. 2º, III) como um limitador ou contrapeso em relação ao direito à privacidade (DONEDA, 2020) é também uma extensão de direitos fundamentais também estabelecidos na Constituição Federal de 1988 (PINHEIRO, 2018).

Como um segmento do direito à privacidade, positivou-se o direito à inviolabilidade da vida intimidade, honra e imagem como direito do titular de se opor à exposição de sua privada, "excluindo da informação alheia os fatos e os dados pertinentes a si próprio" (QUEIROZ, 2021, p. 45). Dispõe ainda, como fundamento, o desenvolvimento econômico, tecnológico e à inovação (art. 2º, IV), que reafirma um compromisso em não impedir o desenvolvimento econômico desse setor, mas implementar uma metodologia de atuação para um ambiente com segurança jurídica acerca da proteção de dados (QUEIROZ, 2021).

Notadamente, há outros fundamentos na Lei Geral de Proteção de Dados, como exposto, todavia, busca-se dar atenção aos fundamentos que, intrinsecamente, tratam do direito à

privacidade ou servem como contrapeso a esse direito. Ainda assim, a Lei Geral de Proteção de Dados traz à tona terminologias e previsões mais específicas em relação às tecnologias digitais e ao uso de dados, como a própria definição de "dados pessoais", contida no art. 5º, I, e as demais terminologias dos incisos seguintes, até então ausentes no ordenamento jurídico (BRASIL, 2018).

Dentre os princípios contidos no artigo 6º da Lei nº 13.709/2018, destaca-se a finalidade, que exige que o controlador informe ao titular sobre qual a finalidade do tratamento a qual os dados estarão vinculados (MIRAGEM, 2018). De acordo com Miragem (2018), a finalidade é requisito do consentimento, sendo que, ao consentir com o tratamento de dados, o titular está concordando com a específica finalidade então apresentada. Em derivação a esse consentimento, surge a figura da autodeterminação informativa, que pressupõe um controle dos dados pelo titular da informação, que consciente da coleta e do uso dos dados, poderá consentir ou não com a continuidade do tratamento (MIRAGEM, 2018).

Para Bioni (2019), o consentimento na Lei Geral de Proteção de Dados coloca o titular como protagonista da proteção de seus dados, sendo esse princípio o "vetor central" da legislatura e quase um sinônimo de autodeterminação informativa. Esses institutos jurídicos abordados na LGPD preceituam a proteção do indivíduo quanto ao tratamento de dados no uso das diversas tecnologias atuais, não somente ao direito à privacidade, embora esse seja o objeto central desta pesquisa.

Cabe elucidar que, de modo geral, a Lei Geral de Proteção de Dados ocupou-se de tutelar, além do direito à privacidade, mais de uma espécie dos direitos de personalidade. Partindo dessa constatação, Bioni (2019) defende ser incoerente analisar essa norma somente sob a ótica de uma garantia de proteção à privacidade, considerando que a LGPD vai além de uma proteção da privacidade, e classifica como uma categoria própria como "um novo direito da personalidade".

O contexto histórico normativo acerca da privacidade e da proteção de dados encaminhou a criação de uma normativa específica sobre proteção de dados, que é a LGPD. Todavia, no tocante à proteção de usuários de algumas tecnologias ainda mais específicas como a Internet das Coisas, é ainda questionável a amplitude de sua aplicabilidade como garantidora de direitos e especialmente, da privacidade. Como observado até aqui, a Lei Geral de Proteção de Dados traz em seu bojo a tutela de mais de um direito de personalidade, e dentre eles, a privacidade. Como defendido por alguns juristas, como Miragem (2018), é a privacidade a própria justificativa para uma lei de proteção de dados.

Do ponto de vista normativo, a LGPD eleva a discussão sobre a proteção do consumidor acerca da privacidade, da liberdade e de outros direitos fundamentais. Como destaca o autor, a LGPD não anula as tutelas protetivas já conquistadas pelo Código de Defesa do Consumidor, sendo um mecanismo que deve ser adotado para "assegurar a efetividade de direitos do consumidor" (MIRAGEM, 2018, p. 28). Notoriamente, em relação ao código consumerista, a Lei Geral de Proteção de Dados traz uma gama maior de proteção da privacidade, não sendo uma previsão implícita, mas expressa, como um dos fundamentos da lei constante no art. 2º, I, o "respeito à privacidade" (BRASIL, 2018).

De forma análoga, como já abordado neste capítulo (3.2.1. Tutela jurídica da privacidade e a CRFB/1988), a distinção entre vida privada e intimidade é muito tênue. Para alguns juristas já citados, a intimidade é um gênero englobado pela amplitude da privacidade, e assim sendo, pode-se interpretar que o art. 2º, IV, ao tratar da "inviolabilidade da intimidade, da honra e da imagem", também está resguardando o direito à privacidade de forma derivada (BRASIL, 2018).

Assim, de fato, pode se afirmar haver mecanismos protetivos, como a criação de um órgão regulador e fiscalizador, como a Autoridade Nacional de Proteção de Dados – ANPD (art. 55-C e seguintes), a regulação de responsabilidade civil sobre os agentes atuantes no tratamento de dados (art. 42 e seguintes) e a previsão de sanções administrativas para coibir práticas abusivas (art. 52 e seguintes) (BRASIL, 2018).

Ao pensar-se hipoteticamente no uso da Lei Geral de Proteção de Dados como mecanismo de proteção do usuário de tecnologias de Internet das Coisas, encontram-se possíveis mecanismos de atuação que podem auxiliar o usuário na observância de seus direitos. Como exemplo, por meio do princípio do livre acesso previsto no art. 6º, IV, o titular da informação pode exigir a consulta facilitada e gratuita sobre seus dados, no que consiste o tratamento e qual o tempo de duração, sendo uma previsão legal de acesso à informação que pode ser utilizada na tomada de conhecimento sobre possíveis abusividades, como o tratamento de dados que o usuário desconhecia estar sendo alvo de tratamento, bem como a existência de um órgão regulador o qual o usuário pode acionar para denunciar suspeitas de conduta abusiva no tratamento de dados, sendo a fiscalização específica uma das necessárias ações na observância do direito à privacidade.

Contudo, algumas previsões da normativa esbarram na realidade fática com problemas do cotidiano que não são tão observados pelo legislador nesse aspecto. Bioni (2019) contextualiza que a partir da Lei Geral de Proteção de Dados, o usuário passa a ocupar um papel de participação com seu consentimento no tratamento de dados pessoais, defendendo que o

consentimento é a base em que se funda a Lei nº 13.709/2018, assim, em tese o indivíduo é que estaria no protagonismo da proteção de dados.

Porém, o consentimento esbarra no desconhecimento do usuário comum sobre todo o contexto tecnológico, afinal, educação informacional ainda não é uma realidade absoluta para os consumidores no Brasil. Denota-se que há uma grande dificuldade em operacionalizar o consentimento do usuário, justamente por este desconhecer os termos que estão inseridos nas operações digitais, chamada de "racionalidade limitada" por Bioni (2019), além de uma capacidade cognitiva reduzida que tende a aceitar benefícios imediatos, sem sopesar os prejuízos à privacidade.

Ao adquirir um objeto simples como um relógio inteligente, o consumidor certamente espera algumas funções básicas como um marcador de horas e data, e o equipamento ainda vai um pouco além de registrar o número de passos, calorias queimadas, notificações de agenda e mensagens. Mas certamente o consumidor não espera que o registro de seus hábitos alimentares em sua agenda eletrônica possa influenciar o recebimento de propagandas, cupons de delivery, campanhas nutricionais ou um mês de desconto em alguma academia próxima a ele.

A imposição do consentimento parece ignorar a potencial capacidade do usuário em identificar os riscos que está sujeito ao adquirir o produto, uma espécie de vício oculto no qual o consumidor está no cerne do consentimento. Nesse sentido, cabe observar a conclusão de Bioni (2019, p. 213) sobre uma pesquisa empírica realizada na Universidade de Stanford sobre modelos mentais dos usuários acerca do funcionamento da publicidade comportamental on-line:

> As conclusões dessa pesquisa empírica trazem uma série de argumentos que convergem para a conclusão de que os usuários não estão capacitados para tomar decisões informadas no tocante ao controle de seus dados pessoais 62 , como: i) falta de conhecimento no que diz respeito ao 4.1.3.2 funcionamento das tecnologias de coleta dos dados pessoais e da sua inserção no contexto da publicidade comportamental, que determina o fluxo de suas informações em meio aos diversos atores que operam esse mercado; ii) idiossincrasia do trade-of da economia informacional, uma vez que o controle aos dados pessoais é visto, respectivamente, como um benefício mediato e uma perda mediata, o que o desvaloriza nesse processo de tomada de decisão; iii) em último lugar, porque os próprios usuários discordam da lógica econômica pela qual eles teriam que despender uma quantia para assegurar o seu direito à privacidade, enxergando tal dinâmica como uma extorsão.

Cabe destacar que somente 23% dos entrevistados diziam utilizar navegação privada, frente a 50% que não utilizavam; somente 17% deletam cookies, e quanto a isso, somente 30% realiza a limpeza por questões de segurança (BIONI, 2019). Logo, parece se confirmar que o consentimento e a autodeterminação, como possíveis garantidores de uma tutela sobre a

privacidade, não necessariamente atendem ao nível de proteção necessária, justamente por colocar o titular como responsável pelo controle de suas informações. No tocante específico do tratamento de dados por uma comunicação entre pessoas-máquinas, máquina-máquina, ou máquina-computadores, a LGPD não possui nenhuma menção específica que lide com as minúcias das tecnologias da Internet das Coisas para os direitos do usuário.

De acordo com Magrani (2020, p. 25), ainda se busca o "balanço adequado na regulação jurídica" entre a inovação e o direito, com a constituição de uma norma que se mostre apropriada ao cenário da Internet das Coisas. Para o autor, ainda é possível a criação de uma normatização com padrões e índices, para classificação e implantação de tecnologias IoT, como um padrão de atuação e incentivo para seguir boas práticas em conformidade com os direitos fundamentais do usuário e as políticas protetivas.

> a pesquisa na horizontal normatização e certificações deverá ter como objetivo definir e validar uma metodologia de avaliação de padrão de IoT pela perspectiva de valor público, composta por um modelo de referência e um método de avaliação aplicável à realidade brasileira (MAGRANI, 2020, p. 178).

De mais a mais, a Lei Geral de Proteção de Dados oferece mais especificidade do que o Código de Defesa do Consumidor na proteção do direito à privacidade do usuário consumidor, o que pode se afirmar como solução parcial à positivação de uma proteção à privacidade. Todavia, ainda é um título normativo insuficiente para a proteção específica do usuário consumidor de dispositivos com Internet das Coisas.

4.4 A PROTEÇÃO DA PRIVACIDADE DO CONSUMIDOR NO CENÁRIO ATUAL E A FORMAÇÃO DE NOVAS ESTRUTURAS JURÍDICAS PROTETIVAS

> "Uma vez que a IA toma decisões melhor do que nós sobre carreiras e até mesmo relacionamentos, nosso conceito de humanidade e de vida terá de mudar." Yuval Noah Harari, 2020.

O cenário atual do direito à privacidade do consumidor em rede passa por intensa vulnerabilidade, que vão desde questões conceituais sobre a privacidade e os limites da inovação até o consentimento aparente do usuário, a ignorância informacional do consumidor e o descompasso do avanço tecnológico em relação ao direito. Ciente da conjuntura atual que resguarda o direito à privacidade do usuário consumidor, e ao toque dos avanços da tecnologia da informação para uma sociedade hiperconectada, a problemática hipervulnerabilidade surge no horizonte e abre o debate ávido por uma solução. Se é a atual conjuntura normativa

insuficiente para proteger a privacidade do usuário da IoT, é possível que novas estruturas jurídicas possam dar tal proteção?

4.4.1 Hipervulnerabilidade: problemas da vigilância em rede

A vulnerabilidade do consumidor é um tema reconhecido do Código de Defesa do Consumidor e, sobretudo, a vulnerabilidade é um estado anímico do ser, como descrevem Marques e Mucelin (2022, p. 2): "*Vulnus* é ferida, *vulnerare* é ferir, daí que vulnerabilidade (*vulnerabilis*) é a situação, a possibilidade, ou o status daquele que tem uma fraqueza, susceptibilidade e pode ser ferido".

De tal modo, o consumidor é conhecidamente o agente com maior probabilidade de ser lesado em uma relação comercial, por isso é reconhecidamente como o sujeito vulnerável dentro do ordenamento jurídico, a fim de tentar reequilibrar os poderes ante o fornecedor (MENDES, 2015). Em uma relação comum de consumo, a vulnerabilidade do consumidor é presumida, sendo patente que do ponto de vista fático e técnico, está o consumidor em posição vulnerável em relação ao fornecedor, para ter acesso a informações ou para exigir a reparação de danos (MIRAGEM, 2016).

Contudo, na sociedade hiperconectada, algumas vulnerabilidades são acentuadas pela tônica da era digital. Como explica Mendes (2015), algumas situações são de extrema vulnerabilidade para o consumidor nesse meio, como o consentimento aparente, a falta de transparência sobre o tratamento de dados e o risco de discriminação. Para Miragem e Marques (2020, p. 21), a vulnerabilidade do consumidor no contexto hiperconectado enseja o reconhecimento de outra dimensão da vulnerabilidade informacional, "que não se resume à falta ou à pouca qualidade da informação prestada, mas a ausência de habilidade ou familiaridade com o ambiente digital".

Nesse sentido, a inaptidão e o desconhecimento dos mecanismos do universo digital podem repercutir negativamente para o consumidor, resultando em interpretações errôneas sobre o meio digital e na capacidade do consumidor de defender seus interesses juridicamente nesse meio (MIRAGEM, 2020). A vulnerabilidade nesse âmbito pode ser demonstrada de diversas maneiras, mas vale observar em dois aspectos apresentados por Miragem (2020) para reconhecimento de uma vulnerabilidade digital. Primeiramente, uma vulnerabilidade neuropsicológica, que se dá pela interferência no consumo a partir de estímulos digitais e padrões comportamentais dos consumidores, criando uma estrutura constante de incentivos, especialmente na indução ao consumo. A estrutura de incentivos e inteirações estão baseadas

nas análises comportamentais sobre o consumidor, programadas para despertar gatilhos humanos fundamentais, interferindo na tomada de decisão (MARQUES; MUCELIN, 2022).

Em outro aspecto, uma vulnerabilidade de ambiente onde a própria ambiência da internet cria um local propício para incentivar necessidades de consumo, com softwares, Inteligência Artificial, personalização de ofertas e publicidade o tratamento de dados acentua os "incentivos sensoriais e emocionais" para o consumo (MIRAGEM, 2020). Além do mais, de acordo com Miragem (2020, p. 240-249), o Superior Tribunal de Justiça utilizou de outro elemento para reconhecer a vulnerabilidade digital a partir da "dependência", no julgamento do REsp nº 476.428/SC, em que "a dependência de uma das partes de uma relação interempresarial, em acordo com circunstâncias específicas, poderá caracterizar sua vulnerabilidade para efeito da aplicação das normas do CDC de modo exclusivo".

O que se detecta é uma mercantilização das vulnerabilidades do consumidor. Como explicam Marques e Mucelin (2022, p. 17), na "sociedade digital a vulnerabilidade é arquitetural", as estruturas de navegação são programadas/projetadas para alcançar nossas vulnerabilidades ou até mesmo criar ou especificar novas vulnerabilidades. E a tendência não é de que as empresas envolvidas se conformem com deduções simples sobre o comportamento, cada vez mais a busca por predições mais íntimas sobre os usuários é acentuada e desenvolvida em novas tecnologias. Como cita Micklitz *et al. in* Marques e Mucelin (2022, p. 17):

> As empresas contemporâneas não se limitam a identificar e a visar vulnerabilidades claramente observáveis e já presentes; muito pelo contrário, a verdadeira vantagem competitiva reside na capacidade de identificar e direcionar as circunstâncias pessoais e características que tornam uma pessoa vulnerável em termos de disposição [potenciais], mas que ainda não resultaram em vulnerabilidades reais e ocorrentes.

Do ponto de vista do uso de capilaridades físicas – objetos inteligentes –, as vulnerabilidades à privacidade estão presentes desde a dificuldade na detecção das atividades, o domínio dessas informações por poucas empresas, a criação de trocas e as transações desconhecidas ou não detectáveis com as informações, (CAMARGO, 2021).

De acordo com Camargo (2021, p. 43),"os métodos tradicionais não são capazes de salvaguardar os direitos e liberdades individuais no tratamento de dados pessoais", assim a proposição de novos métodos para encarar as ameaças atuais aos direitos são necessários. De modo geral, o uso exponencial de tecnologias com essa capacidade computacional de vigilância costuma ser "leve, politicamente ágil e relativamente impermeável" a regulações, e como descreve Cohen (2016, p. 1), assim se inserem no cotidiano individual de maneira quase imperceptível.

Além disso, Cohen (2016) apresenta três aspectos que atuam na continuidade do ambiente de vulnerabilidade para garantia de direitos fundamentais. Primeiramente, o reconhecimento de que os mecanismos tradicionais de direitos fundamentais se mostram insuficientes para lidar com as violações contemporâneas à privacidade do usuário. Por conseguinte, os benefícios rápidos oferecidos pelas tecnologias da informação obscurecem os possíveis malefícios para direitos fundamentais, especialmente à privacidade, em razão da arquitetura estrutural de vigilância (COHEN, 2019). E o monopólio de grandes empresas sobre as tecnologias da informação e logicamente sobre a grande coleta de dados dos usuários, muitas vezes, se apropria da defesa de direitos fundamentais, exigindo direitos como liberdade de expressão e informação frente a possíveis regulações (COHEN, 2019).

Nesse contexto, o modelo tradicional de defesa da privacidade mostra-se ultrapassado. De acordo com Cohen (2013), a tônica da discussão entre privacidade nos moldes de um direito só acaba por perder espaço para o avanço da inovação e da livre concorrência. Compreendendo-se que a definição do direito à privacidade é um conceito que pode se transformar conforme a necessidade e cultura humana, a privacidade já foi compreendida de maneiras distintas até alcançar o status de um direito positivado.

Para fins de delimitação e acordo semântico, este estudo adota como definição de direito à privacidade contemporânea, o conceito de Rodotà (2008, p. 109), qual seja "o direito de manter o controle sobre as próprias informações e de determinar as modalidades de construção da própria esfera privada". Conscientizando-se sobre o estado de hipervulnerabilidade do consumidor, é importante tentar vislumbrar mecanismos e novas estruturas protetivas dos direitos fundamentais, especialmente ao direito à privacidade, objeto deste estudo.

4.4.2 Mecanismos legislativos e institucionais e o Plano Nacional de Internet das Coisas

> "Assim, faríamos melhor em invocar juristas, políticos, filósofos e mesmo poetas para que voltem sua atenção para essa charada: como regular a propriedade de dados? Essa talvez seja a questão política mais importante de nossa era. Se não formos capazes de responder a essa pergunta logo, nosso sistema sociopolítico pode entrar em colapso." Harari, 2020.

Com intuito de ampliar a atuação do país no desenvolvimento tecnológico, em 2019, foi aprovado o Decreto nº 9.854, que institui o Plano Nacional da Internet das Coisas, cuja finalidade era implementar e desenvolver a Internet das Coisas do Brasil, tendo por princípios norteadores a livre concorrência e livre circulação (BRASIL, 2019).

A normativa dispõe sobre as terminologias referentes à IoT, como a definição do que é: Internet das Coisas; Coisas; Dispositivos; e Serviços de valor econômico (BRASIL, 2019), ao passo que impõe objetivos fortemente vinculados à inovação e a livre concorrência, que se resumem a e melhorar a qualidade de vida e ganhos de eficiência em serviços (I), capacitação profissional e geração de empregos (II), produtividade e competitividade entre empresas desenvolvedora de IoT (III), parcerias entre setor público e privado (IV), e integração no cenário internacional e internacionalização de soluções via IoT (V) (BRASIL, 2019).

No tocante à privacidade, o texto faz uma única menção no artigo 5º, V, como um dos temas que integrarão um plano de ação para soluções que viabilizarão o Plano Nacional de Internet das Coisas, entre outros temas majoritariamente ligados ao desenvolvimento concorrencial (BRASIL, 2019). Observa-se que o decreto sucintamente projeta políticas públicas de incentivo à inovação na área da Internet das Coisas, não lidando com questões de direitos fundamentais, como o direito à privacidade, que é mencionado minimamente em um único momento e do qual a norma dá a entender que dependerá de outro instituto normativo como "plano de ação".

De modo geral, também não há vinculação com a Lei nº 13.709/2018, devendo-se pressupor que a proteção sobre dados em relação à Internet das Coisas nas políticas públicas implementadas pelo Decreto nº 9.854/2019 será disciplinada pela LGPD e pelos demais ordenamentos já existentes sobre privacidade.

Acerca do Plano Nacional de Internet das Coisas, Magrani (2018, p. 11) destaca que embora outras leis já versem sobre o direito à privacidade como a Constituição Federal, Código Civil, Código de Defesa do Consumidor e Lei Geral de Proteção de Dados, "é necessário e premente que haja regulações que protejam a privacidade e os dados pessoais de usuários de modo mais minucioso" ao uso de tecnologias como a IoT.

Para o autor, uma proposta de regulação deve também enfrentar a dicotomia entre privacidade e inovação tecnológica, assumindo-se que a privacidade é fundamental para o desenvolvimento tecnológico adequado e ao cumprimento de direitos fundamentais, podendo ser um elemento concorrencial positivo na conquista de confiança dos usuários (MAGRANI, 2018).

Nesse sentido, de acordo com Magrini (2018, p. 11), além dos incentivos à inovação e livre concorrência, carece ainda que o Estado e as empresas assumam um compromisso como princípio norteador no "aprimoramento da sua capacidade de garantir a segurança e a privacidade dos usuários nos momentos de coleta, tratamento e compartilhamento de dados".

O autor ainda defende que é possível um modelo de negócio mais eficiente na proteção de direitos que não vise somente a lucratividade.

A regulação sobre a privacidade de maneira mais específica ao contexto da vigilância tecnológica é proposta também por Cohen (2013), que defende uma abordagem estrutural sobre a privacidade, que possa proteger o espaço individual e o espaço da inovação. Para a autora, uma simples proposta regulatória sobre a privacidade não é suficiente para abranger as verdadeiras dificuldades de lidar com a dicotomia de inovação e privacidade; políticas regulatórias devem encontrar soluções dinâmicas para permitir a inovação e garantir direitos (COHEN, 2013).

Ademais, uma governança sobre Internet das Coisas é um modelo normativo que se mostra necessário. De acordo com Rover e Sabo (2019), a fragmentação legislativa sobre proteção de dados e ferramentas distintas na tecnologia acaba por gerar ainda mais segurança jurídica e interpretações distintas acerca da proteção de direitos e da IoT. Além de instituir uma governança específica sobre IoT, os autores defendem a criação de uma Autoridade sobre o tema para regular e fiscalizar os protocolos de proteção da informação (ROVER; SABO, 2019).

Ainda é possível utilizar em uma proposta de mecanismos práticos, proposta por Bioni (2019, p. 345) de releitura da autodeterminação do indivíduo sob seus dados com um dirigismo informacional, assumindo-se que o indivíduo é hipervulnerável, e demanda "seu empoderamento para emancipá-lo e a sua intervenção para assisti-lo". O dirigismo informacional importa a capacitação do indivíduo para saber autodeterminar o controle de suas informações e de intervenção para garantir livre acesso e transparência sobre dados, o suficiente para que possa exercer plenamente seus direitos de personalidade (BIONI, 2019).

Nesse contexto, concorda-se com a predição de Cohen (2019), pois além de criar novos institutos normativos, é necessário pensar em novas formas institucionais, isto é, repensar os direitos fundamentais na sociedade informacional e especialmente o dinamismo do direito à privacidade para a construção de uma governança protecionista que consiga dialogar com a inovação. Além disso, compreender a importância de novos formatos institucionais que possam ser assistência ao protagonista da relação de proteção de dados, o usuário, titular das informações.

No tocante à Internet das Coisas, considera-se imperativo que se há criação de textos normativos, regulamentações que fomentam seu rápido desenvolvimento e sua ampliação, cabe também ao legislador observar como o desenvolvimento dessas tecnologias afetarão direitos fundamentais como a privacidade. A atuação legislativa a respeito da Internet das Coisas deve compreender que a tecnologia que está se buscando desenvolver pode apresentar riscos à

privacidade dos indivíduos e não pode ser tratada de modo genérico, que não reconheça suas especificidades e o *modus operandi*. É importante, portanto, avançar para uma governança sobre Internet das Coisas e direitos fundamentais, dentre eles a privacidade.

Ao mesmo passo que uma governança sobre a Internet das Coisas deve implementar mecanismos práticos de assistência ao usuário consumidor das tecnologias desenvolvidas, desde a capacitação do usuário por meio de ampliação da educação informacional até a criação de canais de atendimento ao usuário consumidor e o direcionamento para uma Autoridade Fiscalizadora especializada.

5 CONSIDERAÇÕES FINAIS

O cenário até aqui estudado demonstra o avanço da Sociedade de Informação para um contexto moderno de Sociedade de Vigilância, em que cada vez mais os dados e as informações privadas são objetos centrais da manutenção do novo formato econômico entabulado, sendo que as mais diversas maneiras de tratar dados e tornar a informação um ativo agregado de valor atribuível evoluem dia após dia.

Como se observou, há um monopólio da indústria informacional nas mãos de algumas poucas empresas, gigantes na área da tecnologia da informação, que correspondem a grandes formuladoras das regras autorregulatórias e, muitas vezes, se opõem à imposição de normas que tentem a regular o mercado de trocas informacionais. Nesse sentido, a economia de vigilância comporta mais de um modelo de negócio, e a diversificação sustenta a economia de vigilância. Por isso, são os aparatos tecnológicos que conduzem cada negócio, o que consequentemente gera a necessidade de coletar cada vez mais dados ou atingir maior profundidade dos dados, expandindo-se a zona de coleta para redes sociais, sites e dispositivos inteligentes.

Vislumbra-se, então, um moderno paradigma do panóptico da vigilância em produtos e serviços que cumpram o papel de coletar dados com a opacidade de apetrechos, *cookies* e objetos, por meio da "inevitável" Internet das Coisas. É quase inevitável não fazer parte da sociedade informacional, pois equivale a excluir-se socialmente quase que de forma absoluta, tendo em vista que as mais simples tarefas dos dias atuais exigem alguma forma de conexão, uma identidade virtual, um cadastro em uma plataforma de trabalho ou uma página de identificação nas redes sociais, já se tornaram requisitos para uma vaga de trabalho.

A Internet das Coisas está presente em todos os lugares, nas câmeras com reconhecimento facial no shopping, nas geladeiras que avisam quando um item acabou, nos sites que aceitam o uso de cookies, nas redes sociais e no sensor que aciona e desliga qualquer dispositivo eletrônico, bem como na Alex, na Siri e no Android. Ou seja, a IoT já é parte integrante do nosso cotidiano, mas é importante ressaltar que o contexto contemporâneo de outras tecnologias tem sido fundamental para que a IoT alcance o patamar atual de aceitação. Vivemos em um universo hiperconectado, com moedas criptografadas e certificações de segurança baseadas em *blockchain*. E dentro desse mesmo universo, temos o Metaverso, em que a realidade virtual não é mais "aumentada", mas sim onipresente.

A computação é ubíqua e inevitável, e os modelos econômicos buscam maximizar o escopo, a ação, a predição e a personalização, com o objetivo de captar hábitos, incentivar o

consumo, criar vontades e descobrir comportamentos. Dessa forma, o sensoriamento e a codificação precisam estar presentes para atingir a maior acuracidade possível e o maior potencial da tecnologia. E no epicentro de toda essa ebulição da computação ubíqua e do capitalismo de vigilância, os reflexos jurídicos começam a surgir, afinal, as condutas sempre refletem no campo jurídico, ainda que muitas vezes o campo da inovação busque se autorregular antes de aceitar uma regulamentação.

A presente pesquisa abordou especialmente o direito à privacidade, sendo necessário analisar desde seus primeiros aparecimentos na história até seu reconhecimento no cenário jurídico, com positivação legal. Inicialmente conceituado como um direito de estar só, a privacidade representava a necessidade humana de isolar-se de tempos em tempos, como uma liberdade negativa do indivíduo perante o Estado e a sociedade. Foi reconhecido como um Direito Humano, e por muitos países, positivado como um Direito Fundamental. A privacidade evoluiu de um direito de concepção patrimonial, atrelado à propriedade, como a preservação do domicílio como asilo inviolável, até ser reconhecido como um direito de personalidade, que o indivíduo preza pela própria condição humana do ser.

A Constituição Federal de 1988 incluiu o direito à privacidade entre os direitos fundamentais, e por meio da expansão da norma constitucional, o direito privado o positivou como direito de personalidade no Código Civil. O Código de Defesa do Consumidor O Código de Defesa do Consumidor interpreta a proteção da privacidade como um direito básico do consumidor contra publicidade enganosa e abusiva, e a Lei Geral de Proteção de Dados a utiliza como um dos fundamentos da norma. Contudo, diante do desenvolvimento das tecnologias de Internet das Coisas, amplamente incentivadas por políticas públicas que visam a difusão na economia nacional e na produção de dispositivos e tecnologias IoT, resta o questionamento se há proteção suficiente à tutela do direito à privacidade no contexto normativo.

Sendo a problemática desta pesquisa a análise sobre uma possível (in)suficiência normativa sobre a proteção do direito à privacidade do usuário consumidor da Internet das Coisas, cabem algumas ponderações. Do conteúdo relatado na pesquisa, nota-se que há um conflito conceitual acerca da terminologia “privacidade”, sendo para muitos autores conflitante a definição tradicional da privacidade como um direito de liberdade meramente negativa de estar só, de isolar-se da sociedade, frente aos verdadeiros desafios enfrentados na proteção da privacidade.

Do ponto de vista prático, discute-se na doutrina a criação de mecanismos que vão além da regulação, como autoridades fiscalizadoras, canais de atendimento e direcionamento informacional para uma autonomia do usuário consumidor no controle de suas informações. E

acerca das normas, ainda que tenha ocorrido a promulgação da Lei Geral de Proteção de Dados por meio da Lei nº 13.709/2018, discute-se a necessidade de uma regulamentação específica sobre Internet das Coisas.

Diante desses apontamentos, concluiu-se que há, de modo geral, uma insuficiência normativa quanto a proteção do direito à privacidade em três ângulos: a insuficiência conceitual por uma definição contextualizada ao uso das tecnologias IoT, uma vez que as definições tradicionais não acompanham as especificidades dos riscos que essa tecnologia pode oferecer aos usuários; uma insuficiência normativa, pois apesar de haver avanços com a Lei Geral de Proteção de Dados, não há lei própria para um plano estratégico para implementação da IoT que contemple adequadamente as garantias de proteção da privacidade e relega a um plano estratégico ainda inexistente a integração da privacidade com a IoT; e uma insuficiência prática, pois faltam mecanismos técnicos de proteção voltados à instrução informacional do usuário, à conquista de sua autonomia informacional e, especialmente, à fiscalização.

REFERÊNCIAS

ANDERSON, Chris. **A cauda longa**: do mercado de massa para o mercado de nicho. Rio de Janeiro: Elsevier, 2006. p. 256.

ARAUJO, Regina Borges. Computação ubíqua: Princípios, tecnologias e desafios. *In*: **XXI Simpósio Brasileiro de Redes de Computadores**. 2003. Disponível em: http://www.professordiovani.com.br/rw/monografia_araujo.pdf. Acesso em: 30 nov. 2022.

ARENDT, Hannah. **A condição humana**. 10. ed. Tradução de Roberto Raposo. Rio de Janeiro: Forense Universitária, 2007. p. 352.

BAUDRILLARD, Jean. **A sociedade de consumo.** Lisboa: Edições 70, 2014. p. 272.

BAUMAN, Zygmunt. **Modernidade líquida**. Tradução de Plínio Dentzien. Rio de Janeiro: Zahar, 2001. p. 280.

BAUMAN, Zygmunt. **Vida para consumo**: a transformação das pessoas em mercadoria. São Paulo: Zahar, 2001. 159 p. Tradução de: Carlos Alberto Medeiros.

BENTHAM, Jeremy. **O panóptico.** 2. ed. Belo Horizonte: Autêntica, 2008. p. 201.

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 423.

BRASIL. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade 0090566-08.2020.1.00.0000 nº 6387. **Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade 6.387**. Brasília, 07 maio 2020. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165. Acesso em: 23 jun. 2021.

BULOS, Uadi Lammêgo. **Curso de direito constitucional**. 8. ed. São Paulo: Saraiva, 2014. 1696 p.

CAMARGO, Gustavo Xavier de. **A vedação à gratuidade compulsória dos serviços digitais como forma de proteção dos dados pessoais dos usuários consumidores e mitigação do abuso de posição dominante pelas plataformas de dois ou múltiplos lados**. 2020. 213f. Dissertação (Mestrado em Direito) – Universidade Federal de Santa Catarina, Florianópolis, 2020.

CANCELIER, Mikhail Vieira de Lorenzi. **Infinito particular**: privacidade no século XXI e a manutenção do direito de estar só. 2017. 266f. Tese (Doutorado em Direito) – Universidade Federal de Santa Catarina, Florianópolis, 2017. Disponível em: https://repositorio.ufsc.br/bitstream/handle/123456789/174424/PDPC1275-T.pdf?sequence=1&isAllowed=y. Acesso em: 10 jan. 2023

CANCELIER, Mikhail Vieira de Lorenzi. O direito à privacidade hoje: perspectiva histórica e o cenário brasileiro. **Seqüência**: Estudos Jurídicos e Políticos, [S.L.], v. 38, n. 76, p. 213, 20 set. 2017. Universidade Federal de Santa Catarina (UFSC). DOI: 10.5007/2177-7055.2017v38n76p213. Disponível em:

https://www.scielo.br/j/seq/a/ZNmgSYVR8kfvZGYWW7g6nJD/?lang=pt. Acesso em: 10 jan. 2023.

CARVALHO, Victor Miguel Barros de. **O direito fundamental à privacidade ante a monetização de dados pessoais na internet**: apontamentos legais para uma perspectiva regulatória. 2018. 146f. Dissertação (Mestrado em Direito) – Universidade Federal do Rio Grande no Norte, Natal, 2018. Disponível em: https://repositorio.ufrn.br/handle/123456789/26851. Acesso em: 09 jan. 2023.

CASTELLS, Manuel. **A era da informação: economia, sociedade e cultura**: a sociedade em rede. 6. ed. São Paulo: Paz e Terra, 2018. 1 v. p. 629.

COHEN, Julie. **Between truth and power**: the legal constructions of informational capitalism. New York: Oxford University Press, 2019. p. 377.

COHEN, Julie. **The surveillance-innovation complex**: the irony of the participatory turn. The Participatory Condition. University of Minnesota Press, 2016. ISBN: 97808116697700.

COHEN, Julie. What privacy is for. **Harvard Law Review**, Massachusetts, v. 126, n. 7, p. 1904-1933, 20 maio 2013. Disponível em: https://harvardlawreview.org/2013/05/what-privacy-is-for/. Acesso em: 12 jan. 2023.

DESNICA, Marin *et al.* **Google AdSense**: user modeling and recommender systems ⧟ case exercise. User Modeling and Recommender Systems − Case exercise. 2014. Disponível em: https://dokumen.tips/documents/google-adsense-htktlueehtktlueerecommendersystemsimagesaaagoogle-adsense-v12pdf.html?page=1. Acesso em: 15 jun. 2022.

DONEDA, Danilo. **Da privacidade a proteção de dados pessoais**. 2. ed. São Paulo: Revista dos Tribunais, 2020. p. 364.

DONEDA, Danilo *et al.* (org.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021. p. 1125.

FOUCAULT, Michel. **Vigiar e punir:** nascimento da prisão. Petrópolis: Vozes, 1999. 16ª ed. p. 347.

FROW, John. Cookie. **Cultural Studies Review**, [S.L.], v. 25, n. 2, p. 208-210, 13 nov. 2019. University of Technology, Sydney (UTS). http://dx.doi.org/10.5130/csr.v25i2.6899.

GANSKY, Lisa. **The mesh**: why the future os business is sharing. New York: Penguin, 2010. p. 251.

GATTES, Bill. **A estrada do futuro.** São Paulo: Companhia das Letras, 1995. p. 350.

HARARI, Yuval Noah. **21 lições para o século 21**. Tradução de Paulo Geiger. São Paulo: Companhia das Letras, 2020. p. 343.

HARARI, Yuval Noah. **Homo Deus**: uma breve história do amanhã. Tradução de Paulo Geiger. São Paulo: Companhia das Letras, 2016. p. 448.

LEVY, Steven. **Google a biografia**: como o google pensa, trabalha e molda nossas vidas. Tradução de Luis Protássio. São Paulo: Universo dos Livros, 2012. p. 464.

LIPOVETSKY, Gilles. **A felicidade paradoxal:** ensaio sobre a sociedade de hiperconsumo. Tradução de Maria Lucia Machado. São Paulo: Companhia das Letras, 2007. p. 402.

LOVELUCK, Benjamin. **Redes, liberdades e controle**: uma genealogia política da internet. Petrópolis: Vozes, 2018. p. 387.

MAGRANI, Eduardo. **A internet das coisas no Brasil**: estado da arte e reflexões críticas ao fenômeno. Rio de Janeiro: Instituto Igarapé, 2018. 25 p. Disponível em: https://igarape.org.br/wp-content/uploads/2018/11/A-Internet-das-Coisas-no-Brasil-Estado-da-arte-e-reflexo%CC%83es-cri%CC%81ticas-ao-feno%CC%82meno-Eduardo-Magrani.pdf. Acesso em: 22 jan. 2023.

MAGRANI, Eduardo. **Internet das coisas**. 1 ed. Rio de Janeiro: FGV, 2018. p. 192.

MAGRANI, Eduardo. **Entre dados e robôs**: ética e privacidade na era da hiperconectividade. 2. ed. Porto Alegre: Arquipélogo, 2019. p. 304.

MARQUES, C. L.; MUCELIN, G. Vulnerabilidade na era digital: um estudo sobre os fatores de vulnerabilidade da pessoa natural nas plataformas, a partir da dogmática do Direito do Consumidor. **civilistica.com**, v. 11, n. 3, p. 1-30, 25 dez. 2022.

MENDES, Laura Schertel. **Transparência e privacidade**: violação e proteção da informação pessoal na sociedade de consumo. 2008. 158f. 1v. Dissertação (Mestrado em Direito) – Universidade de Brasília, Brasília, 2008.

MIRAGEM, Bruno. Novo paradigma tecnológico, mercado de consumo digital e o direito do consumidor. **Revista dos Tribunais**, São Paulo, v. 125, n. 1, p. 1-35, set. 2019.

MOROZOV, Evgeny. **Big Tech**: a ascensão dos dados e a morte da política. Tradução de Claudio Marcondes. São Paulo: Ubu, 2018. p. 192.

MUCELIN, Guilherme. **Conexão online e hiperconfiança**: os players da economia do compartilhamento e o direito do consumidor. São Paulo: Revista dos Tribunais, 2020. p. 358.

MYSTAKIDIS, Stylianos. Metaverse. **Encyclopedia**, [S.L.], v. 2, n. 1, p. 486-497, 10 fev. 2022. MDPI AG. http://dx.doi.org/10.3390/encyclopedia2010031.

O'NEIL, Cathy. **Algoritmo de destruição em massa**: como o big data aumenta a desigualdade e ameaça a democracia. Santo André: Rua do Sabão, 2020. p. 342.

ORWELL, George. **1984**. Tradução de Heloisa Jahn e Alexandre Hubner. São Paulo: Companhia das Letras, 2020. p. 416.

PARISER, Eli. **O filtro invisível**: o que a internet está escondendo de você. Tradução de Diego Alfaro. Rio de Janeiro: Zahar, 2012. p. 291.

PEREIRA, Ricardo *et al*. O metaverso e o dilema da informação. In: CONGRESSO BRASILEIRO DE GESTÃO DO CONHECIMENTO DA AMÉRICA LATINA, 17., 2022, [S.I]. **Dossiê Especial KM Brasil 2022.** [S.I]: Revista Inteligência Empresarial, 2022. v. 46, p. 1-16. Disponível em: https://inteligenciaempresarial.emnuvens.com.br/rie/issue/view/51. Acesso em: 25 jul. 2022

PESSOA, João Pedro Seefeldt. **O efeito Orwell na sociedade em rede**: cibersegurança, regime global de vigilância social e direito à privacidade no século xxi. Porto Alegre: Editora Fi, 2020. p. 214.

QUEIROZ, Renata Capriolli Zocatelli. **A proteção de dados pessoais**: a lgpd e a disciplina jurídica do encarregado de proteção de dados. 2021. 137 f. Tese (Doutorado) - Curso de Direito, Programa de Pós-Graduação em Direito, Universidade de São Paulo, São Paulo, 2021.

RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008. 382 p. Tradução de: Danilo Doneda e Luciana Cabral Doneda.

ROSNER, Max; RITCHIE, Hannah; ORTIZ-OSPINA, Esteban. **The internet history has just begun**.Internet. 2022. Our Word in Data. Disponível em: https://ourworldindata.org/internet#the-internet-s-history-has-just-begun. Acesso em: 26 ago. 2022.

SANTAELLA, Lucia *et al*. Desvelando a Internet das Coisas. **Revista GEMInIS**, *[S. l.]*, v. 4, n. 2, p. 19–32, 2013. Disponível em: https://www.revistageminis.ufscar.br/index.php/geminis/article/view/141. Acesso em: 18 maio. 2022.

SANTOS, Bruno P. *et al.* Internet das Coisas: da teoria à prática. In: SIQUEIRA, Frank Augusto *et al* (org.). **Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos**. 34. ed. Salvador: Sociedade Brasileira de Computação, 2016. Cap. 1. p. 1-50. Disponível em: http://www.sbrc2016.ufba.br/anais-slides/trilha-principal/. Acesso em: 04 abr. 2022.

SCHWAB, Klaus. Tradução de Daniel Moreira Miranda. **A Quarta Revolução Industrial**. São Paulo: Edipro, 2016. p. 176.

SILVA, Everton *et al.* Computação ubíqua–definição e exemplos. **Revista de Empreendedorismo, Inovação e Tecnologia**, v. 2, n. 1, p. 23-32, 2015. DOI: 10.18256/2359-3539/reit-imed.v2n1p23-32. Disponível em: https://core.ac.uk/display/270152395?utm_source=pdf&utm_medium=banner&utm_campaign=pdf-decoration-v1. Acesso em: 30 nov. 2022.

SOARES, Jonas. **Avaliação de Máquinas Preemptáveis nos Provedores de Nuvem Pública Amazon e Google**. 2019. 66 f. TCC (Graduação em Engenharia da Computação) – Universidade de Brasília, Brasília, 2019. Disponível em: https://bdm.unb.br/handle/10483/28901. Acesso em: 10 ago. 2022.

STONE, Brad. **A loja de tudo**: jeff bezos e a era da amazon. Tradução de: Andrea Gottlieb. Rio de Janeiro: Intrínseca, 2013. p. 358.

TARTUCE, Flávio. **Manual de direito civil.** São Paulo: Editora Forense, 2018. Volume único. 2691 p.

TAVARES, Letícia Antunes. O direito à privacidade em suas mais exclusivas esferas: a intimidade e a vida privada na era informacional. *In*: LOUREIRO, Francisco Eduardo *et al* (org.). **A vida dos direitos nos 30 anos da Constituição Federal**. São Paulo: Escola Paulista da Magistratura, 2019. p. 453-472.

TEPEDINO, Gustavo *et al* (org.). **O código civil na perspectiva civil-constitucional**: parte geral. Rio de Janeiro: Renovar, 2013. p. 540.

VALENTE, Jonas. Promovendo a privacidade e a proteção de dados pela tecnologia: privacy by design e privacy enhancing-technologies. *In*: BRANCO, Sérgio; TEFFÉ, Chiara de (org.). **Privacidade em perspectivas**. Rio de Janeiro: Lumen Juris, 2018. p. 111-128.

VARIAN, Hal. Economics of Information Technology. **Cambridge University Press**, Cambridge, v. 1, n. 1, p. 1-99, mar. 2003. Disponível em: https://people.ischool.berkeley.edu/~hal/Papers/mattioli/mattioli.pdf. Acesso em: 20 set. 2022.

VARIAN, Hal. The economics of internet search. **Rivista di Politica Economica**, [*s. l*], v. 96, n. 6, p. 9-23, nov. 2006. Disponível em: https://www.econbiz.de/Record/the-economics-of-internet-search-varian-hal/10005015537. Acesso em: 15 jun. 2022.

WARREN, Samuel D.; BRANDEIS. Louis D.; **The right to privacy.** Harvard Law Review, Vol. 4, No. 5. (Dec. 15, 1890), pp. 193-220.

WAZLAWICK, Raul Sidnei. **História da computação.** Rio de Janeiro: Elsevier, 2016. p. 931.

WIENER, Norbert. **Cibernética e sociedade:** o uso humano de sêres humanos. Tradução de José Paulo Paes. São Paulo: Cultrix, 1950. p. 190.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância:** a luta por um futuro humano na nova fronteira do poder. Tradução de: George Schlesinger. Rio de Janeiro: Íntrinseca, 2019. p. 820.