ARTIGO

A implementação do Contact Tracing e a Montagem de Vigilâncias na pandemia da COVID-19

Rodrigo Glasmeyer
rglasmeyer@protonmail.com

Graduando em Direito na UFPR,
membro do GEDAI UFPR e bolsista do
grupo PET - Direito.

V. 1 / N. 2 / DEZEMBRO DE 2020
PÁGINAS 200 A 220

A implementação do Contact Tracing e a Montagem de Vigilâncias na pandemia da COVID-19

Palavras-chave
Contact Tracing
Montagem de Vigilâncias
Capitalismo de Vigilância

Resumo
A chegada da pandemia da COVID-19 ocorre em um momento em que o mundo se encontra em intensa mudança social. Neste momento, o crescimento de um novo modelo econômico baseado na coleta e produção de informação por meio da vigilância constante da população vem desestabilizando as convenções sociais e o funcionamento das instituições. Para compreender a implementação das medidas de combate à pandemia, é necessário compreender também o funcionamento das estruturas sociais nas quais estas estão baseadas. Uma revisão do desenvolvimento da estrutura de vigilância panóptica proposta para a sociedade disciplinar até a montagem de vigilâncias descentralizada que marca a sociedade contemporânea em seu avanço para um capitalismo de vigilância serve como aporte metodológico para a análise das propostas de *contact tracing* para o combate da COVID-19. Foram analisadas as abordagens para o mapeamento de contatos por meio de aplicativos de celular tanto com base em dados de geolocalização quanto por contatos por *Bluetooth*, bem como a utilização de estruturas centralizadas ou descentralizadas de informação. Diversos problemas relacionados à privacidade e à autodeterminação informativa são encontrados, bem como em relação à efetividade da medida e à adesão da população aos aplicativos. A aplicação do *contact tracing* precisa levar em consideração a importância da proteção de dados em meio ao crescimento exponencial da montagem de vigilâncias, considerando também a existência de medidas diretas de prevenção e combate à pandemia que não colocam em risco o direito fundamental à privacidade da população.

V. 1 / N. 2 / DEZEMBRO DE 2020
PÁGINAS 200 A 220

The implementation of Contact Tracing and the Surveillant Assemblage in the COVID-19 pandemic

Keywords
Contact Tracing
Surveillance Assemblage
Surveillance Capitalism

Abstract
The arrival of the COVID-19 pandemic happens in a moment in which the world goes through intense social change. At this point, the growth of a new economic model based on the collection and production of information through constant surveillance of the population is destabilizing the social conventions and the performance of the institutions. In order to understand the implementation of policies tackling the pandemic, it is also necessary to understand the workings of the social structures in which they are based. A review of the development of the panoptical surveillance structure designated to the disciplinary society up until the decentralized Surveillance Assemblage which brands the contemporary society in its stride to surveillance capitalism serves as methodological input to the analysis of the proposals of contact tracing tacking COVID-19. This article analyses the approaches to contact tracing through cell phone apps both via the collection of geolocation data and via Bluetooth contacts, as well as the utilization of centralized and decentralized structures of information. Several issues relating to privacy and informational self-determination were found, as well as issues over the effectiveness of the proposals and the public adherence to the apps. The application of contact tracing needs to take into consideration the importance of data protection amidst the exponential growth of the surveillance assemblage, considering other direct prevention actions to tackle the pandemic which do not put the fundamental right to privacy of the population at risk.

1. Considerações iniciais acerca do panorama da vigilância e do combate à COVID-*19*

A pandemia da COVID-19 desestabilizou o mundo como poucos eventos antes dela na história. Porém, antes mesmo de sua chegada, este já estava abalado profundamente por diversas mudanças sociais e tecnológicas que engatinhávamos para compreender.

Se o mundo após a pandemia será completamente diferente do que existia antes dela, sua chegada já ocorreu em um momento em que a sociedade sentia os efeitos de uma mudança de paradigma de grandes proporções. O chamado "capitalismo de vigilância" (ZUBOFF, 2019), uma nova estrutura econômica e social baseada em uma evolução do capitalismo informacional, que nos levaria a uma terceira modernidade (ZUBOFF, 2020), dissolvia as distinções entre mercado e sociedade, entre mercado e mundo, entre mercado e indivíduo, substituindo o contrato legítimo, a lei, a política e a confiança social por uma nova soberania que se encontra nas mãos de poucas empresas privadas que monopolizam o chamado "império de modificação comportamental" (LANIER, 2018).

Ao mesmo tempo, a partir das informações providenciadas por Edward Snowden em 2013, junto com demais informações disponibilizadas ao público por *whistleblowers* e *hackers*, se tornava notório o fato de que os Estados nacionais também tinham e têm grande posição como atores neste panorama de vigilância de tudo e de todos, potencializado especialmente a partir dos ataques terroristas de 11 de setembro de 2001 (LYON, 2015; LYON, 2003).

Esta simbiose de vigilâncias entre a espionagem governamental e a vigilância como modelo de negócios (RICHARDS, 2012) desafia alguns dos conceitos desenvolvidos a partir das décadas de 1970 e 1980 para compreender a própria ideia de vigilância em nossa sociedade, em especial os conceitos construídos a partir da análise que Foucault faz do Panóptico de Bentham.

A pandemia da COVID-19 e as respostas apresentadas por diferentes governos e empresas para a contenção do vírus estão, então, profundamente relacionadas com o paradigma de vigilância em que se encontra o mundo, e a compreensão e o desenvolvimento de conceitos que nos ajudem a compreendê-lo também ajudam a entender e melhor lidar com as possibilidades de novos caminhos escancaradas pela atual conjuntura.

Assim, o presente artigo trabalha com uma abordagem metodológica que parte de uma breve revisão bibliográfica acerca do paradigma do panoptismo entre os estudos da vigilância seguida pela apresentação de novas teorias chamadas "pós-panópticas", focando no modelo de "montagem de vigilâncias" construído por Haggerty e Ericson (2000) a partir das contribuições conceituais de Deleuze e Guattari (2011). Após a exposição destes conceitos, o artigo analisa diferentes modelos propostos para a criação de sistemas que efetuem a prática do *contact tracing* por meio da coleta e tratamento de dados com o fim de combater a pandemia da COVID-19. O artigo foca especificamente no *contact tracing*, que é somente um modelo dentre diversas medidas propostas para o combate ao COVID que podem ter repercussões na autodeterminação informativa dos cidadãos. Nesta etapa serão consultados *whitepapers*, políticas de privacidade e uso de dados de aplicativos, bem como notícias recentes sobre a implementação dos sistemas e pareceres e relatórios de organizações sociais acerca do tema, tomando os casos brasileiros do Sistema de Monitoramento Inteligente - SIMI, do estado de São Paulo, e o aplicativo CORONAVÍRUS SUS, implementado pelo Ministério da Saúde como exemplos de diferentes maneiras de se implementar medidas

de processamento de dados para a prevenção e combate à COVID-19. Por fim, a conclusão do artigo relaciona os modelos propostos com a Lei Geral de Proteção de Dados brasileira e com o contexto geral da autodeterminação informativa no país, considerando a importância da aplicação dos princípios e regras dispostos na lei para que qualquer tipo de utilização de dados pessoais possa ser utilizada para a construção de políticas públicas de combate à pandemia.

O objetivo geral deste artigo é situar a prática do *contact tracing*, além de uma medida de contenção da pandemia, também como uma ferramenta marcada pelos modelos de vigilância e regimes de visibilidade que permeiam nossa sociedade, especificamente em uma montagem de vigilâncias simbiótica com o Capitalismo de Vigilância. Para atingir este objetivo, os capítulos deste artigo buscam objetivos específicos de, respectivamente, apresentar os modelos teóricos que explicam as estruturas de vigilância de um dado momento histórico, apresentar a tecnologia do *contact tracing* bem como suas diferentes possibilidades de utilização, cuja escolha das possibilidades é definida por desejos e conveniência política e social, e por fim compreender, dentre as possibilidades existentes e em consonância com os modelos de vigilância, como o *contact tracing* vem sendo implementado no Brasil.

2. As estruturas de vigilância e o "Surveillant Assemblage"

Dentre as diversas mudanças trazidas pela era informacional e pela implementação global do Capitalismo de Vigilância, são visíveis os efeitos de uma reordenação dos regimes de visibilidade envolvida pela reorientação das tecnologias com as quais convivemos cotidianamente, como apresentado por Fernanda Bruno, Marta Kanashiro e Rodrigo Firmino (2010). Segundo os autores, cada sociedade e cada época tem seu regime de visibilidade próprio, que não consiste tanto no que é visto, mas no que torna possível o que se vê.

O poder de vigilância e os impactos à privacidade e proteção de dados resultantes da miríade de novas tecnologias, dispositivos, formas organizacionais e corporativas, modelos preditivos e práticas sociais que modificaram o Zeitgeist dos últimos 30 anos fizeram com que a vigilância se tornasse um tema proeminente no debate acadêmico e público, que veio a formar a área de estudos transdisciplinar dos "Surveillance Studies" (LYON; HAGGERTY; BALL, 2012).

A vigilância, que emergiu na segunda metade do século XX como a prática organizacional dominante da modernidade tardia, de modo que Frantz Fanon, em suas aulas no curso de psicopatologia social lecionadas no Institut des Hautes Études de Tunis, chega a afirmar que a modernidade pode ser caracterizada pela alocação do indivíduo em fichas e registros (GENDZIER, 1974), não é exclusividade deste momento histórico, sendo componente constante dos procedimentos institucionais e da sociabilidade humana.

Faz-se necessário, então, compreender não somente que a vigilância é presente, mas que ela está intimamente conectada com o regime de visibilidade de nossa época e que pode ser direcionada ou compreendida a partir de diferentes modelos teóricos com diferentes implicações. Para tratar do *contact tracing* dentro do momento histórico de uma pandemia global, se torna relevante apresentar os modelos teóricos de vigilância do Panóptico de Bentham analisado por Foucault e da montagem de vigilâncias proposta por Haggerty e Ericson, bem como compará-los aos modelos de vigilância aplicados no contexto de outras doenças que

causaram grande impacto: a peste negra e a lepra.

2.1. O Panoptismo e a gestão da praga

A leitura que Foucault faz da obra do utilitarista inglês Jeremy Bentham, em especial da teorização da estrutura arquitetônica denominada de panóptico é de inegável relevância para a área acadêmica dos *Surveillance Studies* e para os estudos acerca das estruturas de vigilância nos séculos XX e XXI.

Na introdução do capítulo "O Panoptismo", de seu livro Vigiar e Punir, porém, o filósofo francês nos lembra de que a teorização e implementação do panóptico não são o início do projeto moderno de vigilância, mas sim a culminação de uma construção composta por elementos que vêm desde a Idade Média sendo implementados para o controle de populações. Dentre estes elementos, cita as estruturas e a operação da vigilância decorrente do tratamento da peste negra e da lepra na Europa.

As duas doenças, que tiveram resultados avassaladores para a sociedade europeia em suas respectivas épocas, exigiram respostas coletivas que possibilitassem o controle do contágio e o tratamento devido dos infectados, mas que também serviram como impulsionadoras da aplicação de projetos de "sonhos políticos".

Com a peste negra, as cidades foram fechadas e os moradores proibidos de sair sob pena de morte. Todos são ordenados a se trancarem em suas casas, e cada rua fica sob a supervisão de um síndico, que tem a autoridade de carregar as chaves que fecham as famílias em seus domicílios. Para além dos síndicos de cada rua, postos de vigilância e sentinelas são distribuídos pela cidade, impondo as regras do sistema de combate à doença e tornando visível a ameaça da utilização da força para quem tentar descumpri-las (FOUCAULT, 1999).

O sistema criado para reger a peste negra é, para Foucault, um "modelo compacto do dispositivo disciplinar", consistindo na fixação dos indivíduos cada um em seu respectivo lugar e no controle e o registro dos movimentos e acontecimentos. A resposta à peste vem com o sonho político da ordem e da disciplina, que fazem valer seu poder de análise para combater a confusão que surge da mistura que representa a doença. O sonho político que tentou ser implementado com a peste é composto por divisões estritas e com a "penetração do regulamento até nos mais finos detalhes da existência e por meio de uma hierarquia completa que realiza o funcionamento capilar do poder", como apresenta Foucault (1999, p. 221).

Diferente da peste negra, porém, o tratamento da lepra se dá a partir de uma prática de rejeição e da exclusão, que exige um policiamento meticuloso que é posto em prática também a partir de um funcionamento capilar do poder. O leproso, que não mais tem esperança de se integrar com o todo, é meramente exilado e marcado, enquanto com a peste negra todos são divididos e analisados. Assim, enquanto o sonho político da peste negra é o de uma sociedade disciplinar, o da lepra é o de uma "comunidade pura", institucionalizando um sistema de exclusão sem volta.

Ambos os sistemas, porém, dependem de uma estrutura de registro permanente dos indivíduos, que deve ser "constante e centralizado", sendo que "a relação de cada um com sua doença e sua morte passa pelas instâncias do poder, pelo registro que delas é feito, pelas decisões que elas tomam." (FOUCAULT, 1999, p. 220). Esta estrutura envolve a "individualização da patologia pela codificação burocrática" (NORRIS, 2003, p. 250), sendo a ameaça da utilização da força um fator essencial para o funcionamento e a aplicação do sistema.

Em Bentham (2000), Foucault vê a junção

do controle da lepra e da peste culminarem na figura arquitetural do panóptico. A estrutura, que nas palavras de seu idealizador buscava possibilitar um "novo modo de garantir o poder da mente sobre a mente" por meio do que ele chama de "princípio da inspeção", não representava somente um plano arquitetônico, mas um projeto político, sendo, segundo Elmer (2012), a expressão da filosofia política do liberalismo reformista de sua época. Ainda segundo o autor, enquanto Bentham coloca em foco a estrutura e o seu poder de governança, Foucault modifica o centro da questão para o sujeito, para os prisioneiros, pacientes, trabalhadores governados pelo princípio da inspeção.

Este princípio teoriza um método ótimo de vigilância resultante da situação em que o sujeito, ao saber da possibilidade constante de estar sendo vigiado, mas sem saber se o está sendo em um dado momento, age como se vigiado fosse mesmo quando este não é o caso. O plano do panóptico consiste não em uma vigilância presente a todo momento, mas exatamente na impressão que uma forma de poder institucional ubíquo gera no sujeito, que causa uma internalização deste poder, exigindo no sujeito sua autogestão disciplinar.

O projeto panóptico era, principalmente, um mecanismo disciplinar centrado na economia política, que, como todo mecanismo disciplinar, deve buscar o menor custo político e econômico possível e que deve ligar o crescimento econômico do poder disciplinar com o desempenho institucional, por meio do aumento da docilidade e da utilidade de todos os indivíduos sujeitos ao mecanismo.

A figura do panóptico foi extensamente utilizada ao longo das décadas de 70 e 80, relacionada às análises sobre o controle social e sobre o poder disciplinar do século XX, além de ser utilizada como base para diversas reinterpretações de suas ideias em um movimento que Murakami Wood (2003) categoriza como "panopticismo", ou a trajetória social do conceito de panóptico. Dentre as interpretações surgidas a partir do conceito estão o Sinóptico proposto por Mathiesen (1997), os "panópticos pessoais" que regem o mercado de trabalho neoliberal, como apresentado por Bauman e Lyon (2014), e o ban-óptico conceituado por Didier Bigo (2006).

Se, para Foucault, o panóptico representa o poder arquétipo da modernidade, sendo um dispositivo-chave para a criação da subjetividade moderna (WOOD, 2003), Paul Gilroy (1993) traz uma contundente crítica à própria ideia de modernidade, em especial à constituição do indivíduo moderno que deixa à margem os indivíduos não-europeus, e principalmente os indivíduos escravizados, e ignora o papel fundante que a escravidão e o colonialismo tiveram e têm na construção da modernidade e do sujeito moderno. Assim, Simone Browne (2015) traz uma relevante releitura do panóptico ao compará-lo com a figura do navio negreiro *Brooks*, uma vez que, para Marcus Rediker (2007) o navio negreiro consistia de uma "prisão móvel" em um tempo em que a prisão moderna não havia ainda sido criada, e que para Gilroy os navios negreiros constituíam verdadeiras unidades culturais e políticas que foram essenciais para o desenvolvimento do Atlântico Negro, formação transcultural internacional composta de uma estrutura rizomática e fractal (GILROY, 1995).

2.2. Pós-panoptismo e o "Surveillant Assemblage"

Ainda que seja proposto por Foucault e por Bentham como um dispositivo polivalente em suas aplicações, o Panóptico encontra limites em sua utilização, não podendo toda e qualquer forma de vigilância ser abarcada por seus

pressupostos e, consequentemente, suas características próprias.

Do mesmo modo, a teoria por detrás dele não encontra sua aplicação na prática sem dispor de certas contradições, sendo notórios os exemplos trazidos por Lorna Rhodes (2004) acerca de seu estudo empírico dentro das prisões *supermax* e os diversos estudos desenvolvidos acerca do panopticismo no contexto do consumo, como a análise de Gandy (1993). Como aponta David Lyon (2006), estes estudos demonstram um paradoxo presente na execução do panóptico: enquanto as aplicações mais extremas e diretas do panóptico geram uma resistência dos sujeitos a ele impostos que não fora teorizada por Foucault, os corpos sujeitos às aplicações mais sutis e menos diretas do dispositivo são mais facilmente produzidos como corpos dóceis.

Como sumariza Lyon (2006), a teoria da vigilância não pode ignorar o panóptico, mas pode certamente ir para além dele. Kevin Haggerty (2006) propõe que abandonemos o panopticismo, uma vez que, para o autor, o modelo do panóptico, ao ser superestimado e transformado no modelo proeminente de análise e estudo da vigilância, assume um papel reificado, focando os estudos sobre vigilância em aspectos específicos do dispositivo idealizado no século XIX e excluindo ou negligenciando muitos processos e sistemas de vigilância, sejam eles inovadores em relação ao panóptico ou não. Haggerty compara a utilização do conjunto de noções atreladas ao panopticismo em situações que não o comportam com as anomalias da ciência normal que, na teoria de Thomas Kuhn (1970), preparam e levam o campo científico para uma mudança de paradigma, não sem antes abalar a confiança no paradigma anterior.

Dentre as principais limitações que Haggerty (2006) sinaliza no modelo panóptico, uma das mais relevantes diz respeito à omissão das novas tecnologias da informação, que representam um dos principais, senão o principal desenvolvimento da vigilância na segunda metade do século XX. O papel dos agentes e vigias, centrais na teoria do panóptico e no princípio da inspeção, assim como o papel dos seres humanos em geral, se torna cada vez menos relevante frente às novas tecnologias de análise, predição, extração de dados e de informação.

Outro ponto levantado diz respeito à crença de Foucault de que o efeito da estrutura no sujeito é o mesmo independente de quem esteja situado na posição de vigia. Ao contrário, a subjetividade dos vigias demonstra sua importância em diversos exemplos contemporâneos, justificando até o sucesso do capitalismo de vigilância, em que consumidores se sentem confortáveis em serem vigiados pelas grandes empresas de tecnologia ou no contexto das redes sociais em que, conforme afirmam Lyon e Bauman (2014), o desconforto maior não é o de ser vigiado mas sim seu oposto: o medo de ser ignorado.

Bauman, porém, toma uma posição menos extrema do que a de Haggerty, discordando da necessidade de os "Surveillance Studies" deixarem para trás o panóptico em uma mudança de paradigma. Para o autor, o modelo proposto por Foucault está "vivo e bem de saúde", com capacidades e poderes que excedem as análises do filósofo francês, porém concorda que este já não é mais o padrão de dominação universal ou a estratégia universal de controle social, sendo "confinado às partes 'não administráveis' da sociedade", seguindo o conceito de instituições totais criado por Goffman (1961).

Outra interessante proposta que pode ser classificada como pós-panóptica, mas que não propõe o fim do uso do conceito é a de "vigilância distribuída", utilizada por Fernanda Bruno (2013). A autora pondera sobre a posição do modelo panóptico no atual panorama da sociedade informacional ao constatar que a vigilância não passou necessariamente por uma mudança em intensidade, mas sim em uma mudança no seu modo de funcionamento. Esta

constatação permite a compreensão de que o panóptico pode se manter como um modelo presente em diversos contextos de nossa sociedade, ao mesmo tempo em que passamos pelo surgimento e consolidação de outros modos de funcionamento de vigilância.

A obra de Gilles Deleuze e Félix Guattari permite novas reflexões dentre os estudos sobre vigilância. Ao tratar da passagem das sociedades disciplinares às sociedades de controle, Deleuze (1992) demonstra que, não sendo o capitalismo informacional baseado na produção e no produto, perde-se a relevância de manter o sujeito dentro das estruturas e dos espaços desenvolvidos para disciplinã-lo. Do mesmo modo, não se trata mais do dualismo entre massa e indivíduo, pois o indivíduo é quebrado e todas as suas informações relevantes são transformadas em dados, enquanto a massa se torna o conjunto, as bases, o banco de dados.

Outro conceito relevante para compreender as contribuições de Deleuze e Guattari para a área é o de rizoma. Em oposição às estruturas de árvore ou de raiz, o rizoma propõe uma estrutura descentralizada, em que qualquer ponto da estrutura pode e deve ser conectado aos demais. Do mesmo modo, o rizoma é uma multiplicidade, e como tal "não tem sujeito nem objeto, mas somente determinações, grandezas, dimensões que não podem crescer sem que mude de natureza" (DELEUZE; GUATTARI, 2011, p. 23). Em um rizoma a ruptura é assignificante, no sentido de que o rompimento de qualquer componente da estrutura não afeta de maneira significativa o todo, existindo uma maleabilidade da estrutura, composta por linhas de segmentaridade. Haggerty e Ericson (2000) apresentam duas características do rizoma que são acentuadas no contexto dos estudos sobre vigilância: o crescimento exponencial do rizoma e o seu efeito de nivelar hierarquias.

Assim, o modelo do panóptico antes trabalhado é um exemplo de um sistema arborescente, ou seja, um sistema que comporta "centros de significância e de subjetivação" (DELEUZE; GUATTARI, 2011, p. 36). Em contraste, Haggerty e Ericson (2000) propõem que a vigilância em uma era informacional é composta por um modelo rizomático de uma montagem de vigilâncias, uma *Surveillant Assemblage*.

A base para a montagem de vigilâncias parte da composição do sujeito em uma nova dimensão, da criação de um *data double*, uma duplicata do indivíduo em seus dados. A abstração dos corpos humanos de seus territórios e sua transformação em fluxos de informação se dá de maneira descentralizada, sendo o corpo dividido e recortado em milhares de diferentes dados, úteis ou inúteis nos mais diferentes contextos. A montagem de vigilâncias, porém, consiste na fixação temporal e espacial destes fluxos de dados. A transformação de fluxos em uma montagem ocorre da mesma maneira em que a força compõe o poder: forças fluidas e primárias, em uma determinada montagem, constituem o poder, secundário.

Tal montagem, contudo, não existe como uma entidade estável que tem seus próprios limites fixados, mas sim como uma potencialidade. A criação, extração e o armazenamento de toda espécie de dados não forma um corpo fixo e centralizado, criado ou submetido à alguma instituição ou entidade. A existência destes dados existe como a potencialidade de todos os diferentes usos por diferentes atores que o conjunto de dados pode vir a ter.

Assim, é possível caracterizar a montagem de vigilâncias não como um dispositivo único e central, focado em seus objetivos e pressupostos fixos, mas como a construção rizomática de uma rede de informações, dados e fontes de dados que surgem dos mais distintos dispositivos e com os mais distintos objetivos.

O que transforma fluxos independentes em uma montagem é o desejo, e, nesse sentido, a montagem de vigilâncias pode ser atribuída ao desejo de congregar sistemas, bases de dados, fontes de informação em um todo que possa

atribuir novas funções e inferir ainda mais informação do que cada componente sozinho. As últimas duas décadas viram um constante crescimento não somente no número de dispositivos utilizados, mas também em suas áreas de aplicação e nos tipos de dados gerados. Assim, a dimensão informacional do indivíduo, englobando desde seus dados médicos, informações genéticas, geolocalização, interesses políticos, atividade em redes sociais, presenças em bases de dados de serviços governamentais ou privados, constrói corpos de dados cada vez mais completos e complexos do ser humano.

Do mesmo modo, cada novo dispositivo, cada nova fonte de dados introduzida e aplicada gera um crescimento exponencial no potencial da montagem de vigilâncias, uma vez que promove um crescimento nos dados que podem ser inferidos do cruzamento das informações já existentes.

A montagem destes dados agrega aqueles passados dos indivíduos, em um momento em que deixamos rastros permanentes de nossas atividades e cada vez menos somos permitidos esquecer (SNOWDEN, 2019), os dados presentes constantemente registrados, e, por meio de técnicas de predição baseadas em modelos de probabilidade, os possíveis futuros dos indivíduos. O infame exemplo dos algoritmos que pretendem calcular a probabilidade de um preso reincidir no crime nos demonstra como essa a futurologia dos dados pode gerar profecias autorrealizáveis se não for analisada criticamente. Haggerty e Ericson (2000) afirmam que a função dos *data doubles* não é a de serem retratos precisos dos indivíduos, mas que estes têm uma função pragmática de possibilitar que quem os analisa possa fazer discriminações entre populações. Estas discriminações não dependem de precisão, mas sim de probabilidade.

A função da multiplicidade do rizoma na montagem de vigilâncias significa afirmar que a montagem não é composta por um sujeito e um objeto específico, de modo que seu crescimento ocorre de maneira indiscriminada. Os seus efeitos, por outro lado, claramente não são indiscriminados, sendo recorrentes exemplos de racismo, sexismo e de diversos tipos de efeitos negativos de discriminações a minorias (SILVA, 2019; RITCHIE, 2020; SILVA, SILVA, 2019). Ainda assim, esta característica significa afirmar que algoritmos que geram discriminação racial na concessão de crédito, a inteligência artificial que lista recomendações de conteúdo individualizadas, vazamentos de conversas e documentos de indivíduos em posições de poder, etc. compõem todos a mesma montagem de vigilâncias. Assim, todos os aspectos de observação (surveillance, McVeillance, Veillance e Sousveillance) incluídos no esquema proposto por Mann (2013) estão igualmente presentes na montagem, bem como seus diferentes potenciais.

Por fim, uma importante característica decorrente da natureza rizomática da montagem de vigilâncias diz respeito à ruptura assignificante do sistema. Assim como o modelo de rizoma proposto por Deleuze e Guattari (2011), a montagem de vigilâncias não é significativamente afetada pelo rompimento de alguma de suas pontas. A estrutura, que é descentralizada e não é direcionada a nenhuma direção ou objetivo específico, mantém-se firme e forte se perde uma ou diversas fontes de dados. Esta característica tem diversas implicações, como por exemplo a conclusão de que a proibição de qualquer tipo de dispositivo ou da coleta e tratamento de certo tipo de dado não irá desmontar o todo da montagem de vigilância, assim como o ataque ou a crítica a um ator ou instituição sozinho. Importante apontar que isto não significa que ela seja "neutra", mas que, sendo uma potencialidade, abarca mais de uma possibilidade de utilização. Pelo contrário, tanto a utilização da potencialidade criada pela montagem de vigilâncias quanto a criação de cada tecnologia que a compõe consistem em escolhas inerentemente políticas, seja por seus

pressupostos, ou seja pelos fins que se esperam que tenham na sociedade, conforme preceitua Winner (1980, p. 127).

Como será analisado de forma mais profunda na próxima seção deste artigo, o *contact tracing* consiste em uma técnica que apresenta distintos modos de implementação, os quais refletem estas escolhas e objetivos políticos. Ainda assim, consideramos as contribuições de Foucault tanto sobre o modelo panóptico de vigilância quanto sobre a vigilância da lepra e da peste negra como exemplos históricos de modelos de vigilância. Isto não significa que seus pressupostos ou objetivos estejam atrelados à Idade Média e à virada do século XVIII para o século XIX, sendo possível considerar que dispositivos que compõem a montagem de vigilâncias no ano de 2020 compartilhem de elementos, que segundo Foucault (2000, p. 244) podem ser discursos, proposições filosóficas ou morais, entre outros, com os dispositivos presentes no panóptico, no controle da lepra e no controle da peste negra.

3. O *Contact Tracing* e o oportunismo vigilante

Após o intenso aumento do número de contágios e vítimas da COVID-19 ao longo do primeiro trimestre de 2020, em que o isolamento social foi definido como método mais indicado na contenção da propagação do vírus, implementado em diferentes graus ao redor do mundo, pesquisadores e órgãos de saúde passaram a traçar estratégias de contenção da doença a longo prazo, ao mesmo tempo em que buscam modos de a sociedade retornar gradualmente à normalidade. Um fator de grande importância para se atingir este retorno é a possibilidade de os órgãos de saúde obterem as informações necessárias sobre a situação da doença e do isolamento da população.

Um processo de monitoração que almeja obter estes dados é o chamado "*contact tracing*". Segundo a OMS (2020), o *contact tracing* pode ser dividido em 3 etapas: 1) identificação de contato; 2) listagem dos contatos; 3) acompanhamento dos contatos.

Seguindo estes passos, o objetivo deste processo é obter os números de infectados em um determinado local, mas também efetuar o isolamento não somente dos indivíduos com a doença confirmada, mas também de potenciais portadores, diminuindo a velocidade e amplitude do contágio.

O *contact tracing* não é um processo novo, tendo sido utilizado para o combate e prevenção de diversas outras doenças, como o Ebola (DIXON, 2015), porém a utilização de coleta e mineração de dados modificam a amplitude e a dinâmica da prática, que anteriormente era relacionada com a aplicação de formulários e perguntas aos indivíduos infectados, e que se baseava na memória e na cooperação destes. Esta mudança na dinâmica da prática do *contact tracing* traz consigo diversas questões relacionadas à sua implementação, em especial em relação aos possíveis riscos para a privacidade e levando em consideração a autodeterminação informativa e a proteção de dados pessoais.

De modo genérico, existem dois possíveis métodos de implementação do uso de dados para a efetivação do *contact tracing*: por meio da utilização de dados de geolocalização e por meio de contatos registrados pela tecnologia *Bluetooth*. Paralelamente, também se discute a implementação de sistemas centralizados ou descentralizados de processamento de dados.

3.1. *Contact tracing* por geolocalização

A utilização de dados de geolocalização para efetuar o *contact tracing* está ocorrendo em diversos países no mundo, com ênfase nos

exemplos da Coréia do Sul, Israel e de Taiwan. Woodhams (2020) desenvolveu um registro completo indexando os países que utilizam diferentes métodos de vigilância física e digital para combater a COVID-19.

Os dados sobre a localização de um indivíduo podem ser coletados de diversas maneiras diferentes. Segundo Stanley e Granick (2020), dentre os principais métodos de se inferir a localização de um dispositivo se encontram a utilização do registro de conexão do dispositivo às antenas de telefonia (Estações rádio-base), o acesso a dados de GPS e o registro de conexões por *Wi-Fi* do dispositivo.

A localização gerada pela triangulação de antenas de telefonia sofre com uma falha em precisão, em especial em áreas rurais ou com menor concentração de antenas, e por sua imprecisão foi descartada pelo governo chinês para fins de controle da COVID-19, segundo Valentino-Devries (2020). O acesso ao GPS e aos registros de *Wi-Fi*, por outro lado, tem o problema de exigir que suas respectivas funcionalidades estejam habilitadas nos dispositivos e que haja algum sistema de compartilhamento destes dados, como por exemplo um aplicativo, uma vez que estes não estão à disposição das telecoms sem que o usuário os compartilhe. Do mesmo modo, a localização por relação de registros de Wi-Fi depende de levantamentos que registram e identificam a localização de cada fonte de sinal, trabalho extenso que não está disponível em grande parte do mundo e que exige constante atualização.

Para além destas limitações pragmáticas, o mapeamento de contatos entre indivíduos por meio da geolocalização gera altos riscos ao direito de privacidade dos usuários.

A prática do *contact tracing* exige a individualização dos dados, diferentemente de outras táticas que possam utilizar dados agregados, por exemplo. Ao mesmo tempo, mesmo que os dados de geolocalização utilizados sejam anonimizados, a sua própria natureza faz com que a identificação dos indivíduos por métodos de *cross-referencing* seja possível e, por vezes, fácil, como demonstrado por Tatiana Dias (2020). Neste sentido, Xia e Yang (2018) analisam a eficácia do *cross-referencing* e propõem possíveis modificações nos sistemas de geolocalização que priorizem a privacidade dos usuários.

Do mesmo modo, muitas das iniciativas de *contact tracing* dependem da criação de bases de dados centralizados, disponíveis a governos ou órgãos e instituições. O compartilhamento destas bases de dados entre diferentes instituições, as medidas de segurança necessárias para o impedimento do acesso indevido a essas bases e a certificação de que estas iniciativas vão zelar para com o uso destes dados para a finalidade exclusiva de combate à pandemia e que o tratamento destes dados terá seu término em períodos de tempo razoáveis que não permitam sua utilização para outros fins após, ou até mesmo durante, o período de quarentena são pontos que geram extrema preocupação, em especial nos contextos em que não há leis de proteção de dados ou atuação satisfatória das autoridades de proteção de dados.

3.2. Contact tracing por Bluetooth e a construção de sistemas descentralizados

Em alternativa aos métodos que utilizam da geolocalização, diversas iniciativas propuseram a construção de sistemas descentralizados e que substituem a necessidade pela identificação da localização do indivíduo pelo uso de tecnologia *Bluetooth*. Entre estas iniciativas, pode ser citado o aplicativo TraceTogether (2020), utilizado pelo governo de Singapura. Em detrimento das boas práticas desenvolvidas pelo aplicativo, a resposta do governo de Singapura à COVID-19 é

passível de críticas por se utilizar não somente do *contact tracing* por *Bluetooth*, mas também utilizar do cruzamento de informações provenientes de câmeras de circuito fechado e dados compartilhados por companhias de transporte, de modo prejudicial à privacidade da população. Outro exemplo consiste de um sistema de mapeamento de proximidade focado na preservação da privacidade proposto por Troncoso et al. (2020), resultado de trabalhos conjuntos de pesquisadores de 8 diferentes instituições, bem como o sistema PACT: *Private Automated Contact Tracing* criado por Rivest et al. (2020) e o protocolo desenvolvido pela Apple em conjunto com a Google (2020).

O funcionamento destes sistemas, em geral, parte da utilização de aplicativos que criam identidades anônimas e criptografadas que são periodicamente renovadas e que não tem nenhuma identificação com o indivíduo por detrás do dispositivo. Estas identidades, então, são constantemente compartilhadas por *Bluetooth*, e cada dispositivo guarda temporariamente um registro das identidades criptografadas com as quais teve contato próximo.

No caso de o usuário ser testado positivo para COVID-19, ele mesmo pode informar o aplicativo, que então avisa todos os demais dispositivos que tenham registrado o contato com as identidades anônimas do usuário infectado. Assim, quem esteve em contato com alguém infectado recebe esta informação sem precisar de detalhes sobre quem é ou onde ocorreu o contato, e sem que estas informações sejam repassadas por bases centralizadas de dados ou com governos e instituições.

Quanto aos sistemas descentralizados, qualquer método em que a informação de quem foi testado positivo para COVID-19 é dada pelo próprio usuário infectado traz consigo alguns problemas: tanto usuários testados podem não informar seu diagnóstico ao sistema, tornando-o inútil, quanto trolls e usuários de má-fé podem dar falsos positivos, gerando medo e reações desnecessárias para as pessoas que com estes mantiveram proximidade. Ambos os problemas são os custos destes métodos, que tem como benefício evitar a centralização de informação na mão de empresas ou governos. De maneira geral, mostram-se métodos mais inclinados a proteger a privacidade dos cidadãos, e são a única possibilidade de se garantir esta privacidade em países em que não estão vigentes leis de proteção de dados ou em que o governo tenha maior tendência a utilizar os dados da população para fins autoritários.

Outros problemas que podem ser suscitados pelo uso de ambas as formas de *contact tracing* em sua implementação dizem respeito à incerteza em relação à sua eficácia epidemiológica e prática (ARMBRUSTER, BRANDEAU, 2007), e à possível compulsoriedade de seu uso, em detrimento do consentimento livre e informado.

Enquanto os estudos de Fraser et al. (2020) apontam para a necessidade de que pelo menos 60% de uma determinada população utilizem os aplicativos de *contact tracing* para que estes sejam suficientes para obter resultados práticos, o aplicativo *Healthy Together*, que custou 2.75 milhões de dólares ao governo do estado norte americano de Utah, foi baixado por aproximadamente 45 mil pessoas, o que significa menos de 2% da população do estado, segundo Haskins (2020), por exemplo.

Não restam dúvidas de que o dispositivo que é formado pelo conjunto heterogêneo dos discursos, escolhas técnicas e tecnológicas, as leis e medidas normativas, as proposições filosóficas e morais ditas e não ditas sobre a prática do *contact tracing* compõe o todo da montagem de vigilância apresentada anteriormente. Nesta seção foram apresentadas quatro possibilidades distintas para a implementação do *contact tracing*: a utilização de dados de geolocalização, a utilização de contatos mediados por conexão *Bluetooth*, as bases de informações centralizadas e as bases descentralizadas. Estas possibilidades representam somente algumas das escolhas

técnicas e organizacionais que podem ser feitas, dentre diversas outras que dizem respeito, por exemplo, à obrigatoriedade de participação, à transparência dos dados, às medidas de segurança da informação implementadas. Cada escolha destas representa uma escolha política que direciona os impactos sociais do *contact tracing*, e ao fazê-lo, direciona também parcialmente a potencialidade gerada pela montagem de vigilâncias. Neste sentido, é possível analisar o sentido que está sendo dado para esta tecnologia em sua implementação no Brasil, a partir das escolhas e decisões feitas.

4. Considerações da aplicação do *contact tracing* no Brasil

A Lei Geral de Proteção de Dados (LGPD) deve servir de norte para toda e qualquer utilização de dados pessoais, em especial aqueles inerentes ao *contact tracing* no país. Isto significa que, no momento da escolha dentre as possibilidades existentes para a aplicação da tecnologia (bem como da escolha entre a implementação ou não da tecnologia), devem ser levados em consideração os princípios e regras dispostos pela LGPD.

Enquanto os arts. 7º, incisos VII e VIII, 13 e 26 da lei permitem o tratamento de dados "para a proteção da vida ou da incolumidade física do titular ou de terceiro" e "para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária" e regulam o compartilhamento de dados para pesquisa científica, são frisados os fundamentos dispostos no art. 2º da lei e os princípios no art. 6º, em especial os princípios da finalidade, adequação e necessidade.

Neste sentido, a Lei Geral de Proteção de Dados está em uma posição não de impedir que dados sejam coletados e utilizados para a construção de políticas de saúde pública, em especial de combate à COVID-19, mas sim na posição de legitimar este tratamento, desde que este esteja de acordo com suas regras e princípios.

Por este motivo, é imperioso que seja instituída assim que possível a Autoridade Nacional de Proteção de Dados (ANPD), criada pela Lei 13.853/2019, que tem atribuições cuja aplicação é urgente e cuja existência poderia trazer maior segurança jurídica para a criação de medidas que tenham como base a utilização de dados pessoais de cidadãos brasileiros. Zastrow (2020) afirma que um ponto crucial para a efetividade de medidas de contenção da pandemia, particularmente da aplicação do *contact tracing*, é a confiança da população no governo, que no Brasil passa pela confiança na ANPD.

A coleta e o tratamento de dados da população brasileira têm efeitos diretos sobre os direitos de proteção de dados e de privacidade de cada cidadão. Neste sentido, é importante trazer uma resumida diferenciação entre estes dois direitos. Considera-se aqui a proposição de Danilo Doneda (2019) que constata que há uma mudança recente no conteúdo do direito à privacidade que faz com que ele deixe de se estruturar em um eixo "pessoa-informação-segredo", passando para um eixo "pessoa-informação-circulação-controle". Por este motivo, a necessidade de funcionalização deste direito à privacidade levou ao seu desdobramento entre uma proteção do respeito pela esfera privada e a proteção de dados. O autor afirma que a proteção de dados pode ser considerada uma "continuação por outros meios" do direito à privacidade, sendo estes meios referentes não ao segredo da informação que diz respeito ao indivíduo, mas ao controle deste sobre esta informação, permitindo que o indivíduo tenha autonomia e poder de decisão sobre como e quando seus dados serão utilizados.

Sendo a privacidade um direito fundamental não absoluto, sua proteção está sujeita a ponderações e limitações, porém estas devem seguir sempre os princípios da legalidade, necessidade e proporcionalidade, conforme afirma Renieris (2020). Para a autora, estes três princípios devem ser ponderados nesta ordem. Após confirmar que uma dada medida pode ser considerada legal, a análise de sua necessidade não pode ser genérica e exige não somente que se aponte uma justificativa ampla, mas uma específica que relacione diretamente um problema delimitado à solução proposta. Ao deferir a Medida Cautelar na Ação Direta de Inconstitucionalidade 6.387, contra o inteiro teor da Medida Provisória n. 954, de 17 de abril de 2020, a ministra relatora Rosa Weber afirma que "permanece como denominador comum da privacidade e da autodeterminação o entendimento de que a privacidade somente pode ceder diante de justificativa consistente e legítima" (2020, p. 9).

Além da justificativa consistente e legítima, é importante que a interferência ao direito à privacidade seja a menor possível para atingir os objetivos desta justificativa. Assim, dois exemplos de implementação do processamento de dados de localização no Brasil servirão para exemplificar como o cuidado com a implementação, não somente do ponto de vista da tecnologia, mas também da transparência e do respeito aos direitos dos cidadãos, permite que a mesma prática seja implementada de modos mais ou menos danosos à privacidade do cidadão.

Serão apresentados os exemplos do Sistema de Monitoramento Inteligente - SIMI, do estado de São Paulo, e do aplicativo CORONAVÍRUS SUS, do Ministério da Saúde. É importante ressaltar que não é o objetivo deste estudo efetuar uma análise completa dos dois exemplos trazidos, nem o de avaliar seus resultados, sendo estes casos somente exemplificativos.

Instituído pelo decreto nº 64.963, de 05 de maio de 2020, o Sistema de Monitoramento Inteligente - SIMI do estado de São Paulo consiste de um ambiente computacional pelo qual o governo do estado pode consultar informações agregadas e anonimizadas sobre a localização dos usuários de telefonia das prestadoras de serviços de telecomunicação (Vivo, Claro, Tim, Oi), segundo o Instituto de Pesquisas Tecnológicas - IPT (2020). De acordo com o instituto, o sistema disponibiliza para o estado e para a população informações sobre o índice de isolamento social, informações estas produzidas pelas próprias empresas de telecomunicação por intermédio da Associação Brasileira de Recursos em Telecomunicações (ABR Telecom).

O isolamento social é calculado a partir do registro da localização de cada aparelho celular. Diariamente, a localização do aparelho entre os horários de 22h e 02h é registrada, e o isolamento é definido quando o aparelho não se distancia desta localização ao longo do dia. Caso o aparelho saia da área em que estava entre este horário, o sistema computa um indivíduo não praticando o isolamento social. Com base nestas informações, o SIMI-SP disponibiliza em seu website a porcentagem da população do estado de São Paulo e de suas cidades que se enquadrou no isolamento social diariamente.

A localização do aparelho celular é definida com base nas Estações Rádio Base (ERBs) com as quais este se comunica e troca informações ao utilizar qualquer serviço de dados (2G, 3G, 4G), toda vez que o celular é usado para realizar ligações ou acessar dados. Por meio de uma plataforma de Big Data gerida pela ABR Telecom, as prestadoras de serviços de telecomunicação processam os dados de localização dos aparelhos de modo a gerar o índice de isolamento social. Este índice, com os dados já anonimizados e agregados, é então repassado para o governo do estado por meio da plataforma do SIMI-SP.

Dentre os riscos à privacidade e proteção de dados trazidos por este sistema, é possível citar

que o processamento dos dados de localização pelas empresas de telefonia e pela ABR Telecom não tem um prazo definido para exclusão dos dados. Ainda que não seja possível definir uma data para o fim do período de isolamento social e da pandemia, podem ser criados prazos prorrogáveis ou condicionados a objetivos específicos. Além disso, considerando que o índice de isolamento social é criado diariamente, é de se considerar a necessidade do armazenamento dos dados por um período indefinido.

Porém, outra grande falha da iniciativa do SIMI-SP consiste na sua falta de transparência. Além de poucas medidas no sentido de tornar os processos abertos e auditáveis, fator essencial tanto para a garantia das melhores práticas de privacidade do sistema quanto de segurança da informação, a implementação do projeto teve início antes mesmo da assinatura ou publicação do acordo entre o governo do estado e as empresas de telecomunicação. O sistema, que passou a funcionar desde 24 de março de 2020, só foi tornado público em 9 de abril, anunciado pelo governador do estado, João Doria (GOMES, 2020).

O índice de isolamento social disponibilizado pelo SIMI-SP não se enquadra como a prática de *contact tracing*, porém, por consistir do processamento de dados de localização a partir da coleta de registros de ERBs, se enquadra em muitos dos aspectos levantados sobre as implicações deste tipo de processamento na privacidade.

O Ministério da Saúde brasileiro, por outro lado, a partir de 31 de julho de 2020 passou a implementar o *contact tracing* por meio de seu app CORONAVÍRUS SUS (2020). Diferente, do modelo seguido em São Paulo, o aplicativo do Ministério da Saúde se utiliza de registros de contato por *Bluetooth*, com base no protocolo desenvolvido em conjunto pela Apple e Google, citado acima.

O sistema consiste na criação de identidades anônimas e criptografadas que não tem registros identificadores com nenhum usuário e que são renovadas de 15 em 15 minutos. Além do sistema de identificação de contato anônimo com base em conexões *Bluetooth*, o registro de infectados pela COVID-19 é efetuado de modo descentralizado. Os usuários que tiverem diagnóstico positivo para a doença podem escolher se compartilham ou não seu contágio, informando a situação ao app. Para evitar os problemas citados acima de falsos diagnósticos, o Ministério da Saúde confirma o resultado do diagnóstico em uma plataforma separada, chamada de Portal Validador COVID-19. Neste portal, o usuário poderá confirmar seu diagnóstico com as bases de dados do Ministério da Saúde, e no caso de um resultado positivo o portal gera para o usuário um código PIN. Este código PIN poderá ser inserido pelo usuário no app CORONAVÍRUS SUS, de modo que o aplicativo poderá garantir o diagnóstico de acordo com as informações do Ministério da Saúde mas mantendo a anonimidade do usuário, vez que o PIN não dá acesso ou revela nenhum dado pessoal, somente a confirmação do diagnóstico.

É necessário ponderar também que medidas como o *contact tracing* são medidas secundárias no combate à COVID-19, que tem pouca utilidade no caso de medidas primárias como a ampla disponibilidade de testes de diagnóstico da doença e a preparação da estrutura do sistema de saúde nacional não serem atingidas, sendo que estas medidas devem ser prioridade em frente às secundárias.

Doneda (2020), tratando diretamente da proteção de dados em meio ao combate à pandemia, reforça a importância de que os dados coletados para modelar e executar políticas públicas sigam estritamente as finalidades propostas, colocando as leis de proteção de dados como garantias da proteção às liberdades individuais e coletivas. O autor relembra que a disciplina da proteção de dados foi construída exatamente em cima de discussões acerca do tratamento de dados médicos e dados sensíveis

e com base em boas práticas desenvolvidas na área, como por exemplo a prática de pseudonimização. A possibilidade de utilização e tratamento de dados pessoais não é, conforme o autor, uma "carta em branco", sendo essencial que sejam feitas medidas para "a minimização de riscos através da utilização de um conjunto mínimo de dados possível, a anonimização e pseudonimização sempre que possível, o emprego das medidas de segurança necessárias" (DONEDA, 2020).

5. Conclusão

A proposição de que seria necessário disponibilizar dados pessoais, diga-se dados referentes à localização dos indivíduos bem como potencialmente dados médicos, que são dados sensíveis nos termos da Lei Geral de Proteção de Dados, para poder gerar a proteção da população contra a COVID-19 ao mesmo tempo em que medidas efetivas para o combate do mesmo não são aplicadas se enquadra bem no contexto do "Capitalismo de Vigilância" proposto por Zuboff (2019).

Como cita Rodotà (2008), a perda da autodeterminação informativa é cada vez mais um "preço compulsório" para a participação dos indivíduos na sociedade, em um movimento que se inicia com o acesso destes à redes sociais, prestação de serviços personalizados e utilização de serviços virtuais e que cada vez mais vem condicionando o acesso também à bens essenciais para uma vida digna, como o acesso a sistemas de saúde. Ao mesmo tempo, os dados que são exigidos em troca da participação e do acesso são retirados dos indivíduos e apropriados pelas empresas que compõem o Grande Outro (Big Other) proposto por Zuboff (2020), de modo que a informação, que é parte constitutiva da identidade do sujeito, dele é retirada para posteriormente ser utilizada muitas vezes contra ele mesmo.

Mais grave ainda, para Rodotà, é quando os dados que são retirados do indivíduo são dados referentes ao seu corpo, como o são dados médicos, uma vez que estes se referem "à nua condição humana" (RODOTÀ, 2008, p. 250). Ainda assim, a gravidade do tema não significa o impedimento completo da utilização dos dados, mas sim que esta deve ser limitada e determinada. A chave para a integração entre a utilização de dados médicos para desenvolvimentos na saúde pública e a proteção de dados é a estrita utilização destes dentro das finalidades propostas.

É importante, porém, ter a consciência de que quaisquer novas tecnologias e novos dispositivos que tenham como resultado a coleta e o tratamento de dados pessoais são fruto de uma série de escolhas em âmbito técnico, econômico, político, filosófico e moral, e que estas escolhas determinam o direcionamento da potencialidade gerada pelo tratamento dos dados. Ao inserir os dados provenientes do *contact tracing* ou do processamento de geolocalização na montagem de vigilâncias, escolhas que possibilitem que estes dados sejam provenientes de processos mais ou menos intrusivos à população, ou que gerem maior ou menor desequilíbrio de poder na relação entre o indivíduo e o Estado e entre o indivíduo e o mercado terão uma consequência direta de levar à montagem de vigilâncias à potencialidades mais ou menos intrusivas e mais ou menos desequilibradas.

No mesmo sentido, é essencial reconhecer, como o faz Foucault (1999) no contexto da lepra e da peste negra, que há sempre um "sonho político" à espreita de medidas necessárias para o combate das doenças, e que estes sonhos políticos refletem e avançam as estruturas e o controle social de seu tempo, sendo a implementação de sistemas e aplicativos que produzem e compartilham não somente dados de localização dos indivíduos, mas possivelmente também com dados médicos e redes de contato

uma relevante aquisição para a montagem de vigilâncias, com graves riscos para a privacidade dos cidadãos, criando potencialidades que colocam em risco os direitos e liberdades individuais e coletivos, quando implementadas sem um desejo ativo de proteger a privacidade. Segundo Foucault, "nem tudo é ruim, mas tudo é perigoso, o que não significa exatamente o mesmo que ruim. Se tudo é perigoso, então temos sempre algo a fazer." (DREYFUS; RABINOW, 1995, p. 256).

Referências

Apple, Google. Contact Tracing: Bluetooth Specification. V 1.1, abr. 2020. Disponível em: https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ContactTracing-BluetoothSpecificationv1.1.pdf Acesso em 12 abr. 2020.

Armbruster, B.; Brandeau, M. L. Contact tracing to control infectious disease: when enough is enough. Health care management science, 2007, 10.4: 341-355.

Bauman, Z, & Lyon, D. (2014). Vigilancia líquida. Editora Schwarcz-Companhia das Letras.

Bentham, J. (2000). O panóptico ou a casa de inspeção. O panóptico. Belo Horizonte: Autêntica, 11-74.

Bigo, D. (2006). Security, exception, ban and surveillance. Theorizing surveillance: The panopticon and beyond, 46-68.

Browne, S. (2015). Dark matters: On the surveillance of blackness. Duke University Press.

Bruno, F. (2013). Máquinas de ver, modos de ser: vigilância, tecnologia e subjetividade. Porto Alegre: Sulina.

Bruno, F., & Kanashiro, M., & Firmino, R. J. (Eds.). (2010). Vigilância e visibilidade: espaço, tecnologia e identificação. Editora Sulina.

Deleuze, G. (1992). Postscript on the Societies of Control. October, 59, 3-7.

Dias, T. (2020). Vigiar e Lucrar: nós identificamos dois clientes dos dados de localização 'anônimos' vendidos pela Vivo. The Intercept Brasil. Disponível em: https://theintercept.com/2020/04/13/vivo-venda-localizacao-anonima/

Dixon, M. G., Taylor, M. M., Dee, J., Hakim, A., Cantey, P., Lim, T., ... & Touré, L. Y. (2015). Contact tracing activities during the Ebola virus disease epidemic in Kindia and Faranah, Guinea, 2014. Emerging infectious diseases, 21(11), 2022.

Doneda, D. (2020) A proteção de dados em tempos de coronavírus. Jota. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/a-protecao-de-dados-em-tempos-de-coronavirus-25032020

Doneda, D. (2019). Da privacidade à proteção de dados. 2ª Edição. São Paulo: Revista dos Tribunais.

Dreyfus, H. L., Rabinow, P., & Carrero, V. P. (1995). Michel Foucault, uma trajetória filosófica: para além do estruturalismo e da hermenêutica. Rio de Janeiro: Forense Universitária.

Elmer, G. (2012). Panopticon-discipline-control. Routledge handbook of surveillance studies, 21, 29.

Foucault, M. (1999). Vigiar e punir: nascimento da prisão. 20ª Edição. Petrópolis: Editora Vozes,[1975].

Fraser, C. et al. (2020). Digital contact tracing: comparing the capabilities of centralised and decentralised data architectures to effectively suppress the COVID-19 epidemic whilst maximising freedom of movement and maintaining privacy. Disponível em: https://github.com/BDI-pathogens/covid-19_instant_tracing/blob/master/Centralised%20and%20decentralised%20systems%20for%20contact%20tracing.pdf

Gandy Jr, O. H. (1993). The Panoptic Sort: A Political Economy of Personal Information. Critical Studies in Communication and in the Cultural Industries. Westview Press, Inc.

Gendzier, I. L. (1974). Frantz Fanon: A critical study.

Gilroy, P. (1993). The black Atlantic: Modernity and double consciousness. Harvard University Press.

Goffman, E. (1961). Manicômios, prisões e conventos. In Manicômios, prisões e conventos (pp. 316-316).

Gomes, H. S. (2020). Sem avisar, SP iniciou monitoramento de celular antes de acordo formal. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2020/05/13/sem-avisar-sp-iniciou-monitoramento-22-dias-antes-de-acordo-formal.htm

Guattari, F., & Deleuze, G. (2011). Mil platôs-vol. 1 (Vol. 1). 2ª Edição. São Paulo: Editora 34.

Haggerty, K. D., & Ericson, R. V. (2000). The surveillant assemblage. The British journal of sociology, 51(4), 605-622.

Haggerty, K. D. (2006). Tear down the walls: on demolishing the panopticon. In Theorizing surveillance (pp. 37-59). Willan.

Haskins, C. (2020). Utah's Contact Tracing App Was Supposed To Help The State Open Up. It Isn't Going Very Well. Buzzfeed News. Disponível em: https://www.buzzfeednews.com/article/carolinehaskins1/utah-spent-millions-contact-tracing-app-covid-19-coronavirus

Instituto de Pesquisas Tecnológicas - IPT. (2020). IPT responde perguntas frequentes (FAQs) sobre índices de isolamento social divulgados pelo Governo de SP. Disponível em: https://www.ipt.br/noticia/1623-_perguntas_sobre_isolamento_social.htm

Kuhn, T. S. (1970). A estrutura das revoluções científicas. Ed. Perspectivas. São Paulo.

Lanier, J. (2018). Ten arguments for deleting your social media accounts right now. Random House.

Lyon, D. (2015). Surveillance after Snowden. John Wiley & Sons.

Lyon, D. (2003). Surveillance after september 11 (Vol. 11). Polity.

Lyon, D. (Ed.). (2006). Theorizing surveillance: The panopticon and beyond. Willan Pub.

Lyon, D., Haggerty, K. D., & Ball, K. (2012). Introducing surveillance studies. In Routledge handbook of surveillance studies (pp. 33-44). Routledge.

Mann, S. (2013, June). Veilance and reciprocal transparency: Surveillance versus sousveillance, AR glass, lifelogging, and wearable computing. In 2013 IEEE International Symposium on Technology and Society (ISTAS): Social implications of wearable computing and augmediated reality in everyday life (pp. 1-12). IEEE.

Medida Cautelar na Ação Direta de Inconstitucionalidade 6.387. (2020). Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI6387MC.pdf

Mathiesen, T. (1997). The viewer society: Michel Foucault'sPanopticon'revisited. Theoretical criminology, 1(2), 215-234.

Norris, C. (2005). From personal to digital: CCTV, the panopticon, and the technological mediation of suspicion and social control. In Surveillance as social sorting (pp. 263-295). Routledge.

Organização Mundial da Saúde (OMS). (2005). International health regulations (2005). World Health Organization, 2008.

Organização Mundial da Saúde (OMS). (2020). Contact Tracing. Online Q&A, mai. 2017. Disponível em: https://www.who.int/features/qa/contact-tracing/en/ Acesso em 14 abr. 2020.

Rediker, M. (2007). The slave ship: A human history. Penguin.

Renieris, E. M. (2020). Applying core international human rights principles to coronavirus-related privacy interferences. Berkman Klein Center Collection. Disponível em: https://medium.com/berkman-klein-center/when-privacy-meets-pandemic-fbf9154f80b3

Rhodes, L. A. (2004). Total confinement: Madness and reason in the maximum security prison (Vol. 7). Univ of California Press.

Richards, N. M. (2012). The dangers of surveillance. Harv. L. Rev., 126, 1934.

Ritchie, M. (2020). Fusing Race: The Phobogenics of Racializing Surveillance. Surveillance & Society, 18(1), 12-29.

Rivest, R. L. et al. The PACT protocol specification. Versão 0.1 8 abr. 2020. Disponível em: https://pact.mit.edu/wp-content/uploads/2020/04/The-PACT-protocol-specification-ver-0.1.pdf

Rodotà, S. (2008). A vida na sociedade da vigilância: a privacidade hoje. In A vida na sociedade da vigilância: a privacidade hoje

Silva, R. L. & Silva, F. S. R. (2019). Reconhecimento Facial e Segurança Pública: Os perigos do uso da Tecnologia no Sistema Penal Seletivo Brasileiro. 5º Congresso Internacional de Direito e Contemporaneidade: mídias e direitos da sociedade em rede.

Silva, T. (2019). Racismo Algorítmico em Plataformas Digitais: microagressões e discriminação em código. COMUNIDADES, ALGORITMOS E ATIVISMOS DIGITAIS, 121.

Snowden, E. (2019). Permanent record. Macmillan.

Stanley, J.; GRANICK, S. (2020). The Limits of Location Tracking in an Epidemic. ACLU, 8 abr. 2020. Disponível em: https://www.aclu.org/report/aclu-white-paper-limits-location-tracking-epidemic?redirect=aclu-white-paper-limits-location-tracking-epidemic

Tracetogether. (2020). TraceTogether Privacy Safeguards. 2020. Disponível em: https://www.tracetogether.gov.sg/common/privacystatement

Troncoso et al. (2020). Decentralized Privacy-preserving Proximity Tracing. Versão 3 abr. 2020. Disponível em: https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf

Valentino-Devries, J. (2020). Translating a Surveillance Tool into a Virus Tracker for Democracies. The New York Times, 19 mar. 2020. Disponível em: https://www.nytimes.com/2020/03/19/us/coronavirus-location-tracking.html

Valida Coronavírus SUS. (2020).Termo de Consentimento para Tratamento de Dados. Disponível em: https://validacovid.saude.gov.br/politica-privacidade

Winner, L. (1980). Do artifacts have politics?. Daedalus, 121-136.

Wood, D. (2003). Foucault and panopticism revisited. Surveillance & Society, 1(3), 234-239.

Woodhams, S. (2020). COVID-19 Digital Rights Tracker. TOP10VPN, 20 mar. 2020. Disponível em: https://www.top10vpn.com/news/surveillance/covid-19-digital-rights-tracker/

Xia, H., & Yang, W. (2018). Implicit Privacy Protection in Spatio-temporal Data Distribution. Journal of Information Hiding and Multimedia Signal Processing, 9(5), p. 1199-1211.

Zastrow, M. (2020). Coronavirus contact-tracing apps: can they slow the spread of COVID-19? Nature. Disponível em: https://www.nature.com/articles/d41586-020-01514-2 DOI: 10.1038/d41586-020-01514-2.

Zhang, B., Kreps, S., & McMurry, N. (2020). Americans' perceptions of privacy and surveillance in the COVID-19 Pandemic.

Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. Profile Books.

Zuboff, S. (2020). Nuovi Capitalismi (della sorveglianza). Formiche: Orwell 2020. Il virus della sorveglianza, 158, 8-13.