XXIX CONGRESSO NACIONAL DO CONPEDI BALNEÁRIO CAMBORIU - SC

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS III

DANIELLE JACON AYRES PINTO

MARCOS VINÍCIUS VIANA DA SILVA

D597

Direito, governança e novas tecnologias III [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Danielle Jacon Ayres Pinto; Marcos Vinícius Viana da Silva.

– Florianópolis: CONPEDI, 2022.

Inclui bibliografia
ISBN: 978-65-5648-625-3
Modo de acesso: www.conpedi.org.br em publicações
Tema: Constitucionalismo, Desenvolvimento, Sustentabilidade e Smart Cities

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direito. 3. Governança e novas tecnologias.

XXIX Congresso Nacional do CONPEDI Balneário Camboriu - SC (3: 2022: Florianópolis, Brasil).

CDU: 34

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

XXIX CONGRESSO NACIONAL DO CONPEDI BALNEÁRIO CAMBORIU - SC

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS III

Apresentação

O XXIX Congresso Nacional do CONPEDI – Balneário Camboriú, em seu Grupo de trabalho Direito, Governança e Novas Tecnologias, apresentou temas relacionados às novas tecnologias, seus impactos na vida em sociedade, o papel do Estado nas demandas internacionais e o papel central ocupado pela governança nestes cenários.

Assim, a presente apresentação introduz os artigos apresentados no GT, informando desde já, que os temas se completam e permitem o devido aprofundamento teórico prático.

O primeiro trabalho apresentado, de autoria de Sílvia Helena Schimidt e Romulo Rhemo Palitot Braga, e denominada "SEGURANÇA HUMANA E PROTEÇÃO DE DADOS: DOS RISCOS DA DISCRIMINAÇÃO ALGORÍTMICA EM TEMPOS DE COVID-19" enfrenta os riscos da discriminação algorítmica durante a pandemia da COVID-19 e os direitos da personalidade. A pesquisa analisou os contornos do capitalismo de vigilância à proteção de dados do usuário, a problemática do reconhecimento facial e seu eventual viés preconceituoso e discriminatório.

Na sequencia o artigo intitulado "VÍDEOS VEICULADOS NO YOUTUBE: ARTE OU INCITAÇÃO AO SUICÍDIO?", de Manoella Miranda Keller Bayer e Eduardo Biavatti Lazarini, discorre sobre a dificuldade de compatibilizar o rápido desenvolvimento da tecnologia frente ao ritmo mais lento de atualização do direito, tratando em especial dos vídeos veiculados no youtube e a responsabilidade civil atrelada.

O artigo das autoras Agatha Gonçalves Santana, Raíza Barreiros e Andreza Maria Nascimento De Mattos, intitulado "OS IMPACTOS TECNOLÓGICOS NOS SERVIÇOS PÚBLICOS NO BRASIL: A FORMAÇÃO DE UMA ADMINISTRAÇÃO PÚBLICA DIGITAL", traz a questão da Administração Pública no contexto tecnológico e seus serviços prestados. Questiona-se se o Brasil está vivenciando uma transformação de sua Administração Pública, a ponto de se poder afirmar haver de fato a observância de uma Administração Pública Digital no âmbito dos serviços públicos.

Na sequência os autores Gustavo Ferraro Miranda e Raphael da Rocha Rodrigues Ferreira, apresentaram o artigo "PROCESSO DE DEMOCRATIZAÇÃO DA PROTEÇÃO DOS

DADOS PESSOAIS E PRIVACIDADE: UM ESTUDO COMPARADO E HISTÓRICO PARA A REFLEXÃO DO CASO BRASILEIRO", tal trabalho trata da democratização da proteção de dados pessoais e privacidade no caso brasileiro à luz do cenário internacional, realizando uma análise do desenvolvimento histórico da autodeterminação informativa e de sua vinculação aos direitos da personalidade,

"O DEVIDO PROCESSO LEGAL NA ERA DOS ALGORITMOS: UMA PROPOSTA DE RELEITURA DOS PRINCÍPÍOS CONSTITUCIONAIS DE PROCESSO CIVIL" é obra da autoria de José Antonio de Faria Martos, Oniye Nashara Siqueira e José Sérgio Saraiva, discorre sobre a elevação do patamar tecnológico experimentada pela sociedade desde o advento da internet proporcionou ao Poder Judiciário a modificação expressiva da gestão processual.

"CONSIDERAÇÕES ACERCA DA REGULAÇÃO TRANSNACIONAL PARA O DESENVOLVIMENTO ÉTICO DA INTELIGÊNCIA ARTIFICIAL", de Hernani Ferreira e Jose Everton da Silva, demonstra como a discussão inovadora relativa a IA poderá facilitar a criação de uma legislação transnacional, baseada em uma ética global.

"O DIREITO FUNDAMENTAL À INFORMAÇÃO FRENTE AO ACESSO DESIGUAL ÀS TECNOLOGIAS DE COMUNICAÇÃO NO BRASIL" da autoria de Mariana Mostagi Aranda e Zulmar Antonio Fachin, apresenta uma reflexão sobre o direito fundamental à informação e a internet frente ao acesso desigual às tecnologias de comunicação, em especial o direito fundamental de informação e comunicação, a partir das limitações de acesso aos meios de comunicação digital e da internet no Brasil.

"A UTILIZAÇÃO DA INTELIGÊNCIA ARTIFICIAL PARA APRECIAÇÃO DE PEDIDOS DE TUTELA PROVISÓRIA DA EVIDÊNCIA EM CARÁTER LIMINAR" da lavra de Bruno Berzagui e Jose Everton da Silva, enfrenta a possibilidade de utilização da inteligência artificial (IA) para apreciação de pedidos de tutela provisória de evidência em caráter liminar, de forma mais específica nestes casos, uma vez que dependem de prova já constituída em decisão que cabe reversão.

"RESPONSABILIDADE CIVIL DO MÉDICO PELO USO DA INTELIGÊNCIA ARTIFICIAL NOS PROCEDIMENTOS ESTÉTICOS", escrito por Divaneide Ferreira Dos Santos e José Carlos Francisco dos Santos, aborda a responsabilidade do médico em procedimentos estéticos utilizando a Inteligência Artificial (IA) e examinar quais direitos e

obrigações são devidos à relação de consumo entre médico e paciente, identificando também as formas pelas quais o erro médico é reparado, especialmente sob a tutela do Código de Defesa do Consumidor.

A obra dos autores Eduardo Lincoln Domingues Caldi e Zulmar Antonio Fachin é intitulada: "A COLONIZAÇÃO DIGITAL DA ESFERA PESSOAL DO INDIVÍDUO E VIOLAÇÕES AO DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS", e aborda a colonização digital da esfera pessoal do indivíduo e seu impacto no direito fundamental à proteção de dados pessoais, discutindo como o movimento de extração dos dados pessoais ocorre frente ao posicionamento do Direito contemporâneo.

O artigo intitulado "ARTICULAÇÕES EPISTEMOLÓGICAS E A CONVERGÊNCIA INTERDISCIPLINAR DA CIÊNCIA DA INFORMAÇÃO COM A CIÊNCIA JURÍDICA NO CONTEXTO DIGITAL" da autoria de Marcos Alexandre Biondi e José Carlos Francisco dos Santos enfrenta as articulações da epistemologia tradicional e suas limitações perante a epistemologia complexa. Evidenciando a interdisciplinaridade entre a Ciência da Informação e a Ciência Jurídica no contexto contemporâneo digital.

O artigo intitulado "A ALGORITMIZAÇÃO DO PROCESSO: NUANCES SOBRE OS PROJETOS DE INTELIGÊNCIA ARTIFICIAL NO PODER JUDICIÁRIO", redigido por Oniye Nashara Siqueira, José Antonio de Faria Martos e José Sérgio Saraiva debruça sobre a desatualização do sistema de justiça brasileiro, que digitalizou o sistema processual, porém não otimizou sua utilização, em claro atraso na aplicação de diferentes possibilidades tecnológicas.

Os autores Andrey Luciano Bieger, Reginaldo Pereira e Idir Canzi apresentam o trabalho intitulado "PREVALECE NO SUPREMO TRIBUNAL FEDERAL O CARÁTER FRACO DA PRECAUÇÃO? PROBLEMATIZAÇÕES A PARTIR DO JULGAMENTO DO RECURSO EXTRAORDINÁRIO 627.189/SP", o qual aborda a interpretação do princípio da precaução a partir do julgamento do Recurso Extraordinário 627.189/SP, informa que a compreensão deferida por cada julgador pode representar resultados completamente distintos em um mesmo caso.

Os autores Marcelo Markus Teixeira, Reginaldo Pereira e Idir Canzi apresentam o trabalho intitulado "TRANSNORMATIVIDADE E GOVERNANÇA DE RISCOS SOCIOAMBIENTAIS DE NOVAS TECNOLOGIAS", discutindo, entre outros, como as novas tecnologias (ainda que apresentam riscos socioambientais), possibilitam a superação de distintas adversidades, conferindo base material para a economia informacional.

Os autores Frederico Thaddeu Pedroso, Gabriel Lima Mendes e Isabel Christine Silva De Gregori apresentam a obra “O USO DO SISTEMA DE GEOLOCALIZAÇÃO DE APLICATIVOS DE STARTUPS EM TEMPOS DE PANDEMIA COVID-19: UMA RELAÇÃO DE BIOPOLÍTICA E SURVEILLANCE A PARTIR DE FOUCAULT”, narrando as relações da biopolítica como sistema de poder e controle dos indivíduos com o uso do sistema de geolocalização de aplicativos de Startups que visam a localização de seus usuários em tempos de pandemia COVID-19.

A obra intitulada “A IMPORTÂNCIA DA REGULAMENTAÇÃO LEGAL DAS STARTUPS POR MEIO DA UTILIZAÇÃO DA PROPRIEDADE INTELECTUAL COMO PROPRULSORA DA SEGURANÇA JURÍDICA E DO SEU CRESCIMENTO EXPONENCIAL”, de Frederico Thaddeu Pedroso e Gabriel Lima Mendes, aborda a importância das inovações tecnológicas promovidas por empresa startups, bem como a respeito da possibilidade de implantação jurídica desse modelo no âmbito da propriedade intelectual.

O texto de Ana Paula Bustamante, Eduardo Dos Santos Pereira e Ruan Silva Gomes, intitulado “DIREITO E TECNOLOGIA: INTELIGÊNCIA ARTIFICIAL E FERRAMENTAS TECNOLÓGICAS COMO CATALISADORES PROCEDIMENTAIS NO PODER JUDICIÁRIO”, expõe como o Poder Judiciário brasileiro padece de uma crise procedimental em razão da quantidade exorbitante de processos distribuídos, e que somente a aplicação tecnológica permitirá a redução desta quantidade que apenas aumenta.

Por fim, o trabalho “ESTRATÉGIA JURÍDICA: ONLINE DISPUTE RESOLUTION - ODR COMO INSTRUMENTO A RESOLUÇÃO EXTRAJUDICIAL DE CONFLITOS”, de autoria de Gustavo Silva Macedo e Frederico de Andrade Gabrich, analisa a viabilidade da plataforma Online Dispute Resolution (ODR) como estratégia jurídica viável para acesso do cidadão à justiça, preferencialmente sem a judicialização dos conflitos relativos aos direitos patrimoniais disponíveis.

Por todo este conteúdo, os trabalhos do GT do Conselho Nacional de Pesquisa em Direito, renderam uma tarde profícua de produção intelectual aplicada ao bom serviço do Sistema Nacional de Pós-Graduação na área do Direito.

Tenham uma excelente leitura.

Dra. Danielle Jacon Ayres Pinto.

Dr. Marcos Vinícius Viana da Silva.

SEGURANÇA HUMANA E PROTEÇÃO DE DADOS: DOS RISCOS DA DISCRIMINAÇÃO ALGORÍTMICA EM TEMPOS DE COVID-19

HUMAN SECURITY AND DATA PROTECTION: THE RISKS OF ALGORITHMIC DISCRIMINATION IN TIMES OF COVID-1

Sílvia Helena Schimidt
Romulo Rhemo Palitot Braga

Resumo

O presente artigo tem por objetivo analisar os riscos da discriminação algorítmica durante a pandemia da COVID-19 aos direitos da personalidade. Assim, a pesquisa analisou os contornos do capitalismo de vigilância à proteção de dados do usuário, a problemática do reconhecimento facial e seu eventual viés preconceituoso e discriminatório e a propagação da desinformação por ocasião da crise sanitária, por meio de bolhas sociais virtuais. Para tanto, o trabalho utilizou o método hipotético-dedutivo, fundamentado em pesquisa e revisão bibliográfica de obras, artigos de periódicos, legislação e jurisprudência. Como resultado, verificou-se que durante a pandemia houve um aumento exponencial quanto à utilização de algoritmos e dispositivos de inteligência artificial, especialmente tendo em vista a necessidade de isolamento social e a prevenção do contágio da doença. Entretanto, é fundamental garantir que tais ferramentas sejam elaboradas com base em tendências democráticas, em respeito à igualdade e à dignidade humana, bem como aos direitos à privacidade, à intimidade, à autodeterminação informativa, à saúde, à informação e à imagem, principalmente de grupos vulneráveis.

Palavras-chave: Direito à saúde, Direitos da personalidade, Discriminação algorítmica, Inteligência artificial, Lei geral de proteção de dados

Abstract/Resumen/Résumé

This paper aims to analyze the risks of algorithmic discrimination in COVID-19 times to personality rights. Thus, the research examined the survillance capitalism to protection of data user, the question of face recognition and its eventuals prejudiced and discriminatory bias and the propagation of misinformation during the health crisis in virtual social bubbles. Therefore, the work used the hipothetical-deductive method, based on bibliografic review of books, articles, legislation and court decisions. As a result, it was found that during the pandemic there has been a exponential increase of the use of algorithms and devices of artificial intelligence, especially because the need to social isolation and the prevention of disease contagion. However, it is essencial to garantee that this tools are developed based on democratic trends, in respect to equality and human dignity, as well as the rights to privacy, intimacy, self determination, health, information and image, mainly concerning vulnerable groups.

Keywords/Palabras-claves/Mots-clés: Right to health, Personality rights, Algorithmic discrimination, Artificial intelligence, Geral data protection law

1 INTRODUÇÃO

Em razão da crise de saúde pública ocasionada pela pandemia da COVID-19 e da consequente necessidade de isolamento social proposto ao redor do mundo, tendo em vista a inexistência, até o presente momento, de imunização eficaz, 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.

Nesse contexto, surgem discussões quanto à aplicabilidade desses sistemas inteligentes, assim como de eventuais vieses discriminatórios e que colocam em risco os direitos fundamentais e de personalidade do cidadão, especialmente quanto à proteção de dados, o acesso à informação, direito à saúde e casos de racismo, sexismo e preconceito propagados pela discriminação algorítmica em face de grupos vulneráveis.

Desta forma, o presente artigo tem por objetivo analisar os riscos da discriminação algorítmica aos direitos da personalidade no cenário pandêmico, especialmente de grupos vulneráveis. Logo, escolheu três situações específicas que envolvem a inteligência artificial e a COVID-19: a vigilância excessiva e seus reflexos na privacidade, autodeterminação informativa e proteção de dados; a utilização do reconhecimento facial e os riscos de políticas que adotem caracteres físicos, biológicos e fenótipos para a predição de comportamentos e da criminalidade; e o cenário de desinformação provocado pela propagação de *fake news* no ambiente virtual, que prejudica o acesso à saúde e à informação.

Para tanto, o trabalho utilizou o método hipotético-dedutivo, fundamentado em pesquisa e revisão bibliográfica de obras, artigos de periódicos, legislação e jurisprudência aplicável. O artigo compreendeu pesquisa por meio das bases de dados SSRN, Scielo, Google Acadêmico e EBSCO, buscando artigos e material em revistas científicas ligadas à área do Direito, bem como da Saúde, tendo em vista que a proposta do artigo é contextualizada a partir da análise de fatores que envolvem a pandemia da COVID-19. Quanto à legislação, foram analisados dispositivos da Constituição Federal e da Lei de Geral de Proteção de Dados (Lei nº 13.709/2018). Já em relação à jurisprudência, foi examinada a questão levantada em sede do julgamento que declarou a inconstitucionalidade da Medida Provisória nº 954, de 2020.

No primeiro capítulo abordar-se-á a utilização de algoritmos e dispositivos de inteligência artificial em razão da crise sanitária ocasionada pelo novo *coronovírus*, bem como as vantagens e os riscos ligados à elaboração e à utilização destas inteligências, especialmente quanto a eventuais vieses preconceituosos, discriminatórios, propostos por agendas privadas e

que desrespeitem a necessidade de proteção de dados e os direitos da personalidade, sobretudo de grupos vulneráveis.

O segundo capítulo tem por objetivo analisar os contornos do capitalismo de vigilância em tempos de COVID-19 e a necessidade de proteção de dados devido ao monitoramento remoto, diante da possibilidade de coleta, tratamento e compartilhamento de dados no ambiente virtual por parte de empresas privadas e pelo Estado, examinando a retórica de vigilância como forma de segurança no âmbito das políticas de biopoder.

No terceiro capítulo do desenvolvimento realizar-se-á o exame do reconhecimento facial em tempos de COVID-19 para a contenção da propagação de vírus e os riscos de que esta política represente premissas preconceituosas e de predição de comportamento relacionadas a caraterísticas biológicas e físicas, promovendo discriminação e preconceito.

O quarto capítulo abordará a temática das *Fake News* no ambiente virtual e como estas interferem na disseminação da desinformação quanto à prevenção e contenção da COVID-19, de modo a prejudicar o acesso à saúde e a fomentar o discurso reacionário e antidemocrático no contexto de bolhas sociais, promovidas pelos algoritmos e aplicativos de inteligência artificial.

2 DA UTILIZAÇÃO DE ALGORITMOS E DISPOSITIVOS DE INTELIGÊNCIA ARTIFICIAL DURANTE A PANDEMIA

Diante da necessidade de prevenção do novo *coronavírus* e da contenção de novos surtos, muitos países ao redor do mundo adotaram estratégias envolvendo o uso de tecnologias, a coleta de dados pessoais, o monitoramento remoto populacional, políticas de reconhecimento facial, para verificar o cumprimento das medidas de segurança, e a adoção de estratégias de *e-government*, com a utilização de aplicativos para fornecer serviços e benefícios aos cidadãos.

Como demonstram Santin, Magro e Fortes (2017, p. 3), a Internet já faz parte do cotidiano das pessoas na sociedade pós-moderna, uma vez que 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", tendo em vista sua dinamicidade e capacidade de produção.

De acordo com Sousa e Silva (2020, p. 5), hodiernamente, a Internet é considerada um importante recurso para o fornecimento de informações, em razão da rapidez e facilidade com que estes conteúdos e dados circulam neste ambiente, o que permite o aumento do contingente

de documentos disponíveis ao usuário. 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*.

Assim, recai sobre o aparato governamental a difícil tarefa de se aprofundar em medidas e propostas de *e-governmet*, adaptando a comunicação e serviços para o atendimento em rede, levando em conta as diferenças econômicas e sociais entre os cidadãos. Todavia, é fundamental mencionar que tal inserção social no ciberespaço "é passível de exploração por uma miríade de atores capazes de operacionalizar as lógicas e peculiaridades do universo digital segundo agendas particulares" (MEDEIROS *et al.*, 2020, p. 652).

Conforme Pellizzari e Barreto Junior, os algoritmos representam ativos valiosos na era da informação e podem ser considerados verdadeira matéria-prima para a geração de dados. A inteligência artificial propicia a criação de algoritmos de inteligência artificial que possuem a capacidade de aprender com a própria experiência e conseguem distinguir de forma autônoma as variáveis mais adequadas para sanar determinado percalço (PELLIZZARI; BARRETO JUNIOR, 2019, p. 61). Tal cenário provoca questionamentos acerca da proteção destes dados pessoais, da necessidade de controle e transparência acerca de quando e como serão utilizados e dos riscos do surgimento de eventuais Estados de vigilância, alheios à observância de ideais democráticos em razão da hodierna hiperconectividade.

Neste ponto, 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 com terceiros 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, a doutrina majoritária compreende 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.

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 Federativa do Brasil, 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).

Neste contexto, Almeida *et al*. (2020) destaca que para uma governança responsável em relação a dados pessoais é essencial a descrição de metodologias de processamento, a análise de padrões e de predições dos algoritmos utilizados. A metodologia utilizada tem papel essencial para legitimar medidas e ampliar a confiança na credibilidade destes sistemas, especialmente quanto à possibilidade de eventuais vieses, valores e suposições que possam distinguir opiniões de evidências e dados científicos.

Conforme pontua Calabrich:

> o maior problema que se erige sobre o tema da discriminação algorítmica, contudo, diz respeito à realização concreta dos direitos do titular do dado que seja prejudicado por um tratamento indevidamente discriminatório, especialmente seu direito de explicação – e seu correlato dever de transparência por parte do controlador –, considerando as próprias peculiaridades da tecnologia hoje empregada para o tratamento de dados pessoais. Explicação (ou explicabilidade) e transparência são as palavras-chave para que qualquer decisão amparada no tratamento de dados pessoais possa ser identificada como racionalmente justificável ou ilicitamente discriminatória. Implementar tais atributos ao tratamento automatizado de dados pessoais é o desafio que se apresenta a controladores, operadores, autoridades responsáveis pela aplicação da lei e aos próprios titulares dos dados pessoais (CALABRICH, 2020, p. 12).

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).

Assim, uma vez que a evolução da inteligência artificial e a utilização de algoritmos e aplicativos *online* já é parte do cotidiano das pessoas, é fundamental garantir que estas tecnologias respeitem os direitos fundamentais dos usuários, especialmente tendo em vista a necessidade de proteção de dados pessoais. Em razão da pandemia da COVID-19, a discriminação algorítmica, fruto de vieses preconceituosos, baseados em cor, raça, sexo, faixa etária, entre outros, ofende os direitos da personalidade e a dignidade humana do indivíduo, sobretudo, a privacidade e o acesso à saúde, em um momento tão delicado da história humana.

3 PROTEÇÃO DE DADOS E CAPITALISMO DE VIGILÂNCIA

É uma das características da sociedade pós-moderna a vida compartilhada e ambientada no contexto virtual, de modo que há tempos se fala nas facilidades e, ao mesmo tempo, consequências, da vida hiperconectada, que pode trazer uma gama de benefícios ao usuário, mas também deixá-lo vulnerável em relação à privacidade e à proteção de dados pessoais, que podem ser utilizados pelo Estado e por empresas privadas, o que inevitavelmente representa riscos ao exercício da cidadania e à própria democracia.

Tal discussão é importante já que cada vez mais os dados processados são valorados pelos mercados tecnológico e econômico, 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).

Em face da pandemia e da urgência por soluções rápidas e ágeis ao enfrentamento do vírus a serem adotadas pelas autoridades sanitárias diante dos desafios por ele colocados em relação à saúde da população mundial, a coleta e a utilização de dados de diferentes fontes vem 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).

A China foi o primeiro país a enfrentar o vírus e rapidamente implementou uma série de estratégias, tais como: o "controle de trânsito; o uso de câmeras de medição de temperatura corporal; a utilização pela polícia de capacete de reconhecimento termal; o mapeamento epidemiológico; o monitoramento via drones"; o uso de "*software* para reconhecimento facial

e medida de temperatura; a checagem de dados telefônicos para verificar contato com infectados" (FINKELSTEIN; FEDERIGHI; CHOW, 2020, p. 11).

A Coreia do Sul investiu pesado em testagens rápidas e massivas da população, bem como em entrevistas, cruzamento de geolocalização, *tracking*, uso de algoritmos, imagens de câmeras de segurança e transações de cartão de crédito com o objetivo de determinar locais de infecção (FINKELSTEIN; FEDERIGHI; CHOW, 2020, p. 14). Já o governo de Singapura, em conjunto com o Ministério da Saúde, desenvolveu um aplicativo de *tracking* que é capaz de, por meio de *Bluetooth*, identificar cidadãos expostos ao vírus e utilizar tal informação para elaborar uma rede de possíveis contatos, a fim de alertar pessoas que poderiam ser infectadas com a doença (FINKELSTEIN; FEDERIGHI; CHOW, 2020, p. 14).

Israel, que já possuía uma política de vigilância massiva, alterou as regras de privacidade e o compartilhamento de dados pessoais para que o Ministério da Saúde tivesse acesso a informações presentes nos celulares dos cidadãos durante a pandemia. A nova regulamentação prevê novas políticas de geolocalização e *tracking* (FINKELSTEIN; FEDERIGHI; CHOW, 2020). A França passou a utilizar sistemas de inteligência artificial para monitorar se os franceses estavam cumprindo as regras estipuladas pelo governo, da mesma forma que a Itália, principalmente a região da Lombardia, utilizou dados de geolocalização para averiguar movimentos da população e analisar a observância do isolamento social (FINKELSTEIN; FEDERIGHI; CHOW, 2020, p. 19).

Mesmo com a contenção do contágio, as previsões recentes apontam que os próximos meses serão de adaptação ao vírus, de modo que a utilização de aplicativos e dispositivos que permitem a coleta de dados pessoais terão papel de destaque não somente na medição do contato, mas também "para finalidades como verificar o cumprimento do isolamento, de quarentena, de verificação probabilística de contágio, do gerenciamento de permissões para a pessoa sair em público, entre muitas outras" (ALMEIDA *et al*., 2020, p. 2488-2489).

No campo das inovações tecnológicas, os *wearables*, que são relógios, óculos, pulseiras, joias, e-têxteis e tecidos inteligentes, ganham cada vez mais destaque em razão de suas funcionalidades (MATOS, 2015, p. 783-784). Para Guimarães e Américo, as tecnologias vestíveis podem ser conceituadas como tecnologias que utilizam o corpo humano como apoio, sendo digitais e integradas (com acesso à Internet ou *Bluetooth*) e que podem coletar e transmitir dados para computadores, *smarthphones* e transformá-los em informações acerca do usuário mediante uma *interface* (GUIMARÃES; AMÉRICO, 2017, p. 3). Logo, tais tecnologias coletam dados dos indivíduos e geram discussão quanto à utilização destes por empresas privadas.

Além disso, 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). Conforme elucidam Freitas, Capiberibe e Montenegro, a narrativa que fundamenta tais ações:

> supõe que o bem-estar – traduzido, no momento, por controle e eliminação da covid-19 – viria com uma vigilância maior sobre as ações cotidianas dos cidadãos, garantindo-os um mínimo de bem-estar. Para tanto, seria necessário o uso de rastreadores e outros artefatos para a extração de dados de celulares, possível com parcerias estabelecidas com operadoras de telefonia. Identificar padrões de movimentos das pessoas e verificar se as pessoas estariam seguindo recomendações do governo de distanciamento social seriam algumas das atividades que justificariam tal uso. Entretanto, a maioria das ações governamentais vem sendo implementadas sem considerar questões como a estipulação de um prazo de duração da vigilância ou o tipo de proteção de privacidade que seria garantida ao cidadão durante o processo (FREITAS; CAPIBERIBE; MONTENEGRO, 2020, p. 193).

Para Finkelstein; Federighi e Chow (2020, p. 9) "a quantidade de meios tecnológicos utilizados para a gestão da crise da COVID-19 é infindável". Ao longo do ano de 2020, já foram utilizados "dados de geolocalização; passaportes de imunidade; câmeras térmicas; tecnologias de reconhecimento facial; *contact tracing*, *tracking*, etc". 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).

O sistema funciona utilizando um mapa de calor, que mostra os locais que apresentam o maior número de casos. Estes dados poderiam ser utilizados para antecipar medidas sanitárias. A empresa alega que não terá acesso aos dados que são monitorados, mas que necessita de informações fornecidas pelas empresas de telecomunicações (CELLAN-JONES, 2020 *apud* FREITAS; CAPIBEIBE; MONTENEGRO, 2020, p. 193).

Como visto, o monitoramento remoto populacional tem sido uma estratégia utilizada por vários Estados para tentar conter a disseminação e a propagação da COVID-19. Contudo,

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 e cumpridas regras específicas acerca da necessidade de ciência e do consentimento para a coleta e o tratamento de dados pessoais.

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. Segundo Balkin (2008), o Estado de Vigilância:

> caracteriza-se pela coleta, ordenamento e análise de dados, usando-os na identificação de possíveis ameaças à segurança, na prestação de serviços sociais e na governança da população. A segurança nacional é utilizada como argumento, pelos governos, para realizarem a mineração de dados. No entanto, o processamento dessas informações pode ser utilizado para diversos finis, inclusive na obtenção de vantagens políticas e econômicas entre nações. (*apud* SANTIN; MAGRO; FORTES, 2017, p. 3).

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 e disponibilizar 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, que não utilizavam a coleta de dados e as redes sociais como massa de manobra política e ideológica. Isto é, com base nos dados do usuário é

possível fomentar conteúdos democráticos ou antidemocráticos com maior probabilidade de adesão e compartilhamento em rede.

Aliás, é exatamente neste cenário que tendem a ganhar voz discursos extremistas, reacionários e antidemocráticos, ainda tutelados pelo senso comum de que a Internet é terra de ninguém e que por meio de perfis *fakes* e *bots* replicadores de mensagens é possível dizer o que se pensa, mesmo que vá contra o Direito ou ofensa os direitos de outras pessoas. É a escusa do direito à liberdade de expressão para a propagação de discurso do ódio.

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). De acordo com Fornasier e Beck, um dos ensinamentos que o escândalo da *Cambridge Analytica* apresenta é que:

> infelizmente se está fadado a apenas um único e fatídico episódio de (i) usurpação de dados pessoais, (ii) de coleta de informações em grande quantidade e de forma continuada e (iii) que podem tecer toda uma narrativa comportamental de quem é cada indivíduo. Mesmo que essas narrativas sejam verossímeis, indivíduos serão sempre mais do que apenas métricas; conjuntos de indicadores transformados em estatística e logo permitindo que algumas conclusões sejam inferidas (FORNAZIER; BECK, 2020, p. 189).

Tanto o caso Snowden como o da *Cambridge Analytica* demonstram que a dinâmica de coleta, tratamento e utilização de dados pessoais em rede ainda é muito desconhecida pelo usuário. Geralmente, este aceita participar de uma rede social, se identifica para realizar compras *online* ou preenche formulários que lhe beneficiam, entretanto, não concorda ou tem a dimensão da utilização de seus dados por agendas privadas e pelo Estado. Como aponta Estrada (2016) os aplicativos e dispositivos tecnológicos hoje existentes captam dados a cada minuto que o cidadão anda na rua, estaciona seu carro e utiliza seu *smartphone* ou cartão de crédito. Assim, diante da utilização e tratamento destes dados, surgem questões como a criação de "perfis, discriminação, exclusão, vigilância do governo e perda de controle" (*apud* MAGRANI, 2019, p. 62).

Conforme Freitas; Capiberibe e Montenegro, a pandemia realçou a existência de práticas biopolíticas, tendo em vista a necessidade do enfrentamento deste problema de saúde pública. No caso específico do combate ao novo *coronavírus*, aos poucos se delineia uma narrativa de que há uma necessidade de "acesso aos dados pessoais como imprescindíveis à

ordem, ao bem-estar e ao desenvolvimento humano – seja lá o que isso signifique" (FREITAS; CAPIBERIBE; MONTENEGRO, 2020, p. 194-195).

Como afirmam Freitas, Capiberibe e Montenegro (2020, p. 195-196; ZUBOFF, 2015), o capitalismo de vigilância se fundamenta na coleta e na utilização de dados pessoais. Assim, as empresas de tecnologia, o setor que mais é beneficiado com este contexto, cria parcerias com governos que passam a depender a cada dia mais do fluxo dos dados que são gerenciados por estas empresas privadas. 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. Isso porque 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.

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 dados sejam utilizados para além do contexto de prevenção e controle do vírus (REQUIÃO, 2020 *apud* FINKELSTEIN; FEDERIGHI; CHOW, 2020).

No Brasil, em abril de 2020, o governo federal editou a Medida Provisória (MP) 954, que obrigava empresas de telecomunicação a compartilharem dados, tais 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 (PNAD Contínua) durante o período da COVID-19. Embora a medida contemplasse o descarte destes dados pelo IBGE em no máximo trinta dias após o fim do estado de emergência e proibisse o seu compartilhamento com empresas privadas ou órgãos públicos, foram apresentadas cinco ações diretas de inconstitucionalidade perante o Supremo Tribunal Federal, questionando os seus delineamentos (FINKELSTEIN; FEDERIGHI; CHOW, 2020).

Em sede de julgamento da ADI 6387, dez dos onze ministros da Corte entenderam que a MP 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. Para Finkelstein, Federighi e Chow (2020, p. 22), a decisão "preocupando-se com a possibilidade de surgimento de um verdadeiro Estado de vigilância".

É diante deste cenário que surge o direito à autodeterminação informativa, 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. Com a autodeterminação informativa, tem-se por objetivo assegurar:

> um direito constitucional de personalidade que tem por objeto o poder do indivíduo sobre três aspectos: de decidir sobre a divulgação e o uso dos seus dados pessoais; de decidir sobre quando e dentro de quais limites esses dados podem ser revelados; e, por fim, de ter conhecimento sobre quem sabe e o que sabe sobre ele, além de quando e em que ocasião (FINKELSTEIN; FEDERIGHI; CHOW, 2020, p. 24).

Para Sousa e Silva, o direito à autodeterminação informativa 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 (SOUSA; SILVA, 2020, p. 11).

Conforme Zanini *et al*. (2018, p. 2018) "o processo de socialização das relações patrimoniais, capitaneado pelo direito constitucional, não deve ser trazido para o campo das relações extrapatrimoniais", uma vez que se estaria diante de uma atuação prejudicial por parte do Estado, visto que o íntimo da personalidade humana e sua dignidade não podem ser subordinadas completamente ao interesse público, tendo em vista que há uma dimensão individual e privada da pessoa humana essencial para o desenvolvimento de sua personalidade.

O aprimoramento e o desenvolvimento de novas tecnologias são fundamentais para a sociedade pós-moderna, de modo que o que se espera é que se alcance um equilíbrio entre elas e o direito, especialmente em relação a políticas e à implementação de pseudonimização em bases de dados no âmbito da saúde. A pandemia é um teste para as democracias liberais e "esse momento não pode implicar em retrocessos nas liberdades individuais". Para tanto, é fundamental um debate público a respeito da forma com que os dados pessoais serão tratados pelas autoridades sanitárias, com o intuito de impedir a vigilância excessiva e intrusiva, que vem ocorrendo em diversos países em redor do globo (FINKELSTEIN; FEDERIGHI; CHOW, 2020, p. 27). Assim, também é fundamental:

> (i) realizar uma avaliação a respeito da necessidade de políticas de saúde centradas em dados, assim como quais são suas necessidades e objetivos, amparando-se na ciência; (ii) definir proporcionalidade do tratamento de dados, para fim de restringir a intervenção na esfera privada; (iii) definir rigidamente o ciclo de vida dos dados e a forma de descarte; (iv) garantir ampla transparência a todos os processos; (v) estabelecer salvaguardas específicas e concretas a todos os processos. (FINKELSTEIN; FEDERIGHI; CHOW, 2020, p. 26).

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.

Logo, é essencial a defesa do direito à autodeterminação informativa, já delineado pela Lei Geral de Proteção de Dados, em seu art. 2º, inciso II (BRASIL, 2018) e pelo Supremo Tribunal Federal em 2020, e que tem por objetivo dar maior controle ao cidadão quanto à coleta, o tratamento, o compartilhamento e os limites da utilização de seus dados; direito que é essencial para a subsistência de regimes democráticos, o exame de biopolíticas e a repressão de vigilância indevida e exaustiva. Isso porque é essencial um debate público e colaborativo quanto à política de utilização de dados pessoais, de forma que a utilização destes ocorra à luz da transparência, segurança, da adoção de medidas específicas e com limites bem estabelecidos, que não deixem dúvidas quanto às finalidades e os riscos de compartilhamento indevido e arbitrário.

4 RECONHECIMENTO FACIAL, PRECONCEITO E DISCRIMINAÇÃO

A segurança nos centros urbanos demanda constante atuação por parte do Estado, sendo um grande desafio às autoridades públicas, logo, a possibilidade de reconhecimento facial de criminosos e suspeitos por meio de programas de inteligência artificial que envolvem vigilância e controle social tem ganhado adesão por governos.

Negri, Oliveira e Costa citam exemplos do uso de tecnologias de reconhecimento facial para fins de vigilância ao redor do mundo:

> na China, 200 milhões de câmeras compõem um sistema de vigilância capaz de identificar basicamente qualquer um dos 1.4 bilhões de habitantes do país. Em Dubai, capital dos Emirados Árabes Unidos, um gigantesco "túnel-aquário" localizado no principal aeroporto da cidade conta com mais de 80 câmeras de segurança, que capturam e digitalizam, por meio de escâneres, o rosto das pessoas à medida que caminham por ele; por fim, realizada a análise das imagens obtidas, o sistema de segurança ou permite que a pessoa ingresse livremente no país ou emite um alerta, indicando a necessidade de uma análise mais aprofundada acerca da entrada do indivíduo. Nos Estados Unidos da América, no ano de 2016, ao menos 50% dos cidadãos adultos já constavam em bases de dados de reconhecimento facial do governo (NEGRI; OLIVEIRA; COSTA, 2020, p. 83).

No Brasil, destaca-se o programa "Rio+Seguro", da cidade do Rio de Janeiro, que corresponde a um *software* de reconhecimento facial e tem por intuito identificar e deter suspeitos e foragidos. Já na Bahia, o projeto "Vídeo Policiamento" é uma ferramenta que tem por escopo reconhecer criminosos e a intenção é que no futuro identifique toda a população do estado (NEGRI; OLIVEIRA; COSTA, 2020, p. 83-84).

Conforme Vu (2018), as técnicas de reconhecimento facial têm por intuito auxiliar diante da incapacidade do cérebro humano de processar, memorizar e identificar as milhares de faces com as quais se depara todos os dias. O desenvolvimento de programas nesse âmbito foi intensificado após os ataques terroristas em setembro de 2001, nos Estados Unidos, de modo que "agências governamentais têm se utilizado de todos os meios para desenvolver maneiras eficientes e precisas de regular o afluxo de pessoas por meio da identificação dos indivíduos", com o objetivo de "garantir que nenhuma ameaça conhecida seja permitida, pois, argumenta-se, isso pode colocar em risco os cidadãos de uma sociedade" (*apud* NEGRI; OLIVEIRA; COSTA, 2020, p. 86).

De acordo com Misugi, Freitas e Efing (2016, p. 436) o potencial das tecnologias de reconhecimento facial já chamou atenção de grandes empresas como a *Apple* e o *Google*. Estima-se que cerca de 1,35 bilhões de pessoas utilizem ativamente a rede social *Facebook*, que já conta com mais de 250 bilhões de fotos publicadas, com a identificação da foto do perfil, uma vez que a rede social faz uso de uma política de "identidade real", para que o usuário mantenha a veracidade de suas informações pessoais, sob pena de exclusão da conta. Deste modo, todos podem ser identificados mediante um sistema de reconhecimento facial (MISUGI; FREITAS; EFING, 2016, p. 436).

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. Logo, o controle passa a ser baseado em uma "análise moral complexa de caráter, que avalia o comportamento, a identidade, a aparência e o comportamento da pessoa por meio das lentes de relevância específica do contexto" (NEGRI; OLIVEIRA; COSTA, 2020, p. 93-94).

Conforme Norris (2003) alguns grupos, como negros, mulheres e homens jovens são mais vulneráveis em relação a análises de sistemas de vigilância, que não se baseiam em critérios objetivos ou comportamentais individualizados, realizando somente análises fundamentadas em suspeitas categóricas, que abrem margem para exames discriminatórios (NEGRI; OLIVEIRA; COSTA, 2020, p. 93). Acerca disso, Ramiro pontua que:

> é possível situar a IBM no atual centro dessas questões: foi documentado que o Departamento de Polícia de Nova York fornecia filmagens de câmeras de vigilância para que a empresa desenvolvesse sistema de reconhecimento facial baseado no tom de pele, o que poderia ser usado, consequentemente, para o monitoramento de minorias étnicas. Para além das sérias questões sobre o fornecimento de dados de toda uma coletividade para uma companhia privada, sem política de privacidade ou escrutínio público, estabelecer critérios raciais e étnicos para criar *targets* sobre suspeitos pode ser considerada uma política de perseguição mascarada por uma agenda de segurança pública. Outra investigação, liderada pela Human Rights Watch, aponta para o fornecimento de tecnologia de reconhecimento facial ao programa de segurança pública filipino, encabeçado por Rodrigo Duterte, chefe de Estado famoso pela perseguição e assassinato de dissidentes políticos através de seus "esquadrões da morte". Aqui, a identificação facial possibilitada pela tecnologia é aplicada à supressão das liberdades políticas, uma crescente expressão da vigilância governamental (RAMIRO, 2019).

Já a cidade de São Francisco baniu o uso do reconhecimento fácil no âmbito das agências governamentais e constatou que o uso de tecnologias que objetivam a vigilância somente poderia se dar mediante relatório específico comprovando os reais benefícios à área de segurança pública, de forma a superar os impactos aos direitos humanos. Na China, sistemas de vigilância já são elaborados com o intuito específico de marginalizar minorias, especialmente na região de Xinjiang, fronteira chinesa com países como o Cazaquistão, Afeganistão e o Paquistão, onde tais sistemas segregam minorias, monitorando e controlando a imigração de muçulmanos na região (RAMIRO, 2019).

Para Ramiro, há ainda o risco de que inteligências artificiais sigam correntes da Medicina e Psicologia já rechaçadas pelas ciências criminais, a exemplo da *fisiognomia*, que propõe a identificação da personalidade com base na topografia facial; políticas segregacionistas raciais do século XIX e utilizadas pelo regime nazista; ou a *frenologia*, popularizada por Cesare Lombroso, que associava traços faciais à propensão de cometimento de delitos (RAMIRO, 2019). No Brasil, a Constituição Federal de 1988, em seu art. 3º, inciso IV, pontua ser um dos objetivos fundamentais da República "promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação".

Já a Lei Geral de Proteção de Dados (LGPD) em seu 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).

A Lei Geral de Proteção de Dados prevê de forma expressa o direito do cidadão de não ser submetido a um tratamento discriminatório em sede de decisões automatizadas. Essa previsão "é extraída não só do art. 20 mas também dos arts. 1º, 2º, e, principalmente, de seu art. 6º, que é categórico, em seu inciso IX, ao estatuir que as atividades de tratamento de dados pessoais deverão observar a boa-fé e o princípio da não discriminação", que não permite a realização de tratamento com intuitos discriminatórios, ilícitos ou abusivos (CALABRICH, 2020, p. 6).

Contudo, como pontua Ramiro (2019) a Lei Geral de Proteção de Dados brasileira não abrange "regras prévias ao uso de tecnologias críticas baseadas no uso de dados biométricos por políticas públicas de vigilância", de modo que o seu art. 4º, incisos I e II (tratamento de dados pessoais para fins de segurança pública e defesa nacional) ratifica eventuais programas de reconhecimento facial (BRASIL, 2018). O autor afirma que "a sociedade civil deve ser manter atenta aos rumos que o monitoramento social pode tomar, sobretudo no que se refere às finalidades políticas e segregacionistas que essas tecnologias podem carregar". Natta *et al*. adverte que:

> without adequate regulation, unmonitored inaccuracies may inadvertently harm individuals who are flagged while attempting to shop, travel, or work and who, absent robust regulations, may have little recourse for rectification. In the event that individuals' health profiles are logged continuously in the form of virtual, multimodal immunity certificates, such harms could be ongoing in discriminatory ways [...]. Furthermore, studies have shown that facial recognition algorithms demonstrate algorithmic bias. Such bias against protected categories, such as race, sex, nationality, or religion, may be illegal in applications such as employment and housing (NATTA *et al*., 2020, p. 11).

Como exemplo de problemas com a utilização de programas de reconhecimento facial Magrani (2019) apresenta o algoritmo utilizado pelo Registro de Motores de Massachusetts, EUA, que equivocadamente etiquetou um indivíduo como criminoso e revogou sua carteira de motorista. Já quanto à possibilidade de tendências racistas e sexistas no âmbito da inteligência artificial e do *learning machine*, o autor cita o caso do perfil robótico Tay, da empresa *Microsoft*, que foi criado para interagir na rede social *Twitter* e que, em menos de 24 horas, se converteu em *bot* de propagação de ofensas racistas e discurso de ódio.

Logo, a problemática que envolve o reconhecimento facial é a o risco de análises simples e reducionistas, fundamentadas em caracteres físicos e vieses com premissas

preconceituosas e que atinjam o direito à imagem e a privacidade do indivíduo, ofendendo sua dignidade humana por meio de conduta discriminatória quanto à raça, cor, sexo, idade, origem, etnia, etc.

Conforme Calabrich (2020, p. 3) tais sistemas de inteligência artificial podem ser utilizados para a definição de perfis pessoais, profissionais, de crédito, de consumo ou concernentes a aspectos da personalidade. 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".

Durante a pandemia, a discriminação algorítmica baseada no reconhecimento facial pode afetar a contratação no mundo corporativo de pessoas que se encontram dentro de grupos vulneráveis; obstaculizar o acesso à saúde, tendo em vista programas com análises simplistas e baseadas em vieses preconceituosos ligados ao sexo e a questões raciais, étnicas e de faixa etária mediante escolhas de sistemas que privilegiem certas pessoas em detrimentos de outras; e constranger indivíduos no âmbito de ações de segurança pública, fundamentadas no exame da criminalidade por meio de predição de comportamentos e caraterísticas faciais.

6 CONCLUSÃO

Com a pandemia, a utilização de algoritmos e dispositivos de inteligência artificial cresceu de forma exponencial e permitiu que fossem encontradas soluções ao isolamento social por meio de algoritmos e aplicativos. Contudo, tais tecnologias desencadeiam uma série de questionamentos relacionados à proteção de dados e à possibilidade de discriminação algorítmica, especialmente em face de grupos vulneráveis.

Uma das problemáticas que tomou novos delineamentos em razão da pandemia é a retórica da vigilância como forma de segurança, promovida pelo capitalismo contemporâneo, baseado na coleta, no tratamento e compartilhamento de dados para fins de predições informacionais e publicidade comportamental. Com a pandemia da COVID-19, países ao redor do mundo adotaram estratégias envolvendo o monitoramento remoto populacional para prever locais e conter possíveis surtos da doença, bem como verificar o cumprimento de medidas de segurança por parte da população. Contudo, tais políticas aos poucos delineiam uma vigilância excessiva, baseada em dados pessoais e que pode ser utilizada por políticas de biopoder, tanto

democráticas como antidemocráticas, e que possuem o condão de ofender os direitos à privacidade e à autodeterminação informativa.

Já a possibilidade de reconhecimento facial por meio da tecnologia é uma discussão que permeia os direitos à imagem e à privacidade diante de eventuais vieses preconceituosos, fundamentados em predição de comportamentos, criminalidade e segurança com base em características biológicas, fenótipos, 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 para que não ofendessem direitos de grupos vulneráveis, como mulheres, negros, idosos, índios, etc.

Outra problemática abordada pelo trabalho é a propagação das *fake news* no contexto das bolhas sociais no ambiente virtual. As notícias falsas prejudicam o acesso à informação de qualidade, promovem a desinformação e obstam o acesso à saúde, tendo em vista que no cenário pandêmico proliferam nas redes sociais a indicação de medicamentos sem comprovação científica quanto à eficácia contra o vírus, receitas caseiras e questionamentos quanto às medidas sanitárias adotadas em prol da contenção da transmissão da doença. As *fake news* deixam vulneráveis, sobretudo, os idosos, grupo de maior risco e que deveria receber informações quanto à prevenção do vírus e ter o acesso à saúde facilitado. Sem contar que as bolhas sociais são utilizadas para propagar teorias conspiracionistas e ataques à democracia, já que são massa de manobra e manipulação política e ideológica.

Desta forma, visualiza-se que os questionamentos apontados pela pesquisa giram em torno da proteção e gestão de dados pessoais no ambiente virtual por empresas privadas e pelo próprio Estado. Diante do cenário de pandemia é essencial o desenvolvimento de estratégias referentes à tecnologia para o controle da propagação do vírus diante da necessidade de isolamento social, principalmente enquanto não houver imunização total e medicamento eficaz.

É certo que o desenvolvimento de tecnologias está sujeito a falhas e erros, de modo que também é esperado que estas necessitem de ajustes quando constatadas irregularidades. Contudo, existem riscos previsíveis, que podem ser identificados desde a elaboração dos algoritmos e aplicativos, essencialmente quanto a vieses, tendências, contexto ideológico, político e mercadológico.

De modo que também é fundamental que as políticas que envolvam a coleta, o tratamento e o compartilhamento de dados sejam específicas e assinalem de forma clara e concreta como e quando os dados do usuário serão utilizados, com vistas a impedir a utilização e o compartilhamento indevido, bem como algoritmos que tenham como base vieses

preconceituosos, discriminatórios e antidemocráticos, que acentuem a desigualdade, ofendendo os direitos da personalidade do usuário, sobretudo de grupos vulneráveis.

REFERÊNCIAS

ALMEIDA, Bethania de Araújo *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. Disponível em: https://www.scielo.br/pdf/csc/v25s1/1413-8123-csc-25-s1-2487.pdf. Acesso em: 6 set. 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.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [2016]. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/ Constituiçao.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. Disponível em: https://dspace.almg.gov.br/bitstream/11037/38411/1/Bruno%20Freire%20de%20Carvalho%20Calabrich.pdf. Acesso em: 7 out. 2020.

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

GALHARDI, Cláudia Pereira *et al*. Fato ou Fake? Uma análise da desinformação frente à pandemia da Covid-19 no Brasil. **Ciência & Saúde Coletiva**, v. 25, n. 2, p. 4201-4210, 2020. Disponível em: https://scielosp.org/pdf/csc/2020.v25suppl2/4201-4210/pt. Acesso em: 20 nov. 2020.

GUESS, Andrew; NAGLER, Jonathan; TUCKER, Joshua. Less than you think: Prevalence and predictors of fake news dissemination on Facebook. **Science Advances**, v. 5, n. 1, eaau4586, jan. 2019. Disponível em: https://advances.sciencemag.org/content/5/1/eaau4586. Acesso em: 4 set. 2020.

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. Disponível em: http://www.coloquiomoda.com.br/anais/Coloquio%20de%20Moda%20-%202017/COM_ORAL/co_1/co_1_TECNOLOGIA_VESTIVEL_DIGITAL.pdf. Acesso em: 15 ago. 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.

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. Disponível em: https://rbiad.com.br/index.php/rbiad/article/view/7. Acesso em: 10 out. 2020.

FORNASIER, Mateus de Oliveira; BECK, Cesar. Cambridge Analytica: escândalo, legado e possíveis futuros para a democracia. **Revista Direito em Debate**, v. 29, n. 53, p. 182-195, 2020. Disponível em: https://www.revistas.unijui.edu.br/index.php/revistadireitoemdebate/article/view/10033. Acesso em: 20 nov. 2020.

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

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.

MERCEDES NETO *et al*. Fake News no cenário da pandemia de COVID-19. **Revista Cogitare Enfermagem – UFPR**, v. 25, e72627, 2020. Disponível em: https://revistas.ufpr.br/cogitare/article/view/72627. Acesso em: 4 set. 2020.

MISUGI, Guilherme; FREITAS, Cinthia Obladen de Almeida; EFING, Antônio Carlos. Releitura da privacidade diante das novas tecnologias: realidade aumentada, reconhecimento facial e Internet das Coisas. **Revista Jurídica Cesumar**, v. 16, n. 2, p. 427-453, maio/ago. 2016. Disponível em: https://periodicos.unicesumar.edu.br/index.php/revjuridica/article/view/4433/2804. Acesso em: 10 set. 2020.

NATTA, Meredith Van *et al*. The rise and regulation of thermal facial recognition technology during the COVID-19 pandemic. **Journal of Law and the Biosciences**, v. 7, n. 1, p. 1–17, jan./jun. 2020. Disponível em: https://doi.org/10.1093/jlb/lsaa038. Acesso em: 6 set. 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. Disponível em: https://portal.idp.emnuvens.com.br/direitopublico/article/view/3740. Acesso em: 10 set. 2020.

NORRIS, Clive. From personal to digital CCTV, the panopticon, and the technological mediation of suspicion and social control. *In*: LYON, David. **Surveillance as social sorting**: privacy, risk, and digital discrimination. Routledge: New York, 2003.

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.

OTERO, Cleber Sanfelici; MASSARUTTI, Eduardo Augusto de Souza. Em conformidade com o direito fundamental à saúde previsto na Constituição brasileira de 1988, é possível exigir do Estado a prestação de fosfoetanolamina sintética para pessoas com câncer? **Revista Jurídica Cesumar**, v. 16, n. 3, p. 847-876, set./dez. 2016. Disponível em:

http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_boletim/bibli_bol_2006/Rev-Jur-CESUMAR_v.16_n.03.10.pdf. Acesso em: 20 nov. 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. Disponível em: https://www.indexlaw.org/index.php/revistadgnt/article/view/5856/pdf. Acesso em: 4 set. 2020.

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. Disponível em: http://coral.ufsm.br/congressodireito/anais/2017/6-11.pdf. Acesso em: 10 set. 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.

VASCONCELLOS-SILVA, Paulo R.; CASTIEL, Luis David. COVID-19, as fake news e o sono da razão comunicativa gerando monstros: a narrativa dos riscos e os riscos das narrativas. **Cadernos de Saúde Pública**, v. 36, n. 7, jul. 2020. Disponível em: https://www.scielosp.org/pdf/csp/2020.v36n7/e00101920/pt. Acesso em: 4 set. 2020.

YABRUDE, Angela Theresa Zuffo *et al*. Desafios das Fake News com Idosos durante Infodemia sobre Covid-19: Experiência de Estudantes de Medicina. **Revista Brasileira de Educação Médica**, Brasília, v. 44, n. 1, out. 2020. Disponível em: https://www.scielo.br/pdf/rbem/v44s1/1981-5271-rbem-44-s1-e140.pdf. Acesso em: 6 set. 2020.

ZANINI, Leonardo Estevam de Assis *et al*. Os direitos da personalidade em face da dicotomia direito público – direito privado. **Revista de Direito Brasileira**, São Paulo, v. 19, n. 8, p. 208-220, jan./abr. 2018. Disponível em: https://www.indexlaw.org/index.php/rdb/article/view/3203/3534. Acesso em: 20 nov. 2020.

ZUBOFF, Shoshana. Big other: surveillance capitalism and the prospects of an information civilization. **Journal of Information Technology**, v. 30, p. 75-89, 2015. Disponível em: https://link.springer.com/article/10.1057/jit.2015.5. Acesso em: 10 out. 2020.