DOI: 10.5433/1981-8920.2020v25n4p31

DO 11/9 À COVID-19: A VIGILÂNCIA DE ESTADO NA PERSPECTIVA DA ÉTICA INTERCULTURAL DA INFORMAÇÃO

FROM 9/11 TO COVID-19: STATE SURVEILLANCE FROM THE INTERCULTURAL INFORMATION ETHICS PERSPECTIVE

Arthur Coelho Bezerra[a]

RESUMO

Introdução: o presente artigo aborda as práticas de vigilância e monitoramento de informações pessoais levadas a cabo pelas duas principais potências econômicas mundiais (Estados Unidos e China), em dois momentos críticos da história recente: o ataque às torres do World Trade Center, em 11 de setembro de 2001, e a pandemia do coronavírus (COVID-19) em 2020. **Objetivo:** Demonstrar que, em tais períodos, ações de vigilância de informações pessoais tendem a ser reforçadas por governos de distintas matrizes culturais, sem enfrentar grande resistência por parte das populações que se encontram amedrontadas pela perspectiva da morte. **Metodologia:** a pesquisa parte de dois estudos de caso para verificar possíveis semelhanças entre as ações de vigilância estatal norte-americanas, realizadas a partir do 11 de setembro de 2001, e as ações de vigilância estatal realizadas pela China durante a pandemia da COVID-19. **Resultados:** é possível afirmar que, embora as motivações declaradas sejam distintas (referentes à segurança nacional, em 2001, e à saúde pública, em 2020), ambos os fenômenos – ação terrorista e pandemia – servem como justificativa moral para o recrudescimento das ações de vigilância nas potências mundiais citadas, que se valem do temor público para aumentar o controle sobre seus cidadãos e cidadãs. **Conclusões:** a vigilância de Estado, em países autoritários e também nos que se dizem democráticos, opera em uma perspectiva dialética de proteção e opressão, sendo necessário estabelecer limites ao uso de dados pessoais por governos e a defesa da privacidade dos indivíduos.

Descritores: Vigilância. Privacidade. Ética da informação. Ética intercultural da informação. Coronavírus.

1 INTRODUÇÃO

O coronavírus de 2019 é o novo 11 de setembro de 2001, ao menos no

[a] Pesquisador Titular do Instituto Brasileiro de Informação em Ciência e Tecnologia. Docente do Programa de Pós-graduação em Ciência da Informação (PPGCI/IBICT-UFRJ). E-mail: arthurbezerra@ibict.br.

que diz respeito às justificativas formais de governos para práticas de vigilância da população pelo Estado. Este é o argumento que será explorado no presente artigo, bem como a percepção de que, confrontados com a perspectiva da morte, cidadãos e cidadãs tendem a admitir, sem grande resistência, o recrudescimento de tais ações de monitoramento estatal, trocando parte de sua privacidade por uma rarefeita sensação de segurança.

O medo da morte, instaurado após o atentado contra as torres gêmeas do World Trade Center em Nova Iorque no dia 11 de setembro de 2001, tragédia que deixou mais de três mil mortos (seguida, nos anos seguintes, por outros ataques em países europeus como França, Espanha, Inglaterra, Alemanha e Dinamarca, somando centenas de assassinatos), teve como principal gatilho – em termos literais e psicológicos – a chamada ação terrorista. Na Enciclopédia Britânica[1], o substantivo "terrorismo" é definido como "o uso calculado da violência para criar um clima geral de medo em uma população e, assim, trazer um objetivo político específico". Entende-se, portanto, que o número de vítimas físicas (ou seja, de pessoas mortas ou feridas em uma ação terrorista) é ultrapassado de longe pelo número de pessoas psiquicamente afetadas pelo evento, alastrando-se exponencialmente graças à reverberação da tragédia, em tempo real, pelos avançados meios e dispositivos tecnológicos de comunicação e informação. É precisamente o caso do ataque às torres gêmeas, que ocorre em 2001 nos Estados Unidos e é, em alguma medida, "sentido" nos mais diversos cantos do mundo.

Em 2020, o referido "clima geral de medo em uma população" ganha nova escala mundial, alimentado, dessa vez, não pelo uso calculado da violência em ações terroristas, mas por um outro inimigo, não humano, invisível e de alta capacidade de disseminação e contágio: o coronavírus. No momento de submissão deste artigo (final de abril de 2020), segundo dados oficiais que, na opinião de grande parte da comunidade científica especializada, possuem um alto nível de subnotificação, a COVID-19 (*coronavirus disease 2019*) já havia infectado mais de 2,6 milhões de pessoas e matado quase 200 mil, em centenas

[1] Disponível em: https://www.britannica.com/topic/terrorism Tradução nossa. Acesso em 20 de abril de 2020.

de países ao redor do planeta (seguramente, todos esses números estarão desatualizados quando este artigo for publicado)[2].

Em resposta, dentre uma série de ações de saúde pública, tais como a construção de hospitais de campanha e a fabricação de testes, máscaras e respiradores, governos ao redor do mundo têm adotado medidas de distanciamento ou isolamento social – que incluem o fechamento de bares, restaurantes, estádios, casas noturnas e outros estabelecimentos comerciais e locais de aglomeração pública – e incentivado a população a permanecer em suas casas. Na esteira de tais medidas, diversas práticas de vigilância estatal têm sido implementadas, incorporando desde o monitoramento de dados biométricos (por meio de câmeras de reconhecimento facial e medidores de temperatura) até o controle da movimentação física dos indivíduos, que pode ser feito através do rastreamento de sinais de GPS emitidos por *smartphones* e captados por antenas e satélites.

À medida que o vírus viceja, a China, país onde o primeiro caso da doença foi descoberto, ainda em 2019, desponta como uma das nações que tem obtido maior sucesso na implementação de ações de controle para o combate à pandemia. Dentre tais ações, destacam-se a checagem da temperatura corporal de indivíduos em estabelecimentos e transportes públicos, bem como em todos os voos que chegam ao país, e a atribuição de códigos de QR (*QR codes*) a cidadãos e cidadãs, que são identificados, em lugares de aglomeração pública como estações de metrô e centros comerciais, como parte dos grupos verde (se não há motivo para se isolarem), amarelo (sendo necessário sete dias de isolamento) ou vermelho (14 dias de isolamento). Tal identificação é feita com base na passagem dos indivíduos por áreas atingidas pelo vírus nas duas semanas anteriores (os deslocamentos são acompanhados pelo governo mediante georreferenciamento via *smartphone*), e apenas quem faz parte do grupo verde tem direito a entrar no prédio ou no vagão, sendo necessário aos demais cumprir o período de isolamento (monitorado da mesma forma).

[2] Oito meses depois, no momento de publicação deste artigo, o número chega a mais de um milhão e meio de mortos e mais de 75 milhões de infectados em todo o mundo. Leitores e leitoras deste artigo terão acesso a números ainda maiores. Disponível em https://www.paho.org/pt/covid19 acesso em 18 de dezembro de 2020.

O recente aumento de práticas estatais de vigilância e sua aparente aceitação social é o fenômeno que motiva a escrita destas linhas, inspiradas pela percepção de que, em tempos de pânico social, a insegurança em relação à vida contribui para que governos implementem, sem grande resistência popular, medidas de vigilância e controle que ultrapassam o mero combate à "ameaça" em questão, venha de inimigo humano ou não humano. Partindo dessa percepção, a pesquisa investiga possíveis semelhanças entre as ações de vigilância estatal norte-americanas, realizadas após 11 de setembro de 2001, e as ações de vigilância estatal empreendidas pela China durante a pandemia da COVID-19 em 2020.

Uma vez que o monitoramento de informações pessoais carrega uma série de implicações éticas, e pelo fato das referidas ações estarem baseadas em realidades culturais tão distintas como a norte-americana e a chinesa, o estudo parte da perspectiva da ética intercultural da informação, conforme seu desenvolvimento por Rafael Capurro (2009; 2010), tendo como foco as diferentes noções de privacidade nas sociedades em questão.

Em um mundo que adota discursos e práticas econômicas "globalizadas", a abordagem intercultural se torna cada vez mais relevante, como afirma o filósofo:

> A EII [ética intercultural da informação] aumenta no momento em que o questionamento teórico da(s) moral(ais) se torna cada vez mais urgente devido ao profundo impacto prático das TIC na sociedade. Os conflitos, que antes se davam em nível local, se transformam rapidamente em conflitos globais e vice-versa (CAPURRO, 2010, p. 3-4, tradução nossa).

Na presente análise, serão contemplados ambos os sentidos atribuídos por Capurro à ética intercultural da informação: o sentido restrito, que aborda o impacto das tecnologias de informação e comunicação nas diferentes culturas, e o sentido amplo, que engloba a forma como questões específicas (como a privacidade) são entendidas a partir de diferentes tradições culturais – não apenas no âmbito do uso das tecnologias, mas, também, por outras formas e meios de comunicação, o que permite ao pesquisador construir "[...] uma grande visão histórica comparativa" (CAPURRO, 2009, p. 67-68, tradução nossa).

2 A VIGILÂNCIA ESTATAL NORTE-AMERICANA NA RESSACA DO 11 DE SETEMBRO DE 2001

Foi necessário apenas um mês e meio para que o congresso norte-americano aprovasse uma nova legislação voltada para o declarado objetivo de "fortalecimento da segurança nacional". O USA PATRIOT Act, acrônimo para *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*, foi assinado pelo então presidente George W. Bush em 26 de outubro daquele ano, como resposta aos ataques às torres gêmeas de 11 de setembro. O texto da lei autoriza que uma série de medidas de prevenção ao terrorismo sejam tomadas pela Agência de Segurança Nacional (*National Security Agency*, ou NSA).

Na prática, porém, o Patriot Act concedeu permissão para que a NSA estruturasse um sofisticado aparato de vigilância em massa, que inclui detenção indiscriminada de imigrantes, buscas feitas por autoridades policiais a residências ou empresas sem o consentimento ou conhecimento dos proprietários, acesso ampliado de agentes da lei a registros comerciais de empresas (incluindo bibliotecas) e o uso ampliado das *National Security Letters* (NSL), cartas de segurança nacional expedidas por um órgão federal dos Estados Unidos que exigem a entrega ao FBI de "dados de não conteúdo" (os metadados), como registros de IP (a identidade do computador), telefonemas, e-mails, contatos e transações financeiras, de qualquer pessoa ou empresa, sem necessidade de ordem judicial. Conforme explica o fundador do Wikileaks, Julien Assange:

> A utilização de NSLs aumentou muito após a aprovação do Patriot Act em 2001. Os destinatários das NSLs normalmente são prestadores de serviço, como provedores de internet ou instituições financeiras, e os dados buscados normalmente se referem aos seus clientes – e o destinatário não pode informá-los de que seus registros foram exigidos pelas NSLs. Apesar de os destinatários terem o direito de contestar as NSLs em juízo, a provisão de ordem de silêncio impede que os alvos finais sejam informados sobre a NSL, impedindo assim que eles apelem em juízo (ASSANGE *et al.*, 2013, p. 78)

As práticas de vigilância em massa feitas pela NSA vieram à tona após as denúncias de Assange e de outros *whistleblowers*, dentre os quais se destaca o

ex-funcionário da Central Intelligence Agency (CIA), Edward Snowden. Graças a Snowden, o mundo descobriu que, sob a justificativa de "unir e fortalecer os Estados Unidos através da provisão de ferramentas requeridas para interceptar e obstruir o terrorismo", como argumenta o acrônimo do Patriot Act de 2001, a agência norte-americana de segurança, na prática, atropelou os direitos de privacidade de cidadãos e empresas em todo o mundo, tendo, dentre outros expedientes, monitorado companhias petrolíferas no Brasil e na Venezuela, mapeado a movimentação das Forças Revolucionárias da Colômbia (Farc) e registrado conversas telefônicas de líderes políticos, como a então presidente do Brasil, Dilma Rousseff, e a chanceler da Alemanha, Angela Merkel (BEZERRA, 2016, p. 238).

Sem embargo, as graves denúncias de Assange e Snowden, ao invés de resultarem em uma responsabilização do governo norte-americano pelos crimes de violação de privacidade perpetrados, fizeram com que ambos se tornassem perseguidos e tivessem que buscar asilo político fora dos Estados Unidos. E em que pesem as alterações feitas no Patriot Act desde então, como a emenda de 2015 que impede que a NSA continue a usar o *Prism*, programa de coleta e armazenamento de informação em massa (embora dados de indivíduos ainda possam ser solicitados pelo governo às companhias de telefone), é possível afirmar que o desenvolvimento de uma miríade de práticas de vigilância estatal tornou-se um dos principais legados do 11 de setembro norte-americano para o mundo, tendo como corolário o encolhimento das dimensões da privacidade de cidadãos e cidadãs.

3 AS INOVAÇÕES TECNOLÓGICAS DA VIGILÂNCIA ESTATAL CHINESA NA PANDEMIA DE 2020

Diferentemente dos Estados Unidos, onde práticas de monitoramento da população pelo Estado são mascaradas sob o véu de uma aparente liberdade de expressão, o imponente sistema de vigilância operado pelo governo chinês é um velho conhecido dos chineses, e também um velho alvo de críticas de entidades internacionais de proteção aos direitos humanos. A jornalista norte-americana Rebecca MacKinnon (2013), que trabalhou na filial chinesa da rede

de jornalismo CNN cobrindo temas ligados a privacidade e liberdade de expressão, detalha em livro as concessões que empresas como Yahoo, Microsoft e Google tiveram de fazer para disponibilizar seus serviços no país, especialmente a partir de 2005, ano em que a blogosfera chinesa saltou de menos de meio milhão para mais de cinco milhões de usuários. Segundo a autora, “2005 foi também o ano em que o governo começou a montar seu sistema de ‘autodisciplina’ para controlar e censurar redes sociais através das próprias companhias”, obrigando-as a concordar com as políticas chinesas acerca do que consideram “conteúdo politicamente sensível” para não serem bloqueadas pelo “grande *firewall*” (MacKINNON, 2013, p. 136-137, tradução nossa).

O Relatório Mundial 2020, revisão anual realizada pela *Human Rights Watch* sobre a situação dos direitos humanos no mundo todo, apresenta a seguinte avaliação em seu capítulo introdutório:

> No plano doméstico, o Partido Comunista Chinês, preocupado com o fato de que permitir a liberdade política poderia comprometer seu poder, construiu um Estado orwelliano de vigilância altamente tecnológico e um sofisticado sistema de censura na internet para monitorar e abafar o criticismo público. No exterior, ele tem usado sua crescente influência econômica para silenciar críticos e realizar o mais intenso ataque ao sistema global de proteção dos direitos humanos desde sua emergência em meados do século XX (ROTH, 2020, não paginado)

Para Kenneth Roth, diretor executivo da organização, o mais notável sistema de vigilância e engenharia de comportamento que está sendo construído pelo governo chinês é o "sistema de crédito social", em que, a partir de dados coletados na internet, em registros governamentais e por meio de técnicas aprimoradas de reconhecimento facial, cada cidadão chinês recebe uma pontuação pelo seu comportamento. Más condutas, como direção imprudente no trânsito ou o atraso no pagamento de contas, podem ser punidas, ao passo que boas condutas são passíveis de recompensas. Nesse sistema, a avaliação governamental da “confiabilidade” das pessoas “[...] determina o acesso a bens sociais desejáveis, como o direito de viver em uma cidade agradável, colocar as crianças em uma escola particular ou viajar de avião ou trem de alta velocidade” (ROTH, 2020, não paginado).

O extenso monitoramento de dados biométricos é uma destacada

inovação tecnológica da China de 2020 em comparação com os Estados Unidos de 2001. Atualmente, são estimadas cerca de 170 milhões de câmeras de vigilância no país asiático, uma média de uma câmera para cada 12 habitantes (em um país com cerca de 1.4 bilhão de habitantes). Muitas dessas câmeras possuem um avançado sistema de reconhecimento facial, que capta dados biométricos das pessoas em espaços públicos e privados. A coleta e análise digital de informação biométrica (por traços faciais, impressão digital, íris, DNA ou outro dado sensível), que se faz presente em aeroportos, caixas eletrônicos de bancos, portarias de residências e edifícios comerciais, bem como em computadores, *smartphones* e em uma série de outros lugares e dispositivos tecnológicos, é utilizada não apenas para identificar criminosos ou dissidentes do governo, mas também para prevenir acidentes, ações terroristas e até mesmo doenças. Em relação ao atual combate à COVID-19, a China foi considerada pela Organização Mundial da Saúde (OMS) um exemplo para o mundo, graças às medidas que vêm sendo tomadas e às pesquisas que vêm sendo realizadas no país, ambas apoiadas no extensivo uso de macrodados (*big data*) obtidos por meio de tecnologias de rastreio biométrico e georreferencial.

Em artigo publicado em março de 2020 no jornal El País, o filósofo sul-coreano Byung-Chul Han menciona o sistema chinês de captação automática da temperatura dos corpos que saem das estações de trem da capital, Pequim. O sistema reconhece os rostos dos indivíduos por meio de câmeras de vigilância e notifica, por *smartphone*, pessoas que estiverem próximas a alguém com temperatura corpórea elevada. Segundo o filósofo,

> [...] para enfrentar o vírus os asiáticos apostam fortemente na vigilância digital. Suspeitam que o big data pode ter um enorme potencial para se defender da pandemia. Poderíamos dizer que na Ásia as epidemias não são combatidas somente pelos virologistas e epidemiologistas, e sim principalmente pelos especialistas em informática e macrodados. Uma mudança de paradigma da qual a Europa ainda não se inteirou (HAN, 2020, não paginado)

Não obstante, no tocante ao melhor desempenho da China e de outros países asiáticos no combate à pandemia, quando comparados aos Estados Unidos e outros países ocidentais, há uma série de fatores culturais que precisam ser observados, especialmente em relação às distintas dimensões que

a privacidade, vista da perspectiva da ética, apresenta nas diferentes tradições culturais mencionadas. Este é o assunto que será tratado a seguir.

4 A PRIVACIDADE NA PERSPECTIVA DA ÉTICA INTERCULTURAL DA INFORMAÇÃO

O tema da privacidade é utilizado por Rafael Capurro (2009; 2010) como exemplo de problema a ser discutido no âmbito da ética intercultural da informação. Nas palavras de Capurro:

> A reflexão ética se move entre os polos de universalização e concretização em uma situação singular. Discutir sobre, por exemplo, o tema da privacidade não é igual em uma cultura do que em outra e com um fundo histórico e cultural determinado (...) (CAPURRO, 2010, p. 3, tradução nossa)

Para abordar a privacidade a partir do ponto de vista chinês, o filósofo recorre ao pensamento de Lü Yao-huai, professor da *Suzhou University of Science and Technology* (localizada na província de Jiangsu, na China), que escreve sobre as transformações culturais vividas na China desde as reformas econômicas e políticas da década de 1980. A partir dos anos 1990, o advento da internet e dos dispositivos digitais de informação e comunicação no país vem acompanhado de uma mudança no entendimento da ideia de privacidade que, de acordo com Lü Yao-huai (2005), deixa de se referir somente a um entendimento de “segredo vergonhoso” (*Yinsi*) para incluir todas as informações pessoais, vergonhosas ou não, que as pessoas não querem que outras pessoas saibam.

No entanto, no plano das regulamentações legais sobre proteção de dados digitais na China, além dos princípios de respeito e de “consentimento informado”, há uma tendência a levar em conta o que Lü (2005) chama de “princípio do equilíbrio (entre a segurança da privacidade pessoal e a segurança da sociedade)” e o “princípio de retificação social” (*apud* CAPURRO, 2009, p. 74, tradução nossa), princípios estes que “tomam a sociedade como o valor maior”, conforme avalia o próprio Capurro (2009, p. 74, tradução nossa). Nesse sentido, ainda que sua proteção tenha se expandido nas últimas décadas na China, em grande medida graças à influência da cultura ocidental no país, a privacidade continua a ser vista como um “bem instrumental” ao invés de um “bem

intrínseco", e submetida ao entendimento de que o interesse público é superior ao interesse individual (LÜ, 2005).

Tome-se como exemplo a temperatura do corpo: em princípio, um dado biométrico como esse é de interesse privado – em condições normais, ninguém é obrigado a revelar para outras pessoas se está ou não febril. No entanto, em uma situação de pandemia, o interesse público pode se impor sobre o direito individual à privacidade: se a febre significa um possível contágio pelo vírus, cidadãos e cidadãs podem ser obrigados a revelar essa informação pessoal, como no citado caso da implementação e obrigatoriedade do uso de medidores de temperatura em diversos estabelecimentos, espaços e transportes públicos e em todos os voos comerciais que desembarcam em território chinês durante a pandemia.

Essa vigilância disseminada, segundo Byung-Chul Han (2020, não paginado), é fruto de uma "mentalidade autoritária, que vem de sua tradição cultural (confucionismo)", o que faz com que as pessoas sejam "menos relutantes e mais obedientes do que na Europa":

> Na China e em outros Estados asiáticos como a Coreia do Sul, Hong Kong, Singapura, Taiwan e Japão não existe uma consciência crítica diante da vigilância digital e o big data. A digitalização os embriaga diretamente. Isso obedece também a um motivo cultural. Na Ásia impera o coletivismo. Não há um individualismo acentuado. O individualismo não é a mesma coisa que o egoísmo, que evidentemente também está muito propagado na Ásia (HAN, 2020, não paginado).

No caso norte-americano, entretanto, também é possível detectar uma permissividade em relação à vigilância estatal, especialmente em um momento de crise como o pós-11 de setembro. Segundo Roberta MacKinnon (2013, p. 81), a população norte-americana é capaz de ser vista, em alguns casos, "[...] apoiando ativamente a erosão das liberdades civis em nome do combate ao terror e ao crime, ou de outro modo consentindo [tal erosão] porque sua atenção e prioridades estão em outro lugar".

Ao mencionar a aceitação popular do aumento da vigilância estatal na ressaca do ataque ao World Trade Center, o sociólogo David Lyon (2010, p. 116) pondera: "é possível que, de uma forma geral, cidadãos aceitem que a perda da privacidade seja o preço a ser pago pela segurança". Ao contrário da China, no entanto, a noção de privacidade na sociedade norte-americana estaria se

contraindo ao invés de se dilatar:

> Minha hipótese é que a vigilância – que em sua raiz social e etimológica está ligada à observação – é aceita facilmente porque vários tipos de observação tornaram-se comuns em uma "sociedade espectadora" (*viewer society*) encorajada pela cultura da TV e do cinema. À medida que coisas antes consideradas "privadas" tornam-se abertas ao olhar público de muitos, e à medida que certas áreas íntimas e reclusas da vida são "vasculhadas", parece ser cada vez menos importante que esse ou aquele dado privado, certa vez protegido, esteja agora disponível (LYON, 2010, p. 116-117).

A hipótese de Lyon, como indica a perspectiva da ética intercultural da informação aqui adotada, não se aplica à realidade do povo chinês, cujas matrizes culturais forjam diferentes contornos para a privacidade dos indivíduos. No entanto, embora esteja claro que a relação entre o espaço público e o espaço privado possa variar conforme o ambiente cultural e político de uma sociedade, a análise de momentos críticos da história, como os vividos nos Estados Unidos, em 2001, e na China (e no mundo todo), em 2020, fortalecem o argumento de que, mesmo em tradições culturais distintas, o medo de um povo pode ser usado como justificativa moral para o recrudescimento de práticas de vigilância estatal, mediante o argumento de garantia de proteção e de uma rarefeita sensação de segurança.

É o que MacKinnon percebe ao comparar as práticas de vigilância realizadas tanto pelos norte-americanos quanto pelos chineses: "*todos* os governos, de ditaduras a democracias, estão rapidamente aprendendo como usar a tecnologia para defender seus interesses" (MacKINNON, 2013, p. 5, tradução nossa, grifo da autora). O Relatório Mundial 2020 da Human Rights Watch pode ser citado como um bom e atual exemplo do que diz a jornalista:

> Em outros lugares [além da China], populistas autocráticos assumem cargos demonizando minorias, e depois se mantêm no poder atacando os freios e contrapesos a seus governos, como jornalistas independentes, juízes e ativistas. Alguns líderes, como o presidente dos Estados Unidos, Donald Trump, o primeiro-ministro indiano, Narendra Modi, e o presidente do Brasil, Jair Bolsonaro, desafiam o mesmo corpo de normas internacionais de direitos humanos do qual a China desdenha, atiçando seus públicos ao forjar um combate fantasioso com os "globalistas" que ousam sugerir que todos os governos devem respeitar as mesmas normas (ROTH, 2020, não paginado)

Um outro documento de 2020, divulgado pelo instituto *Data Privacy Brasil* para servir de defesa ao "[...] dever de incorporação de salvaguardas e

mecanismos de mitigação de riscos a direitos fundamentais, decorrente do ordenamento jurídico brasileiro" (BIONI *et al*, 2020, p. 5), traz uma série de recomendações a serem observadas para o uso legítimo de dados pessoais no combate à COVID-19, dentre as quais se destacam a fundamentação técnica e científica quanto à necessidade e eficiência do uso de dados pessoais, a delimitação da ideia de finalidade, a transparência máxima das medidas adotadas, bem como da governança destas, e o uso de tecnologias de código aberto. Para os autores, esse conjunto de recomendações mostra que a proteção de dados não rivaliza com o propósito de contenção à pandemia da COVID-19, "[...] mas sim permite que o Estado seja eficiente no combate à epidemia e o faça com respeito aos direitos e garantias fundamentais da população" (BIONI *et al*, 2020, p. 26-27).

Que fique claro: não se advoga que não haja medidas de controle. O uso de dados agregados de geolocalização para identificação de aglomerações em tempos de quarentena, por exemplo, revela-se uma ferramenta eficaz no combate ao alastramento do coronavírus. Para garantir o respeito à privacidade, no entanto, é importante que esses dados sejam "anonimizados", de forma a impedir sua associação, direta ou indireta, a indivíduos. Esse equilíbrio tem variado nos diferentes países que adotam tais práticas de monitoramento, sendo a China um dos países em que a balança pesa em favor do não anonimato, como visto nos exemplos apresentados.

Cabe lembrar, finalmente, que muitas das medidas de vigilância que são postas em prática durante momentos críticos, algumas delas positivadas juridicamente através de novas leis, não são abandonadas posteriormente e firmam-se como um legado, conforme visto no caso do 11 de setembro norte-americano. As denúncias de Edward Snowden devem servir como um espelho retrovisor que lembra à sociedade a necessidade de estar atenta a práticas de invasão de privacidade por governos, que se utilizam do medo para vigiar ainda mais seus cidadãos e cidadãs.

5 CONSIDERAÇÕES FINAIS

Em maio de 2015, David Lyon esteve na Coordenação de Ensino e

Pesquisa do Instituto Brasileiro de Informação em Ciência e Tecnologia (COEPE/IBICT), no Rio de Janeiro, para oferecer um curso sobre vigilância. Na fala de abertura, o sociólogo conta que, ao aterrissar no Rio, não pôde deixar de notar o principal símbolo turístico da cidade, com seus braços abertos sobre a Guanabara, a "olhar por nós" do alto do morro Corcovado. Lyon viu o Cristo como um interessante exemplo de vigilância, exercida com a finalidade de cuidado – uma vigilância considerada boa, como a das mães e pais que utilizam a chamada "babá eletrônica" para monitorar o sono e a fome de seus bebês. Visto a partir desses e de outros exemplos, a vigilância pode ser entendida como uma fonte de proteção e segurança. Mas haverá motivos para sempre sorrirmos ao saber que estamos sendo vigiados, como sugerem alguns avisos acompanhados da famosa *smiley face*?

Em definição proposta por Lyon, o termo vigilância se refere ao "[...] monitoramento do comportamento, atividades ou outras informações, geralmente de pessoas, com o objetivo de influenciar, gerir, dirigir ou protegê-las" (LYON, 2007, p. 1, tradução nossa). Há, portanto, diferentes motivações que podem justificar práticas de monitoramento e controle, sendo estas aplicadas a situações que vão do microcosmo da relação amorosa de duas pessoas (como os casais que se vigiam mutuamente em redes sociais) à dimensão macro das questões de segurança e de saúde nacional, como nos dois casos analisados neste artigo.

A pandemia do coronavírus que se impôs como o principal assunto de 2020, mobilizando discursos dos mais variados estratos científicos, políticos, econômicos e culturais, abre espaço para uma abordagem do fenômeno da vigilância considerando o seu caráter *dialético*, que problematiza e denuncia a *opressão* que subjaz o discurso da *proteção*. Tal perspectiva pode ser cotejada mediante a realização de diagnósticos interdisciplinares, que procurem identificar as potencialidades e os obstáculos à liberdade e autonomia informacional que se colocam no cenário a ser investigado, conforme a proposta metodológica da *teoria crítica da informação* (BEZERRA, 2019, p. 28). No caso aqui estudado, isso significa valorizar as *potencialidades* das práticas de vigilância de dados biométricos e georreferenciais para o bem da humanidade, sem deixar de denunciar os *obstáculos* que os usos perversos de tais

informações podem trazer para a privacidade e a autonomia dos indivíduos.

No ano seguinte aos ataques às torres gêmeas, durante um diálogo com o então exilado Julien Assange, o também jornalista Jacob Applebaum, ativista de direitos digitais e pesquisador de segurança da informação, faz uma referência ao que chama de “Quatro Cavaleiros do Infoapocalipse: lavagem de dinheiro, drogas, terrorismo e pornografia infantil”; para Applebaum (2013), “essas quatro ameaças são sempre enfatizadas e usadas como argumento para derrubar tecnologias de preservação da privacidade, porque ninguém questiona que são grupos que devem ser derrotados” (*apud* ASSANGE *et al*, 2013, p. 87). Oito anos depois daquela conversa, um vírus até então desconhecido desponta como o Quinto Cavaleiro do Apocalipse, e derrotá-lo se torna a justificativa moral para novas violações estatais de privacidade, que podem se tornar recorrentes mesmo após a “ameaça” ter sido vencida.

Se a situação do mundo em 2020 nos força a repensar questões econômicas, comportamentos sociais e até mesmo nossa própria relação com o planeta, é sem dúvida importante, também, incluirmos em nossa agenda de questionamentos a relação que desejamos ter, como indivíduos, com o Estado e com a sociedade após a pandemia, e quais direitos queremos garantir no futuro incerto que se avizinha.

REFERÊNCIAS

ASSANGE, J.; MÜLLER-MAGUHN, A.; ZIMMERMANN, J. APPELBAUM, J. **Cypherpunks**: liberdade e o futuro da internet. São Paulo: Boitempo, 2013.

BEZERRA, A. C. Privacidade como ameaça à segurança pública: uma história de empreendedorismo moral. **Liinc em Revista**, Rio de Janeiro, v. 12, n. 2, p. 231-242, nov. 2016. Disponível em: http://revista.ibict.br/liinc/article/view/3720/3139. Acesso em 20 de abril de 2020

BEZERRA, A. C. Teoria crítica da informação: proposta teórico-metodológica de integração entre os conceitos de regime de informação e competência crítica em informação. *In:* BEZERRA, A. C.; SCHNEIDER, M.; PIMENTA, R. M.; SALDANHA, G. S. **iKRITIKA**: estudos críticos em informação. Rio de Janeiro: Garamond, 2019.

BIONI, B.; ZANATTA, R.; MONTEIRO, Renato; RIELLI, Mariana. Privacidade e pandemia: recomendações para o uso legítimo de dados no combate à COVID-

19. **Conciliando o combate à COVID-19 com o uso legítimo de dados pessoais e o respeito aos direitos fundamentais**. São Paulo: Data Privacy Brasil, 2020.

CAPURRO, R. Intercultural Information Ethics: foundations and applications. **Signo y Pensamiento**, Bogotá, v. 28, n. 55, jul./dec., 2009. Disponível em: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0120-48232009000200004. Acesso em 20 de abril de 2020

CAPURRO, R. Desafios teóricos y prácticos de la ética intercultural de la información. *In:* Simpósio Brasileiro de Ética da Informação, 1, João Pessoa, 18 de março de 2010. Disponível em: http://www.capurro.de/paraiba.html. Acesso em: 20 de abril de 2020

HAN, B. O coronavírus de hoje e o mundo de amanhã. **El País**, 22 de março de 2020. Disponível em: https://brasil.elpais.com/ideas/2020-03-22/o-coronavirus-de-hoje-e-o-mundo-de-amanha-segundo-o-filosofo-byung-chul-han.html. Acesso em: 20 de abril de 2020

LÜ, Y. Privacy and data privacy in contemporary China. **Ethics and Information Technology**, n. 7, p. 7-15, 2005.

LYON, D. **Surveillance studies:** an overview. Cambridge: Polity Press, 2007.

LYON, D. 11 de setembro, sinóptico e escopofilia: obervando e sendo observado. *In:* BRUNO, F.; KANASHIRO, M.; FIRMINO, R. (orgs.). **Vigilância e visibilidade**: espaço, tecnologia e identificação. Porto Alegre: Sulina, 2010.

MacKINNON, R. **Consent of the networked**: the worldwide struggle for internet freedom. New York: Basic Books, 2013.

ROTH, K. A ameaça global da China aos direitos humanos. *In*: HUMAN RIGHTS WATCH, **Relatório Mundial 2020.** Disponível em: https://www.hrw.org/pt/world-report/2020/country-chapters/337660. Acesso em 20 de abril de 2020

FROM 9/11 TO COVID-19: THE STATE SURVEILLANCE FROM THE PERSPECTIVE OF THE INTERCULTURAL INFORMATION ETHICS

ABSTRACT

Introduction: this article focuses on the practices of surveillance and monitoring of personal information carried out by the two main world economic powers (United States and China), at two critical moments in recent history: the attack on the World Trade Center towers, on September 11, 2001, and the coronavirus disease (COVID-19) pandemic in 2020. **Objective**: demonstrate that, in such periods, personal information surveillance actions tend to be reinforced by governments, from different cultural

backgrounds, without facing great resistance from the populations that are frightened by the prospect of death. **Methodology**: the research is based on two case studies to verify possible similarities between the US state surveillance actions, carried out after September 11, 2001, and the state surveillance actions carried out by China during the COVID-19 pandemic. **Results**: it is possible to affirm that, although the motivations declared are different (referring to national security, in 2001, and public health, in 2020), both phenomena (terrorist action and pandemic) serve as a justification for the increase in surveillance actions in the aforementioned world powers, which use public fear to increase control over their citizens. **Conclusions**: State surveillance, whether in so-called democratic or authoritarian countries, operates from a dialectical perspective of protection and control, being necessary to establish limits to the use of personal data by governments and the defense of the privacy of individuals.

Descriptors: Surveillance. Privacy. Information ethics. Intercultural information ethics. Coronavirus. COVID-19.

DEL 9/11 AL COVID-19: VIGILANCIA ESTATAL DESDE LA PERSPECTIVA DE ÉTICA INTERCULTURAL DE LA INFORMACIÓN

RESUMEN

Introducción: este artículo se centra en las prácticas de vigilancia y monitoreo de información personal llevadas a cabo por las dos principales potencias económicas mundiales (Estados Unidos y China), en dos momentos críticos de la historia reciente: el ataque a las torres del World Trade Center, el 11 de septiembre de 2001, y la pandemia de coronavirus (COVID-19) en 2020. **Objetivo**: Demonstrar que, en tales períodos, las acciones de vigilancia de la información personal tienden a ser reforzadas por gobiernos de diferentes orígenes culturales, sin una gran resistencia de las poblaciones que están asustadas por la perspectiva de la muerte. **Metodología**: la investigación se basa en dos estudios de caso para verificar posibles similitudes entre las acciones de vigilancia del estado de EE. UU., llevadas a cabo después del 11 de septiembre de 2001, y las acciones de vigilancia del estado realizadas por China durante la pandemia del COVID-19. **Resultados**: es posible afirmar que, aunque las motivaciones declaradas son diferentes (refiriéndose a la seguridad nacional, en 2001, y la salud pública, en 2020), ambos fenómenos (acción terrorista y pandemia) sirven como justificación para el aumento de las acciones de vigilancia en las potencias mundiales antes mencionadas, que utilizan el miedo público para aumentar el control sobre sus ciudadanos. **Conclusiones**: La vigilancia estatal, ya sea en los llamados países democráticos o autoritarios, opera desde una perspectiva dialéctica de protección y control, siendo necesario establecer límites al uso de datos personales por parte de los gobiernos y la defensa de la privacidad de las personas.

Descriptores: Vigilancia. Privacidad. Ética de la información. Ética intercultural de la información. Coronavirus. COVID-19.

Recebido em: 23.04.2020

Aceito em: 21.09.2020