TECNOAUTORITARISMO EM TERRA BRASILIS: A FRAGILIDADE DOS DIREITOS FUNDAMENTAIS NA ERA DOS DADOS

Matheus Dalta PIMENTEL[1]
Ana Lara Sardelari SCALIANTE[2]
Renato Tinti HERBELLA[3]

RESUMO: Com o avanço das tecnologias e a exploração do *big data,* a monetização de dados pessoais tornou-se uma vantagem competitiva e econômica. Todavia, a exploração de tais dados não é restrita somente aos *players* integrantes do capital privado, haja vista que recentes estudos apontam que o Brasil (assim como alguns outros países) vem caminhando para uma tendência tecnoautoritária, onde os dados pessoais, sejam eles sensíveis ou não, são utilizados pelo Estado para a ampliação de seu poder de vigilância. Nesse toar, esse trabalho se debruçará acerca da utilização de dados pelo Estado e as recentes guinadas ao tecnoautoritarismo, contrastando-a com a as normativas gerais de proteção de dados e os tênues limites que devem ser respeitados para que o Estado não cometa excessos e fragilize o exercício de direitos e garantias fundamentais.

Palavras-chave: Tecnoautoritarismo. Direitos Fundamentais. Dados Pessoais. Vigilância. Democracia.

1 INTRODUÇÃO

A Constituição Federal de 1988, classificada como uma das mais garantistas de todo o histórico legislativo mundial, traz em seu bojo de direitos fundamentais a proteção à propriedade, à segurança e à intimidade, classificados como de máxima

[1] Discente do décimo termo do curso de Direito do "Centro Universitário Antônio Eufrásio de Toledo" de Presidente Prudente – SP. Bolsista de Iniciação Científica e membro do grupo de estudos "Constitucionalismos e Direitos Fundamentais" pela mesma IES. E-mail: matheus_dalta@hotmail.com.
[2] Discente do décimo termo do curso de Direito do "Centro Universitário Antônio Eufrásio de Toledo" de Presidente Prudente – SP. Bolsista de Iniciação Científica e membro do grupo de estudos "Novo Processo Civil Brasileiro: Garantias Fundamentais e Inclusão Social" pela mesma IES. E-mail: lara.sardelari@hotmail.com.
[3] Docente do curso de Direito do Centro Universitário Antônio Eufrásio de Toledo de Presidente Prudente. Mestre em Direito Negocial pela Universidade Estadual de Londrina – UEL. E-mail: renatoherbella@toledoprudente.edu.br. Orientador do trabalho.

necessidade, devendo o Estado, dentro de suas atribuições, zelar pela sua preservação.

Contudo, desde meados de 1960, o pesquisador Alan Westin iniciou o debate acerca dos efeitos negativos causados às liberdades em razão do uso indiscriminado da tecnologia, do compartilhamento e manipulação de dados pessoais (WESTIN, 1967).

É nesse contexto que surge o chamado tecnoautoritarismo, classificado como o conjunto de práticas de vigilância intimamente conectadas com o uso de tecnologia e informação, com o intuito de promover ações e políticas apresentadas à sociedade como necessárias para a garantia do bem-estar social e da segurança, ao custo da fragilização de direitos fundamentais, como a privacidade e a proteção aos dados pessoais (LIPPERT; WALBY, 2016, p. 331).

Nesse contexto, o objetivo deste trabalho é analisar algumas medidas que vem sendo tomadas pela Administração Pública brasileira, tanto na esfera federal como estadual, que podem vir a caracterizar práticas tecnoautoritárias. Para tanto, utilizar-se-á o método indutivo, pautado em pesquisas bibliográficas e jurisprudenciais acerca do tema, incluindo um estudo comparativo envolvendo os instrumentos e práticas empregadas pelo Governo Central Chinês para a consolidação de seu poderio de vigilância.

2 A TUTELA JURÍDICA DOS DADOS PESSOAIS E O COMBATE AO TECNOAUTORITARISMO

A tutela jurídica da proteção dos dados pessoais não é fruto dos estudos contemporâneos do direito. O primeiro documento legislativo que tratou acerca dessa importante temática surgiu há cerca de cinquenta anos, na Alemanha. O '*German State of Hesse'* foi responsável por inaugurar uma era de codificações do direito à proteção aos dados, potencializado com os avanços tecnológicos e com a exploração dos dados pessoais para fins econômicos (RUARO; RODRIGUES; FINGER, 2011, p. 55).

Uma década após a edição do State of Hesse, a Organização para Cooperação e Desenvolvimento Econômico (OCDE) editou o *Guidelines on the Protection of Privacy and Transborder Flows Personal Data*, documento fundamental para a estruturação da tutela do direito à proteção dos dados pessoais,

manifestando-se como um antecedente próximo do atual *General Data Proteccion Regulation* (GDPR), instrumento jurídico-normativo de relevância mundial.

É oportuno destacar que o próprio Marco Civil da Internet (Lei nº 12.965/2014), antecedente normativo da Lei Geral de Proteção de Dados, foi criado após o vazamento de uma série de espionagens supostamente cometidas pelo governo dos EUA contra diversos países, incluindo o Brasil (KEMENY, 2020 p. 34).

Hodiernamente, a tutela jurídica dos dados pessoais tornou-se sintomática dentre os principais países do mundo, podendo-se citar: *a)* o Código Civil da República Popular da China, que traz em seu bojo um capítulo específico para tratar sobre o direito à privacidade do povo chinês; *b)* o *California Consumer Privacy Act of 2018* (CCPA), destinado à proteção de dados dos consumidores no estado da Califórnia, nos EUA; e *c) o Act on the Protection of Personal Information* (APPI), em vigor no Japão desde 2003, mas com recentes atualizações feitas em 2015 e 2017.

> Muito sinteticamente, esses marcos regulatórios reconhecem os dados pessoais e o seu tratamento como fenômenos juridicamente relevantes, estabelecendo direitos e garantias para os cidadãos, limites para a sua utilização por empresas e organizações e mecanismos que procuram reduzir o risco proporcionado pelo tratamento de dados. Esses elementos são organizados de forma a proporcionar maior controle e proteção ao cidadão sobre seus dados, indo além de uma abordagem vinculada meramente à proteção da privacidade e, ainda, têm como uma de suas consequências mais importantes a consolidação de espaços dentro dos quais os dados pessoais possam ser tratados licitamente, proporcionando garantias para utilizações legítimas de dados pessoais e fomentando espaços de tratamento e livre fluxo de dados (DONEDA, 2020, p. 23).

Em *terra brasilis*, a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) unificou a proteção jurídica sobre o tratamento de dados pessoais. Tida inicialmente como uma alteração ao Marco Civil da Internet (proposta derrogada pela Lei nº 13.853/2019), a LGPD preocupa-se tanto com o tratamento de dados pessoais realizado por agentes de tratamento privados, quanto pelo próprio Poder Público, trazendo dispositivos específicos para regular tais situações.

A Lei Geral de Proteção de Dados exige, com vistas à proteção do Titular, que o tratamento de dados pessoais seja realizado com fundamento em ao menos uma das bases legais instituídas pela Lei. No caso da Administração Pública, há previsão de base *sui generis*, específica para o tratamento de dados pelos entes

públicos[4]. Além disso, a LGPD dispõe de um capítulo específico que estatui regras para o tratamento coordenado pela Administração Pública, alocado entre os artigos 23 e 32.

Ainda nesse contexto, é oportuno pontuar que a nova Lei também excepciona – em prol da Administração Pública – o tratamento de dados pessoais sensíveis, permitindo-se a sua ocorrência quando for necessário à "*execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos",* desde que os procedimentos e finalidades do tratamento sejam devidamente informados aos titulares de forma clara e direta, sendo vedado o tratamento "as escuras", na forma do artigo 23, inciso I da Lei.

> Outro quadro de interdependência, sobrevêm do agudo desafio que a LAI tratará sobre dados pessoais sensíveis, independentemente da dispensa de consentimento aos órgãos e entidades públicas, §2º, do art. 11 da LGPD, ou seja, a garantia à proteção de dados, precipuamente na Administração Pública, impõe uma problemática singular, sem perda de tempo, quanto à adequação das bases de dados computacionais de informações públicas abarcadas pela LAI, cuja a disposição de informações individualizadas se espraiam no universo digital das conexões internet (WONS; BORGES; OLIVEIRA, 2020, p. 195).

O Brasil está a um passo legislativo de encartar o direito à privacidade à Constituição da República como um direito fundamental irrevogável, haja vista que a Proposta de Emenda à Constituição nº 17/2019 foi recentemente aprovada em segundo turno de votação pela Câmara dos Deputados[5]. Esse processo legislativo acompanha o movimento jurisprudencial que já vem reconhecendo o direito à proteção de dados como um direito fundamental, com destaque à decisão exarada pelo Supremo Tribunal Federal nas Ações Diretas de Inconstitucionalidade nºs 6.388, 6.390, 6.393, 6.387 e 6.389, que objetivaram a suspensão da Medida Provisória 954/2018, norma esta que tornava compulsório o compartilhamento de dados

---

[4] Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

[5] Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2210757 . Acesso em: 07 set 2021.

pessoais de usuários pelas operadoras de telefonia ao Instituto Brasileiro de Geografia e Estatística (IBGE)[6].

2. SORRIA! SEUS DADOS ESTÃO SENDO MONITORADOS: O ESTADO DE VIGILÂNCIA NO BRASIL

De acordo com um relatório divulgado em 2020 pelo Centro de Análise da Liberdade e do Autoritarismo (LAUT) e a Associação Data Privacy Brasil de Pesquisa (DPBR):

> A ideia de tecnoautoritarismo pode ser usada para explicar os processos de expansão do poder estatal, por meio do uso de tecnologias de comunicação da informação de ponta, com o objetivo de incrementar as capacidades de vigilância e controle sobre a população, mediante violação de direitos individuais ou ampliação importante dos riscos de violação a direitos fundamentais.

Em reforço, assim leciona David Murakami Wood (2017, p. 362):

> In this s tate, there are no limits on what the state can know about the citizen, indeed, to be a citizen of totalitarian society is by definition to be known entirely. There is no accountability or openness from the state. Further, whatconstitutes "knowledge" in the totalitarian state is determined by the state itself. Historically, it has actually been quite rare for such states to exist in the most extreme form – even the former East German Stasi, for all its intensive surveillance effort, only had files of any level of detail on one third of the population. One of the major concerns about the contemporary turn to authoritarianism is that readily available technologies allow far easier surveillance of greater numbers across space and time.[7]

Em recente pesquisa publicada na edição da *Technology Review* do MIT (*Massachusetts Institute of Technology*), coordenado pelo jornalista Richard Kemeny e comentado pelo diretor do Data Privacy Brasil, Razael Zanatta, apontou-se que o

---

[6] MENDES, Laura Schertel. Decisão histórica do STF reconhece direito fundamental à proteção de dados pessoais. **JOTA**, 2020. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/decisao-historica-do-stf-reconhece-direito-fundamental-a-protecao-de-dados-pessoais-10052020

[7] **Tradução livre:** "Nesse estágio, não há limites para o que o estado pode saber sobre o cidadão, de fato, ser cidadão de uma sociedade totalitária é, por definição, ser inteiramente conhecido. Não há responsabilidade ou lisura por parte do estado. Além disso, o que constitui "conhecimento" no estado totalitário é determinado pelo próprio estado. Historicamente, é muito raro que tais estados existam na forma mais extrema - até mesmo a antiga *Stasi* da Alemanha Oriental, com todo o seu intenso esforço de vigilância, só tinha arquivos de qualquer nível de detalhe sobre um terço da população. Uma das principais preocupações sobre a virada contemporânea para o autoritarismo é que as tecnologias prontamente disponíveis permitem uma vigilância muito mais fácil de um número maior no espaço e no tempo".

Brasil vem guinando para a consolidação de um estado tecnoautoritário, destacando o Cadastro Base do Cidadão (CBC) como o principal exponente do tecnoautoritarismo, haja vista que o programa concentra uma rede quase irrestrita de dados, incluindo dados biométricos.

> There's ample reason to fear such misuse. During the 2018 presidential election that brought Bolsonaro into office, WhatsApp became a platform for widespread misinformation, most of it favoring Bolsonaro, according to an analysis by the Guardian. Some think the Cadastro could open the door to more targeted propaganda campaigns. Advanced profiling, including data gathered during the pandemic, could identify the voters most likely to believe and spread misinformation, who could then be unwittingly used to broadcast it, says Zanatta (KEMENY, 2020, p. 34)[8].

O CBC, instituído pelo Decreto n° 10.046/2019, ainda está em processo de implementação, mas já conta com a adesão de 34 órgãos e autarquias federais, incluindo os principais ministérios: Economia, Ciência e Tecnologia e Justiça e Segurança Pública.[9]

Segundo o já citado relatório divulgado pelo DPBR e LAUT, é possível identificar ao menos 13 acontecimentos que podem ser catalogados como manifestações tecnoautoritárias, coordenadas pelo Estado. Destes, é possível destacar os seguintes:

Em meados de 2020, foi amplamente divulgado que o Ministério da Justiça, por intermédio da Secretaria de Operações Integradas (SEOPI) teria realizado o monitoramento de cerca de 579 servidores públicos que seriam vinculados à movimentos tidos como 'antifascistas', materializando o monitoramento em um dossiê que inclui dados pessoais como fotografias e endereços de redes sociais.

A ação coordenada pelo Ministério da Justiça foi objeto de Arguição de Descumprimento de Preceito Fundamental nº 722, que já teve medida cautelar

---

[8] **Tradução livre:** "Há muitas razões para temer esse uso indevido. Durante a eleição presidencial de 2018 que trouxe Bolsonaro ao cargo, o WhatsApp se tornou uma plataforma para a desinformação generalizada, em grande parte favorecendo-o, de acordo com uma análise do Guardian. Alguns acham que o Cadastro pode abrir a porta para campanhas de propaganda mais direcionadas. Perfis avançados, incluindo dados coletados durante a pandemia, poderiam identificar os eleitores com maior probabilidade de acreditar e espalhar informações incorretas, que poderiam ser involuntariamente usados para transmiti-las, diz Zanatta".

[9] VALENTE, Jonas. O que é o Cadastro Base do Cidadão. Agência Brasil, 2020. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2020-12/agencia-brasil-explica-o-que-e-o-cadastro-base-do-cidadao. Acesso em: 06 set 2021.

deferida pelo Supremo Tribunal Federal, no sentido de determinar a suspensão imediata da produção e veiculação de informações do 'dossiê antifascista'.

Em seu voto, o Ministro Gilmar Mendes asseverou:

> Além disso, essa atuação estatal indevida também tem um efeito pernicioso sobre a sociedade como um todo, a partir do momento em que gera desestímulos ao debate de ideais contrárias àquelas defendidas pelos governantes, caracterizando o denominado efeito dissuasório ou "chilling effect" [...]
> Anote-se que o Sistema de Inteligência Brasileiro é um instrumento de Estado, e não de Governo. Deve se ocupar das macro questões de segurança pública e de proteção à soberania nacional, não podendo ser utilizado para monitorar a oposição e os críticos aos atuais ocupantes do poder.

Ainda na esfera federal, é oportuno resgatar a Medida Provisória nº 954/2020, editada pelo Presidente da República com o objetivo de determinar o compartilhamento obrigatório de dados pessoais (nomes, números de telefone e endereço)[10] por empresas integrantes do sistema de telecomunicações ao IBGE, com a justificativa de que tais dados subsidiariam a Pesquisa Nacional por Amostra de Domicílios Contínua (PNAD), voltada para o acompanhamento do desenvolvimento socioeconômico do Brasil.

A medida provisória foi objeto de cinco ações Diretas de Inconstitucionalidade, relatadas pela Ministra Rosa Weber, que concedeu medida cautelar para a suspensão da vigência da medida provisória (posteriormente referendada pelo plenário da Corte), fundamentando a sua decisão no respeito à privacidade a à autodeterminação informativa, bem como na ausência de medidas técnicas voltadas para a proteção de tais dados[11].

Já em âmbito estadual, muito comentou-se acerca da utilização de técnicas de monitoramento dos cidadãos paulistas pelo governo do estado, por meio do Sistema de Monitoramento Inteligente (SIMI). Tal rastreamento era realizado por meio de uma parceria com operadoras de aparelhos celulares móveis que transmitiram dados de georreferenciamento dos portadores para o Governo do

---

[10] Art. 2º As empresas de telecomunicação prestadoras do STFC e do SMP deverão disponibilizar à Fundação IBGE, em meio eletrônico, a relação dos nomes, dos números de telefone e dos endereços de seus consumidores, pessoas físicas ou jurídicas.

[11] BRASIL. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade nº 6389/DF. Min. Rosa Werber. Disponível em: http://portal.stf.jus.br/processos/downloadPeca.asp?id=15342959352&ext=.pdf. Acesso em: 04 set 2021.

Estado. Assim, a Administração teria, em tempo real, o controle dos deslocamentos durante a vigência dos decretos de restrição em razão da pandemia.

Apesar das críticas, o Tribunal de Justiça do Estado de São Paulo, em decisão exarada pelo Órgão Especial da Corte, reputou como legal o Sistema de Monitoramento Inteligente, entendo que a sua utilização não violaria o direito à privacidade e garantiria a proteção aos dados pessoais, já que tais dados seriam anonimizados.

> Como se infere, o acompanhamento ocorrerá por meio de dado anonimizado, ou seja, "dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;" (art. 5º, inciso III, da Lei Geral de Proteção de Dados Pessoais, ainda em *vacatio legis*).
> Em resumo: assegurado o anonimato, preservado o sigilo dos dados apurados pelas empresas de telefonia móvel antes da transferência ao IPT, não há afronta a direito individual, inviabilizando o acolhimento da demanda.

Vale ressaltar que todas as práticas de vigilância possuem, ao menos em tese, justificativas pautadas no bem comum, segurança pública, e preservação da ordem. Contudo, tais práticas não podem ser indiscriminadas e sem qualquer cautela, haja vista o risco de colisão direta com direitos fundamentais, tais como a liberdade, a autodeterminação informativa e a proteção aos dados pessoais.

2.1 Sistema de crédito social chinês: discussão acerca do primeiro precedente tecnoautoritário

"Tiang gao, Huangdi yuan", livremente traduzido como "As montanhas são altas e o Imperador está longe" é um histórico provérbio chinês comumente associado ao distanciamento entre a atuação do Governo central da China e os impactos e influências em relação à população em geral[12]. Contudo, com a crescente e questionável adesão a políticas de vigilância pelas autoridades chinesas, o provérbio vem perdendo, pouco a pouco, o seu significado.

O primeiro *case* relevante de que se tem notícia ocorreu a partir de 2015, quando o governo chinês anunciou a integração da base de dados governamental com o software de cálculo de score "*Sesame Credit*", mantido pela Ant Financial,

[12] WANG, Maya. China's Techno-Authoritarianism Has Gone Global: Washington Needs to Offer an Alternative. **Foreign Affairs,** 2021. Disponível em: https://www.foreignaffairs.com/articles/china/2021-04-08/chinas-techno authoritarianism-has-gone-global. Acesso em: 02 set 2021.

empresa coligada ao poderoso grupo econômico Alibaba. O algoritmo do Sesame realiza uma avaliação que não se limita ao resgate do histórico financeiro do usuário, e sim de diversas operações costumeiras que são realizadas pelos cidadãos, variando desde o "rankeamento" de compras (um livro, por exemplo, concede uma pontuação de score maior do que a compra de um videogame), até o relacionamento com amigos. Logo, caso você mantenha convivência com amigos que possuem um score social não muito considerável, o seu também irá diminuir (ZUBOFF, 2020, p. 444).

O *score* social é apenas um dos vários exemplos de medidas de vigilância adotadas pelo governo chinês. Recentemente foi divulgado o interesse do país em expandir o uso de moedas digitais, o que permitirá que as autoridades supervisionem diretamente o uso do dinheiro pelos cidadãos[13]. Com a implementação de todas essas medidas alinhadas ao uso da tecnologia, a China alcança um feito até então inédito no cenário político: a onipresença do Governo em todos os quadrantes da vida social de seus cidadãos.

> No contexto chinês, o Estado conduz o espetáculo, que lhe pertence, não como um projeto de mercado, mas como projeto político, uma solução de máquina que molda uma nova sociedade de comportamento automatizado para obter resultados políticos e sociais garantidos: certeza sem terror. Todos os encanamentos provenientes de todas as cadeias de suprimento transportam superávit comportamental para esse novo e complexo meio de modificação comportamental. A liberdade será abandonada em nome do conhecimento, mas será o conhecimento do Estado a ser exercido, não em defesa de receitas, mas sim, de sua perpetuação (ZUBOFF, 2020, p. 447).

Na esteira do trabalho de Zuboff, é possível denotar sem maiores esforços que a China vem empenhando-se em utilizar a tecnologia de vigilância com o objetivo de fixar e propagar a sua política ideológica entre os seus cidadãos por meio do aplicativo "*Study Xi, Strong Nation*", desenvolvido pelo Partido Comunista Chinês (PCC). O objetivo do aplicativo (que também se formata como uma rede social) é disseminar entre os jovens a cultura e os ensinamentos do partido e do

[13] KYNGE, James. Virtual Control: the agenda behind China's new digital currenncy,. **Financial Times**, 2021. Disponível em: https://www.ft.com/content/7511809e-827e-4526-81ad-ae83f405f623. Acesso em: 03 set 2021.

regime, sendo possível acompanhar o '*ranking*' dos amigos que tem mais conhecimento sobre esse assunto[14].

Durante a pandemia de *sars-cov-2*, o Governo chinês avançou o as políticas de monitoramento de seus cidadãos. Sob a justificativa de controle da pandemia, o governo chinês desenvolveu o aplicativo *Alipay Health Code*, responsável por monitorar diuturnamente os cidadãos por meio de um sistema de concessão de códigos: caso o cidadão receba um código verde, ele poderá circular livremente pelas províncias chinesas. Contudo, caso receba códigos amarelos ou vermelhos, a sua circulação está restrita ou totalmente impedida, sendo que o Governo chinês possui acesso em tempo real da localização e pode compartilhá-las com as autoridades policiais.[15]

É válido ressaltar que a República Popular da China possui, desde 2021, uma legislação de proteção de dados considerada como uma das mais rígidas já criadas, tendo se formalizado como uma alteração ao Código Civil da República Popular da China.

O Código traz um capítulo específico, denominado "Privacidade e Proteção de Informações Pessoais[16]", abarcando oito artigos. Os dispositivos tratam diversas matérias: desde a classificação do termo "privacidade" (Artigo 1.032) até a identificação dos princípios que devem nortear o processamento das informações pessoais (Artigo 1.035).

O Capítulo também garante ao Titular o direito à exclusão dos dados quando o tratamento for ilegal (Artigo 1.037), bem como elenca as obrigações dos agentes de tratamento ("processadores de informações", em tradução livre), como a vedação de divulgação, adulteração e armazenamento de dados sem o consentimento dos titulares. O dispositivo legal também impõe que os mesmos processadores devem tomar as medidas necessárias para garantir a segurança das informações pessoais

---

[14] KUO, Lilly; LYONS, Kate. China's most popular app brings Xi Jinping to your pocket. **The Guardian**, 2019. Disponível em: https://www.theguardian.com/world/2019/feb/15/chinas-most-popular-app-brings-xi-jinping-to-your-pocket. Acesso em: 01 set 2021.

[15] MOZUR, Paul; ZHONG, Raymond; KROLIK, Aaron. In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags. **The New York Times**, 2020. Disponível em: https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html. Acesso em: 05 set 2021.

[16] Disponível em: http://www.npc.gov.cn/englishnpc/c23934/202012/f627aa3a4651475db936899d69419d1e/files/47c16489e186437eab3244495cb47d66.pdf . Acesso em: 03 set 2021.

que coletam e armazenam, evitando vazamentos, adulterações e perdas de informações (Artigo 1.038).

3 CONCLUSÃO

Apesar de parecer uma guerra quase perdida, o tecnoautoritarismo e consequente expansão ruinosa do estado de vigilância deve ser combatido, haja vista a gravosa ameaça aos direitos e garantias individuais e coletivos, com destaque para a privacidade e a proteção de dados pessoais, direito este classificado como fundamental pelo Supremo Tribunal Federal.

Logo, é necessário que a Administração Pública execute seus deveres para com o povo de modo íntegro, e respeitando os limites estabelecidos pela Constituição e pela legislação infraconstitucional, mantendo-se o estado de vigilância dentro dos quadrantes legais.

Dessa feita, denota-se a relevância da Lei Geral de Proteção de Dados brasileira (Lei nº 13.709/2018) nesse contexto, acompanhada de uma atuação ativa da Autoridade Nacional de Proteção de Dados (ANPD) e do Judiciário, que já vem desempenhando um papel importantíssimo no combate à políticas tecnoautoritárias.

A renomada professora Shoshana Zuboff, em sua obra ‘A Era do Capitalismo de Vigilância’, descreve que “estamos à caça dos mestres dos fantoches, e não do fantoche”. Essa brilhante alegoria representa que o verdadeiro inimigo não é a tecnologia e nem as inovações que dela decorrem, e sim quem a utiliza para finalidades questionáveis, alcunhando-o de “mestre dos fantoches”.

Nesse toar, pode-se citar diversos casos de boa utilização da tecnologia para a melhoria e aperfeiçoamento e desburocratização dos serviços prestados pela Administração Pública, como o aceleramento de processos por meio do trâmite digital, a virtualização dos atendimentos em órgãos públicos e a utilização de documentos digitais e eletrônicos.

REFERÊNCIAS

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil.** Brasília: Senado, 1988.

BRASIL. Lei nº 13.709, 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**, Brasília, DF. Disponível: http://www.planalto.gov.br/lei/l13709.htm. Acesso em: 07 set 2021.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade nº 6389/DF**. Rel. Min. Rosa Werber. Disponível em: http://portal.stf.jus.br/processos/downloadPeca.asp?id=15342959352&ext=.pdf. Acesso em: 04 set 2021.

DONEDA, Danilo. **Panorama Histórico da Proteção de Dados Pessoais**. Tratado de Proteção de Dados Pessoais, Grupo GEN, 2020.

GROSS, Clarissa; ZANATTA, Rafael; NUNEZ, Izabel; LEITÃO, Clara; SANTOS, Bruna; VICENTE, João Paulo. **Retrospectiva Tecnoautoritarismo 2020**. Disponível em: https://laut.org.br/retrospectiva-tecnoautoritarismo-2020. Acesso em: 03 set 2021.

KEMENY, Richard. Register to rule them all. *In***: MIT Technology Review. Power: who has it, who wants it, and who's losing it**. The technotationalism issue, vol. 123, number 5, p. 33-37, 2020.

KUO, Lilly; LYONS, Kate. China's most popular app brings Xi Jinping to your pocket. **The Guardian**, 2019. Disponível em: https://www.theguardian.com/world/2019/feb/15/chinas-most-popular-app-brings-xi-jinping-to-your-pocket. Acesso em: 01 set 2021.

KYNGE, James. Virtual Control: the agenda behind China's new digital currenncy,. **Financial Times**, 2021. Disponível em: https://www.ft.com/content/7511809e-827e-4526-81ad-ae83f405f623. Acesso em: 03 set 2021.

LIPPERT, Randy K; WALBY, Kevin. Governing Through Privacy: Authoritarian Liberalism, Law, and Privacy Knowledge. *In:* **Law, Culture and the Humanities**. Vol. 12(2) 329–352, 2016.

MENDES, Laura Schertel. Decisão histórica do STF reconhece direito fundamental à proteção de dados pessoais. **JOTA**, 2020. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/decisao-historica-do-stf-reconhece-direito-fundamental-a-protecao-de-dados-pessoais-10052020.

MOZUR, Paul; ZHONG, Raymond; KROLIK, Aaron. In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags. **The New York Times**, 2020. Disponível em: https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html. Acesso em: 05 set 2021.

MURAKAMI, David Wood. The Global Turn to Authoritarianism and After. *In:* **Surveillance & Society**. P. 357-370, 2017. Disponível em: https://ojs.library.queensu.ca/index.php/surveillanceandsociety/article/view/6835/6505. Acesso em: 03 set 2021.

RUARO, Regina Lindes; RODRIGUES, Daniel Piñero; FINGER, Brunize. O Direito à proteção de dados pessoais e a privacidade. *In*: **Revista da Faculdade de Direito** - UFPR, Curitiba, n.47, p.29-64, 2011.

VALENTE, Jonas. O que é o Cadastro Base do Cidadão. **Agência Brasil**, 2020. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2020-12/agencia-brasil-explica-o-que-e-o-cadastro-base-do-cidadao. Acesso em: 06 set 2021.

WANG, Maya. China's Techno-Authoritarianism Has Gone Global: Washington Needs to Offer an Alternative. **Foreign Affairs,** 2021. Disponível em: https://www.foreignaffairs.com/articles/china/2021-04-08/chinas-techno-authoritarianism-has-gone-global. Acesso em: 02 set 2021.

WESTIN, Alan F. **Privacy and Freedom**. Athenum New York, 1967.

WONS, Leonardo; BORGES, André Leonardo Pitangueiras; OLIVEIRA, Pamela Danelon Reina Justen de. Lei Brasileira de Acesso à Informação e o Princípio da Publicidade: uma reflexão sintética à transparência e ponderações da publicidade de informações. *In* **Revista Tuiuti: Ciência e Cultura**, v.6 n.60, p.175-200, Curitiba, 2020.

ZUBOFF, Shoshana. **A Era do Capitalismo de Vigilância: a luta por um futuro humano na nova fronteira do poder.** Tradução de Georhe Schlesinger. 1 ed. Rio de Janeiro: Intrísenca, 2020.