Organização Comitê Científico
Double Blind Review pelo SEER/OJS
Recebido em: 16.07.2021
Aprovado em: 29.07.2021

Revista de Direito, Governança e Novas Tecnologias

TECNOLOGIAS VESTÍVEIS E CAPITALISMO DE VIGILÂNCIA: DO COMPARTILHAMENTO DE DADOS SOBRE SAÚDE E A PROTEÇÃO DOS DIREITOS DA PERSONALIDADE

Raíssa Arantes Tobbin[*]
Valéria Silva Galdino Cardin[*]

RESUMO: O presente artigo tem por objetivo analisar a utilização das tecnologias vestíveis no contexto do capitalismo de vigilância, tendo em vista os riscos de compartilhamento indevido de dados acerca da saúde e a violação de direitos da personalidade dos usuários. Para tanto, utilizou o método hipotético-dedutivo, fundamentado na revisão bibliográfica de obras, artigos, doutrina, legislação e jurisprudência. Como resultado, verificou-se que a coleta e o tratamento de dados realizados pelos *wearables* levantam questionamentos acerca do direito à privacidade e à autodeterminação informativa, já que tais dados podem ser monetizados pelo mercado tecnológico para fins de publicidade comportamental e *online profiling*.

PALAVRAS-CHAVE: Autodeterminação Informativa; Direito à Privacidade; Direitos da Personalidade; Lei Geral de Proteção de Dados (LGPD); *Wearables*.

WEARABLE TECHONOLOGIES AND SURVEILLANCE CAPITALISM: DATA SHARING ON HEALTH AND THE PROTECTION OF PERSONALITY RIGHTS

ABSTRACT: This paper aims to analyze the use of wearable technologies in the context of surveillance capitalism, in view of the risks of improper sharing of data about health and the violation of users' personality rights. The research used the hypothetical-deductive method, based on the bibliographic review of books, articles, doctrine, legislation and court decisions. As a result, it was found that the collection and processing of data carried out by wearables raises questions about the right to privacy and informational self-determination, since these data can be monetized by the technological market for the purposes of behavioral advertising and online profiling.

KEYWORDS: Informative Self-Determination; Right to Privacy; Personality Rights; General Data Protection Law (LGPD); Wearables.

1 INTRODUÇÃO

[*] Mestranda em Ciências Jurídicas pela Universidade CESUMAR; Graduada em Direito pela Universidade Paranaense (UNIPAR); Graduada em Letras – Português/Espanhol pela Universidade Estadual de Ponta Grossa (UEPG); Advogada no Paraná; E-mail: tobbinraissa@hotmail.com

[*] Pós-Doutora em Direito pela Universidade de Lisboa; Doutora e mestre em Direito das Relações Sociais pela Pontifícia Universidade Católica de São Paulo (PUCSP); Docente da Universidade Estadual de Maringá e no Programa de Pós-Graduação em Ciências Jurídicas pela Universidade CESUMAR; Pesquisadora pelo ICETI; Advogada no Paraná; E-mail: valeria@galdino.adv.br

É uma determinante da sociedade pós-moderna a hiperconexão por meio da interatividade em rede. Neste contexto, computadores, celulares, tablets, *smartphones* e outros aparelhos tecnológicos passam a ser cada vez mais fundamentais para a vida cotidiana do indivíduo, uma vez que a cidadania passa a ser exercida constantemente por meio da obtenção de informação e do discurso midiático e informático em aplicativos e redes sociais. Em razão da crise de saúde pública ocasionada pela pandemia da COVID-19 e da consequente necessidade de isolamento social, tendo em vista a inexistência de cobertura de imunização até o presente momento, a utilização de algoritmos e dispositivos relacionados à inteligência artificial cresceu de forma exponencial, possibilitando a continuação da educação, da atividade laborativa, do comércio e alternativas de acesso à saúde pela via remota.

Assim, ganham espaço as tecnologias vestíveis, do inglês *wearables*, que unem elementos de tecnologia, moda e *design* para facilitar ao usuário diversas atividades do cotidiano. Cita-se relógios, pulseiras, joias, tecidos inteligentes, entre outros dispositivos que podem ser acoplados ao corpo humano para o monitoramento de batimentos cardíacos, nível de glicose no sangue, acompanhamento de clico menstrual, performance esportiva, qualidade de sono, auxílio em atividades de geonavegação, bem como de sintomas da COVID-19.

Contudo, apesar das potencialidades das tecnologias vestíveis, um dos questionamentos que surgem diante da hiperconexão é a coleta de dados dos usuários diante da vigilância digital constante e da consequente perda da privacidade. Esta última, é muito diferente de outrora, uma vez que é o usuário quem diariamente a coloca em segundo plano em nome de *views*, *likes*, seguidores e prestígio virtual. Todavia, será que este usuário concorda ou tem consciência da real dimensão dos termos do armazenamento de dados pelos aplicativos e aparelhos que utiliza? Ou tem conhecimento acerca dos riscos da utilização indevida de seus dados para fins mercadológicos, a exemplo da criação de perfis comportamentais, discriminação e utilização de publicidade direcionada?

Diante de tais questionamentos, o presente trabalho pretende investigar os riscos do uso das tecnologias vestíveis aos direitos da personalidade, especialmente os direitos à privacidade e à proteção de dados sobre a saúde na era digital. Para tanto, utilizou o método hipotético-dedutivo, fundamentado em pesquisa e revisão bibliográfica de obras, artigos de periódicos, legislação, doutrina e jurisprudência aplicáveis ao caso. Inicialmente, investigou-se o que são as tecnologias vestíveis e as suas potencialidades e benefícios à vida pós-moderna. Posteriormente, o artigo examinou a coleta de dados acerca da saúde realizada pelos

wearables e os riscos aos direitos da personalidade do usuário, verificando a importância da tutela dos direitos à privacidade e à autodeterminação informativa para a preservação da dignidade humana no contexto de hiperconectividade.

2 INTERNET DAS COISAS: OS *WEARABLES* E SUAS APLICAÇÕES

A *Internet das Coisas* (do inglês *Internet of Things* – ou IoT) é a expressão que atualmente designa o conjunto de serviços e dispositivos que reúne conectividade, o uso de sensores e a capacidade computacional para processar e armazenar dados. Conforme Magrani (2019, p. 19-20) o que todas as definições de IoT "têm em comum é que elas se concentram em como computadores, sensores e objetos (artefatos) interagem uns com os outros e processam as informações/dados em um contexto de hiperconectividade". Logo, o contexto atual de conexão é "baseado na estreita relação entre seres humanos, objetos físicos, sensores, algoritmos, *Big Data*, Inteligência Artificial (computacional), *cloud computing* etc.".

Já *Big Data*, segundo o autor, é o termo em evolução "que descreve qualquer quantidade volumosa de dados estruturados, semiestruturados ou não estruturados que podem ser explorados para se obter informações", sendo que a "primeira propriedade envolvendo *Big Data* consiste no volume crescente de dados" (MAGRANI, 2019, p. 22). Pesquisas recentes estimam que, em 2020, "a quantidade de objetos interconectados passou dos 25 bilhões, podendo chegar a 50 bilhões de dispositivos inteligentes" e a estimativa "de impacto econômico global corresponde a mais de US$11 trilhões em 2025" (MAGRANI, 2019, p. 24).

Ainda que desconhecidos ou inacessíveis a muitos cidadãos, as tecnologias vestíveis têm ganhado nos últimos anos muita atenção no âmbito do mercado tecnológico, prometendo facilitar e monitorar uma série de atividades humanas por meio da coleta de dados que seriam armazenados nestes dispositivos e convertidos em informações pertinentes aos seus usuários.

São exemplos de *wearables* na área da eletrônica os "óculos, relógios, pulseiras, joias, e-têxteis e tecidos inteligentes, dispositivos que podem ser acoplados no corpo, entre outros" (MATOS, 2015, p. 783-784). Para Guimarães e Américo (2017, p. 3) as tecnologias vestíveis podem ser conceituadas como toda "forma de tecnologia que utiliza o corpo como suporte e são digitais e integradas (proporcionam acesso à internet ou por *Bluetooth*), podendo ou não transmitir os dados colhidos a um dispositivo com maior poder de processamento

(computador, *smartphone*, *tablet*)" e, por meio de "aplicativos, transformar esses dados em informações e comunicá-los ao usuário através de uma interface". Segundo Geraldo (2018, p. 57) os *wearables* podem ser utilizados para o "cuidado com a saúde, monitoramento de crianças e idosos, soldados em campo de batalha, assim como em esportes radicais, pois os sensores podem captar a informação proveniente do indivíduo e também do ambiente onde se encontra esta pessoa".

Como observam Guimarães e Américo (2017, p. 5) "a vestimenta está se tornando um mediador da tecnologia digital, amplificando as potencialidades das roupas e do corpo através do uso da tecnologia". As "possibilidades ilimitadas para a dinâmica personalização de roupas e as experimentações mostrando-se favoráveis a cada vez mais expansões do que a tecnologia aliada à Moda podem fazer". A tecnologia vestível digital "serve como mediador das informações e dados que coletamos e enviamos a terceiros assim como as informações que o meio oferece, uma comunicação transmidiada e ubíqua que ocorre o tempo todo".

Para Magrani (2017, p. 118) a tecnologia torna-se "parte integrante do cotidiano, ou seja, pervasiva". Já a característica senciente trata da competência dos aparatos tecnológicos de "perceberem e responderem ao ambiente. É na capacidade dos objetos de produzir funcionalidades eficazes que o contexto da internet das coisas almeja uma atuação não-humana de forma autônoma". Logo, "como intermediadora da relação do homem com um espaço cada vez mais interativo, as expectativas das tecnologias vestíveis ampliam de forma significativa".

São exemplos de tecnologias vestíveis o *Android Wear* e o *Google Glass*, que são dispositivos móveis fabricados pelo mercado de tecnologia voltados para as práticas esportivas e a telecomunicação (MARINI, 2017, p. 117). No setor esportivo se destacam aparelhos "de monitoramento de corrida, como a pulseira da Nike, *FuelBand*, e a da Adidas, *miCoach*". Neste último, "o sistema tecnológico se torna uma espécie de treinador virtual: os dados físicos do corpo são transformados em informações digitais, armazenadas, processadas e analisadas pelos algoritmos (códigos de programação)". A roupa possui um suporte acoplado que coleta, processa e armazena "movimentos corporais em dados digitais" (MARINI, 2017, p. 120).

Conforme Guimarães e Américo, os monitores voltados para o esporte profissional contam com:

> a análise de fisioterapeutas, preparadores físicos e treinadores, pessoas com conhecimento da fisiologia humana e que podem interpretar melhor os dados

> apresentados pelo dispositivo [...]. Eles permitem que os treinadores meçam a fadiga e o desempenho de seus jogadores durante as sessões de treinamento e competições. Quando um jogo está em andamento, os treinadores têm acesso a uma abundância de dados em tempo real, o que os ajuda a tomar decisões que antes eram tomadas através da observação a olho nu e por instinto - como quando um jogador deveria ser substituído [...] a tecnologia vestível também pode destacar pontos fortes e fracos dentro das táticas das equipes e indivíduos em geral, especialmente porque quanto mais tempo passa, mais dados são processados, criando uma linha da evolução performática do atleta. Tornou-se cada vez mais útil para os treinadores analisar os parâmetros de articulação, músculo, coração, respiratório, cadência e resistência de seus atletas, não só para desempenho, mas de forma mais crítica para fins de saúde e bem-estar (GUIMARÃES; AMÉRICO, 2017, p. 5-6).

Geralmente, as tecnologias vestíveis de estrutura rígida surgem no mercado por meio de grandes empresas, enquanto as que possuem suporte têxtil se encontram mais relacionadas às atividades acadêmicas e pesquisas independentes. A empresa *Wearable Experiments* criou projetos como o *Fundawear*, para a empresa de preservativos *Durex* e permite que pessoas com vestimentas íntimas tecnológicas consigam sentir a "reprodução do toque do parceiro em qualquer lugar". O casal realiza o cadastro no sistema do produto e acessa um aplicativo de simulação pelo celular. Trata-se de "um sistema de conexão sem fio que integra os *smartphones* e os *wearables* (roupas íntimas) do casal" (MARINI, 2017, p. 120).

Outro projeto de reprodução de toque da *Wearable Experiments* é o *Alert Shirt*, desenvolvido para a Foxtel, cuja:

> intenção é aproximar o telespectador das sensações dos jogadores. O usuário veste o *wearable*, uma camisa, e conectado ao sistema wireless, por meio do smartphone consegue, por exemplo, sentir o nervosismo do jogador ou o impacto quando ele cai através dos diversos atuadores da tecnologia vestível. Segundo descrito no site do WE:EX, Ben Moir explica que "o Alert Shirt pretende conectar seres humanos através de grandes distâncias e trazer emoções, frustrações e alegrias do jogo ativo para a vida de uma maneira que nós nunca fomos capazes de experimentar antes". As tecnologias vestíveis possibilitam novas experiências entre o corpo e o mundo de conexões wireless (sem fio). Os cinco sentidos do corpo humano não são capazes de perceber as informações digitais que estão em constantes fluxos de movimentações nos espaços urbanos. A incorporação do *wearable* proporciona uma nova percepção adquirida artificialmente ao corpo (MARINI, 2017, p. 121).

A mesma empresa também criou a tecnologia vestível *Navigate*, "um blazer, que auxilia o usuário na localização da cidade, conduzindo-o até o seu destino". Assim, permite a apreciação do espaço urbano por meio de uma experiência diferenciada, já que não é necessário ficar atento ao mapa na tela do referido dispositivo. A tecnologia utiliza *smartphones* e a "indicação de virar à direita ou esquerda é feita por meio de vibrações sutis

na roupa do lado direito ou esquerdo, respectivamente. Além disso, a frequência e a intensidade das vibrações indicam instruções específicas" (MARINI, 2017, p. 122).

Na área da saúde, até pouco tempo, "o monitoramento contínuo dos parâmetros fisiológicos só era possível no ambiente hospitalar". Contudo, "com os avanços no campo da tecnologia *wearable*, a possibilidade de monitoração precisa, contínua, em tempo real de sinais fisiológicos se tornou realidade". Os sensores de movimento "são baratos, pequenos e requerem muito pouca energia, tornando-se altamente atraentes para aplicações de monitoramento de pacientes" (KUMAR; ASHOK; VIGNESWARAN, 2015 *apud* GERALDO, 2018, p. 61).

Isso porque "as redes de sensores de corpo (BSNs) compreendem sensores portáteis ou implantados que coletam, processam e comunicam informações fisiológicas do corpo". Diante dos altos custos dos cuidados de saúde, é necessária uma abordagem mais eficiente em relação ao diagnóstico e tratamento. O *wearables* poderiam "revolucionar os cuidados de saúde, oferecendo monitores miniaturizados, discretos, para fornecer níveis sem precedentes de observação médica, reduzindo ao mesmo tempo a necessidade de visitas ao médico" (ASHOK; VIGNESWARAN, 2015 *apud* GERALDO, 2018, p. 61; ELLOUZE *et al*., 2014).

Tais tecnologias seriam capazes de detectar, comunicar e processar dados que auxiliassem os médicos na tomada de decisões clínicas, por meio de sensores portáteis e implantáveis de "eletrocardiograma (ECG), eletroencefalograma (EEG), sensores de glicose, acelerômetros, pressão arterial e saturação de oxigênio (SpO2), sensores de temperatura e até mesmo pílulas de câmera ingeríveis" (GERALDO, 2018, p. 61).

O *Google Glass* já é utilizado para a realização de cirurgias e têm ganhado popularidade na medicina "como ferramenta de ensino, registrando e transmitindo cirurgias a colegas ou alunos". Segundo o cirurgião cardiotorácico Pierre Theodore, "o principal benefício da utilização desse tipo de dispositivos na sala de cirurgia é tornar as informações mais acessíveis aos médicos constantemente para a tomada de decisões críticas". Para ele, o "fornecimento tecnologia de computação vestível para cirurgiões em partes remotas do mundo poderia ajudar na quebra das barreiras geográficas, ensinando-lhes técnicas cirúrgicas modernas através do *feedback* ao vivo durante a cirurgia" (KIM, 2013 *apud* MATOS, 2015, p. 786).

Dentre os fatores que influenciam a adoção de tecnologias vestíveis, destacam-se, segundo Cantanhede *et al*. (2018, p. 263) a "preferência dos usuários pela diferenciação social

a partir da obtenção de *status*, a utilização do dispositivo para fins hedônicos, que concedem momentos de prazer e diversão", podendo "a compra ser justificada por motivações utilitárias, sendo estas possibilitadas por intermédio da convergência de diversos elementos funcionais presentes neste dispositivo". Em razão do crescimento do número de serviços disponíveis, as tecnologias vestíveis tem ganhado cada vez mais importância no âmbito do mercado econômico e a tendência é que no futuro apresentem ainda mais funcionalidades (KAUFFMAN; SOARES, 2018, p. 514), já que se convertem em informações que propiciam ampliar e maximizar o campo de atuação e qualidades das empresas voltadas para o consumo (SOUSA; SILVA, 2020, p. 5). Assim, verifica-se que os algoritmos ligados a estes dispositivos representam ativos valiosos na era da informação e podem ser considerados verdadeira matéria-prima para a geração de dados no ambiente virtual.

3 DA UTILIZAÇÃO DE ALGORITMOS E DISPOSITIVOS DE INTELIGÊNCIA ARTIFICIAL DURANTE A PANDEMIA DA COVID-19

Em face da pandemia e da urgência por soluções rápidas e ágeis ao enfrentamento do vírus a serem adotadas pelas autoridades sanitárias, a coleta e a utilização de dados de diferentes fontes vêm sendo avultada para questões científicas, a partir de características dos indivíduos e dados de hospitais e laboratórios, informações que podem ser utilizadas desde que sigam parâmetros éticos e legais (ALMEIDA *et al*., 2020, p. 2488).

Muitos países, como China, Coreia do Sul, Singapura, Israel, Itália e França têm utilizado estratégias tecnológicas de inteligência artificial para o monitoramento remoto de pacientes e da população em geral, por meio de reconhecimento termal, monitoramento via *drones*, checagem de dados telefônicos, aplicativos de *tracking*, cruzamentos de geolocalização, uso de imagens de câmeras de segurança e transações de cartão de crédito com o objetivo de determinar possíveis locais de infecção e averiguar se as pessoas estão cumprindo as medidas sanitárias adotadas (FINKELSTEIN; FEDERIGHI; CHOW, 2020, p. 11-14).

Apesar da importância do enfrentamento ao vírus, tais medidas ainda levantam muitos questionamentos acerca da proteção de dados do usuário e de como estes serão utilizados pelo Estado tanto em tempos de crise como após o período de emergência. A criação de bancos de dados com informações dos cidadãos pode ser muito útil durante a tentativa de contenção da

pandemia, entretanto, esta não pode ser utilizada em desfavor do cidadão tanto pelo Estado como por empresas privadas caso não sejam estabelecidas regras específicas acerca da necessidade de ciência e do consentimento para a coleta e o tratamento de dados pessoais (TOBBIN; CARDIN, 2020). Em 2020, a NSO, empresa de *cyber* segurança israelense, que já vem sendo questionada no âmbito judicial, tendo em vista a acusação de espionar ativistas e jornalistas, está sendo acusada de manipulação e espionagem, por meio de dados do aplicativo *WhatsApp*, com o intuito de fortalecer regimes antidemocráticos, já que vem oferecendo a alguns governos um *software* que monitora telefones celulares, com o objetivo de conter a disseminação do vírus (CELLAN-JONES, 2020 *apud* FREITAS; CAPIBEIBE; MONTENEGRO, 2020).

Vale ressaltar que no Brasil, em abril de 2020, o governo federal editou a Medida Provisória (MP) 954, que obrigava empresas de telecomunicação a compartilharem dados como nomes, números de telefone celular e endereços com o Instituto Brasileiro de Geografia e Estatística (IBGE) para fins de continuidade da Pesquisa Nacional por Amostra de Domicílios Contínua durante o período da COVID-19, e foi declarada a sua inconstitucionalidade pelo Supremo Tribunal Federal, já que que não explicava de forma satisfatória qual era a finalidade do compartilhamento durante a pandemia de dados das empresas de telecomunicação com o IBGE, de modo que esta não especificava quando, como e para que seriam utilizados tais dados (FINKELSTEIN; FEDERIGHI; CHOW, 2020, p. 22). Durante a pandemia, as tecnologias vestíveis são eficientes para o rastreio e monitoramento de pacientes com sintomas relacionados ao novo *coronavírus*. O que se indaga é o que será feito com as informações e os dados pessoais dos cidadãos coletados durante a pandemia quando a situação de crise mundial acabar. Isto é, o risco de que estes sejam utilizados para além do contexto de prevenção e controle do vírus (REQUIÃO, 2020 *apud* FINKELSTEIN; FEDERIGHI; CHOW, 2020). Logo, apesar das potencialidades já destacadas dos *wearables*, essencial é que se investigue como se dá a coleta de dados pessoais do usuário destas tecnologias e os possíveis riscos do armazenamento e compartilhamento destes no contexto virtual de forma indevida e de modo a prejudicar o indivíduo no futuro, ofendendo os seus direitos da personalidade.

4 CAPITALISMO DE VIGILÂNCIA E PROTEÇÃO DE DADOS PESSOAIS

A Internet já faz parte do cotidiano das pessoas na sociedade pós-moderna e conecta indivíduos ao redor do globo e diminui distâncias e fronteiras. Diante disso, "criou-se um novo modelo de relacionamento, que alterou a organização e as estruturas sociais, políticas, econômicas e culturais, tornando a informação o eixo da sociedade", considerando sua dinamicidade e capacidade de produção. Logo, um grande volume de informações, que outrora se encontrava disposto de forma esparsa, passa a ser armazenado em conjunto e possibilita que estes dados possam ser utilizados tanto por governos como por empresas privadas (LEONARDI, 2012 *apud* OLIVEIRA; BARROS; PEREIRA, 2017, p. 573).

Este cenário faz com que vários setores sociais passem a se estruturar a partir do meio virtual e incentivem os indivíduos a compartilharem, divulgarem e postarem conteúdos e seus dados pessoais no ambiente virtual, de forma espontânea ou por meio da captura por empresas do ramo da informática, que objetivam utilizar tais dados para "fins pacíficos ou prejudiciais, para o Estado e para o usuário" (OLIVEIRA; BARROS; PEREIRA, 2017, p. 573). Até mesmo o próprio exercício da cidadania é gradativamente incentivado por meio do mundo virtual, uma vez que vários serviços e benefícios à população passaram a ser regulados e/ou requeridos por meio do preenchimento de cadastros e formulários *online* (TOBBIN; CARDIN, 2020).

Conforme Guimarães e Américo (2017, p. 2-3) a coleta de dados por meio de tais dispositivos acaba passando despercebida pelo usuário "devido ao funcionamento autônomo". Isto é, "seu processamento, obtenção da informação e de conteúdo, entre outros, continuam funcionando de maneira independente da interação ou da necessidade de ativação do usuário".

Assim, questiona-se: será que o usuário que utiliza uma tecnologia vestível tem o controle e a real dimensão da coleta e armazenamento de seus dados pelo aplicativo ou produto, compreendendo análises de algoritmos e a possibilidade de criação de perfis comportamentais para fins de publicidade, consumo e mercantilização? (TOBBIN; CARDIN, 2020). De acordo com Corso (2014, p. 14) é interessante observar que muitos usuários "não saberiam como agir caso estivessem inseridos em situações de vigilância envolvendo computadores vestíveis", mesmo que a relação entre sujeito e vigilância seja uma premissa básica da cibercultura pós-moderna. Conforme observa Magrani, "não se tem, hoje, clareza do tratamento dispensado aos dados. Aspectos sobre a coleta, o compartilhamento e o potencial uso deles por terceiros ainda são desconhecidos pelos consumidores" (MAGRANI, 2020, p. 36).

Os *wearables* não apenas reagem aos corpos dos usuários, "mas reconfiguram a si mesmos – atualizando modelos computacionais e programas de ação algorítmica da rede – e aos corpos com os quais se acoplam durante o fluxo das experiências de uso", já que são objetos sencientes, dotados de "sensibilidade performativa" – a capacidade de captar "sensações através de sensores e atuadores, produzir ações imediatas, futuras e sistêmicas em função de uma inteligência que deriva da coleta e do processamento computacional de dados". Logo, "não só reconfiguram os modelos dos serviços de saúde e cuidado como também convocam o corpo a exercer um novo papel na política econômica atual" (BITENCOURT, 2020, p. 159).

Em 2016, "a Oral Roberts University, universidade americana localizada em Tusla, Estado de Oklahoma, anunciou que passaria a exigir que todos os seus 900 calouros utilizassem um dispositivo vestível (*wearable*) para o monitoramento de atividades físicas da *Fitbit*", como "requisito à aprovação semestral nas disciplinas de educação física da instituição". Os estudantes deveriam "compartilhar, semanalmente, os dados de qualidade de sono, o número de passos e os batimentos cardíacos com o sistema da universidade". Como exigência, deveriam efetuar "10 mil passos diários e 150 minutos semanais de atividades em ritmo cardíaco intenso – parâmetros definidos pelas zonas de frequência cardíaca *Peak* e *Fat Burn1* do sistema *Fitbit*" (EL CLARÍN, 2016; FRANKEL, 2016 *apud* BITENCOURT, 2020, p. 158).

Ainda, a difusão das tecnologias vestíveis também tem se intensificado no âmbito corporativo, para medir a produtividade, bem como "para a redução de custos com seguros de saúde" (KAU, 2015; NIELD, 2014; OLSON; TILLEY, 2014) e para "políticas de gestão remota da saúde" (BIGGS *et al*., 2016; CAMPBELL, 2014; GEORGE, 2016; GOULD, 2016), ações que demonstram que os *wearables* cada vez mais representam "uma modalidade bem mais complicada de extrair e produzir informação". Em 2019, a marca *Fitbit*, "registrou um total de 29.6 milhões de usuários ativos distribuídos em 110 países, reassegurando o título de maior rede social fitness do planeta". Além disso, cerca de "6.5 milhões de clientes atualmente compartilham dados corporais com planos de saúde e serviços corporativos que compõem seu ecossistema" (FITBIT, 2017; FITBIT, 2018). Adquirida pela *Google*, no final de 2019, tem se destacado "no campo das pesquisas em monitoramento populacional para fins de gestão pública da saúde" (*apud* BITENCOURT, 2020, p. 158-159).

Como observa Bauman (2013, p. 20) atualmente, "os próprios usuários consentem em abandonar sua privacidade "em troca das maravilhas oferecidas na Internet", confundido o que "deveria ser público" com o que "deveria ser privado". Para o autor, diante do tema vigilância no contexto informático, questões como "anonimato, confidencialidade e privacidade não devem ser ignoradas", uma vez que estas constantemente se relacionam com "imparcialidade, justiça, liberdades civis e direitos humanos". Logo, os usuários passam a ter um "papel ativo em sua própria vigilância e fala em sociedade confessional, onde a vida social já se transformou em cibervida", visto que "o medo da exposição foi abafado pela alegria de ser notado" (BAUMAN, 2013, p. 29 *apud* CORSO, 2014, p. 5-6).

Apesar dos riscos quanto à coleta e o compartilhamento de dados pessoais, o discurso publicitário em torno das tecnologias vestíveis tende a somente enfatizar "performance corporal voltada à quantificação e à produção de dado como uma via para o autoconhecimento e para a otimização de si". Cita-se alguns slogans: "*Reveal more about your health and your heart*" (Fitbit Versa 2); "*Find inspiraton for miles with a deeper understanding of your body and health*" (Fitbit Charge 4); "*Sempre à vista, sempre de olho*" (Apple Watch S5); "*Aprimore-se e viva melhor*" (Xiaomi MiBand 4) (BITENCOURT, 2020, p. 161).

O isolamento provocado pela COVID-19 impulsionou uma espécie de retórica no campo político de "guerra ao novo *coronavírus*", o que estimulou a propositura de soluções voltadas à "digitalização da vida social" (BENNET; BERENSON, 2020; NIENABER; CARREL, 2020 *apud* MEDEIROS *et al*., 2020, p. 651). Tal contexto aqueceu o discurso de alguns governos de controle social e o monitoramento remoto em tempo real dos cidadãos que não respeitam o isolamento, apesar de estudos e pesquisas que relevarem que estes dados não seriam tão efetivos ao enfrentamento do vírus (RONDON; KOGAN, 2020 *apud* FREITAS; CAPIBERIBE; MONTENEGRO, 2020). Tal controle do Estado sobre o indivíduo e seus dados pessoais em tempos de crise provoca o debate acerca de Estados de vigilância, que são realidades não muitos distantes da atual, tendo em vista a hiperconectividade e o fato de que o exercício da cidadania é paulatinamente exercido no ambiente virtual.

Se já pairavam suspeitas quanto à privacidade do usuário e a possibilidade de monitoramento populacional em razão do uso de tecnologias, com a consequente violação de princípios democráticos e de direitos fundamentais, o caso Edward Snowden, que divulgou um complexo sistema de coleta de dados e monitoramento de cidadãos americanos e

personalidades importantes ao redor do globo, por parte da NSA e do governo dos Estados Unidos, evidenciou a necessidade de transparência quanto à coleta e o tratamento de dados, bem como o seu consentimento e riscos de utilização indevida (SANTIN; MAGRO; FORTES, 2017, p. 3-4).

Outro caso de repercussão internacional é o da *Cambridge Analytica*, empresa de consultoria que foi contratada pelo grupo que promovia o *Brexit* e, posteriormente, pela campanha de Donald Trump à presidência nas eleições americanas de 2016, e que comprou dados de mais de 50 milhões de usuário da rede social *Facebook*, sem que estes tivessem conhecimento ou consentissem acerca desta transação (BBC NEWS BRASIL, 2018).

A acusação é a de que a empresa utilizou tais dados para propagar conteúdos de acordo com interesses e preferências dos usuários, a fim de direcioná-los aos poucos para publicações e informações (verídicas ou não) que privilegiavam certos candidatos ou opiniões políticas em detrimento de outras. Isto é, com base nos dados do usuário é possível fomentar conteúdos democráticos ou antidemocráticos com maior probabilidade de adesão e compartilhamento.

Tal quadro evidencia que os dados pessoais do indivíduo relevam muitas informações acerca de seus interesses, opiniões, medos e, sobretudo, personalidade, de modo que podem ser utilizados para o desenvolvimento de algoritmos que padronizem e direcionem conteúdos de cunho comercial, político, publicitário e social, de acordo com a possibilidade de ocasionar maior impacto no usuário (BBC NEWS BRASIL, 2018).

Outro exemplo é que, em 2015, a empresa Uber ofereceu à cidade de Boston a possibilidade de acesso aos dados de viagens já realizadas naquela região pelo aplicativo. O intuito era melhorar o tráfego e o planejamento urbano. A Uber tem domínio sobre informações (dados) que auxiliariam muito as políticas públicas estatais voltadas para os grandes centros urbanos e o tráfego de veículos. Adverte Ramiro que por trás da narrativa de segurança, eficácia e otimização de serviços, é possível perceber intenções políticas, bem como éticas em relação às empresas que criam tais soluções e sistemas utilizados pelos agentes estatais e que podem violar os direitos humanos por meio da tecnologia (RAMIRO, 2019).

Como visualizam Bioni e Luciano, tais sistemas "carregam escolhas das entidades e pessoas envolvidas na sua construção, sendo modulados pela agenda política e aspectos socioeconômicos, de forma implícita ou explícita, que lhes são subjacentes". Além disso, todo

este cenário provoca implicações comportamentais e, sobretudo, quanto à identidade do sujeito, cuja construção tende a ser definida por meio de algoritmos e dispositivos de inteligência artificial. Conforme Calabrich (2020, p. 3) os algoritmos podem realizar diagnósticos, classificação e julgamentos que sirvam como base para decisões automatizadas, que podem ofender o indivíduo em várias esferas de sua vida, enquanto "empregado, eleitor, consumidor ou contratante (de planos de saúde, de financiamentos, de seguros etc.), réu ou parceiro sexual – para citar apenas algumas de suas praticamente incontáveis possibilidades de aplicação".

O grande risco é a possibilidade de análises simples e reducionistas, fundamentadas em caracteres físicos e vieses com premissas preconceituosas, ofendendo a dignidade humana por meio discriminação quanto à raça, cor, sexo, idade, origem, etnia etc. Deste modo, é fundamental que as políticas que envolvam a coleta e o tratamento de dados sejam específicas e assinalem de forma clara e concreta como e quando os dados serão utilizados, com vistas a impedir a utilização e o compartilhamento indevido, bem como algoritmos que tenham como base vieses preconceituosos e discriminatórios, que acentuem a desigualdade, ofendendo os direitos da personalidade do usuário, sobretudo de grupos vulneráveis.

5 DO COMPARTILHAMENTO DE DADOS SOBRE SAÚDE E A PROTEÇÃO DOS DIREITOS DA PERSONALIDADE

Diante da expansão das tecnologias e do mundo virtual, fundamental é investigar os direitos à privacidade e à proteção de dados dos usuários, tendo em vista que estes diariamente preenchem formulários *on-line*, baixam aplicativos com termos de uso que permitem o acesso de dispositivos e algoritmos a informações pessoais e particulares. Conforme disposto no art. 1º, inciso III, da Constituição Federal de 1988, é um dos fundamentos da República Federativa do Brasil, a dignidade da pessoa humana. Ainda, nos termos do art. 5º, inciso X, da Constituição, são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.

Para Magrani (2019) hodiernamente, para a tutela da dignidade humana é fundamental assegurar a proteção dos dados pessoais do usuário. Destaca-se que o tratamento de dados é uma atividade de risco, diante da possibilidade de coleta, exposição e utilização indevida e

abusiva; os dados podem não representar de forma correta o titular ou serem compartilhados sem o seu conhecimento ou consentimento. Os dados são a expressão direta da personalidade de seu titular, de modo que a sua tutela é imprescindível à dignidade humana (DONEDA, 2011).

A personalidade, segundo Szaniawski (2002, p. 35) corresponde ao conjunto de características únicas do indivíduo e inerentes à pessoa humana. "Trata-se de um bem, no sentido jurídico, sendo o primeiro bem pertencente à pessoa, sua primeira utilidade". É por meio da personalidade que a pessoa poderá adquirir e defender seus bens e direitos, entre eles, a vida, a honra, a liberdade etc. Os direitos da personalidade são mencionados em capítulo próprio no Código Civil de 2002, (arts. 11 a 21), contudo, muitos autores, como Elimar Szaniawski e Maria Celina Bodin de Moraes, compreendem que este rol não é taxativo, de modo que outros direitos não contemplados pelo Código também podem ser fundamentais para o desenvolvimento da personalidade humana, especialmente tendo em vista a constante evolução social e a dificuldade de o Direito acompanhar e regular todas as esferas e temáticas da ordem social ao tempo que estas são identificadas e reconhecidas (SZANIAWSKI, 2002).

Parte da doutrina também compreende que a dignidade da pessoa humana, prevista no art. 1º, inciso III, da Constituição Federal, anunciada como um dos fundamentos da República, seria uma cláusula geral de proteção da personalidade, protegendo o ser em sua totalidade, diante de toda e qualquer situação que implicasse em ofensa ao que o ser humano teria de mais caro, a sua individualidade e, consequentemente, personalidade (SZANIAWSKI, 2002).

A privacidade em uma sociedade cada vez mais hiperconectada não pode mais ser observada e conceituada como outrora, fato é que ganha novos delineamentos, sobretudo ante o crescente incentivo para que o usuário se torne conectado e compartilhe suas experiências em redes sociais, *blogs* e aplicativos e a importância concedida à obtenção de informações no mundo digital para o exercício da cidadania, entrada no sistema educacional e competitividade no mercado de trabalho. Na nova sociedade da informação, conforme Magrani (2019, p. 88) "a privacidade deve ser entendida de forma funcional, de modo a assegurar a um sujeito a possibilidade de conhecer, controlar, endereçar, interromper o fluxo das informações a ele relacionadas", bem como o direito de manter controle sobre suas próprias informações. Essa perspectiva "deriva do contexto social advindo de evoluções tecnológicas no qual a informação assume um papel de bem econômico" (MAGRANI, 2019,

p. 88) e "elemento estruturante para o desenvolvimento das relações sociais, sendo, pois, o signo maior desta anunciada e consolidada revolução socioeconômica" (BIONI, 2014 *apud* MAGRANI, 2019, p. 88).

Para Leonard (2011) o acesso "a sites gratuitos, como a referida rede social, é pago com os dados pessoais, devendo esta opção do usuário ser respeitada, pois válida, mas não significa a perda de controle das suas informações", tendo em vista "que devem ser adequadamente informados das concessões, assim como das trocas a serem realizadas, quando da opção pelo serviço gratuito". Entretanto, "admite a necessária melhoria das informações disponibilizadas para o usuário, inseridas em termos de uso e políticas de privacidade de websites, compostas de documentos longos, incompreensíveis e muitas vezes ignorados" (*apud* OLIVEIRA; BARROS; PEREIRA, 2017). É esperado que os produtos tecnológicos falhem, mas é essencial que se "faça o maior esforço técnico possível" para "enviá-los ao mercado como produtos adequados à utilização da coletividade, ou seja, somente após passarem por uma robusta fase de testes que reduzam o escopo de imprevistos" (MAGRANI, 2019, p. 65).

Para Magrani (2019, p. 71) outro problema seria a publicidade comportamental, que é capaz de "aumentar a assimetria de informação na relação de consumo, potencializar a discriminação entre os consumidores, minimizar a capacidade de escolha livre e autônoma do consumidor". Na atual sociedade digital, a "mercadoria mais valiosa de todas, como afirmou o economista americano Richard Rakos em 1992, é a informação". O que se discute hoje é o problema da "veiculação dos dados pessoais entre empresas privadas, transformando os dados em ativos comerciais, ou, como o Ministro Luiz Fux colocou no julgamento da ADI 6387, verdadeiras *commodities* informacionais". É o que ocorre em tempos de pandemia da COVID-19: "os dados são um ativo de marketing indispensável", já que "grande parte da população mundial está isolada em casa, sendo mais suscetível a receber publicidade por via digital" (FINKELSTEIN; FEDERIGHI; CHOW, 2020, p. 2).

A publicidade comportamento gera uma espécie de "confinamento informático ao qual são submetidos os usuários de ferramentas *on-line*", que é fruto de programação no âmbito da informática que tem por escopo determinar quais informações e conteúdos serão disponibilizados no ambiente virtual quando o indivíduo acessar suas redes sociais, realizar pesquisas em navegadores de busca, analisar preços em lojas virtuais etc. Tal programação é uma "sequência de comandos formulada por analistas de sistemas computacionais e que são

alimentados pelos dados dos próprios usuários", com base na Psicologia, Ética, Filosofia e Sociologia (PELLIZZARI; BARRETO JUNIOR, 2019, p. 58).

A impressão que o usuário pode ter é a de que os aplicativos e redes sociais lhe proporcionam experiências personalizadas em relação a conteúdos e sugestões conforme seus interesses pessoais, educação, ideais políticos, religiosos e personalidade. Contudo, o algoritmo aos poucos o direciona a ambientes que incentivam à compra de produtos e a polarização de debates, por meio de experiências de entropia e psicologia social (PELLIZZARI; BARRETO JUNIOR, 2019, p. 58; PAULICHI; CARDIN, 2020, p. 242). No âmbito dos *wearables*, que coletam dados acerca de batimentos cardíacos, índices de colesterol, temperatura corporal etc., aparentemente é difícil visualizar como tais dados poderiam ser monetizados ou transformados em informações que levassem à predição de comportamentos ou compra.

Entretanto, com a técnica de sensor de fusão, utilizada pelas tecnologias vestíveis, dados são recolhidos a partir de microssensores que, combinados, podem realizar inferências complexas. Dados que medem movimentos simples (estáveis ou tensos, rápidos ou devagar) do usuário podem inferir o nível de relaxamento, os dados sobre frequência cardíaca podem inferir níveis de estresse e as emoções, a qualidade do sono pode apontar irritabilidade. Além disso, outras atividades diárias, como a forma com que o usuário segura o telefone celular, a suavidade com que digita uma mensagem, a instabilidade de suas mãos, podem inferir emoções e estados mentais, prevendo eventuais hábitos e intenções futuras (PEPPET, 2014).

No Brasil, a Lei Geral de Proteção de Dados Pessoais (LGPD) dispõe, segundo o seu art. 1º, "sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado", com o objetivo de "proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural". Segundo o art. 2º, incisos I, III e VII, prescreve que no Brasil a disciplina da proteção de dados pessoais tem como fundamentos o respeito à privacidade, a inviolabilidade da intimidade, da honra e da imagem e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (BRASIL, 2018).

Para o art. 5º da Lei, considera-se dado pessoal "a informação relacionada a pessoa natural identificada ou identificável" e dado pessoal sensível o "dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de

caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural". (incs. I e II). (BRASIL, 2018).

O consentimento é definido pelo inciso XII do art. 5º como a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada". Além disso, conforme o art. 6º da LGPD, as atividades de tratamento de dados pessoas deverão observar a boa-fé e os princípios da finalidade, adequação, necessidade, livre acesso, qualidade, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas (BRASIL, 2018). A Lei prevê o direito do cidadão de não ser submetido a um tratamento discriminatório em sede de decisões automatizadas.

É diante deste cenário que surge o direito à autodeterminação informativa, um dos princípios da LGPD, na tentativa de proteger e dar maior controle ao titular quanto à utilização de seus dados pelo Estado e empresas privadas ligadas ao domínio da tecnologia. Para Sousa e Silva (2020) seria o direito do cidadão de decidir sobre a utilização de seus dados pessoais. Desta forma, o Estado deve propiciar formas de tutelar a privacidade dos indivíduos, um direito fundamental essencial ao livre desenvolvimento da personalidade. Além disso, tal direito pressupõe uma contrapartida do Estado para a sua proteção, ou seja, são necessárias políticas públicas relacionadas à privacidade e à proteção de dados.

O consentimento do usuário é, portanto, o "elemento central para a permissão do uso de seus dados pessoais (necessidade de "consentimento expresso, livre e informado sobre o tratamento dos dados pessoais"), mas tem se mostrado "ineficaz diante de recorrentes abusos contidos nos termos de uso dos provedores e seu descompasso com os direitos humanos". Ao mesmo tempo, "a necessidade de ter a todo momento um consentimento expresso verdadeiramente informado para o tratamento de dados irá impor um desafio enorme na prática para que seja realmente eficaz" (MAGRANI, 2019, p. 79).

A coleta, o compartilhamento e a utilização de dados em razão de crises de saúde pública, sobretudo por empresas privadas, devem ter termos e cláusulas claras e transparentes quanto ao acesso, uso e possíveis responsáveis em caso de ofensa a direitos do cidadão. Logo, é fundamental demonstrar por quem, quando e como os dados serão acessados, processados e utilizados; com que finalidade; como serão descartados; de que forma serão protegidos e quem será responsabilizado em caso de negligência ou abuso (ALMEIDA *et al*., 2020, p. 2490). Isto é, uma política de proteção de dados de saúde mais efetiva deve levar em

conta maior responsabilização das empresas que gerenciam os aplicativos e redes sociais, mas que não ocorre exatamente porque, aparentemente, o que as sustenta é exatamente esta rede de conexões e possibilidade de compartilhamento e utilização de dados como moeda de troca nas relações com governos e outras empresas privadas.

Essa talvez seja a grande questão que envolve as políticas de proteção de dados, uma vez que a sua coleta e utilização pode tanto beneficiar o indivíduo, diante das facilidades e funcionalidades da rede, como prejudicá-lo em contextos que envolvam seleção e julgamento de características, perfis e conteúdos com base em sua experiência virtual e que ainda não são tão próximos da compreensão do cidadão. É fato que não se questiona a possibilidade ou não de utilização de dados, mas sim os parâmetros desta medida, as metodologias utilizadas e o contexto de utilização, principalmente tendo em vista eventuais discriminações algorítmicas, erros, a utilização indevida, a comercialização e a monetização de dados, o vazamento de informações, a falta de transparência e de segurança, circunstâncias que vulnerabilizam o titular, uma vez que os dados são expressão de seus direitos fundamentais e personalidade.

6 CONCLUSÃO

Os *wearables* são dispositivos tecnológicos em plena expansão e prometem no futuro ter cada vez mais utilidades, facilitando o cotidiano de seus usuários, especialmente diante de suas potencialidades nas áreas da saúde, esportes, geonavegação, lazer e auxílio em atividades domésticas, além de serem artigos que agregam moda, estilo e *status* social, considerando a aquisição de cada aparelho em um contexto de inovações diárias e obsolescência programada.

Com a pandemia, a utilização de algoritmos e dispositivos de inteligência artificial permitiu que fossem encontradas soluções ao isolamento social. Contudo, tais tecnologias desencadeiam uma série de questionamentos relacionados à proteção de dados e à vigilância excessiva por parte de empresas de tecnologia e pelo Estado. Um dos grandes questionamentos levantados diante do uso destas tecnologias vestíveis é a coleta de dados dos usuários, que pode ir desde batimentos cardíacos, performance física, níveis de glicose e pressão arterial à perfis fisiológicos e padrões comportamentais. Isto é, dificilmente o usuário tem a real dimensão acerca da coleta e utilização de seus dados no contexto informático ou o controle deste compartilhamento pelo dispositivo no mercado ou com empresas privadas.

A grande discussão gira em torno dos direitos à privacidade, intimidade e de proteção de dados diante da constante vigilância e programação algorítmica com as quais os usuários destas tecnologias consentem diante da utilização destes aparelhos e o possível risco de que estes dados sejam utilizados para fins de consumo direcionado, publicidade abusiva, sugestividade de conteúdos e análise comportamental para fins de mercado e corporativismo. Ou seja, que esta coleta um dia possa ser utilizada em desfavor dos próprios usuários.

Diante da análise da legislação nacional acerca dos direitos da personalidade, especialmente direitos à privacidade e à proteção de dados pessoais, verifica-se que este são direitos fundamentais e essenciais à preservação da dignidade humana do usuário no ambiente digital. Além disso, verifica-se que há necessidade de que haja cada vez mais transparência por parte das empresas que fabricam as tecnologias vestíveis acerca da dimensão da coleta de dados e do risco de compartilhamento ou vazamento destes no mundo digital.

Por óbvio que diariamente é o próprio indivíduo que abre mão de nuances de seus direitos à privacidade e à proteção de dados pessoais em nome das benesses trazidas pelas inovações tecnológicas. Contudo, dificilmente este usuário/consumidor concordaria que seus dados fossem utilizados a seu revés para fins de discriminação, publicidade direcionada ou para a criação de perfis comportamentais. Ainda, em se tratando de tecnologia, conforme a opinião dos autores mencionados, sempre haverá vulnerabilidades e probabilidade de erro. Assim, é fundamental que o direito garanta que as empresas fornecedoras destas tecnologias vestíveis possuam cada vez mais expertise para a criação de produtos seguros e responsabilize ofensas aos direitos da personalidade em caso de uso, compartilhamento ou vazamento de dados.

Em uma sociedade em que a maior moeda de troca é a informação, é imprescindível que os cidadãos saibam como seus dados pessoais são utilizados pelo Estado, instituições e setor privado ligado à criação destas tecnologias. Além disso, o que se visualiza na prática é que a maioria das redes sociais, aplicativos e dispositivos informam o usuário acerca da coleta de dados, pedem acesso à localização, imagens e outras ferramentas do usuário, contudo, este consentimento é pouco esclarecido e geralmente, por meio de um simples clique, o usuário já cede todas estas informações "necessárias" para usufruir das praticidades do dispositivo.

Neste cenário, cresce a defesa do direito do usuário de proteção de seus dados pessoais e de que este tenha controle acerca do compartilhamento destes com autoridades estatais e empresas privadas, tendo em vista que estes dados são reflexo de sua personalidade, modo de

vida, funções fisiológicas e contexto social. Colocar sobre o usuário o peso exclusivo pelo compartilhamento de dados, considerando a necessidade de consentimento esclarecido, também parece não ser a melhor solução, uma vez que a utilização de aparelhos e dispositivos tecnológicos já é parte fundamental da vida cotidiana dos cidadãos e imprescindível à cidadania.

E, mesmo que o usuário descorde com o compartilhamento destes dados, por vezes este foge de seu alcance, como é o exemplo do caso internacional da compra de dados da rede social *Facebook* pela empresa de consultoria *Cambridge Analytica*. A grande questão é a privacidade dos dados do usuário e eventuais vieses preconceituosos, fundamentados em predição de comportamentos, criminalidade e segurança com base em características biológicas, de sexo, raça, idade, etnia etc. Logo, tendo em vista que os algoritmos são produzidos por pessoas humanas, eles também podem conter preconceitos e a visão corporativa/de mundo de seus idealizadores, de modo que seria fundamental uma análise multidisciplinar desde a sua elaboração e criação.

REFERÊNCIAS

ALMEIDA, Bethania de Araujo *et al*. Preservação da privacidade no enfrentamento da COVID-19: dados pessoais e a pandemia global. **Ciência & Saúde Coletiva**, v. 25, n. 1, jan./jun. 2020.

BAUMAN, Zygmunt. **Vigilância líquida**. Rio de Janeiro: Zahar, 2013.

BITENCOURT, Elias Cunha. "Coletamos dados para o seu bem" O truque retórico do imaginário sobre o dado digital promovido nos termos de uso, documentos de privacidade e relatórios de investidores da plataforma Fitbit. **Revista Texto Digital**, v. 16, n. 1, 157-182, 2020.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, [2014]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 14 ago. 2020.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 10 set. 2020.

CALABRICH, Bruno Freire de Carvalho. Discriminação algorítmica e transparência na Lei Geral de Proteção de Dados Pessoais. **Revista de Direito e as Novas Tecnologias**, v. 8, n. 8, p. 1-18, jul./set. 2020.

CANTANHEDE, Lorena Renata Costa *et al*. Comportamento do consumidor de tecnologia vestível: características que influenciam na intenção de consumo. **ReAd – Revista Eletrônica de Administração**, Porto Alegre, v. 24, n. 3, p. 244-268, set./dez. 2018.

CORSO, Aline. Reflexões sobre Privacidade e Vigilância na Era dos Computadores Vestíveis. *In*: SIMPÓSIO NACIONAL DE ABCiber – COMUNICAÇÃO E CULTURA NA ERA DE TECNOLOGIAS MIDIÁTICAS ONIPRESENTES E ONISCIENTES, 8., 2014, São Paulo. **Anais** [...]. 2014, ESPM: São Paulo.

DONEDA, Danilo. A proteção de dados pessoais como um direito fundamental. **Espaço Jurídico**, Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011.

ELLOUZE, Nourhene *et al*. Security of implantable medical devices: limits, requirements, and proposals. **Security and Communication Networks**, v. 7, n. 12, p. 2475-2491, 2014.

FINKELSTEIN, Carlos; FEDERIGHI, André Catta Petra; CHOW, Beatriz Graziano. O uso de dados pessoais no combate à Covid-19: lições a partir da experiência internacional. **Revista Brasileira de Inteligência Artificial – RBIAD**, v. 1, n. 1, 2020.

FREITAS, Christiana Soares de; CAPIBERIBE, Camila Luciana Góes; MONTENEGRO, Luísa Martins Barroso. Governança Tecnopolítica: Biopoder e Democracia em Tempos de Pandemia. **Revista NAU Social**, v. 11, n. 20, p. 191-201, maio/out. 2020.

GERALDO, Ana Cristina Ferreira. **Tecnologias vestíveis aplicadas à saúde da coluna vertebral**. 2018. 237 f. Dissertação (Mestrado em Tecnologias da Informação e Comunicação – Universidade Federal de Santa Catarina, Araranguá, 2018.

GUIMARÃES, Lúcia Nobuyasu; AMÉRICO, Marcos. Tecnologia Vestível Digital aplicada ao esporte profissional: uma nova vertente na hibridização entre moda e tecnologia. *In*: COLÓQUIO DE MODA, 13., 2017, Bauru, SP. **Anais** [...]. 2017, UNESP: Bauru, 2017.

KAUFFMAN, Marcos E.; SOARES, Marcelo Negri. New technologies and data ownership: wearables and the erosion of personality rights. **Revista de Direitos Sociais e Políticas Públicas**, v. 6, n. 1, 2018.

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

MARINI, Patrícia Sayuri Saga Kitamura. As tecnologias vestíveis de moda e a relação entre humano e não-humano. **Moda Palavra**, v. 10, n. 19, p. 116-134, 2017.

MATOS, Davi Sousa. As tecnologias vestíveis no setor médico e seus desafios. SIMPÓSIO DE ENGENHARIA DE PRODUÇÃO DE SERGIPE, 7., 2015, São Cristóvão. **Anais** [...]. 2015, UFS: São Cristóvão, 2015. p. 783-790.

MEDEIROS, Breno Pauli *et al*. The use of cyberspace by the public administration in the COVID-19 pandemic: diagnosis and vulnerabilities. **Revista de Administração Pública**, Rio de Janeiro, v. 54, n. 4, p. 650-662, jul./ago. 2020.

MING, Damien K. *et al*. Continuous physiological monitoring using wearable technology to inform individual management of infectious diseases, public health and outbreak responses. **International Journal of Infectious Diseases**, v. 96, p. 648-654, maio 2020.

NEGRI, Sergio Marcos Carvalho de Ávila; OLIVEIRA, Samuel Rodrigues de Oliveira; COSTA, Ramon Silva. O uso de tecnologias de reconhecimento facial baseadas em inteligência artificial e o direito à proteção de dados. **Revista de Direito Público**, v. 17, n. 93, 2020.

O escândalo que fez o Facebook perder US$ 35 bilhões em horas. **BBC News Brasil**, 20 mar. 2018. Disponível em: https://www.bbc.com/portuguese/internacional-43466255. Acesso em: 14 ago. 2020.

OLIVEIRA, Rafael Santos; BARROS, Bruno Mello Correa de; PEREIRA, Marília do Nascimento. O direito à privacidade na internet: desafios para a proteção da vida privada e o direito ao esquecimento. **Revista da Faculdade de Direito da UFMG**, Belo Horizonte, n. 70, p. 561-594, jan./jun. 2017.

PAULICHI, Jaqueline Silva; CARDIN, Valéria Silva Galdino. Das formas de inteligência artificial e os impactos nos padrões de consumo e a proteção dos direitos da personalidade. **Meritum**, v. 15, n. 4, 2020.

PELLIZZARI, Bruno Henrique; BARRETO JUNIOR, Irineu Francisco. Bolhas Sociais e seus efeitos na sociedade da informação: ditadura do algoritmo e entropia na Internet. **Revista de Direito, Governança e Novas Tecnologias**, v. 5, n. 2, p. 57-73, jul./dez. 2019.

PEPPET, Scott R. Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent. **Texas Law Review**, v. 93, p. 85-176, 2014.

RAMIRO, André. Psicopolíticas: vigilância e segregação no reconhecimento facial. **Instituto de Pesquisa em Direito e Tecnologia do Recife**, 7 out. 2019. Disponível em: https://ip.rec.br/2019/10/07/psicopoliticas-vigilancia-e-segregacao-no-reconhecimento-facial/. Acesso em: 6 set. 2020.

SANTIN, Thais Dagostini; MAGRO, Diogo Dal; Fortes, Vinícius Borges. Estado de vigilância e democracia: uma análise da dimensão pública e privada da internet frente a violação do direito fundamental à privacidade. *In*: CONGRESSO INTERNACIONAL DE DIREITO E CONTEMPORANEIDADE: MÍDIAS E DIREITOS DA SOCIEDADE EM REDE, 4., Santa Maria, 2017. **Anais** [...]. Santa Maria: UFSM, 2017. p. 1-15.

SCHERER, Felipe. Como as tecnologias vestíveis estão criando novas oportunidades. **Exame**, 24 fev. 2017. Disponível em: https://exame.com/blog/inovacao-na-pratica/como-as-tecnologias-vestiveis-estao-criando-novas-oportunidades/. Acesso em: 14 ago. 2020.

SOUSA, Rosilene Paiva Marinho de; SILVA, Paulo Henrique Tavares da. Proteção de dados pessoais e os contornos da autodeterminação informativa. **Informação & Sociedade**: Estudos, João Pessoa, v. 30, n. 2, p. 1-19, abr./jun. 2020.

SZANIAWSKI, Elimar. **Direitos de personalidade e sua tutela**. São Paulo: Revista dos Tribunais, 2002.

TOBBIN, Raíssa Arantes; CARDIN, Valéria Silva Galdino. Perfis informacionais e publicidade comportamental: direito à autodeterminação informativa e a proteção de dados pessoais no ambiente virtual. **Anais do Congresso Brasileiro de Processo Coletivo e Cidadania**, n. 8, p. 1260-1276, 2020.