ARTIGO

Do rastreamento de contato à vigilância: um estudo sobre o TraceTogether App

From contact-tracing to surveillance: a TraceTogether App study

Sergio Marcos Carvalho de Ávila Negri [a]

Nathan Paschoalini Ribeiro Batista [a]

RESUMO: Em à meio pandemia do SARS-CoV-2, também denominado de Covid-19, houve a intensificação do diálogo entre medidas sanitárias e tecnológicas para o combate e contenção do vírus. Nesse contexto, o presente trabalho tem por objetivo estudar a possível lógica de vigilância que permeia os aplicativos de rastreamento de contato utilizados para combate à pandemia. Valendo-se dos conceitos de Capitalismo de Vigilância e cultura de vigilância, parte-se de um desenvolvimento teórico, ancorado à análise empírica do caso de Cingapura, orientado pelas Regras de Inferência elaboradas por Epstein e King, a fim de verificar se o desvio de finalidade em sua utilização representa um reforço à lógica de vigilância vigente. Ao final conclui-se que, a depender de seu conteúdo, as alterações feitas nas políticas de privacidade podem reforçar uma lógica de vigilância que incide, especialmente, sobre populações historicamente perseguidas e marginalizadas.

Palavras-chave: Capitalismo de Vigilância; Proteção de Dados; TraceTogether App; Rastreamento de Contato.

ABSTRACT: In the midst of the SARS-CoV-2 pandemic, also known as Covid-19, there has been an intensified dialogue between health and technological measures to combat and contain the virus. In this context, this paper aims to study the possible surveillance logic that permeates the contact-tracing applications used to combat the pandemic. Drawing on the concepts of Surveillance Capitalism and surveillance culture, it starts from a theoretical development, anchored in the empirical analysis of the Singapore case, guided by the Rules of Inference developed by Epstein and King, in order to verify whether the deviation of purpose in the app's usage represents a reinforcement of the surveillance logic in place. In the end, we conclude that, depending on their content, the changes made in privacy policies may reinforce a logic of surveillance that especially affects historically persecuted and marginalized populations.

Keywords: Surveillance Capitalism; Data Protection; TraceTogether App; Contact-tracing.

[a] Faculdade de Direito, Universidade Federal de Juiz de Fora, Juiz de Fora, MG, Brasil.

* Correspondência para/*Correspondence to*: Nathan Paschoalini Ribeiro Batista. Endereço: Universidade Federal de Juiz de Fora, Faculdade de Direito - Universidade Federal de Juiz de Fora (Campus UFJF) - São Pedro, 36036900 - Juiz de Fora, MG - Brasil. E-mail: smcnegri@yahoo.com.

Recebido em/*Received*: 23/04/2021; Aprovado em/*Approved*: 17/06/2021.

INTRODUÇÃO

No início de 2020, a partir da decretação da pandemia de Covid-19 pela OMS, diversas iniciativas de contenção e combate ao coronavírus foram desenvolvidas em razão da crise sanitária de escala global. Dentre aquelas práticas consideradas velhas amigas da medicina e epidemiologia, encontra-se o rastreamento de contato que consiste em identificar, avaliar e acompanhar pessoas que foram expostas à doença, com intuito de se prevenir maior alastramento do vírus (Organização Pan-Americana de Saúde 2020).

Contudo, as práticas manuais de rastreamento de contato demonstraram-se insuficientes, considerando as enormes dimensões que a transmissão do Covid-19 tomou. Nesse sentido, iniciou-se o diálogo entre as medidas sanitárias e tecnológicas, de modo que fossem desenvolvidas ferramentas capazes de auxiliar nesse processo. Como resultado disso, surgem os aplicativos de rastreamento de contato – contact-tracing –, baseados nas mais diversas tecnologias de coleta de dados, sejam estes pessoais ou não.

Tal diálogo somente foi possível pela intensa virtualização da vida humana, processo em que há uma constante dataficação dos indivíduos, de maneira que as informações pessoais passam a ocupar posição fundamental na organização econômica e social, razão pela qual desenvolve-se uma nova lógica de acumulação de capital denominada de Capitalismo de Vigilância, permeado e sustentado pelo desenvolvimento de uma cultura de vigilância.

Dessa maneira, o presente trabalho tem por objetivo investigar as relações existentes entre os aplicativos de rastreamento de contato e a cultura de vigilância, questionando se a utilização dessas aplicações móveis favorece o estabelecimento de tal cultura.

Sendo assim, esta investigação pretende estabelecer as estratégias teórico-metodológicas a serem utilizadas para orientar o desenvolvimento da pesquisa (item 1), de modo que seja possível traçar os principais conceitos que orientarão o presente trabalho (itens 2, 3 e 4).

Uma vez desenvolvidas as discussões relativas aos conceitos fundamentais deste artigo, serão discutidos os motivos pelos quais houve a adoção de medidas tecnológicas para combate e contenção da pandemia, bem como haverá uma breve descrição das principais tecnologias utilizadas no rastreamento de contato (itens 5 e 6).

A partir disso, será analisado o aplicativo TraceTogether, desenvolvido pelo governo de Cingapura (item 7), como substrato empírico para desenvolvimentos teóricos posteriores, momento em que serão elaboradas algumas considerações sobre a anonimização de dados pessoais (item 8) e sobre as potencialidades de vigilância decorrentes do desvio de finalidade no uso dos dados pessoais coletados pelo aplicativo (itens 9 e 10).

ESTRATÉGIAS TEÓRICO-METODOLÓGICAS

O presente trabalho possui como horizonte teórico a categoria Capitalismo de Vigilância definida por Shoshana Zuboff em *The Age of Surveillance Capitalism* (2019), bem como a noção de cultura de vigilância estabelecida por David Lyon (2019). Ambas as conceituações serão abordadas mais detalhadamente adiante. Não obstante a isso, em suma, o Capitalismo de Vigilância diz respeito a uma nova expressão do capitalismo, a qual sustenta-se sobre a expropriação de dados gerados a partir do comportamento do usuário no ciberespaço (Zuboff 2019).

Para tanto, a vigilância desempenha um papel fundamental na manutenção dessa nova forma de organização econômica, de maneira que o desenvolvimento e intensificação de uma cultura de vigilância faz-se imprescindível. Tal cultura de vigilância é entendida a partir da compreensão de Lyon (2019), na qual a vigilância passa a ser estabelecida como algo ubíquo e aceito pelos cidadãos, seja conscientemente ou não.

Associado aos dois conceitos anteriores, também será adotada a concepção de *dataveillance*, isto é, a coleta e monitoramento sistemáticos de dados pessoais, com intuito de se efetivar controle social (Clarke 1988).

A partir destas disposições, tendo como suporte teórico os conceitos ora explicitados, questiona-se: considerando a vigência de uma nova lógica de acumulação de capital denominada Capitalismo de Vigilância, é possível afirmar que a utilização de aplicativos móveis de rastreamento de contato para a contenção e combate da pandemia de Covid-19 potencializa uma lógica de vigilância sobre os indivíduos?

Como hipótese ao questionamento acima, sustenta-se que a prática de vigilância intermediada por dados pessoais sensíveis está diretamente vinculada à finalidade e ao tratamento ao qual a coletânea de dados será submetida, tendo em vista que o dado não é ontologicamente nocivo (Doneda 2019). Nesse sentido, caso haja desvio de finalidade na utilização dos dados coletados pelos aplicativos para contenção e combate da pandemia de Covid-19, finalidade esta expressamente consentida pelos usuários, é possível que se potencialize a lógica de vigilância sobre os indivíduos.

A fim de possibilitar a investigação do questionamento feito acima, será adotada, em um primeiro momento, uma abordagem exploratória, o que permitirá uma maior aproximação com o objeto de estudo (Gil 2018). Tal etapa valer-se-á da pesquisa bibliográfica com intuito de definir as bases teóricas que orientarão o desenvolvimento da pesquisa.

Em um segundo momento, será adotada uma perspectiva empírica, a partir do caso de Cingapura, visando identificar as variáveis fundamentais que sustentam a presente pergunta de pesquisa, quais sejam: desvio de finalidade e aumento na lógica de vigilância. Nesse sentido, ao final do trabalho, espera-se que seja possível estabelecer a correlação entre as referidas variáveis, com vistas a se estabelecer formulações teóricas acerca desta relação, assumindo, portanto, um caráter descritivo (Gil 2018).

O referido caso, que servirá de aporte empírico para formulações posteriores neste trabalho, diz respeito ao aplicativo móvel de rastreamento de contato, denominado TraceTogether, desenvolvido pela Smart Nation, iniciativa governamental de digitalização de Cingapura (Smart Nation 2018), com objetivo de contenção e combate à pandemia de Covid-19. A escolha por tal caso justifica-se pelo fato de Cingapura ter sido o primeiro país a implementar um aplicativo nacional de rastreamento do novo coronavírus[1], bem como pelo fato de ter havido uma significativa adesão dos cidadãos ao TraceTogether, tendo em vista que cerca de 80% da população do país realizou o *download* do aplicativo em seu dispositivo móvel, de acordo com informações disponibilizadas pela agência de notícias Reuters em 04 de janeiro de 2021 (Reuters 2021).

A despeito do caráter eminentemente teórico desta pesquisa, há de se destacar também o seu perfil empírico. Segundo Epstein e King (2013), a empiria denota a existência de evidências sobre o mundo, que sejam baseadas tanto na observação, quanto na experiência. Tais evidências podem ser quantitativas ou qualitativas, não se estabelecendo entre ambas uma ordem hierárquica.

O caráter empírico do trabalho, todavia, não é suficiente para que seus resultados sejam considerados válidos e relevantes para a produção científica, sendo necessário, portanto, que o desenvolvimento da pesquisa esteja orientado por regras responsáveis para a condução das inferências a serem realizadas (Epstein, King, 2013). Sendo assim, para que seja possível estabelecer a correlação entre distintas variáveis – quais sejam: desvio de finalidade e aumento da lógica de vigilância – o presente trabalho se vinculará às regras de inferência, especialmente às inferências descritivas, as quais consistem no processo que busca conhecer fatos desconhecidos a partir de informações já conhecidas pelo pesquisador, a fim de fundamentar suas conclusões (Epstein, King 2013).

DADOS PESSOAIS

Para se alcançar a definição de dados pessoais é necessário que se compreenda, antes, suas relações com os direitos da personalidade. Segundo Bioni (2019), o Direito busca tutelar aquelas violações que atingem diretamente as individualidades, em razão dos seres humanos serem constituídos por características que os diferem entre si, bem como entre os demais entes. Sendo, portanto, uma proteção dos elementos "que emprestam conteúdo ao valor-fonte do ordenamento jurídico, aos bens (da personalidade) que individualizam o sujeito perante a sociedade." (Bioni 2019, p. 99).

Dessa maneira, segundo Bioni (2019), um dado que se vincule à pessoa carrega a possibilidade de ser inserido nos direitos da personalidade. Tal possibilidade caminha *pari passu* com a necessidade de que este dado seja "adjetivado como pessoal" (BIONI,

[1] TraceTogether: Singapore turns to wearable contact-tracing Covid tech: https://www.bbc.com/news/technology-53146360

2019, p. 99), de forma que seja possível identificá-lo como uma extensão de seu titular, isto é, uma projeção daquele a quem o dado pessoal diz respeito.

Em um contexto de completa digitalização da vida humana – processo que, segundo, Costa e Oliveira (2019) e Bioni (2019), foi potencializado pelo desenvolvimento tecnológico e amparado pela evolução das Tecnologias da Informação e Comunicação (TICs), especialmente a Internet – os dados pessoais tornaram-se personagens protagonistas, sendo, portanto, fundamental a compreensão sobre o seu conceito.

Nessa toada, pode-se falar em duas perspectivas quanto à conceituação de dados pessoais: reducionista e expansionista. A perspectiva reducionista compreende o dado pessoal como sendo aquele vinculado à pessoa identificada "cujo vínculo com seus dados é direto, preciso ou exato" (Branco 2020, p. 32).

Em contrapartida, a visão expansionista, segundo Branco (2020), é aquela na qual considera-se dado pessoal todo aquele relacionado à pessoa identificada ou identificável "por meio de um vínculo mediato, indireto, impreciso ou inexato entre a pessoa e seus dados (...)" (Branco 2020, p. 32). Tal perspectiva foi a adotada tanto pelo Regulamento Geral sobre Proteção de Dados[2] (RGPD), a diretiva da União Europeia sobre o tema de proteção de dados pessoais, quanto pela Lei nº 13.709/2018, a Lei Geral de Proteção de Dados[3] (LGPD), o diploma legal brasileiro.

DADOS PESSOAIS SENSÍVEIS

A compreensão do conceito de dados pessoais como uma extensão da pessoa leva-nos à identificação de determinada categoria de informações cuja tutela tem de se diferenciar daquela oferecida aos demais tipos de dados. Trata-se da categoria de dados pessoais sensíveis. Segundo Korkmaz (2019), a definição de dados pessoais sensíveis, enquanto categoria autônoma, tem como substrato a presunção de que o uso indevido de determinadas informações poderia ter consequências mais graves ao exercício de direitos fundamentais individuais, como por exemplo o direito à privacidade e a não discriminação, do que aquelas consequências decorrentes do uso indevido de outros dados pessoais (Article 29 Data Protection Working Party 2011).

Dessa maneira, segundo Konder (2019), existe uma verdadeira renovação da dignidade da pessoa humana com intuito de tutelar, frente às possíveis ameaças decorrentes do uso indevido de dados pessoais, a liberdade de se exercer e constituir a personalidade da pessoa humana. Nesse sentido, a preocupação com processos discriminatórios e estigmatizantes decorrentes do uso e tratamento de dados pessoais provocou a necessidade de se classificar aquelas informações que possuem maior facilidade em

[2] Art. 4º do RGPD: "For the purposes of this Regulation: (1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject') [...];" (UNIÃO EUROPEIA, 2018). Disponível em: https://gdpr-info.eu/art-4-gdpr/

[3] Art. 5º da LGPD: "Para os fins desta Lei, considera-se: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;" (BRASIL, 2018). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

ocasionar e evidenciar a exclusão social e segregação, de forma que o controle sobre seu tratamento e uso seja ainda mais severo (Konder 2019).

O "núcleo duro" da privacidade, como aponta Rodotà (2008), estrutura-se ainda hoje sobre as informações que dizem respeito à "tradicional necessidade de sigilo" (Rodotà 2008, p. 95), como aquelas relativas à saúde e a hábitos sexuais. Não obstante isso, outras categorias de informação, segundo Rodotà (2008), ocupam espaço de notável relevância, estando sob proteção com intuito de evitar que sua circulação enseje situações de discriminação, como por exemplo informações relativas à raça e credo religioso.

Justamente pelas potencialidades lesivas decorrentes da circulação dessas informações, a estes dados são impostas medidas mais rigorosas no que diz respeito à sua circulação, com objetivo de se garantir "plenitude à esfera pública" (Rodotà 2008, p. 96). Tais medidas podem expressar-se a partir da proibição da coleta dessas informações por determinados sujeitos e a partir da exclusão da legitimidade de certas formas de coleta e tratamento desses dados (Rodotà 2008).

Mulholland (2020), todavia, entende que tanto a conceituação quanto o conteúdo constitutivo da categoria de dados pessoais sensíveis são passíveis de críticas, tendo em vista que até mesmo um dado que, em si, não é considerado sensível, quando submetido a determinado tipo de tratamento, pode ser elevado à tal categoria, revelando aspectos considerados sensíveis sobre a personalidade do titular desses dados (Doneda 2019). Nesse sentido, Doneda (2019) afirma que o dado não é ontologicamente discriminatório ou perigoso, mas sim o uso que é feito deste.

Portanto, o conceito de dados sensíveis deve ser encarado de maneira funcional, observando o tipo de tratamento ao qual ele é submetido (Mulholland 2020). Isso significa, que o dado é considerado sensível não somente por sua característica "intrinsecamente personalíssima, de forma apriorística, mas devido ao uso e finalidade que é concedido a esse dado por meio de um tratamento que pode gerar uma potencialidade discriminatória abusiva" (Mulholland 2020, p. 123).

Nessa toada, fala-se que os dados relativos à saúde são, em si, considerados sensíveis, pois que sua utilização pode resultar em cenários de discriminação e, consequentemente, de violação de direitos fundamentais. Havendo, inclusive, disposições legislativas, tanto no RGPD[4] quanto na LGPD[5] que, explicitamente, os definem como sendo sensíveis.

[4] Art 9 do RGPD: (1) "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited. " (UNIÃO EUROPEIA, 2018). Disponível em: https://gdpr-info.eu/art-9-gdpr/

[5] Art. 5º da LGPD: "Para os fins desta Lei, considera-se: "II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida

Dessa forma, faz-se necessário, segundo Rodotà (2008), dedicar uma maior atenção à esse tipo de informação pelo fato de que se relaciona com a "nua condição humana [...]" (Rodotà 2008, p. 248), de modo que, conforme Korkmaz (2019), tais informações não dizem respeito somente à tutela da vida privada dos indivíduos, mas expressa-se como garantidor da igualdade entre as pessoas.

Apesar de a conceituação funcional dos dados sensíveis ser uma abordagem mais adequada, capaz de proporcionar uma maior proteção ao titular dos dados, destaca-se que as violações decorrentes do tratamento inadequado de dados sensíveis impactam de maneiras distintas nos diferentes grupos constituintes da sociedade, de forma que os impactos incidirão de maneira ainda mais incisiva sobre grupos historicamente discriminados e oprimidos (Machado, Negri, Giovanini 2020).

CAPITALISMO DE VIGILÂNCIA E CULTURA DA VIGILÂNCIA

De acordo com Bioni (2019), a atual formação social tem na informação o elemento fundamental para o desenvolvimento da economia. Sua reorganização em torno desse novo elemento foi possibilitada pelo crescente desenvolvimento tecnológico, que viabilizou a existência de mecanismos capazes de processar e transmitir informações de formas e velocidades não antes imaginadas. Dessa maneira, a informação passa a ocupar uma posição central no que se denomina de sociedade informacional, considerando seu caráter estruturante no processo de reorganização das conformações sociais (Bioni 2019).

Reconhecendo o valor da posição ocupada pela informação, Alan Westin (1967), na década de 1960, alertava para a possibilidade de vigilância[6] efetivada por meio de dados, especialmente aquela feita pelos governos sobre os indivíduos, justamente pelo aumento na capacidade computacional de processamento de informações. Segundo Westin (1967), para se compreender os impactos na privacidade decorrentes do aumento no processamento de informações, seria necessário observar seis tendências que se iniciavam naquele momento. Resumidamente, tais tendências orbitam o fato de que a sociedade da informação se tornou a maior sociedade produtora de dados da história da humanidade, tendo em vista o processo de digitalização e dataficação da vida, o que pode acarretar, dentre outras possibilidades, a criação de perfis sociais.

Stefano Rodotà (2008), assim como Westin, demonstrava preocupação com o que se denomina de *profiling*, isto é, técnicas de perfilação de grupos de pessoas. Segundo o

sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural; " (BRASIL, 2018). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

[6] Segundo Clarke (1988), trata-se de vigilância a prática sistemática de investigações e monitoramento das ações e/ou comunicações de um ou mais indivíduos, tendo como principal objetivo a coleta de informações sobre estes sujeitos, suas atividades, bem como suas associações

autor, o aumento na quantidade e qualidade das informações fornecidas pelos sujeitos com objetivo de acessar determinados serviços possibilitam

> uma série de usos secundários, especialmente lucrativos para os gestores dos sistemas interativos. Estes, [...], podem 'criar' informações novas (perfis de consumo individual ou familiar, análises de preferência, informações estatísticas, etc.), que interessam a outros sujeitos, a quem estas informações podem ser vendidas (Rodotà 2008, p. 46).

Podendo, assim, ocasionar uma lógica sistemática de vigilância por meio de dados (Westin 1967).

Apesar do constante processo de digitalização das experiências humanas que, segundo Costa e Oliveira (2019), ocorrem sob os auspícios do desenvolvimento das tecnologias da informação e comunicação (TICs), em especial a Internet, Bioni (2019) aponta para o fato de que o atual estágio da sociedade não se resume aos ambientes virtuais, a despeito da potencialização nas dinâmicas de coleta e tratamento das informações que o referido desenvolvimento tecnológico provocou.

Como desdobramento do protagonismo das informações, especialmente no que diz respeito à sua coleta, manipulação e uso, Zuboff (2019) compreende que há uma mudança paradigmática quanto à forma de acumulação de capital nessa nova forma de sociabilidade. Tal modificação dá origem ao que ela denomina de Capitalismo de Vigilância que se desenvolveu com a evolução das TICs, em especial com o desenvolvimento do que se denomina de Web. 2.0. Neste momento, houve a proliferação de sítios eletrônicos, redes sociais e, consequentemente, uma transposição de partes das interações sociais para ambientes virtuais (Dijck 2014), isto é, para o ciberespaço. Sendo este, segundo Levy (2014), o espaço de comunicação possibilitado pela Internet e pelos computadores.

Zuboff (2019) salienta que o Capitalismo de Vigilância não diz respeito à tecnologia em si, mas refere-se a uma lógica que orienta o desenvolvimento das tecnologias, de forma que a vigilância ocupe uma posição central nessa nova forma de acumulação de capital que avança sobre todos os aspectos da vida humana e se alimenta da expropriação de informações sobre os indivíduos, buscando o que ela denomina de superávit comportamental (*behavioral surplus*), extraído a partir do comportamento dos usuários em ambientes digitais. O Capitalismo de Vigilância opera através de assimetrias de conhecimento e de poderes, de maneira que os capitalistas da vigilância têm a possibilidade de saber tudo sobre os vigiados, enquanto estes são incapazes de conhecer quaisquer informações sobre aqueles que vigiam, tendo em vista que suas operações foram desenhadas para esse fim, estabelecendo, assim, uma opacidade na relação entre vigilante e vigiado (Zuboff 2019).

Levando em consideração a centralidade da vigilância para a manutenção dessa forma de capitalismo, Lyon (2018) aponta para o fato de que se vive em um momento no qual há o surgimento de uma cultura de vigilância sem precedentes, cuja característica é a

participação intensa das pessoas com vistas a regular sua própria vigilância e aquela realizada sobre os outros. Fala-se em cultura, pelo fato de que a vigilância não é mais algo externo que se impõe à vida dos indivíduos, mas que é aceita pelos cidadãos, seja de modo consciente ou não, vigilância esta "com que negociam, a que resistem, com que se envolve e, de maneiras novas, até iniciam e desejam" (Lyon 2019, p. 153).

Assim como o protagonismo das informações no seio da sociedade informacional, a cultura da vigilância deve ser analisada sob a ótica do crescimento da "modernidade digital no século XX, mas especialmente no século XXI" (Lyon 2019, p. 154), sendo, portanto, um produto desta. Nesse sentido, partir do final do século passado, a vigilância tornou-se componente fundamental para a organização das sociedades que foram capazes de desenvolver infraestruturas de informação, cujas complexidades eram gerenciadas a partir da categorização (Lyon 2019).

Dessa forma, trata-se, segundo Lyon (2019), de uma obviedade a referência à vigilância como uma verdadeira indústria, haja vista que grandes corporações estão envolvidas nos processos de vigilância, estabelecendo, em muitos casos, íntimas relações com governos. Isso pôde ser evidenciado pelas informações disponibilizadas por Edward Snowden em 2013, quando apontou para o fato de que a Agência de Segurança Nacional (NSA) dos Estados Unidos possuía acesso aos metadados de companhias telefônicas, bem como que tal agência "garimpa as bases de dados de clientes de empresas de internet como Apple, Google, Microsoft, Amazon e Facebook (por vezes mencionadas como as 'Cinco Grandes')" (Lyon 2019, p. 155).

Segundo Lyon (2019), com a expansão da vida mediada por dispositivos digitais, os sujeitos não são tidos como simples alvos da vigilância, mas como "participantes cada vez mais conscientes e ativos" (Lyon 2018, p. 159). Essa relação dos sujeitos com a vigilância expressa-se patentemente quando da utilização das redes sociais, bem como de aplicações para a Internet como um todo, o que fez aumentar o emprego cotidiano de uma gama de mentalidades e práticas de vigilância (Lyon 2019).

Sendo assim, as atuais práticas de vigilância não se caracterizam das formas tradicionalmente conhecidas, nas quais os sujeitos são isolados e imobilizados em espaços de confinamento,

> mas que se aproxima ou mesmo se confunde com o fluxo cotidiano de trocas informacionais e comunicacionais. Uma vigilância que se exerce menos com o olhar do que com sistemas de coleta, registro e classificação da informação; menos sobre os corpos do que sobre dados e rastros deixados no ciberespaço; menos com o fim de corrigir e reformar do que com o fim de projetar tendências, preferências, interesses. (Bruno 2006, p. 153)

Dessa maneira, Bruno (2006), entende que os hodiernos dispositivos de vigilância, especialmente aqueles utilizados para vigilância digital, são constituídos de três características fundamentais: "a informação, os bancos de dados e os perfis computacionais" (Bruno 2006, p. 154), tendo na primeira característica o seu elemento-

base. Tais dispositivos de vigilância são imbuídos de maior capacidade de coleta, registro e processamento de dados provenientes dos sujeitos, de modo que as mesmas tecnologias que possibilitam a amplificação da emissão, acesso e distribuição de informações são transformadas em dispositivos de vigilância e controle. Havendo, portanto, uma confusão entre a vigilância e o ciberespaço (Bruno 2006)

Dessa maneira, assim como alertava Westin (1967), podemos falar em uma vigilância mediada por dados – *dataveillance*. Segundo Clarke (1988), *dataveillance* consiste no uso sistemático de dados pessoais com objetivo de investigar ou monitorar as ações ou comunicações de um ou mais sujeitos. Tal manifestação de vigilância pode-se dar sobre uma massa de sujeitos (*mass dataveillance)* ou sobre pessoas, individualmente compreendidas (*personal dataveillance)* (Clarke 1988).

COMBATE AO COVID-19: POR QUE UTILIZAR FERRAMENTAS TECNOLÓGICAS PARA MONITORAR E RETARDAR A PANDEMIA?

No início do ano de 2020, foi decretada a pandemia[7] ocasionada pela proliferação desordenada do vírus SARS-CoV-2, também denominado de Covid-19. Com o acirramento da crise sanitária, diversas medidas de contenção e combate ao coronavírus foram desenvolvidas e implementadas, inclusive as medidas tradicionais de *lockdown* e rastreamento de contato, práticas já conhecidas da medicina.

A despeito disso, segundo Abeler *et al* (2020), os índices relativos ao vírus aumentariam, assim que as medidas de *lockdown* fossem flexibilizadas. Tal situação levou os cientistas ao desenvolvimento de uma nova forma de abordagem para a contenção da pandemia: o desenvolvimento de aplicativos para o rastreamento de contato – *app-based contact-tracing* (Abeler *et al* 2020).

Dessa maneira, diversos aplicativos foram desenvolvidos e implementados, com intuito de se monitorar os avanços da pandemia, como por exemplo o aplicativo TraceTogether, implementado pelo governo de Cingapura. A justificativa para a implementação de ferramentas tecnológicas para a contenção da pandemia residia no fato de que uma maior rapidez no rastreamento de contato, combinado com testagem em massa poderia retardar o avanço do Covid-19, bem como, considerando os modelos matemáticos elaborados, poderia até interromper, de uma vez por todas, a pandemia (Abeler *et al* 2020).

TECNOLOGIAS DE RASTREAMENTO DE CONTATO

Segundo Negri e Giovanini (2020), para o combate da pandemia, inciativas públicas e privadas valeram-se da coleta de dados de localização passíveis de serem obtidos por meio de diversas tecnologias, como a utilização do Sistema de Posicionamento Global

[7] Ver mais sobre a decretação da pandemia do novo coronavírus em: https://agenciabrasil.ebc.com.br/geral/noticia/2020-03/organizacao-mundial-da-saude-declara-pandemia-de-coronavirus

(GPS) dos telefones celulares, conexões em redes WiFi, triangulação de antenas telefônicas e tecnologias de *Bluetooth Low Energy*.

As informações do GPS disponíveis em celulares são coletadas "a partir do uso de diferentes aplicativos provedores de serviços, como aplicativos de transporte, mapas e rotas, trânsito etc." (Negri, Giovanini 2020, p. 14). A triangulação de antenas telefônicas, por sua vez, opera de modo a monitorar as conexões que telefones celulares fazem com as diversas antenas existentes em um determinado local, indicando que houve uma movimentação (Negri, Giovanini 2020). Quanto à utilização de tecnologias baseadas em *Bluetooth Low Energy*, vale destacar o desenvolvimento, a partir de um esforço conjunto da Apple e da Google, de um protocolo Bluetooth com objetivo de auxiliar as técnicas digitais de *contact-tracing*. Esse novo sistema possibilita uma rede de rastreamento de contato voluntário, mantendo um extenso banco de dados sobre os aparelhos celulares que estiveram próximos uns dos outros. De acordo com Brandom e Robertson (2020), os aplicativos oficiais de autoridades de saúde pública terão acesso a esses dados e os usuários que, voluntariamente, utilizarem o aplicativo poderão informar caso tenham sido diagnosticados com Covid-19.

Segundo Negri e Giovanini (2020), a interface de programação de aplicações (API) desenvolvida conjuntamente pela Apple e Google funciona a partir de códigos de identificação e chaves de rastreamento únicos, disponibilizados aos usuários que decidirem utilizar o sistema. Tais códigos de identificação são compostos por uma sequência de números aleatórios que se altera em períodos entre 10 e 20 minutos (Negri, Giovanini, 2020).

Inobstante aos diversos métodos de se coletar dados com objetivo de promover o rastreamento de contato, Kitchin (2020) aponta para o fato de que tais métodos são imprecisos para um rastreamento de contato significativo, considerando as limitações intrínsecas às tecnologias utilizadas no desenvolvimento dos aplicativos, como por exemplo as próprias limitações de funcionamento de GPS em locais fechados ou o fato de que tanto o GPS quanto o Bluetooth não serem capazes de determinar a existência de alguma barreira física entre os indivíduos em contato.

TRACETOGETHER APP: A SOLUÇÃO TECNOLÓGICA DE CINGAPURA PARA A CONTENÇÃO DO COVID-19

Assim como diversos países, o Governo de Cingapura, por meio de sua Agência de Tecnologia (GovTech) e de seu Ministério da Saúde (MOH), apostou em uma iniciativa tecnológica para a contenção da pandemia de Covid-19. Em 20 de março de 2020, foi lançado o aplicativo móvel TraceTogether, objetivando acelerar o rastreamento de contato daqueles indivíduos que estiveram em contato com casos confirmados de Covid-19 (DUSSUTOUR, 2020). Sendo, portanto, um dos primeiros países a implementar um aplicativo nacional de *contact-tracing*.

Segundo comunicado de imprensa do Governo de Cingapura (2020), a justificativa para o desenvolvimento do aplicativo encontra-se no fato de que os procedimentos

tradicionais de rastreamento de contato dependem da memória dos entrevistados, havendo casos em que estes entrevistados não conseguem se lembrar de todos os contatos que realizaram ou até mesmo não têm informações sobre com quem estiveram em contato (Cingapura 2020).

O aplicativo funciona a partir da troca de sinais Bluetooth de curta distância, de maneira que se torna possível detectar outros usuários do TraceTogether que estejam nas proximidades. Com base nessa informação o aplicativo estima a distância entre os usuários e a duração dos encontros (Cingapura 2020).

De acordo com o governo de Cingapura, os dados produzidos são criptografados e armazenados localmente no telefone do usuário durante um período de 21 dias, período correspondente ao tempo de incubação do vírus (Cingapura 2020). Estabeleceu-se o consentimento como base legal para a coleta e tratamento destes dados, sendo possível retirá-lo a qualquer momento. (Cingapura 2020).

Dessa maneira, o usuário, ao se cadastrar no aplicativo, deve consentir com os seguintes elementos: fornecimento do número de telefone no painel de configuração inicial do TraceTogether; autorizar que os dados de proximidade sejam coletados e armazenados no telefone do usuário pelo período de 21 dias; ser contatado pelo Ministério da Saúde de Cingapura, caso haja provável contato com pessoa contaminada pelo novo coronavírus; e autorizar o envio dos dados coletados pelo aplicativo ao Ministério da Saúde de Cingapura para auxiliar no rastreamento de contato (Cingapura 2020).

Segundo as garantias de privacidade estabelecidas pelo Governo de Cingapura, no momento em que se cadastra no aplicativo, é gerado um código de identificação (User ID) aleatório que será associado ao seu número de telefone e informações de identificação pessoais (TraceTogether 2020). Tais dados, segundo o TraceTogether (2020), são armazenados em um servidor seguro, e não são disponibilizados ao público.

A política de privacidade do aplicativo estabelece que não realizam a coleta de dados provenientes de GPS, WiFi ou rede móvel de Internet. Acrescentam, ainda, que os dados gerados a partir do encontro de usuários do aplicativo são anonimizados, a partir de uma identificação temporária (Temporary ID), que consiste em criptografar a identificação do usuário com uma chave privada mantida em posse do Ministério da Saúde de Cingapura, sendo este o único ente capaz de descriptografar tais dados (TraceTogether 2020).

Ainda nas garantias de privacidade, o TraceTogether assegura a impossibilidade de terceiros rastrearem e identificarem os usuários, tendo em vista que a identidade temporária, aquela trocada entre outros aparelhos de usuários, é atualizada em intervalos regulares, impossibilitando o acesso de tais informações por terceiros (TraceTogether 2020).

Por fim, é estabelecido que os dados compartilhados com o Ministério da Saúde serão usados, tão somente, para propósitos de rastreamento de contato, reforçando que Governo de Cingapura somente terá acesso aos dados que forem manualmente enviados ao servidor pelos usuários.

Não obstante a isso, no dia 04 de janeiro de 2021, houve uma atualização da política de privacidade do aplicativo. Tal atualização estabeleceu que os dados coletados pelo TraceTogether poderão ser utilizados pela polícia de Cingapura em casos que se faça necessário o uso destes para fins de investigação criminal e demais procedimentos relativos à sete categorias de ofensas graves, as quais estarão dispostas no quadro a seguir[8]:

Quadro 01. Categorias de ofensas graves que permitem o acesso à polícia de Cingapura aos dados coletados pelo TraceTogether.

Num.	Categorias de crimes graves
1	Crimes envolvendo o uso ou posse de substâncias corrosivas, e armas perigosas
2	Atos terroristas que estejam sob a Lei Antiterrorismo de Cingapura
3	Crimes contra pessoa, nos quais a vítima esteja gravemente ferida ou morta
4	Crimes relacionados ao tráfico de drogas, que estão sujeitos à pena de morte
5	Fuga da custódia legal, na qual há motivos razoáveis para acreditar que o sujeito poderá causar danos a outrem
6	Sequestro
7	Crimes sexuais graves

Fonte: elaborado pelo próprio autor a partir das categorias de crimes definidas pelo Governo de Cingapura

CONSIDERAÇÕES ACERCA DA RETÓRICA DA ANOMIZAÇÃO DOS DADOS PESSOAIS

Apesar de o objetivo do presente trabalho não ser o de discorrer sobre as implicações decorrentes da retórica da anonimização no enfrentamento da Covid-19, faz-se necessário destacar alguns pontos referentes à esta categoria de dados.

Ao contrário do exposto anteriormente, aquelas informações que não possuem associação com a pessoa identificada ou identificável, desde a sua origem ou após tratamento, são denominadas de dados não pessoais, de maneira que não podem ser identificados nem pelo encarregado de dados ou qualquer outra pessoa (Article 29

[8] Trata-se de reprodução e tradução da tabela disponível em: https://www.sgpc.gov.sg/sgpcmedia/media_releases/sndgo/press_release/P-20210108-1/attachment/Press%20Release_Legislative%20Provisions%20for%20Usage%20of%20TT%20Data%20-%20Final.pdf

Data Protection Working Party 2007). Segundo Finck e Pallas (2020), os dados não pessoais são imbuídos, atualmente, de considerável valor econômico, de modo que a sua conceituação não se restringe a apenas um interesse acadêmico, mas possui relevância "prática para qualquer processamento que venha a ser utilizado" (Negri, Giovanini 2020, p.6).

Como exemplos de dados não pessoais, a regulamentação da União Europeia sobre o fluxo livre de dados não pessoais (2018) estabelece o dado agregado e o anonimizado, sendo este último a que interessa para o presente debate. Segundo Negri e Giovanini (2020), o processo de anominização é responsável por desvincular determinada informação da pessoa à qual ela se refere.

Assim como existe a anonimização de dados pessoais, pode-se falar na existência de uma pseudoanonimização. No entanto, esta, segundo o Grupo de Trabalho do Artigo 29 sobre técnicas de anonimização (2014), não é considerada um método de anonimização, porque a pseudoanonimização somente diminui a vinculatividade de uma coletânea de dados à sua identidade original, a quem o dado diz respeito. Razão pela qual é uma armadilha considerar o dado pseudoanonimizado equivalente a um dado anonimizado (Article 29 Data Protection Working Party 2014).

Dessa maneira, pode-se dizer que os dados coletados pelo TraceTogether, conforme disposição de sua política de privacidade, são submetidos ao processo de pseudoanonimização, haja vista que estes são apenas submetidos a processos de criptografia, uma das técnicas elencadas pelo Grupo de Trabalho do Artigo 29 (2014) sobre Anonimização.

Todavia, mesmo que sejam utilizadas técnicas de anonimização dos dados pessoais, o que não é o caso aqui descrito, os dados não pessoais são passíveis de serem reidentificados, significa dizer que as técnicas de anonimização estão sujeitas aos riscos de reversão destes processos. Deve-se, portanto, se atentar à retórica da anonimização utilizada no enfrentamento da pandemia, uma vez que ela pode ser utilizada, a partir de seu apelo simbólico, para criar uma falsa sensação de segurança, neutralizando e atenuando os possíveis impactos decorrentes de violações quando da utilização de dados pessoais. (Negri, Giovanini 2020).

DESVIO DE FINALIDADE: A POLÍCIA DE CINGAPURA TERÁ ACESSO AOS DADOS COLETADOS PELO TRACETOGETHER

Como revelado anteriormente, na primeira semana de janeiro, o Governo de Cingapura promoveu uma alteração na política de privacidade do aplicativo móvel TraceTogether. Tal alteração permitiu que os dados pessoais coletados pelo aplicativo pudessem ser utilizados pela polícia do país em casos de investigação criminal e demais procedimentos relacionados à sete categorias de crimes, as quais foram reproduzidas acima.

Considerando que, segundo o comunicado de imprensa sobre o lançamento do aplicativo, o desenvolvimento dessa ferramenta estava vinculado ao combate e à contenção da pandemia de Covid-19, pode-se falar que houve desvio de finalidade ao autorizar que os dados pessoais coletados pelo aplicativo fossem utilizados para fins distintos daqueles relacionados ao combate da pandemia. Isto é, a finalidade para a qual os dados seriam coletados consistia no combate à pandemia, conforme pode-se evidenciar na seção da política de privacidade relativa à finalidade da coleta, tratamento e uso dos dados pessoais: "Qualquer dado compartilhado com o MOH (Ministério da Saúde) somente poderá ser usado para propósitos de rastreamento de contato [...]" (TraceTogether 2021)[9].

Destaca-se que, a despeito da mudança na política de privacidade do aplicativo – documento que garante a possibilidade de retirada do consentimento a qualquer tempo – afirma-se ter havido um desvio de finalidade material. Tal categoria, até então inédita, trazida ao presente texto, diz respeito à utilização dos dados pessoais para finalidades diversas daquelas inicialmente pactuadas, havendo alteração posterior na política de privacidade do serviço oferecido, a fim de se estabelecer o novo rol de finalidades.

A finalidade, no interior da tutela dos dados pessoais, é um princípio fundamental que deve nortear toda a manipulação dessas informações. Tal princípio surge a partir da necessidade de se informar o interessado sobre os fins para os quais os seus dados serão coletados, antes que seja realizada tal coleta (Doneda 2020). Dessa forma, garante-se a autodeterminação informativa ao titular dos dados, ou seja, assegura que este tenha controle sobre suas informações, de forma que ele consiga autodeterminar seus dados pessoais (Bioni 2019).

Sobre tal princípio, o Personal Data Protection Act (2012), instrumento de Cingapura para a tutela dos dados pessoais, informa em sua divisão 2, item 20, que podem ser definidas novas finalidades, desde que estas ainda não tenham sido realizadas, o qual encontra-se transcrito abaixo:

> 20. - (1) For the purposes of sections 14(1)(*a*) and 18(*b*), an organisation shall inform the individual of —
>
> (*a*) the purposes for the collection, use or disclosure of the personal data, as the case may be, on or before collecting the personal data;
>
> (*b*) any other purpose of the use or disclosure of the personal data of which the individual has not been informed under paragraph (*a*), before the use or disclosure of the personal data for that purpose; and

[9] Tradução nossa do trecho: "Any data shared with MOH can only be used for the purpose of contact tracing, (....)" (TRACETOGETHER, 2021)

> (*c*) on request by the individual, the business contact information of a person who is able to answer on behalf of the organisation the individual's questions about the collection, use or disclosure of the personal data. (Cingapura 2012)

Inobstante à referida autorização legislativa, a alteração no interior das finalidades de uso da coletânea de dados coletados pelo TraceTogether representa um rompimento na relação de confiança entre os usuários do aplicativo e o Governo de Cingapura, impactando, inclusive, em futuras iniciativas governamentais nas quais a coleta de dados pessoais venha a ser necessária.

Tal relação de confiança, é compreendida, segundo Waldman (2018), como um recurso de capital social entre dois ou mais sujeitos, no que diz respeito às expectativas de que tais sujeitos se comportarão de acordo com as normas aceitas pelas partes. No caso em análise, as normas acordadas pelas partes correspondem às finalidades incialmente estabelecidas pela Política de Privacidade do TraceTogether. Dessa maneira, fala-se em rompimento da relação de confiança, baseado no entendimento de que o exercício da privacidade das informações é construído sobre o estabelecimento de relações de confiança entre aqueles envolvidos no processo de compartilhamento e coleta dos dados (Waldman 2018).

DO DESVIO DE FINALIDADE À VIGILÂNCIA

Considerando o princípio da finalidade como um dos pilares fundamentais para se orientar a manipulação dos dados pessoais, tendo como horizonte a concretização da autodeterminação informativa, o desvio de finalidade material, como categorizado anteriormente, representa verdadeira violação da confiança, visto que a transparência é um dos principais fatores para o estabelecimento da privacidade, bem como para o desenvolvimento da relação de confiabilidade entre o usuário e aquele que manipula seus dados (Fischer-Hübner *et al* 2016).

Em um contexto de intensificação da cultura de vigilância, conforme descrito por Lyon (2019), a possibilidade de se alterar as finalidades para qual os usuários, inicialmente, consentiram e sob a qual os dados seriam coletados e manuseados, indica verdadeiro risco à privacidade. Mas, não somente a ela, tendo em vista que a proteção de dados

> é entendida também como importante termômetro às democracias, às condições de exercício de outros direitos fundamentais, como liberdade de expressão, liberdade de associação, liberdade profissional, sindical, direito à igualdade, e não apenas aos direitos de privacidade e intimidade (Machado, Negri, Giovanini 2020, p. 3-4)

No caso aqui estudado, o acesso aos dados coletados pelo aplicativo foi concedido à polícia de Cingapura, instituição que, necessariamente, exerce um poder sobre os indivíduos, fato que reitera a hipótese defendida neste trabalho.

O reforço de uma lógica de vigilância reitera violências e opressões a grupos que são historicamente perseguidos, tendo em vista que estes encontram-se expostos a riscos ainda maiores, justamente pelo fato de que "dados sobre a transmissão do coronovaírus circulam e são debatidos na esfera pública. Mesmo anonimizados, ao entrarem em domínio público, propiciam inferências, acertadas ou não, voltadas à culpabilização" (Machado, Negri, Giovanini 2020, p. 16)

Nesse sentido, não se pode considerar as demandas urgentes decorrentes da pandemia de Covid-19 como justificativas para a implementação de medidas extremas que possam violar os direitos que estão umbilicalmente relacionados à proteção de dados pessoais.

Não obstante, Machado, Negri e Giovanini (2020) defendem que a utilização de dados pessoais no combate à pandemia não significa, necessariamente, um aumento na vigilância, tampouco tal finalidade representa justificativa para a coleta indiscriminada de informações pessoais.

Sendo assim, o uso de dados pessoais para combate e contenção da pandemia deve ser orientado por garantias jurídicas e outras medidas sanitárias que possuem amparo científico, tendo em vista o caráter extremo dessa utilização (Machado, Negri, Giovanini 2020).

Dessa maneira, infere-se que disposições legislativas como a de Cingapura, que autorizam a modificação do rol de finalidades inicialmente pactuadas, podem potencializar o reforço de uma lógica de vigilância, especialmente aquela vigilância intermediada por dados pessoais (*dataveillance*). Tal reforço está diretamente condicionado ao teor das alterações realizadas nas políticas de privacidade, de maneira que nem todas as alterações desencadearão em um escalada da vigilância.

CONCLUSÃO

O presente trabalho teve por objetivo investigar a possível lógica de vigilância reforçada em decorrência da utilização de aplicativos baseados em rastreamento de contato, cujos funcionamentos ocorrem a partir do tratamento de dados pessoais utilizados para oferecer suporte e aprimorar as práticas convencionais de rastreamento de contato.

A partir dessa necessidade investigativa, foram delineados os principais conceitos orientadores da pesquisa, bem como foi realizado o estudo de caso do aplicativo implementado em Cingapura – TraceTogether –, considerado um país exemplo no combate à pandemia.

Dessa maneira, ao proceder com a análise do aplicativo TraceTogether, foi constatado a existência de um desvio de finalidade material na utilização dos dados coletados pelo *app*, no momento em que a política de privacidade do aplicativo foi atualizada, de modo a autorizar a utilização dessas informações coletadas para fins de investigação

criminal. Tal desvio de finalidade, segundo a análise aqui realizada, configuraria um rompimento na relação de confiança estabelecida com aqueles responsáveis pelo aplicativo cingapurense, elemento fundamental quando se fala em proteção de dados pessoais.

Nesse sentido, em um contexto de intensificação de uma cultura de vigilância, a modificação das finalidades para o tratamento dos dados coletados por aplicativos de rastreamento de contato, a depender de seu teor, pode reforçar uma lógica de vigilância, especialmente sobre grupos historicamente marginalizados e violentados.

Todavia, a utilização de tecnologias para o combate da pandemia não significa, necessariamente, uma reiteração de práticas de vigilância, desde que tais tecnologias possuam garantias jurídicas, estabelecendo íntimas relações com a salvaguarda dos dados pessoais, bem como respaldo científico que justifiquem a sua implementação.

REFERÊNCIAS

ABELER, Johannes *et al*, 2020. COVID-19 Contact Tracing and Data Protection can go together. *JMIR Mhealth Uhealth*, [s.l.], v. 8, n. 4. [Acesso em 10 fevereiro 2021]. Disponível em: https://mhealth.jmir.org/2020/4/e19359/

ARTICLE 29 DATA PROTECTION WORKING PARTY, 2014. *Opinion 05/2014 on Anonymisation Techniques*. Bruxelas: [s.n.]. [Acesso em 10 fevereiro 2021]. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

ARTICLE 29 DATA PROTECTION WORKING PARTY, 2007. *Opinion 4/2007 on the concept o personal data*. Bruxelas: [s.n.]. [Acesso em 05 fevereiro 2021]. Disponível em: http://ec.europa. eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf

ARTICLE 29 DATA PROTECTION WORKING PARTY, 2007. *Advice paper on special categories of data ("sensitive data")*, 2011**.** Bruxelas: [s.n.]. [Acesso em 05 fevereiro 2021]. Disponível em: https://www.pdpjournals.com/docs/88417.pdf

ASHER, Saira, 2020. TraceTogether**:** Singapore turns to wearable contact-tracing Covid tech. *BBC NEWS*. [s.l.]. [Acesso em 17 fevereiro 2021]. Disponível em: https://www.bbc.com/news/technology-53146360

BAHARUDIN, Hariz, 2021. Police's ability to use TraceTogether data raises questions on trust: Experts. *The Straits Times*. [s.l.]. [Acesso em 17 fevereiro 2021]. Disponível em: https://www.straitstimes.com/singapore/politics/polices-ability-to-use-tracetogether-data-raises-questions-on-trust-experts

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

BRANCO, Sérgio, 2020. As hipóteses de aplicação da LGPD e as definições legais**.** Em: MULHOLLAND, Caitlin (Org.). *A LGPD e o novo marco normativo no Brasil*. Porto Alegre: Arquipélago, p. 15-42.

BRANDOM, Russel, ROBERTSON, Ari, 2020. Apple and Google are bulding a coronavirus tracking system into iOS and Android**.** *The Verge*, [s.l.]. [Acesso em 10 fevereiro 2021]. Disponível em: https://www.theverge.com/2020/4/10/21216484/google-apple-coronavirus-contract-tracing-bluetooth-location-tracking-data-app

BRASIL, 2018. Lei 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais (LGPD)***.** [Acesso em 13 dezembro 2020]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

BRUNO, Fernanda, 2006 Dispositivos de vigilância no ciberespaço: duplos digitais e identidades simuladas. *Froteiras*: *Estudos Midiáticos*, São Leopoldo, v. 7, n. 2, p. 152-159. [Acesso em 17 fevereiro 2021]. Disponível em: http://revistas.unisinos.br/index.php/fronteiras/article/view/6129

CINGAPURA, 2012. *Personal Data Protection Act 2012*. [Acesso em 10 janeiro 2021]. Disponível em: https://sso.agc.gov.sg/Act/PDPA2012

CINGAPURA, 2020. *PRESS RELEASE LAUNCH OF NEW APP FOR CONTACT TRACING A community effort to help combat the spread of COVID-19*. Cingapura. [Acesso em 10 fevereiro 2021]. Disponível em: https://www.smartnation.gov.sg/whats-new/press-releases/launch-of-new-app-for-contact-tracing

CINGAPURA, 2018. *Smart Nation***:** the way foward. Cingapura. [Acesso em 10 fevereiro 2021]. Disponível em: https://www.smartnation.gov.sg/docs/default-source/default-document-library/smart-nation-strategy_nov2018.pdf?sfvrsn=3f5c2af8_2

CLARKE, Roger, 1988. A Information technology and dataveillance. *Communications of the ACM*, Nova Iorque, v. 31, n. 5. [Acesso em 17 de fevereiro]. DOI 10.1145/42411.42413. Disponível em: https://dl.acm.org/doi/10.1145/42411.42413

COSTA, Ramon Silva, OLIVEIRA, Samuel Rodrigues de, 2019**.** Os direitos da personalidade frente à sociedade da vigilância: privacidade, proteção de dados pessoais e consentimento nas redes sociais. *Revista Brasileira de Direito Civil em Perspectiva*, Belém, v. 5, n. 2. [Acesso em 21 janeiro 2021]. Disponível em: https://www.indexlaw.org/index.php/direitocivil/article/view/5778

DONEDA, Danilo, 2019. *Da privacidade à proteção de dados pessoais:* elementos da lei geral de proteção de dados. 2. ed. São Paulo: Thomson Reuters Brasil.

DUSSUTOUR, Chloé, 2020. Governments release open source contact-tracing apps to fight Covid-19. *Open Source Observatory*. [Acesso em 10 fevereiro 2021]. Disponível em: https://joinup.ec.europa.eu/collection/open-source-observatory-osor/news/tracing-covid-19-cases

EPSTEIN, Lee, KING, Gary, 2013. *Pesquisa empírica em direito*: as regras de inferência. São Paulo: Direito GV.

ESPOSITI, Sara Degli, 2014. When big data meets dataveillance: the hidden side of analytics. *Surveillance & Society*, [S.L], v. 12, n. 2, p.209-225. [Acesso em 18 fevereiro 2021]. Disponível em: https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/analytics/analytic

EUROPEAN DATA PROTECTION BOARD, 2020. *Diretrizes 4/2020 sobre a utilização de dados de localização e meios de rastreio de contactos no contexto do surto de COVID-19*. Bruxelas: [s.n.]. [Acesso em 18 fevereiro 2021] Disponível em:

https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_pt.pdf

FINCK, Michèle, PALLAS, Frank, 2020. They who must not be identified: distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, Oxford, v. 10, n. 1. [Acesso em 31 março 2021]. DOI 10.1093/idpl/ipz026 Disponível em: https://academic.oup.com/idpl/article/10/1/11/5802594

FISCHER-HÜBNER, Simone *et al,* 2016. Transparency, Privacy and Trust – Technology for Tracking and Controlling My Data Disclosures: Does This Work?. *IFIP Advances in Informacion and Communication Technology*, [s.l.]. [Acesso em 15 fevereiro 2021]. DOI 10.1007/978-3-319-41354-9_1 Disponível em: https://link.springer.com/chapter/10.1007/978-3-319-41354-9_1

GIL, Antônio Carlos, 2018. Como elaborar projetos de pesquisa. São Paulo: Atlas.

ILLMER, Andreas, 2021. Singapore reveals Covid privacy data available to police**.** *BBC News.* [s.l.]. [Acesso em 15 fevereiro 2021]. Disponível em: https://www.bbc.com/news/world-asia-55541001

KITCHIN, Rob, 2020. Civil liberties *or* public health, or civil liberties *and* public health? Using surveillance technologies to tackle the spread of COVID-19. *Space and Policy*, [s.l.], v. 24, n. 3. [Acesso em 17 fevereiro 2021]. DOI 10.1080/13562576.2020.1770587. Disponível em: https://www.tandfonline.com/doi/full/10.1080/13562576.2020.1770587

KONDER, Carlos Nelson, 2019. O tratamento de dados sensíveis à luz da Lei 13.709/2018. Em: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Org.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.* São Paulo: Thomson Reuters Brasil p. 445-463.

KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon, 2019. *Dados Sensíveis na Lei Geral de Proteção de Dados Pessoais*: mecanismos de tutela para o livre desenvolvimento da personalidade. 2019. 119 f. Dissertação (Mestrado) - Curso de Direito, Universidade Federal de Juiz de Fora, Juiz de Fora. [Acesso em 17 fevereiro 2021]. Disponível em: https://repositorio.ufjf.br/jspui/handle/ufjf/11438

LEVY, Pierre, 2014. *Cibercultura.* São Paulo: Editora 34.

LYON, David, 2019. Cultura da vigilância: envolvimento, exposição e ética na modernidade digital. Em: BRUNO, Fernanda, *et al*. (Org.). *Tecnopolíticas da Vigilância*. São Paulo: Boitempo, p. 151-179.

MACHADO, Joana de Souza, NEGRI, Sergio Marcos Carvalho de Ávila e GIOVANINI, Carolina Fiorini Ramos, 2020. Nem invisíveis, nem visados**:** inovação, direitos humanos e vulnerabilidade de grupos no contexto da Covid-19. *Liinc em Revista*, Rio de Janeiro, v. 16, n. 2. [Acesso em 17 fevereiro 2021]. DOI 10.18617/liinc.v16i2.5367. Disponível em: http://revista.ibict.br/liinc/article/view/5367

MULHOLLAND, Caitlin, 2020. O Tratamento de dados pessoais sensíveis. Em: MULHOLLAND, Caitlin (Org.). *A LGPD e o novo marco normativo no Brasil.* Porto Alegre: Arquipélago, p. 121-156.

NEDDEN, Christian zur, 2020. Opinião**:** Cingapura é exemplo na luta contra covid-19. *Deutsch Welle,* [s.l]. [Acesso em 14 fevereiro 2021]. Disponível em: https://www.dw.com/pt-br/opini%C3%A3o-cingapura-%C3%A9-exemplo-na-luta-contra-covid-19/a-52945669

NEGRI, Sergio Marcos Carvalho de Ávila, GIOVANINI, Carolina Fiorini Ramos, 2020. Dados não pessoais: a retórica da anonimização no enfrentamento à covid-19 e o privacywashing. *Revista Internet e Sociedade*, São Paulo, v. 1, n. 2. [Acesso em 17 fevereiro 2021]. Disponível em: https://revista.internetlab.org.br/dados-nao-pessoais-a-retorica-da-anonimizacao-no-enfrentamento-a-covid-19-e-o-privacywashing/

ORGANIZAÇÃO PAN-AMERICANA DE SAÚDE, 2020. *Rastreamento de contatos no contexto da COVID-19.* [s.l.]. [Acesso em 18 fevereiro 2021]. Disponível em: <https://iris.paho.org/handle/10665.2/52377#:~:text=O%20rastreamento%20de%20contatos%20para,o%20controle%20da%20COVID%2D19

REUTERS, 2021. *Singapore COVID-19 contact-tracing data accessible to police*. [Acesso em 15 fevereiro 2021]. Disponível em: https://www.reuters.com/article/us-health-coronavirus-singapore-contact-idUSKBN2990X8

RODOTÀ, Stefano, 2008. *A vida na sociedade da vigilância*: a privacidade hoje. Rio de Janeiro: Renovar.

TRACETOGETHER, 2021. TraceTogether Privacy Safeguards. *TraceTogether*. [Acesso em 10 fevereiro 2021]. Disponível em: https://www.tracetogether.gov.sg/common/privacystatement/index.html.

UNIÃO EUROPEIA, 2016. Regulamento (UE) 2016/679. *Regulamento Geral sobre Proteção de Dados*. [Acesso em 03 março 2021]. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&qid=1614819078267&from=PT>

DIJCK, Jose van, 2014 Datafication, dataism and dataveillance: big data between scientific paradigm and ideology. *Surveillance & Society*, [s.l.], v. 12, n. 2, p. 197-208. [Acesso em 17 fevereiro 2021]. DOI 10.24908/ss.v12i2.4776. Disponível em: https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/datafication

WALDMAN, Ari Ezra, 2018. *Privacy as trust*: information privacy for na information age. Nova Iorque: Cambrige University Press.

WESTIN, Alan, 1967. *Privacy and Freedom*. Nova Iorque: Antheneum.

YUEN-C, Tham, 2021. Police can use TraceTogether data for criminal investigation**.** *The Straits Times*. [s.l.]. [Acesso em 15 fevereiro 2021]. Disponível em: https://www.straitstimes.com/singapore/politics/police-can-use-tracetogether-data-for-criminal-investigations-0

ZUBOFF, Shoshana, 2019. *The Age of Surveillance Capitalism:* the fight fot a new future at the new frontier of power. Londres: Profile Books.

ZUBOFF, 2019. Big Other: capitalismo de vigilância e perspectivas para uma civilização da informação. Em: BRUNO, Fernanda, *et al*. (Org.). *Tecnopolíticas da Vigilância*. São Paulo: Boitempo, p. 17-68.