O que rastreiam as corona-*apps*? Paradoxos da cultura da vigilância na modernidade digital

What do corona-virus apps trace? Paradoxes of surveillance culture in the digital age

Rita Figueiras

Universidade Católica de Lisboa, Faculdade de Ciências Humanas, Centro de Estudos de Comunicação e Cultura — CECC, Lisboa, Portugal
ritafigueiras@fch.lisboa.ucp.pt
ORCID ID: 0000-0001-8092-2264

DOI: https://doi.org/10.34619/ss2b-cr04

Resumo: O capítulo debate as corona-apps e perspetiva estas aplicações de rastreio de contactos como um fenómeno sócio-tecnológico no contexto da modernidade digital. O texto argumenta que estas aplicações, entendidas como uma modalidade de monitoramento personalizado em larga escala, remetem para imaginários e práticas que consolidam a cultura da vigilância que caracteriza as sociedades contemporâneas tecnologicamente desenvolvidas.

Palavras-chave: Aplicações de rastreio, Cultura da Vigilância, Modernidade Digital, Autocratização.

Abstract: *The chapter debates the corona-apps and perceives these contact tracing apps as a socio-technological phenomenon in the context of the digital age. Understood as a personalized large-scale surveillance mechanism, the paper argues that these apps can be seen as an expression of social imaginaries and practices that consolidate the culture of surveillance that characterize contemporary technological advanced societies.*

Keywords: *Contact tracing apps, Culture of surveillance, Digital age, Autocratization.*

Introdução

O ano de 2020 ficará para sempre na história mundial por causa do surto de pandemia causado pelo coronavírus 2, da Síndrome Respiratória Aguda Grave (SARS-CoV-2), também conhecido por COVID-19. A sua taxa de mortalidade é mais baixa do que a de outros vírus conhecidos (como o SARS e o MERS), mas o COVID-19 é altamente infeccioso.

A rápida disseminação deste vírus pelo mundo levou a Organização Mundial da Saúde (OMS) a considerá-lo, a 30 de janeiro de 2020, uma emergência de saúde pública de interesse internacional. Este anúncio impulsionou muitos governos a declararem o estado de emergência, medidas de confinamento, políticas de trabalho e ensino remoto, critérios de distanciamento social e uso de equipamento de proteção pessoal. Simultaneamente, foram instituídas respostas de saúde pública de emergência, como infraestruturas para o tratamento e testes às populações.

Um dos maiores problemas que o COVID-19 coloca é que, inicialmente, os indivíduos infectados podem não apresentar sintomas e alguns permanecem assintomáticos. Por esta razão, uma fracção não desprezível da população pode, a qualquer momento, ser uma fonte oculta de transmissão. No entanto, quando alguém é diagnosticado é necessário dar início ao rastreio de contactos do portador positivo.

A reconstituição dos 14 a 21 dias anteriores (identificado como o período de incubação do COVID-19) é feita por funcionários das autoridades de saúde. A informação recolhida por entrevista manual visa calcular o risco de contágio, estimado a partir do contexto (dentro/fora de casa), duração (tempo de contacto) e proximidade (distância entre os contactos) dos encontros. Se é um desafio recordar todos os contactos estabelecidos, este tipo de rastreio tem uma dificuldade acrescida: o doente pode ter infectado outros que não consegue identificar,

porque não os conhece (e.g., contacto numa fila de supermercado ou num transporte público). Por essa razão, o rastreio de contactos tradicional é uma medida de saúde pública morosa e exige um elevado número de profissionais para sinalizar casos suspeitos ou confirmados de COVID-19.

Tendo em conta a morosidade e o trabalho envolvido no rastreio manual de contatos, bem como a sobrecarga que a pandemia colocou nos sistemas públicos de saúde, vários governos investiram em sistemas digitais para automatizar parte do processo de rastreio. As aplicações de rastreio de contactos foram, assim, desenvolvidas para auxiliarem as autoridades públicas e alertarem os usuários individuais para a exposição ao vírus. Todavia, no quadro das sociedades democráticas, esta solução tecnológica fez emergir um conjunto de apreensões sobre os riscos que as *apps* colocam à privacidade e segurança dos dados e meta-dados dos indivíduos.

Neste capítulo perspetivamos as aplicações de rastreio de contactos como um fenómeno sócio-tecnológico e pensamos sobre elas no contexto da relação entre a vigilância social e a vida quotidiana nas sociedades contemporâneas. Para tal, começamos por analisar o desenho das aplicações e de que modo asseguram o equilíbrio entre eficácia e privacidade no quadro dos valores das sociedades democráticas. De seguida, refletimos sobre a modernidade digital e o seu contributo para a amplificação do significado da vigilância que, no século XXI, tornou-se uma componente da vida. Nas reflexões finais argumentamos que as aplicações de rastreio de contactos, entendidas como mais uma modalidade de monitoramento personalizado em larga escala na modernidade digital, remetem para imaginários e práticas que consolidam a cultura da vigilância nas sociedades tecnologicamente desenvolvidas. O modo como a vigilância é concebida e como ela se relaciona com outras práticas e dimensões da vida social permitem, igualmente, debater dinâmicas paradoxais entre controlo e liberdade nas democracias em crescente processo de erosão.

1. A arquitetura das aplicações de rastreio de contactos

Em setembro de 2020, as aplicações de rastreio de contatos estavam disponíveis em cerca de 50 países[1]. Apesar de haver pouca informação acerca da adesão das populações, dados sobre a União Europeia[2] revelam uma taxa maior de conexão coletiva a estas *apps* nos

1 Inicialmente anunciada para maio, a aplicação portuguesa, Stayaway Covid, foi disponibilizada no final de agosto de 2020. O INESC TEC desenvolveu esta *app* em colaboração com o Centro Nacional de Cibersegurança (CNCS) e o Instituto de Saúde Pública da Universidade do Porto (ISPUP), a Keyruptive e a Ubirider. Por sua vez, o decreto-lei que viabilizou esta solução tecnológica em Portugal foi, igualmente, promulgado no final de agosto de 2020.

2 "Apps para rastrear covid-19, um empreendimento arriscado", *Deutsche Welle*: 28-07-2020, https://www.dw.com/

países com populações menores. Por exemplo, na Islândia, com os seus menos de 400 mil habitantes, mais de 40% fizeram o *download* do Ranking C-19 no mês seguinte à *app* estar disponível. Na Irlanda, numa população de 5 milhões, 1,3 milhões de pessoas descarregaram a Covid Tracker oito dias após o seu lançamento, tornando-se a aplicação com mais *downloads* per capita na Europa.

Enquanto os países da União Europeia desenvolviam as suas aplicações[3], o Conselho Europeu emitia uma declaração sobre a importância da proteção de dados pessoais durante o combate ao COVID-19 e sinalizava os artigos do Regulamento Geral de Proteção de Dados da UE que forneciam as bases legais para o processamento de dados pessoais no contexto de epidemias. Tendo por base estas diretivas, a maioria dos países aprovou regulação para o uso e ciclo de vida dos dados recolhidos, e as autoridades de proteção de dados nacionais realizaram avaliações de risco centradas na privacidade e segurança dos dados[4].

A maioria dos países adoptou a tecnologia Bluetooth para informar os usuários de riscos de infecção, sem associar dados de localização[5]. Foi também instituída a não obrigatoriedade do *download* das aplicações, sendo possível a sua desinstalação a qualquer momento. Esta adesão voluntária implica que nenhuma consequência negativa pode ser associada à recusa do seu uso. Portanto, testes de triagem, capacidade de viajar e acesso a certos serviços (e.g., transporte público) não podem ser condicionados ao uso da *app*. Por outro lado, na generalidade dos casos, o *download* não requer dados pessoais e solicita o consentimento para a partilha desses dados com terceiros.

O sistema híbrido, que combina recursos das arquiteturas centralizada e descentralizada

pt-br/apps-para-rastrear-covid-19-um-empreendimento-arriscado/a-54357321, acesso a 11-08-2020; "Global contact tracing app downloads lag behind effective levels", *Quartz*: 15.07.2020, https://qz.com/1880457/global-contact-tracing-app-downloads-lag-behind-effective-levels/ acedido a 10.08.2020; "Cheap, popular and it works: Ireland's contact-tracing app success", *The Guardian*: 20.07.2020, https://www.theguardian.com/world/2020/jul/20/cheap-popular-and-it-works-irelands-contact-tracing-app-success?CMP=Share_iOSApp_Other, acedido a 12.08.2020.

3 As aplicações de rastreio de contactos foram desenvolvidas pelas autoridades nacionais de saúde pública em parceria com a Apple e a Google. Numa primeira fase foi necessário instalar a aplicação de rastreio para sinalizar portadores do vírus, mas a partir de setembro de 2020 deixou de ser preciso fazer o *download* de uma aplicação específica para se receber as notificações. Isto tornou-se possível graças à atualização dos sistemas operativos iOS e Android. Contudo, continuou a ser necessário instalar uma aplicação para introduzir a informação dos que testam positivo. "Google and Apple to roll out phase two of contact-tracing system", *The Guardian*: 27.08.2020,https://www.theguardian.com/technology/2020/aug/27/google-and-apple-to-roll-out-phase-two-of-contact-tracing-system, acedido a 28.08.2020.

4 Os testes de risco efetuados às aplicações de rastreio de contactos podem ser sintetizados num conjunto de questões: Que dados são produzidos e por quem? Que dados são trocados entre quem e quando? Que dados são armazenados, onde, por quem e durante quanto tempo? Quem pode ter acesso a que dados? (Ahmed *et al.*, 2020 p. 10).

5 A probabilidade de contrair o COVID-19 aumenta com o contacto prolongado e próximo com uma pessoa infectada e, por isso, as estimativas de distância e duração do contacto são informações importantes para avaliar a potencial propagação da infecção. As aplicações de rastreio de contactos visam registar esses encontros. O sistema automatizado de rastreio de contatos baseado em *smartphones* utiliza uma de duas tecnologias: GPS ou Bluetooth. Quando dois usuários se aproximam a uma distância de cerca de dois metros, e assim permanecem por quinze minutos ou mais, os telefones trocam IDs gerados aleatoriamente. Se o teste de um desses usuário for positivo, ele pode inserir o resultado na aplicação para informar todos os contatos armazenados e essa informação é gerida centralmente pelas autoridades de saúde pública.

(Ahmed *et al.*, 2020), é o que predomina nos países da UE: as chaves de contatos são coligidas localmente em cada dispositivo e as chaves carregadas por usuários infectados (e dados adicionais) são armazenadas num servidor central, onde a informação é apenas acessível às autoridades de saúde pública e mantida durante 14 a 30 dias (variações nacionais). Deste modo, os TempID permanecem descentralizados para garantirem privacidade e anonimato aos usuários, enquanto a análise de risco e as notificações, em casos de suspeita de contágio ou de infecção declarada, são da responsabilidade do servidor centralizado.

A maioria das aplicações foi desenhada para preservar a privacidade dos usuários – i.e., não revelar informações de identificação pessoal ou localização dos contatos sem permissão explícita –, no entanto, os *media* internacionais têm noticiado dificuldades em equilibrar eficácia e segurança no plano tecnológico, mas também no dos valores democráticos. Por exemplo, a autoridade francesa de proteção de dados declarou a conformidade da StopCovid aos requisitos legais de proteção de dados da UE e do país, todavia, duas semanas após o seu lançamento, investigadores em criptografia demonstraram que a *app* processava mais dados do que o necessário para rastrear a propagação do vírus e que todos esses dados eram enviados para o servidor central. O governo francês não negou as acusações. Por sua vez, a autoridade de proteção de dados da Noruega realizou testes de risco à Smittestopp, mas o órgão de saúde pública do país suspendeu a *app* pouco tempo depois de entrar em funcionamento e eliminou todos os dados recolhidos por suspeitas de violabilidade do sistema.

Vejamos agora o caso da Polónia. O país desenvolveu duas aplicações distintas para combater o COVID-19. Se uma delas foi desenhada em linha com os requisitos do RGPD (adesão voluntária, uso de Bluetooth, arquitetura semi-centralizada, minimização dos dados e consentimento para partilha com terceiros), a segunda tem características muito diferentes. Esta aplicação é de uso obrigatório para todos as pessoas sujeitas a quarentena domiciliar por terem regressado do estrangeiro ou por suspeita de exposição ao vírus. A *app* usa geolocalização e tecnologia de reconhecimento facial para garantir o cumprimento da quarentena. Várias vezes por dia, até 20 minutos depois do recebimento de uma mensagem de texto, é obrigatório o envio de uma *selfie*, através da *app*, para a polícia certificar o cumprimento da quarentena. A *app* requer os seguintes dados: ID do cidadão, nome completo, número de telefone, endereço de residência, fotografia, localização do cidadão e data final da quarentena. Não é necessário o consentimento do usuário para que os seus dados sejam disponibilizados a terceiros nem para que sejam automaticamente enviados para um sistema centralizado, mas partilhado pelas autoridades de saúde pública, a polícia e as empresas que desenvolveram a aplicação. De notar, ainda, que estes dados são armazenados durante seis anos (exceto as fotografias que são excluídas quando o usuário desativa a conta), e o governo polaco não está vinculado pelas leis de privacidade aplicadas aos dados recolhidos por esta modalidade de rastreio.

Estas duas aplicações, em conjunto, espelham bem a dualidade do regime político em vigor na Polónia. O país está em processo de autocratização há já alguns anos. Ou seja, ao

mesmo tempo que mantém formalmente instituições basilares do regime democrático, estas estão a ser reconfiguradas por dentro no sentido da autocratização. Todavia, mesmo no quadro das democracias liberais, o objetivo de controlar a propagação do COVID-19 tem colocado desafios fundamentais ao equilíbrio entre possibilidades tecnológicas e valores democráticos, questão em reflexão na próxima secção do capítulo.

2. Coronas-*apps*: entre possibilidades tecnológicas e valores democráticos

Quando os países europeus anunciaram o desenvolvimento de aplicações de rastreio de contactos, um conjunto de vozes receosas alertaram para os perigos desta solução tecnológica (como se pode constatar da leitura das referências jornalísticas elencadas no fim deste artigo). Muitos desses receios devem ser entendidos como a continuação, ou a atualização, de apreensões latentes na sociedade e resultantes de dilemas que as possibilidades tecnológicas colocam aos valores democráticos. No âmbito da pandemia, os dilemas construíram-se em torno de dois sistemas de valores difíceis de compatibilizar: privacidade e segurança dos indivíduos. A tensão entre estes valores é complexa *per se*, mas é-o também por causa dos objetivos e significados distintos atribuídos às aplicações de rastreio pelos vários atores envolvidos: autoridades de saúde, governos, entidades reguladoras, empresas tecnológicas e cidadãos.

Um dos riscos associados a estas aplicações relaciona-se com a centralização dos dados em servidores e a susceptibilidade a ataques cibernéticos (terrorismo ou *hackers*), nomeadamente: paralisação do serviço, manipulação de dados dos usuários e uso dessas informações pessoais para outros fins. A utilização do *smartphone* para o rastreio também potencia riscos, porque o anonimato total dos usuários não é garantido. Para além de ser possível a reversão da pseudo-anonimização e a reconstrução do mapa dos laços sociais dos usuários, o facto do Bluetooth estar sempre ligado aumenta a possibilidade do sistema gerar, de modo automático, falsos alarmes.

Por outro lado, a segurança oferecida pelo aspecto voluntário da *app* tem diminuído com o aumento de pressões sociais e económicas. Em vários países têm sido desenvolvidas diligências para o sector privado poder usar as aplicações de rastreio, ou informações por elas fornecidas, para monitorizar o estado de saúde dos funcionários no local de trabalho. A possibilidade crescente de monitoramento digital torna cada vez mais difícil discernir o que pode configurar práticas de vigilância para além do necessário para fins de manutenção de um ambiente de trabalho seguro.

Igualmente relevante é o facto de a Apple e a Google, enquanto provedores dos sistemas operacionais, poderem ter acesso aos dados produzidos pelas aplicações de rastreio de contactos. Esta questão torna-se ainda mais relevante se tivermos em conta que as grandes empresas tecnológicas detêm os ambientes digitais em que os dados são gerados, produzem

os dispositivos pelos quais os dados são recolhidos de modo automatizado e gerem os dados extraídos dos conteúdos produzidos por usuários individuais e coletivos (Couldry & Mejias 2019, p. 44). Estas empresas desempenham um papel central na cadeia de valor do *big data,* cujo peso aumenta à medida que mais atividades sociais ocorrem de modo digital, reforçando o "capitalismo de vigilância" (Zuboff 2015). Em síntese, estamos perante "empresas-estado" (Stern 2011): empresas com um poder enorme de regular o comércio e as políticas públicas, bem como as relações entre as pessoas. Cada vez mais, estas corporações têm a capacidade de regular a vida na modernidade digital, suplantando os próprios estados ou instituições supranacionais, como a União Europeia, que têm enormes dificuldades em regulamentar a atividade destas empresas.

A par da vigilância comercial, a vigilância governamental tem instigado receios crescentes, principalmente associados à falta de confiança nos governos num tempo em que as democracias estão em processo de erosão, a polarização social cresce, a radicalização política aumenta e movimentos políticos anti-sistema, como o populismo, ganham adesão nas sociedades democráticas.

Tal como têm evidenciado os relatórios da Freedom House e V-Dem, várias democracias estabelecidas no mundo estão em processo de reversão. Países como a Hungria e a Polónia são apenas os casos mais evidentes da terceira vaga de autocratização (Lührmann & Lindberg 2019) iniciada há cerca de 10 anos. Este processo sinaliza movimentos que se afastam da democracia em direção à autocracia (Sartori 1970), embora na atualidade esses movimentos tenham características distintas de processos semelhantes ocorridos no passado[6].

De acordo com Anna Lührmann & Staffan Lindberg (2019 p. 1104), a terceira vaga de autocratização caracteriza-se, principalmente, por uma fachada legal. Vários governantes usam estratégias legais para minar dimensões-chave das democracias sem abolirem as suas instituições fundamentais[7]. Ao mesmo tempo que realizam eleições multipartidárias, os políticos autocráticos censuram e/ou hostilizam os *media*, restringem a sociedade civil, constrangem os partidos políticos e minam a autonomia dos órgãos de regulação (Bermeo 2016 p. 14).

A concentração gradual de poder no executivo é, assim, o padrão-chave da autocratização

6 Nas décadas de 1960 e 1970, os colapsos democráticos ocorreram através de eventos repentinos e flagrantes, por exemplo, fraude eleitoral, golpe militar ou golpe interno. Neste último caso, o chefe do executivo chegava ao poder por meios legais, mas, de seguida, abolia instituições democráticas importantes, como eleições ou parlamentos. Todavia, nas décadas de 1990 e 2000, à medida que o poder normativo das democracias se instituiu como um modelo referencial em grande parte do mundo e o próprio regime democrático se disseminou, as violações evidentes das normas democráticas passaram a acarretar custos elevados de legitimidade. Movimentos repentinos e ilegais para a autocracia começaram a provocar oposição nacional e internacional e, por esta razão, a mudança de regime tornou-se cada vez mais gradual e menos perceptível do que os casos históricos anteriores (Bermeo 2016; Schedler 2013).

7 Segundo Robert Dahl (1998) a democracia eleitoral pode ser caracterizada como uma «poliarquia» e pode ser sintetizada nos seguintes elementos: sufrágio universal, governantes eleitos em eleições livres e justas, fontes alternativas de informação, liberdade de expressão e liberdade de associação.

contemporânea, como bem ilustram os casos da Hungria e Polónia. Estes países transformaram-se em democracias iliberais em contínuo processo de consolidação autocrática. Nestes e noutros países onde a erosão democrática é uma realidade, mesmo que em menor grau, a adoção de agendas políticas mais restritivas não deixa de ser uma possibilidade com o prolongamento e a intensificação da pandemia. Nomeadamente, com a obrigatoriedade do uso de aplicações de rastreio para monitorizar os indivíduos infetados e/ou para se aceder a espaços fechados e/ou públicos (e.g., transportes). Acrescem dúvidas sobre possíveis usos posteriores dos dados, quando a pandemia atual terminar. Por outro lado, as *apps* não garantem anonimato absoluto e isso desprotege os cidadãos contra qualquer tipo de vigilância individual.

Neste contexto, é relevante considerar o inquérito sobre as atitudes das populações da Bélgica, Espanha, Itália e Portugal face às aplicações de rastreio de contactos, realizado pela *Euroconsumers*[8], em maio de 2020. Os dados indicam que a maioria dos inquiridos nos quatro países acredita que estas *apps* podem desempenhar um papel fundamental no combate ao COVID-19: 66% na Bélgica, 67% em Espanha, 73% em Itália e 78% em Portugal. Mais de 60% dos respondentes considera também que o uso de dados pessoais pode ajudar a diminuir a disseminação da doença, com os números a alcançarem 70% em Portugal. Isto não significa que as populações não tenham receio que ocorram violações de privacidade, mas como consideram não haver garantias absolutas de anonimidade dos dados em qualquer circunstância, estão dispostas a prescindir temporariamente da sua privacidade em benefício do combate à pandemia.

Este inquérito demonstra bem como a privacidade e a segurança são valores fundamentais no quadro das sociedades democráticas, mas revela também que a importância atribuída a cada um destes valores, bem como a relação entre ambos, é sempre contextual. Qualquer disrupção social de magnitude assinalável, como é o caso de uma pandemia, tem um efeito acelerador de tendências que se desenham paulatinamente nas sociedades, e o coronavírus parece ter-se transformado numa oportunidade para testar (em certos casos) ou aumentar a velocidade (noutros casos) da implementação de medidas que contribuem para o processo de hibridização dos regimes políticos em curso em muitos países democráticos.

Este processo parece ser cada vez mais indissociável das tecnologias. As sociedades contemporâneas caracterizam-se por um aumento geral da importância dos *media* e da tecnologia em uma ampla variedade de dimensões da vida e isto significa que as aplicações de rastreio também podem ser perspetivadas como mais um elemento no crescente processo de indissociabilidade entre vida humana e tecnologia digital. Abordamos esta questão na próxima secção do texto.

8 https://assets.ctfassets.net/iapmw8ie3ije/7BC7L3aIh3SBiIuXDiUSaV/dc74389394f39fae0d2f62b411b58726/Press_release__Consumers_support_the_use_of_apps_in_fighting_virus__although_privacy_concerns_remain_top_of__minds_-_latest_.pdf, acedido a 16.08.2020.

3. As corona-*apps* no contexto da modernidade digital

O funcionamento das sociedades contemporâneas é crescentemente feito a partir, e por meio, de processos e infraestruturas de comunicação mediados tecnologicamente. À medida que mais áreas da vida social dependem de infraestruturas de mediação digital, mais sectores da sociedade se adaptam e se tornam dependentes das tecnologias. Dito de outro modo, a crescente estruturação dos espaços público e privado em infraestruturas tecnológicas e o enfraquecimento do elo entre localização física e experiência social estão na base da transformação das tecnologias em infraestruturas sociais.

Este processo está relacionado com a mobilidade, a conectividade e a interatividade tecnológica, o que ajuda a compreender a integração significativa dos *media* na vida em geral. As rotinas diárias estão profundamente entrelaçadas nos *media* móveis – como *smartphones*, *tablets*, redes Wi-Fi e contas em *media* sociais –, usados para uma ampla variedade de atividades durante o tempo livre, o trabalho, o trânsito ou em outras situações. As tecnologias móveis também facilitam a fusão entre trabalho e lazer, espaços profissionais e domésticos, esferas pública e privada, o que gera frequentemente sentimentos de ambiguidade. As vantagens sociais percebidas de empoderamento, liberdade e libertação coexistem muitas vezes com sentimentos de ansiedade (Jansson 2014 p. 275), por exemplo, devido à descompartimentalização do trabalho: pelo facto de poder ser realizado em qualquer lugar e a qualquer momento perpetua a sua presença em todos os contextos e dias da semana.

As tecnologias móveis tornaram-se fundamentais na vida profissional, pessoal e íntima, sendo o *smartphone* um dos exemplos mais evidentes da crescente indissociabilidade entre a vida humana e a tecnologia digital. Esta interdependência continua a expandir-se com a ajuda da computação omnipresente e da internet das coisas, nomeadamente das tecnologias vestíveis (roupa) e do desenvolvimento de *smart objects* (e.g., frigoríficos e carros) e *smart cities* (ruas, edifícios, transportes). Visto por outro prisma, isto significa que a proporção de operações capazes de produzir, recolher e processar dados está a intensificar-se exponencialmente (Bolin & Schwarz 2015; Couldry & Hepp 2017; Couldry & Mejias 2019).

Atualmente, os dados extraídos de ocorrências quotidianas provêm de múltiplas fontes: *media* sociais, *smartphones* e outros dispositivos conectados e portáteis, assistentes virtuais (e.g., a *Alexa* da Apple ou a *Echo* da Amazon), câmaras inteligentes (como as câmaras de vigilância CCTV no espaço público ou as integradas nas campainhas das portas de casa) e uma gama crescente de sistemas com cada vez mais abrangentes formas de captação de dados, como os já referidos *smart objects* e *smart cities*. Ou seja, a capacidade de rastrear está a crescer com a expansão da internet das coisas, o que tem possibilitado a incorporação do consumo – o que fazemos com os produtos depois de os comprarmos – na cadeia de valor do *big data* através do processamento deste tipo de dados, inéditos até há poucos anos.

Neste contexto, pensemos nas aplicações de rastreio de contactos e nos múltiplos

interesses que elas podem ter no âmbito da vigilância comercial e estatal. Apesar das garantias de sigilo, estas *apps* produzem um conjunto de dados diferenciados e complementares aos já disponíveis, ao mesmo tempo que oferecem possibilidades de sofisticação dos algoritmos. Isto não se verifica necessariamente de forma direta, porque nem todos os dados estão imediatamente disponíveis para serem transformados em valor. Vários dos dados recolhidos podem não ter leitura útil até um uso específico ser descoberto no contexto de *data sets* muito mais vastos (Andrejevic 2019). Acresce que as aplicações de rastreio de contactos também fornecem um incentivo à vigilância horizontal constante, o que reforça a sua aceitabilidade no contexto da vida quotidiana.

A título ilustrativo vejamos como tudo isto se conjuga na China, uma autocracia liberal. Este país articula de forma muito eficiente um elevado aparato de monitorização tecnológica com estratégias de vigilância tradicionais com vista ao controlo social, onde encontramos uma ressonância forte com a sociedade disciplinar teorizada por Michel Foucault, na obra *Vigiar e Punir (*1975).

Um sistema de créditos sociais está a ser implementado no país há cerca de uma década. Este modelo baseia-se num regime de punições e recompensas através do qual a população é disciplinada em conformidade com os parâmetros de bom comportamento definidos pelo estado chinês. O regime estrutura-se num sistema de pontuação aplicado por um algoritmo e elaborado a partir do cruzamento de informaçōes de várias bases de dados, nomeadamente: bancárias, judiciais e policiais, bem como do comportamento dos indivíduos nos *media* sociais (Kshetri, 2020; Ramon, 2017).

Este sistema de pontos estratifica a população por patamares o que, por sua vez, define as suas possibilidades de ação. Ou seja, é necessário ter um número mínimo de pontos para ter acesso a determinados serviços (viagens de avião ou comboio) ou empregos, enquanto uma pontuação abaixo de certo valor inviabiliza encontrar qualquer tipo de emprego ou alugar uma casa, por exemplo. No quotidiano das grandes metrópoles chinesas, o *smartphone* desempenha um papel central neste modelo, porque é através do código QR que se consegue circular e aceder a determinados bens e serviços tendo em conta o escalão em que cada indivíduo se encontra.

Este modelo de organização social ajuda a explicar porque é que a China não desenvolveu aplicaçōes autónomas para o COVID-19. Em vez disso, um recurso de rastreamento foi adicionado automaticamente a aplicações de mensagens instantâneas e pagamentos, como o AliPay e o WeChat. Para além da enorme popularidade que têm no país, estas *apps* são usadas por centenas de milhões de pessoas e estão integradas nas estruturas do estado, nomeadamente no sistema de créditos sociais. Com a atualização das aplicações foram colocadas um conjunto de questões aos usuários, o que permitiu às autoridades ter acesso imediato ao histórico médico e de circulação da população. A partir destes dados foram elaborados perfis de risco com níveis distintos de restrições: verde (baixo risco e livre para se movimentar),

laranja (risco médio e quarentena por sete dias em algumas regiões) ou encarnado (alto risco e quarentena por 14 dias em algumas regiões).

Após o confinamento passou a ser necessário ter um estatuto verde para se poder ter acesso a edifícios ou áreas públicas (e.g., transportes), espaços comerciais e locais de trabalho. Inclusive, em algumas cidades chinesas, o código de saúde QR passou a determinar quem pode sair do bairro de habitação. Não sendo necessário o consentimento dos indivíduos para a partilha dos seus dados, a identidade e a localização dos usuários infectados passou a ser do conhecimento das autoridades de saúde pública e a ser divulgada a outras pessoas. Deste modo, o estado chinês aprimorou tecnologicamente as suas capacidades de monitorizar e controlar os movimentos da população, bem como enriquecer o complexo modelo de estratificação social com os dados adicionais recolhidos através do rastreio ao COVID-19.

Este modelo de organização social traduz bem as possibilidades que advêm quando a crescente indissociabilidade entre a vida humana e a tecnologia digital se cruza com um modelo político autocrático. Todavia, ainda que com uma escala tecnológica e limites legais muito distintos, o uso diário das tecnologias em rede nas sociedades democráticas tem promovido um clima sociocultural de monitoramento digital constante que, por sua vez, está na base da implementação da cultura da vigilância, tal como abordamos não próxima secção deste capítulo.

4. As *apps* de rastreio no contexto da cultura da vigilância

Na modernidade digital, a vigilância tornou-se uma componente estruturante de um novo modo de vida na sua globalidade (Andrejevic 2019). Isto significa que as sociedades com um elevado desenvolvimento tecnológico vivem imersas numa "cultura da vigilância" (Lyon 2018). Esta caracteriza-se pela participação e envolvimento ativos dos próprios sujeitos monitorizados nos processos de vigilância, o que a demarca substancialmente dos "estado de vigilância" e "sociedade da vigilância" de eras anteriores. Ou seja, nas sociedades marcadas pela abundância de *media* móveis e conectados – e da confluência destas propriedades, pela preponderância de *media* sociais – assistiu-se a um conjunto de mudanças que contribuíram para a transformação do significado social da vigilância.

No estado de vigilância, também designado por período orwelliano do pós-guerra, a monitorização era dominada por organismos estatais (agências de inteligência, de segurança e a polícia) (Boersma *et. al.* 2014) e tinha como objetivo assegurar o cumprimento de um determinado modelo de organização social, o que incluía a monitorização de indivíduos, atividades ou práticas específicas durante um período de tempo. Fruto ainda de uma herança histórica, a vigilância tinha uma carga negativa: era temida e era, igualmente, uma fonte de ansiedade social.

Por sua vez, a partir da década de 1970 do século XX, os desenvolvimentos tecnológicos e a proliferação de computadores expandiram massivamente as práticas de monitoramento para o sector comercial. As empresas começaram a usar dispositivos de vigilância electrónica para zelar pelo negócio (segurança e ambiente), mas também para conhecer melhor os consumidores. Com a ajuda dos computadores, potenciada pela posterior ligação em rede, uma quantidade enorme de dados começou a ser recolhida, armazenada, classificada e usada para a produção de lucro. A "sociedade da vigilância" (Marx 1985) emergiu, assim, da crescente porosidade da vigilância e da sua integração em muitos aspectos da vida quotidiana. Na maior parte dos casos, a monitorização passou a ser uma consequência não intencional de outros processos e uma prática efetuada a partir de atividades ligadas a rotinas de consumo.

Ainda que caracterizem contextos distintos, os dois conceitos – "estado de vigilância" e "sociedade de vigilância" – colocam a ênfase na vigilância como uma prática externa às atividades vigiadas: acentuam o ponto de vista do agente que vigia e prestam pouca atenção à experiência e ao envolvimento dos cidadãos com a própria vigilância. Por esta razão, ambos os conceitos tornaram-de insuficientes para explicar a relação entre a vigilância social e a vida quotidiana nas sociedades contemporâneas. Todavia, isto não significa que não continuem a captar aspetos significativos da monitorização realizada atualmente, nomeadamente através das atividades desenvolvidas por serviços de informação em estreita articulação com empresas de telecomunicações e internet. Isto explica, por exemplo, o contexto mais amplo dentro do qual podemos entender as descobertas sobre a vigilância em massa realizada pela *National Security Agency*. As revelações de Edward Snowden sobre os procedimentos da agência norte-americana NSA, em 2013, vieram demonstrar as relações estreitas entre empresas e o estado com vista à partilha de dados sobre os cidadãos (Greenwald 2014; van Dijck 2014; Snowden 2019).

As relações estreitas entre empresas tecnológicas e estados estão igualmente espelhadas no desenvolvimento das aplicações de rastreio de contactos. Neste sentido, os conceitos referidos devem ser convocado para compreender as dinâmicas da vigilância contemporânea, mas apenas em parte, porque o que é experienciado no século XXI depende profundamente da participação dos que estão a ser vigiados: na modernidade digital, vigiar, e não apenas ser vigiado, faz parte das rotinas do quotidiano. Dito de outro modo, práticas de vigilância fazem parte da cultura no sentido em que Raymond Williams (1958) a definiu como a *whole way of life,* porque na cultura da vigilância "watching has become a way of life" (Lyon 2018 p. 4).

As tecnologias interativas e estruturadas em processos de inteligência artificial alteraram a vigilância que se tornou multifacetada, complexa e mutante. Passou de fixa a fluida, de assente em *hardware* para *software* e de estática a móvel. A transição para uma vigilância líquida está interligada com movimentos mais amplos na modernidade (Bauman & Lyon 2013): se todas as formas sociais parecem estar sujeitas a processos de erosão, a vigilância

não é exceção. A liquidificação não é, assim, causada pelas tecnologias, mas é intensificada por elas. Ou seja, a vigilância foi integrada no tecido social como consequência da crescente indissociabilidade entre a vida humana e as tecnologias digitais e móveis, de onde se destacam os *media* sociais.

Enquanto plataformas de partilha, os *media* sociais instigam os utilizadores a disponibilizarem informações sobre as suas atividades, preferências, crenças, emoções e pensamentos através de vídeos, fotografias, *posts*, partilhas e comentários. Esta exposição é uma prática marcada pela reciprocidade – isto é, quando as pessoas divulgam informações sobre si esperam receber algo em troca –, mas pode também ser enquadrada pela noção de vigilância.

O uso diário dos *media* sociais promoveu um clima sociocultural onde muitos indivíduos se acostumaram a monitorar, quantificar e comentar a vida dos outros. André Jansson (2015) designa estas práticas por "interveillance": práticas de monitoramento não hierárquicas, não sistemáticas e não refletidas que se tornaram parte da vida quotidiana. Esta exposição mútua, mesmo que flutuante, revela que o *eu digital* é indissociável da "vigilância participativa" (Albrechtslund 2008 p. 2-3): práticas de exposição e partilha ativamente procuradas pelos indivíduos e vividas de forma positiva. Ou seja, na contabilidade da vida social regida pela lógica dos *media* sociais, ser vigiado é ser visto, reconhecido e valorizado. Deste modo, a vigilância deixou de ser sinónimo de controlo ou de algo coercitivo e temível[9], bem como algo externo e imposto aos sujeitos, e expandiu as suas fronteiras e o seu significado para incluir aspectos sociais e lúdicos que os sujeitos promovem e com os quais se envolvem voluntariamente.

Neste ambiente desenvolveram-se culturas de vigilância menos ansiosas e mais empoderadoras, que refletem mudanças culturais em termos de imaginários e práticas sociais. Charles Taylor (2003) descreve os imaginários sociais como expectativas e compromissos normativos que se traduzem em entendimentos partilhados na vida quotidiana e nas relações sociais. Os imaginários enformam e corporizam-se em práticas, ou seja, fornecem a capacidade de agir na medida em que as práticas ajudam a transportar imaginários e contribuem para a sua reprodução.

No que diz respeito à vigilância, os imaginários contribuem para a aceitação de que a vida moderna é vivida sob vigilância e de que isso afeta as relações sociais de várias maneiras. Neste âmbito, as aplicações de rastreio de contactos podem ser perspectivadas à luz do mito da precisão tecnológica que traduz, acima de tudo, uma valoração cultural (Slack & Wise 2005 p. 4-5). Este entendimento medrou com o desenvolvimento tecnológico no século XIX e colocou expectativas em soluções tecnológicas para problemas sociais, tal como

9 A definição tradicional de vigilância descreve um sistema hierárquico de poder. Esta relação vertical coloca o poder nas mãos do observador, enquanto a pessoa observada é reduzida a um sujeito passivo e impotente sob o controle do «olhar» de quem vigia. Este entendimento é comummente representado nas metáforas do *Big Brother* e do panótico. Estes modelos, em grande medida, mantêm-se os referentes conceptuais para discutir teoricamente a vigilância.

indica o inquérito realizado pelo *Euroconsumers*, e já referido na segunda secção deste texto.

Cada vez mais, a vigilância está integrada no tecido social como uma prática domesticada e indissociável de outras: navegar *online*, andar na rua, apanhar um avião, ir ao supermercado. A normalização da vigilância está, ainda, ligada a benefícios e vantagens que os indivíduos retiram de atividades associadas, mesmo que esses processos gerem sentimentos ambíguos. Estamos perante experiências complexas que produzem complacência e conformidade, mas também confronto e contrariedade. Por vezes alternadamente, outras vezes em simultâneo.

A cultura da vigilância descreve fenómenos multifacetados, porque estes estão ancorados em contextos específicos que determinam o modo como a vigilância é experienciada e o significado que lhe é atribuída. Por exemplo, numa ida ao supermercado, mesmo que os clientes saibam que estas empresas rastreiam as suas atividades e recolhem dados sobre si através dos cartões de fidelidade, os descontos e as vantagens que usufruem nas compras podem minimizar o desconforto. Por outro lado, pode-se não gostar e recear as câmaras biométricas que fazem parte dos sistemas de segurança nos aeroportos, mas se for mais conveniente viajar de avião qual é a alternativa?

A naturalização da cultura da vigilância na modernidade digital está ligada à promessa de conveniência e eficiência de um conjunto vasto de atividades familiares e de pequena escala na vida quotidiana, ao mesmo tempo que está associada a práticas de diversão e sentimentos de medo (Lyon 2018 p. 39). Se a familiaridade normaliza e domestica a vigilância, registando-se uma conformidade pela comodidade, a componente lúdica associada às práticas de vigilância nos *media* sociais é produtora de conformidade pela diversão.

No extremo oposto do espectro emocional, encontramos o medo que potencia a conformidade em nome da segurança. O século passado foi abundante em momentos históricos de pânico generalizado e longas décadas em que reinou uma geopolítica do medo: duas guerras mundiais, a Guerra Fria e os conflitos no Médio Oriente. Posteriormente, o medo acentuou-se com os ataques terroristas ocorridos em solo americano, em 2001, e depois em várias cidades europeias. O "11 de setembro" deu lugar à chamada "guerra ao terror" e a um investimento crescente em tecnologias de vigilância. Isto significa que ao longo do tempo, soluções tecnológicas para minorar riscos e garantir segurança têm sido implementadas crescentemente com maior rapidez, e a tornarem-se permanentes para outros objetivos, mesmo quando anunciadas como medidas temporárias e circunscritas. Mais recentemente, sentimentos de medo e incerteza foram renovados com a pandemia do COVID-19. Neste âmbito, apesar das controvérsias que provocaram inicialmente, as aplicações de rastreio de contactos foram entendidas como mais uma modalidade a integrar um reportório de práticas banais de vigilância rotineiras, que David Lyon designa por *soft surveillance* (2018 p. 122). A questão que aqui se pode colocar é de que modo práticas banalizadas de monitorização do tipo *do-it-yourself*, ao mesmo tempo que geram sentimentos subjetivos de empoderamento podem enfraquecer direitos democráticos de privacidade, segurança e liberdade.

Reflexões finais

No momento da finalização da escrita deste capítulo, no início do segundo semestre do ano de 2020, a pandemia do COVID-19 continua a afetar a vida de biliões de pessoas nos lugares mais variados do mundo. Se muitos indivíduos já instalaram e desinstalaram as aplicações de rastreio de contactos, outros tantos iram fazê-lo enquanto esta pandemia não for debelada.

Neste capítulo debatemos as aplicações de rastreio de contactos como um fenómeno sócio-tecnológico no contexto da terceira vaga de autocratização do mundo e da cultura da vigilância. Viver em sociedades marcadas pela abundância de *media* digitais e móveis implica viver imerso numa cultura de conectividade, cada vez mais indissociável de processos rotineiros de monitorização estatal, comercial e horizontal constantes.

As mudanças tecnológicas e políticas que as sociedades contemporâneas atravessam justificam a necessidade de reconsiderar o modo como pensamos e entendemos as implicações do monitoramento personalizado em larga escala, que inclui as aplicações de rastreio. Se mudanças quantitativas são indissociáveis de transformações qualitativas, não estamos apenas perante uma sociedade em que mais dados circulam em vários sistemas estatais e comerciais, e em que mais pessoas interagem, ainda que com sentimentos contraditórios, com sistemas de vigilância.

As tecnologias são moldadas e integradas na vida em função de um conjunto de necessidades individuais, sociais e políticas. Neste âmbito, importa ter em conta que o processo de naturalização social do monitoramento personalizado em larga escala ocorre num tempo em que se verifica uma crescente autocratização das democracias. Este contexto compromete o debate crítico sobre a amplitude das ameaças que a vida digital pode colocar à vida humana. Importa, igualmente, ter em conta que, na modernidade digital, a vigilância – nomeadamente, as aplicações de rastreio de contactos – tem um significado estruturalmente contraditório: significa cuidar e controlar, e empodera ao mesmo tempo que desprotege os indivíduos. Todavia, na modernidade digital este já não é um problema para se resolver, mas um paradoxo para se gerir.

Referências

Ahmed, N., Michelin, R., Xue, W., Ruj, S., Malaney, R., Kanhere, S., Seneviratne, A., Hu, W., Janicke, H. & Jha, S. (2020). Survey of COVID-19 Contact Tracing Apps. *arXiv*, 2006(10), 1-31. DOI: 10.1109/access.2020.3010226

Albrechtslund, A. (2008). Online social networking as participatory surveillance. First Monday, 13(3), 1-10. DOI: 10.5210/fm.v13i3.2142

Andrejevic, M. (2019). Automating surveillance. *Surveillance & Society*, 17(2), 7-13. DOI: 10.24908/ss.v17i1/2.12930

Bauman, Z. & Lyon, D. (2013). *Liquid Surveillance: A conversation*. Cambridge: Polity Press.

Bermeo, N. (2016). On Democratic Backsliding. *Journal of Democracy*, 27(1), 5-19. DOI: 10.1353/jod.2016.0012

Boersma, K., Van Brakel, R., Fonio, C. & Wagenaar, P. (Eds.) (2014). *Histories of State Surveillance in Europe and Beyond*. New York: Routledge.

Bolin, G. & Schwarz, J. (2015). Heuristics Of The Algorithm: Big Data, User Interpretation and Institutional Translation. *Big Data & Society*, 2(2),1-12. DOI: 10.1177/2053951715608406

Couldry, N. & Mejias, U. (2019). *The Costs of Connection. How data is colonizing human life and appropriating it for capitalism*. Standford: Standford University Press.

Couldry, N. & Hepp, A. (2017). *The Mediated Construction of Reality*. London: Polity Press.

Dahl, R. A. (1998). *On Democracy*. New Haven, CT: Yale University Press.

Freedom House (2020). Freedom in the world 2020. https://freedomhouse.org/sites/default/files/2020-02/FIW_2020_REPORT_BOOKLET_Final.pdf, acedido a 13.08.2020

Fuchs, C. (2012). Google Capitalism. *TripleC*,10(1), 42-48. DOI: 10.31269/*triplec*.v10i1.304

Greenwald, G. (2014). No place to hide. Edward Snowden, the NSA and the US surveillance state. New York: Metropolitan Books.

Jansson, A. (2018). *Mediatization and Mobile Lives*. London: Routledge.

Jansson, A. (2014). Interveillance: A New Culture of Recognition and Mediatization. *Media and Communication*, 3(3), 81-90. DOI: 10.17645/mac.v3i3.305

Kshetri, N. (2020). China's Social Credit System: Data, Algorithms and Implications, *IT Professional*, 14-18. DOI: 10.1109/MITP.2019.2935662.

Lyon, D. (2018). *The Culture of Surveillance*. Cambridge: Polity Press.

Lührmann, A. & Lindberg, S. (2019). A third wave of autocratization is here: what is new about it? *Democratization*, 26(7), 1095-1113. DOI: 10.1080/13510347.2019.1582029

Marx, G. (2015). *Windows into the Soul: Surveillance and Society in an Age of High*

Technology. Chicago: University of Chicago Press.

Sartori, G., (1970). Concept Misformation in Comparative Politics. *The American Political Science Review*, 64(4), 1033-1053.

Schedler, A. (2013). *The Politics of Uncertainty: Sustaining and Subverting Electoral Authoritarianism*. Oxford: Oxford University Press.

Van Dijck, J. (2014). Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology. *Surveillance & Society*, 12(2), 197-208. DOI: 10.24908/ss.v12i2.4776

Salim, D. (2017). Becoming-Infrastructure: Datafication, Deactivation, and the Social Credit System *Journal of Critical Library and Information Studies* 1,(1): 1-23. DOI: 10.24242/jclis.v1i1.19

Slack, J.D. & Wise, J. (2005). *Culture and Technology: A primer*. New York: Peter Lang.

Snowden, E. (2019). *Permanent Record*. New York: Metropolitan Books.

Stern, P. (2011). *The company-state: Corporate Sovereignty and the early modern foundations of the British Empire in India*. Oxford, UK: Oxford University Press.

Taylor, C. (2003). *Modern social imaginaries*. Durham: Duke University Press.

V-Dem (2020). Democracy Report 2020, https://www.v--dem.net/media/filer_public/f0/5d/f05d46d8-626f--4b20-8e4e53d4b134bfcb/democracy_report_2020, acedido a 10.08.2020

Williams, R. (1958). *Culture and Society: 1780-1950*. London: Chatto & Windus.

Zuboff, S. (2015). Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology*, 30, 75-89. DOI: 10.1057/jit.2015.5

Imprensa consultada

"Coronavirus contact-tracing: World split between two types of app", *BBC*: 07.05.2020, https://www.bbc.com/news/technology-52355028, acedido a 16.08.2020

"How Google and Apple outflanked governments in the race to build coronavirus apps", *Politico*: 16.05.2020, https://www.politico.eu/article/google-apple-coronavirus-app-privacy-uk-france-germany/, acedido a 12.08.2020

"Privacy-savvy Germany launches coronavirus contact-tracing app", *Politico*: 16.06.2020, https://www.politico.eu/article/germany-privacy-coronavirus-contact-tracing-app/, acedido a 12.08.2020

"Europe Rolls Out Contact Tracing Apps, With Hope and Trepidation", *The New York Times*: 16.06.2020, https://www.nytimes.com/2020/06/16/world/europe/contact-tracing-apps-europe-coronavirus.html, acedido a 12.08.2020

"Apps de "contact tracing" chegam à UE e Portugal está no radar. Vieram para ficar", Eco: 21.06.2020, https://eco.sapo.pt/especiais/apps-de-contact-tracing-chegam--a-ue-e-portugal-esta-no-radar-vieram-para-ficar/, acedido a 12.08.2020.

"StopCOVID: France's controversial tracing app ready by June, government says", *Euronews*: 05.05.2020, https://www.euronews.com/2020/04/29/coronavirus-french-mps-approve-covid-19-tracing-app-despite-privacy-concerns, acedido a 12.08.2020.

"Norway suspends contact-tracing app over privacy concerns", *Politico*: 15.06.2020, https://www.politico.eu/article/norway-suspends-contact-tracing-app-over--privacy-concerns/ acedido a 10.08.2020.

"Poland's coronavirus app offers playbook for other governments", *Politico*: 02.04.2020, https://www.politico.eu/article/poland-coronavirus-app-offers-playbook--for-other-governments/, acedido 10-08-2020.

"Apps para rastrear covid-19, um empreendimento arriscado", Deutsche Welle: 28-07-2020. https://www.dw.com/pt-br/apps-para-rastrear-covid-19-um-empreendimento-arriscado/a-54357321, acesso a 11-08-2020

"Global contact tracing app downloads lag behind effective levels", *Quartz*: 15.07.2020,
https://qz.com/1880457/global-contact-tracing-app-downloads-lag-behind-effective-levels/ acedido a 10.08.2020.

"Cheap, popular and it works: Ireland's contact-tracing app success", *The Guardian*: 20.07.2020
https://www.theguardian.com/world/2020/jul/20/cheap-popular-and-it-works-irelands-contact-tracing-app-success?CMP=Share_iOSApp_Other, acedido a 12.08.2020.