The emergence of technological tools to control Covid-19: a reinvention of imperfect panopticons

A emergência de ferramentas tecnológicas para controlo da Covid-19: uma reinvenção de panóticos imperfeitos

Antónia do Carmo Barriga*

* Universidade da Beira Interior/CIES-Iscte, Portugal (acab@ubi.pt)

Abstract

In the following text, we intend to discuss the digital epidemiological surveillance caused by the pandemic by Covid-19. The concern with surveillance and privacy is not new, but in the current pandemic situation, the role of the State in electronic surveillance, added to that which has long been played by the Big Tech that corner the market are known, it reconsiders these concerns. To what extent can we, or not, consider that the measures adopted to control contagion by the new coronavirus and in response to the pandemic are part of what were the "disciplinary societies", as Foucault conceptualized them? To contribute to the answer to this question, the empirical approach that we propose to present aims to characterize the current panorama of the governmental use of technological tools to control the pandemic, as well as the limitations that many applications have come to reveal. To this end, information was collected and systematized divulged in various media from different countries.

Keywords: applications (app), surveillance, privacy, automatic systems

Resumo

Neste texto pretende-se problematizar a vigilância epidemiológica digital motivada pela pandemia de COVID-19. A preocupação com a vigilância e a privacidade não é de agora, mas no atual contexto pandémico o papel do Estado na vigilância eletrónica, somado àquele que há muito é desempenhado pelas Big Tech que dominam o mercado, faz reequacionar essas preocupações. Em que medida poderemos, ou não, considerar que as medidas adotadas para controlo do contágio pelo novo coronavírus se inscrevem naquilo que foram as "sociedades disciplinares", tal como Foucault as conceptualizou? Pretendendo contribuir para a resposta a esta questão, a abordagem de cariz empírico que apresentamos, efetuada a partir da recolha de informação veiculada em vários media de diferentes países e da sua sistematização, visa caraterizar o panorama da utilização governamental das ferramentas tecnológicas para controlo da pandemia de COVID-19, bem como as limitações que muitas aplicações vieram a revelar.

Palavras-chave: aplicações(*app*), vigilância, privacidade, sistemas automáticos

Introdução

Durante a pandemia causada pelo novo coronavírus (SARS COV 2), e na tentativa de a mitigar, adotaram-se algumas medidas de vigilância epidemiológica. É certo que essas medidas, e o uso das tecnologias de controle e vigilância que lhe são inerentes, são muito díspares no que respeita à utilização que lhe é dada pelos diversos governos, bem como ao grau de invasão da privacidade e aos atentados aos direitos e liberdades cívicas que promovem. De facto, encontramos uma enorme diversidade de práticas. Poderemos estar, por exemplo, perante a utilização de uma aplicação – doravante designada de app - que é obrigatória e que recolha todo o tipo de dados (biométricos, fiscais) que serão centralizados pelas autoridades; ou, diferentemente, perante uma app que exija consentimento, em que há controlo pelo próprio dos dados

pessoais (anónimos) e em que exista a garantia (ou promessa) que serão destruídos quando deixarem de ser necessários. Para ilustrar esta diversidade apresentaremos o panorama da utilização governamental das ferramentas tecnológicas para controlo da pandemia na atual geografia política. Mas também ilustraremos as resistências e limitações reveladas por algumas apps em alguns países. Para tal, recolheu-se e sistematizou-se a informação sobre a as ferramentas e as medidas adotadas para controlo da pandemia pela COVID-19, veiculada em vários media de diferentes países.

É indubitável que o Sars-Cov-2 representa, ao nível global, uma séria ameaça à saúde pública, mas o combate ao seu contágio trouxe outros riscos e impõe alguns questionamentos, salvaguardando sempre as colossais diferenças que existem entre as medidas que os diferentes países estão a adotar nesta situação concreta A tecnologia digital - e também a que é usada para controlar a propagação deste vírus - quanto mais sofisticada mais opaca é para o cidadão comum; quanto mais intrusiva é, mais testa a democraticidade dos regimes políticos; quanto mais vigilante, mais invisível se torna. Hoje, alguns recursos tecnológicos tornaram-se mais invisíveis que o panótico de Bentham. A preocupação com a vigilância e a privacidade não é de agora, mas no atual contexto pandémico o papel do Estado na vigilância eletrónica, somado àquele que há muito é desempenhado pelos GAFAM (acrónimo para Google, Apple, Facebook, Amazon e Microsoft), como são conhecidas as *Big Tech* que dominam o mercado, faz reequacionar essas preocupações. São essas preocupações e as perspetivas teóricas que têm inspirado que pretendemos destacar neste texto, como veremos à frente. É neste sentido que questionamos em que medida poderemos, ou não, considerar que as medidas adotadas para controlo do contágio pelo novo coronavírus e em resposta à pandemia pela COVID-19 se inscrevem naquilo que foram as "sociedades disciplinares", tal como Foucault as conceptualizou. Ou trata-se de um modelo analítico datado, incapaz de apreender a complexidade do mundo atual?
Em boa medida este texto não deixa de ser mais um dos que continua a explorar a metáfora do panótico (elaborada em Surveiller et Punir, em 1975), considerada um modelo aprimorado da visão Orwelliana. Razão tem, pois, Lyon (2007) ao afirmar que o panótico insiste em não desaparecer do debate sobre a vigilância. Contrariamente à vontade de Haggerty (2006), as paredes do panótico continuam por derrubar, também neste texto. Todavia, sem deixarmos de reconhecer (e incorporar) as críticas a que a metáfora tem sido sujeita, como é o caso das que são feitas por Haggerty (2006), Bauman e Lyon (2013) e Lyon (2014, 2018).

Das sociedades disciplinares ao "pós-panoticismo"

No mundo ocidental o debate público em torno da vigilância, incrementado em muito pelo 11 de setembro de 2001, centrava-se na forma como cada cidadão estava disposto a sacrificar a sua privacidade em nome da segurança. Com a pandemia e os seus riscos, o debate passou a centrar-se mais no difícil equilíbrio entre os ganhos para a saúde (individual e pública) e a as perdas de privacidade. Estamos, aliás, perante a mesma ambivalência notada por Lyon (2001) e Finn et al (2018), que carateriza a vigilância: tanto facilita como constrange a nossa ação; tanto é orientada para cuidar como para o controlar (os mesmos sistemas de vigilância que podem ser utilizados para servir aspetos positivos como a proteção, a otimização da administração e o cumprimento das regras também podem permitir a manipulação, a discriminação e o controlo social) (Finn et al, 2018).

A prática de vigiar e restringir aqueles que se acredita serem contagiosos, em rigor, é quase tão antiga quanto a própria civilização. Talvez seja inapropriado considerar que as medidas adotadas para controlo do

contágio pelo novo coronavírus e em resposta à pandemia pela COVID-19 se inscrevam naquilo que foram as "sociedades disciplinares", tal como Foucault as conceptualizou. Mas é inevitável encontrar semelhanças com as "sociedades disciplinares", pelo que convocamos este conceito, salvaguardando as colossais diferenças que existem entre os países e as políticas que estão a adotar nesta situação concreta.

De acordo com Deleuze (1992) as "sociedades disciplinares" podem situar-se entre o século XVIII e a Segunda Grande Guerra, altura em que dariam lugar à "sociedade de controle", sua herdeira. Na senda de Foucault, Deleuze refere o confinamento como a noção norteadora e a técnica fundamental da sociedade disciplinar, enquanto estratégia de poder. As "sociedades disciplinares" tinham como principal premissa fazer com que o indivíduo modelasse o seu comportamento, sendo essencialmente arquiteturais: a casa da família, a escola, o quartel, a fábrica, o hospital, a prisão… (Deleuze, 1992). Também noutras abordagens, como as Ogura (2006) e Fuchs (2011), por exemplo, a recolha de dados sobre indivíduos ou grupos pode ser utilizada para controlar e disciplinar comportamentos.

No cerne dos dispositivos disciplinares destas sociedades está uma polarização entre a opacidade do poder e a transparência dos indivíduos, encontrando Foucault (1998), no panótico (idealizada por Jeremy Bentham) o seu modelo dominante. Trata-se de uma metáfora marcante nas conceções sobre a vigilância, para a qual Foucault, situando a vigilância num contexto das teorias de poder, contribuiu decisivamente (Haggerty, 2006; Caluya, 2010).

Alterações societais várias têm também conduzindo à critica (teórica) do panótico. Vejamos a de Haggerty (2006): enquanto a vigilância panótica se concentrava em funções relacionadas com a educação, tratamento médico e punição; hoje a vigilância inclui o consumo, o entretenimento, a promoção de saúde, a governança, o uso militar, entre outros; a visão distópica de Foucault revela-se restrita, pois a vigilância pode ser apreciável ou libertadora; as dinâmicas e hierarquias de poder e visibilidade alteram-se e reconfiguraram-se, a vigilância não é só direcionada aos menos poderosos, passou a estar presente em todos os segmentos da hierarquia social (Haggerty, 2006).Outros autores tem também criticado Foucault, argumentando que o panótico se tornou incapaz de captar a realidade. Por exemplo, Bauman e Lyon (2013), assinalam que numa lógica inversa à do panóptico as novas tecnologias facilitaram o escrutínio dos mais poderosos pelos media: "muitos" podem observar "poucos". Surgem também novas metáforas, como a "Surveillant Assemblage" de Haggerty e Ericsson (2000, 2006). Inspirando-se em Deleuze e Guattari, estes autores concentram-se na utilização de infindáveis tecnologias de vigilância, que baseadas em sistemas combinados analisam dados pessoais, tornando-os mais rentáveis para fins comerciais ou outros. Neste sentido, a Surveillant Assemblage considera o envolvimento dos sujeitos da vigilância como consequência dos seus desejos (o consumo, como exemplo maior), a autoexpressão e o entretenimento voyeurístico (Haggerty e Ericson, 2000, 2006; Jansson, 2012).

As abordagens "pós-panoticismo" sublinham, pois, a mudança da sociedade da disciplina de Foucault para uma sociedade do controlo, onde a produção da vida social é governada por relações globais nas quais as práticas da vigilância se integram na mobilidade geográfica, na produção económica e no consumo (Zureik, 2007). A atual "sociedade em rede" é uma "sociedade de controlo", existindo outras maneiras de a abordar conceptualmente, são disso exemplo Lessig (1999), Rheingold (2002), Shapiro (1999). Uma delas, a de Deleuze, consiste em considerá-la herdeira e substituta da sociedade disciplinar foucaultiana, como já se referiu. Neste sentido, Deleuze terá sido premonitório ao alertar para as consequências do uso das novas tecnologias no controlo social e ao entendê-las como a mais nova expressão do exercício do poder na

sociedade moderna. O símbolo do controlo deixa de ser o panóptico, sendo substituído pela Internet. De microfísico, o poder passa a envolver todo o corpo social, recorrendo a tecnologia que funciona a partir da sedução: a sedução do controlo que se opõe à coerção das "sociedades disciplinares" (Deleuze, 1992). É justamente a abolição do confinamento físico que opera a transição para "sociedade de controlo": a lógica do confinamento transpõe-se para toda a sociedade sem, contudo, necessidade de existência de muros que separem o lado de dentro das instituições do seu exterior. Portanto, enquanto a "sociedade disciplinar" se caracteriza pelos poderes transversais operados pelas instituições modernas e pelas estratégias de disciplina e confinamento, a "sociedade de controle" define-se pela invisibilidade e pela mobilidade, características do lugar e postura do indivíduo em novas redes.

Diríamos que os artefactos tecnológicos trouxeram a "vigilância" para dentro de casa, mas que os atuais dispositivos de comunicação móveis comportam a possibilidade (ou o risco) de a levar para todo o lado (Barriga, 2015). Ora, são esses mesmos dispositivos – em particular o smartphone – que no momento atual estão a ser utilizados em algumas partes do globo para controlo do contágio pelo novo coronavírus. Através dos serviços de geolocalização pode saber-se se estamos do lado de dentro (casa) ou, indisciplinados, do lado de fora (num qualquer lugar, que passou a ser fácil de precisar). Assim, se é certo que na atualidade não assistimos ao regresso de uma "sociedade disciplinar" *tout court* – seria um anacronismo - é inegável que nos deparamos com sofisticadas ferramentas tecnológicas de vigilância. E que estas, tendo emergindo na "sociedade do controlo" e sendo a sua utilização muito distinta geograficamente, obedecem a lógicas claramente disciplinares e ameaçadoras do direito à privacidade, conquistado na modernidade. Esta pandemia confrontou-nos também com o aparente paradoxo do retorno à casa (em confinamento) para defesa da comunidade, fazendo-nos reequacionar a fronteira público/privado e o papel que a tecnologia tem no seu traçado.

A ação (desconhecida) dos sistemas automáticos que nos vigiam

Warren e Brandeis, em 1890, já entendiam a privacidade como um direito a proteger pelo Estado, face ao aparecimento de câmaras e ao desenvolvimento aparentemente ilimitado dos meios de comunicação social. Na atualidade, as ameaças à privacidade são inúmeras. Algumas delas são protagonizadas pelos Estados, e quase todas perpetradas pelos meios digitais, alicerçadas nas potencialidades que a tecnologia e a Inteligência artificial permitem. No novo milénio, é indubitável que o quotidiano do cidadão comum se encontra sob um escrutínio que constituí uma situação de invasão de privacidade (Lyon, 2018) [1].

As modalidades e os artefactos de vigilância, indissociáveis dos contextos (sociais, políticos, tecnológicos…) que as promovem e das práticas que as substanciam (ao nível do consumo, do lazer, por exemplo) têm-se alterado substancialmente. Nos anos 90, a vigilância sofistica-se e entra no quotidiano: atividades como levantar dinheiro, usar o telefone ou um cartão de crédito são registadas e analisadas por várias entidades. Neste aumento e sofisticação de artefactos e de modalidades, já Lyon (1994) encontrava um aumento intensivo e extensivo da vigilância. A utilização generalizada da internet (no mundo ocidental, entenda-se)

[1] Note-se a proposta de abordagem teórica de Steeves (2009) que, ao teorizar sobre a negociação social da privacidade e conceptualizar diversos níveis de privacidade, vê na vigilância a ameaça da quebra de fronteiras entre os diversos papéis sociais que um individuo pode desempenhar.

possibilitou novas formas de monitorização, decorrentes também de novas práticas de consumo que a internet propiciou (como as compras online e os riscos que daí passaram a advir no que respeita à proteção dos dados. Na sequência dos ataques ocorridos a 11 de setembro de 2001 as práticas de vigilância eletrónica aprofundaram-se, iniciando-se a as tentativas de criação do mito da vigilância (Marx 2015) e conduzindo às "sociedades da vigilância", ainda que estas já estivessem em curso, como nota Lyon (2003). A extensão da vigilância é uma das caraterísticas que se viria a revelar no novo milénio: se inicialmente a vigilância visava suspeitos, agora incide sobre todos os cidadãos. De um contexto onde parte do quotidiano era monitorizada, passámos outro onde ele é (quase) constantemente monitorizado (Marx, 2016; Lyon, 2018). A estas marcas, soma-se a inexorabilidade: não existe alternativa à exposição à vigilância e, em grande medida, ao fornecimento de dados (Dijck, 2014; Harding, 2014).

Neste quadro, operou-se a mudança da "vigilância tradicional" para a "nova vigilância", definida como o escrutínio de indivíduos, grupos e contextos baseado na utilização de meios técnicos para extrair ou criar informação, tende a ser mais intensiva e extensiva, baseia-se nas potencialidades do Big Data, pelo que é menos visível; envolve frequentemente uma conformidade involuntária; tende a baixar o custo dos processos de vigilância; alcança localizações mais remotas (Marx, 2015). Hoje, tornou-se evidente a relação entre Big Data e vigilância, para tal muito contribuíram e demonstraram as revelações de Snowden sobre a National Security Agency (NSA). Na sua sequência, desvendam-se ligações de empresas multinacionais aos governos (afinal uma agência governamental (NSA) teve dados provenientes de empresas de telecomunicações): multinacionais de software e serviços online como a Apple, Google, Microsoft, Amazon e Facebook recolhiam dados, em grande escala, dos utilizadores e partilhavam-nos com agências governamentais (Lyon, 2018). Na "vigilância de tipo novo", classificam-se indivíduos e agrupam-se em categorias, partindo de dados provenientes de processos e de sistemas digitalizados de vigilância - a que se passou a chamar *social sorting* – recorrendo a códigos e complexos algoritmos.

Neste âmbito, a ação do algoritmo, quer pelo seu obscurantismo quer pelos efeitos que provoca, suscita uma crescente discussão e preocupação. Para o Conselho da Europa[2], o uso abusivo de sistemas com algoritmos está a transformar-se num perigo para a democracia, a inteligência artificial é cada vez mais sofisticada e tem implicações óbvias nas escolhas que fazemos. Um impacto que não se limita a questões comerciais e hábitos de consumo, mas que pode influenciar as opiniões e decisões que tomamos, através de técnicas de direcionamento, o que pode ser usado para manipular comportamentos sociais e políticos. Neste sentido, o uso abusivo de algoritmos pode manipular o comportamento dos eleitores, pelo que defende a urgência de medidas para controlar os sistemas tecnológicos mais avançados.

As redes sociais são um exemplo proeminente da tomada de decisão algorítmica no quotidiano, na medida em que quase todo o conteúdo que se vê nas redes sociais não é escolhido por editores humanos, mas por programas de computador que usam grandes quantidades de dados sobre cada utilizador para fornecer-lhe conteúdo que ele possa achar relevante ou interessante. Muitas das decisões que até então podiam ser tomadas apenas por seres humanos passaram a sê-lo por algoritmos de computador, através de recursos analíticos avançados e do acesso a enormes armazenamentos de dados e à sua posterior análise. Trata-se de um enorme e rentável negócio que se baseia no aperfeiçoamento sistemático dos modelos de gestão e

[2]https://www.tsf.pt/sociedade/ciencia-e-tecnologia/inteligencia-artificial-e-algoritmos-ameacam-a-democracia-10576272.html

classificação algorítmica dos dados. Os algoritmos são instruções matemáticas bem definidas, pelo que a informação digital é classificada através de regras de cálculo.

Esta crescente prevalência dos algoritmos conduziu a diferentes perspetivas acerca do impacto sobre aqueles que são afetados pelas decisões tomadas. Para uns, esses sistemas podem aumentar a precisão e reduzir o viés humano em decisões importantes. Mas em muitos outros autores, em sentido contrário, motiva preocupações. Cathy O'Neil refere-se aos algoritmos como " armas de destruição da matemática ", que simplesmente reforçam os preconceitos e disparidades existentes sob o pretexto de uma suposta neutralidade algorítmica, mas antes promovem discriminação e reforçam desigualdades[3]. Algoritmos de computador e análises de rede podem inferir também os humores, as crenças políticas, a orientação sexual e o estado de saúde, alerta Zeynep Tufekci (2019, 21 de abril). Em suma, como nota José Luís Garcia, os algoritmos produzem sistemas de equivalência, selecionando alguns objetos em detrimento de outros, e impõem uma hierarquização. Ao estruturar decisões, os sistemas de classificação orientados para a definição de situações podem convertê-las em reais (Garcia, 2020, 28 de junho).

Indissociável desta ação opaca e desconhecida para a maioria – quem sabe o que é e como funciona o algoritmo?[4] - está a incomensurável violação da privacidade dos utilizadores das plataformas digitais, por via do roubo dos seus dados. Esta questão já sobejamente conhecida ganhou visibilidade com os escândalos que envolveram a Cambridge Analytica e o Facebook, em 2018[5], mas o seu alcance está muito além. Por exemplo, já quase no final de 2019 os investigadores Bob Diachenko e Vinny Troia descobriram num servidor de internet uma base de dados contendo informações sobre quatro biliões de contas do Facebook, Twitter ou LinkedIn, que dizem respeito a um total de 1,2 bilião de pessoas. Nessa base de dados encontrava-se 622 milhões de endereços de email, nomes, números de telefone ou informações de redes sociais[6].

A sensibilização para a questão dos direitos digitais começou a ganhar acuidade após as revelações de Snowden, até porque se constatou que os dados em causa foram criados, principalmente, por utilizadores comuns da internet. Mas que quadro legal, atualmente, regulamenta a criminalização práticas abusivas, como estas, e protege a privacidade dos cidadãos? As grandes empresas tecnológicas foram crescendo à frente da legislação[7], mas recentemente, a par da crescente desconfiança do público, começaram a sentir o impacto das novas legislações de proteção de dados nos seus modelos de negócios [8]. Num braço de ferro

---

[3] Por exemplo, no mercado de trabalho, "os privilegiados são analisados por pessoas; as massas por máquinas", afirma O'Neil. O algoritmo COMPAS - amplamente usado para prever a reincidência no sistema de justiça criminal dos EUA - apresentou uma taxa de falsos positivos mais alta em negros do que em brancos; os negros eram mais propensos a ser erroneamente preditos a reincidir (Menárguez, 2018, 21 de novembro).

[4] Em 2022 foi assinada a Declaração conjunta europeia sobre os direitos e princípios digitais para a década digital, contemplando-se as Interações com algoritmos e sistemas de inteligência artificial e defendendo que "todas as pessoas devem poder beneficiar das vantagens da inteligência artificial, fazendo escolhas próprias e informadas no ambiente digital, estando simultaneamente protegidas contra os riscos e os danos para a saúde, a segurança e os direitos fundamentais" (Capítulo III: Liberdade de escolha)

[5] Note-se que o Facebook viria a pagar 4,5 mil milhões à Comissão Federal do Comércio dos EUA para que terminasse as investigações abertas nos últimos dois anos por violação da privacidade dos utilizadores desta rede social. Acresce que pagou, na Europa, a multa no valor de meio milhão de euros à agência britânica de proteção de dados. Fonte: jornal Público, 26 de julho de 2019

[6] https://www.lemonde.fr/pixels/article/2019/11/25/les-donnees-personnelles-de-plus-d-un-milliard-d-internautes-decouvertes-en-libre-acces_6020459_4408996.html?utm_term=Autofeed&utm_medium=Social&utm_source=Twitter#Echobox=1574703953

[7] No entanto, o direito à proteção de dados pessoais é explicitamente reconhecido pelo artigo 8.º da Carta dos Direitos Fundamentais da EU, de 2012, bem como pelo Tratado de Lisboa, em vigor desde 2009

[8] A União Europeia impôs mais de 900 sanções desde que o Regulamento Geral de Proteção de Dados (RGPD) foi introduzido em maio de 201, tendo o número de multas aumentado desde 2020. Em 2021, a batalha da UE contra as Big Tech pela proteção dos dados pessoais atingiu 1.300 milhões de euros em multas.

que não é novo, em fevereiro de 2022 a Meta ameaçou acabar com o Facebook e o Instagram na União Europeia, caso não possa armazenar as informações que recolhe acerca dos utilizadores europeus nos seus servidores que estão localizados nos Estados Unidos. A esta questão acresce a que se liga à legislação europeia de mercados e serviços digitais, que potencialmente limita os anúncios direcionados (a publicidade que está no cerne dos lucros do Facebook e do Instagram, mas também de outras empresas tecnológicas. Facebook e Instagram ameaçam sair da Europa devido a leis de proteção de dados[9].

Note-se, pois, a importância da Lei Geral de Proteção de Dados (LGPD), que entrou em vigor em 2020 e do Regulamento Geral sobre a Proteção de Dados (RGPD), aplicável a todos os cidadãos na União Europeia e Espaço Económico Europeu desde 2018. Noutras partes do globo, surgiram regulamentações que visam igualmente o fortalecimento das práticas de segurança e privacidade de dados: por exemplo, a Lei de Proteção de Informações Pessoais (PIPL) entrou em vigor na China em 2021; A Lei Federal de Proteção de Dados, de 2017, da Alemanha (um pais considerado líder na regulamentação sobre privacidade e proteção de dados); e também nos EUA a regulação dos gigantes tecnológicos e a e proteção de dados parecem estar no horizonte da atual Administração[10].

A Vigilância epidemiológica digital: ferramentas tecnológicas para controlo da Covid-19

Pelo exposto no ponto anterior, é fácil concordar que um dos maiores riscos pode estar na utilização combinada de IA e ICTs, aumentando assim o potencial de invasão de privacidade, de vigilância em massa e de condicionamento de opiniões e comportamentos. Através do acesso à vastidão de dados que a maioria dos indivíduos disponibiliza online, as entidades que usam algoritmos são capazes de perceber aspetos sobre a vida de cada um de nós de forma muito mais eficaz do que os próprios indivíduos (Bartlett, 2018).

Ora, no combate à pandemia utilizam-se tecnologias invasivas que incluem reconhecimento facial ou medição da temperatura corporal, mas também *apps* para rastreio de contactos e movimentos, fortemente tributárias da ação (desconhecida) dos sistemas automáticos. É a utilização destas ferramentas, de cuja eficácia agora se duvida, que de seguida se detalha.

As *apps* para controlar a propagação do vírus através da geolocalização dos cidadãos recolocam o velho debate entre segurança e liberdade, o mesmo é dizer, neste contexto, entre saúde e privacidade. Ainda que intrusivas de modo e grau diferentes, observaram-se inúmeros e inquietantes exemplos de vigilância e de violação de direitos, pelo que mais de 100 organizações de direitos humanos, ativistas das liberdades civis e grupos de consumidores de todo o mundo emitiram uma declaração conjunta sobre o Covid-19 e a vigilância digital, pedindo aos governos que usem tecnologias de rastreamento somente se forem executadas estritamente de acordo com os princípios dos direitos humanos (Soguel, 2020, 20 de março).

Existem dois métodos distintos de rastreamento de contactos: a tecnologia de comunicação *Bluetooth* entre aparelhos eletrónicos próximos ou a geolocalização, que permite obter dados sobre deslocação. A União Europeia (UE) não recomendou esta última, dado os problemas de segurança e de invasão de privacidade

[9] https://www.tsf.pt/futuro/facebook-e-instagram-ameacam-sair-da-europa-devido-a-leis-de-protecao-de-dados-14567488.html?utm_source=dlvr.it&utm_medium=twitter

[10] Observa-se noutros países externos à União Europeia o alinhamento com as políticas de privacidade do RGPD. Atualmente 129 países que já se dotaram de legislação em matéria de proteção dos dados.
Fonte: https://www.dn.pt/opiniao/opiniao-dn/convidados/protecao-de-dados-uma-utopia-ou-ja-uma-realidade-10227005.html

que comporta. Na Europa, tal como em muitos outros países democráticos, tentou encontrar-se uma *app* que fosse eficaz no controle epidemiológico, garantindo a privacidade dos utilizadores, pelo que o debate se situou em torno de duas questões: a técnica utilizada no rastreio - por *Bluetooth* ou geolocalização; e o modo de armazenamento dos dados - num modelo centralizado (os dados são concentrados na *cloud* ou no *server* da instituição responsável) ou descentralizado (armazenados no telemóvel). O *Bluetooth* precisa de uma utilização massiva (para ser eficaz precisa de 60% dos utilizadores de telemóvel), porém é menos intrusivo porque analisa os sinais sem recolher dados pessoais. Já a geolocalização precisa que o utilizador aceite o acesso à sua localização.

A Apple e Google uniram-se em torno do desenvolvimento de tecnologia de rastreamento de contágio, baseada na tecnologia *Bluetooth,* e a 20 de maio de 2020 disponibilizaram uma interface de programação de aplicações (API) aos 22 países, dos cinco continentes, que pediram acesso. A abordagem da Apple e da Google é descentralizada, tendo sido apresentada como oferecendo mais privacidade, uma vez que limita a capacidade das autoridades ou de um *hacker* de usar os *logs* do servidor do computador para rastrear indivíduos específicos e identificar as suas interações sociais. Esta abordagem é o modelo que reuniu maior consenso na Europa, apoiado por um movimento de cientistas e tendo tido a adesão da Alemanha.

A fim de conhecer a utilização de ferramentas tecnológicas de controlo pelos diferentes países, recolheu-se toda a informação a que foi possível aceder, publicada no 1º semestre de 2020 nos media nacionais e internacionais e em algumas revistas especializadas de tecnologia[11]. Esta informação é agora resumida e sistematizada nas tabelas que se seguem, numa categorização que obedece: à imposição pelas autoridades do uso dessas ferramentas pelos cidadãos (tabela 1); à natureza massiva da vigilância digital (tabela 2); e à caraterização das apps de rastreio em uso em diversos países (tabela 3).

[11] Neste levantamento aprofunda-se e sistematiza-se e atualiza-se informação anteriormente recolhida. Cf.Barriga, A. C., Martins, A.F., Simões, M.J., Faustino, D. (2020). The COVID-19 pandemic: Yet another catalyst for governamental mass surveillance? Social Sciences & Humanities Open. Volume 2, Issue 1.

As fontes agora utilizadas foram as seguintes:

https://www.publico.pt/2020/04/12/tecnologia/noticia/medo-tecnologia-maos-dadas-controlo-pandemia-1911568
https://tvi24.iol.pt/videos/internacional/o-big-brother-da-vida-real-que-a-china-usou-para-travar-a-pandemia-de-covid-19/5e8ce6800cf2a5883420007f
https://www.publico.pt/2020/04/12/tecnologia/noticia/medo-tecnologia-maos-dadas-controlo-pandemia-1911568
https://visao.sapo.pt/atualidade/politica/2020-04-11-covid-19-coreia-do-sul-vai-usar-pulseira-eletronica-para-quem-violar-quarentena/?fbclid=IwAR1rxucfzqmRl-9ta072qI5F3l4AYzyGQMCceeJo4dsPzbT_NUCakCWqFik
https://www.publico.pt/2020/04/12/tecnologia/noticia/medo-tecnologia-maos-dadas-controlo-pandemia-1911568
https://www.publico.pt/2020/04/12/tecnologia/noticia/medo-tecnologia-maos-dadas-controlo-pandemia-1911568
https://jamanetwork.com/journals/jama/fullarticle/2762689?guestAccessKey=2a3c6994-9e10-4a0b-9f32cc2fb55b61a5&utm_source=For_The_Media&utm_medium=referral&utm_campaign=ftm_links&utm_content=tfl&utm_term=030320
https://www.dw.com/pt-br/apps-para-rastrear-covid-19-um-empreendimento-arriscado/a-54357321
https://www.jn.pt/nacional/protecao-de-dados-arrasa-intencao-de-tornar-app-stay-away-covid-obrigatoria-12921578.html
https://www.theguardian.com/technology/2020/may/05/uk-racing-to-improve-contact-tracing-apps-privacy-safeguards
https://www.terra.com.br/noticias/apps-para-rastrear-covid-19-um-empreendimento-arriscado,68d14e26021ead3a9a45205bbdb9c186awj674hl.html
https://www.wsj.com/articles/to-track-virus-governments-weigh-surveillance-tools-that-push-privacy-limits-11584479841?mod=hp_lead_pos3
https://www.washingtonpost.com/gdpr-consent/?next_url=https%3a%2f%2fwww.washingtonpost.com%2ftechnology%2f2020%2f03%2f17%2fwhite-house-location-data-coronavirus%2f
https://www.infosecurity-magazine.com/news/vulnerabilities-covid19-app/https://www.correiobraziliense.com.br/app/noticia/mundo/2020/04/15/interna_mundo,844807/aplicativo-para-combater-covid-19-e-criado-na-america-latina.shtml
https://www.em.com.br/app/noticia/internacional/2020/05/30/interna_internacional,1152197/panorama-dos-metodos-de-rastreamento-contra-a-covid-19-no-mundo.shtml
https://www.dw.com/pt-002/covid-19-%C3%A1frica-do-sul-cria-app-que-rastreia-o-v%C3%ADrus/a-53442196
https://www.tsf.pt/mundo/policia-de-marrocos-cria-aplicacao-para-rastrear-movimentos-dos-cidadaos-12100780
https://www.dw.com/pt-002/covid-19-%C3%A1frica-do-sul-cria-app-que-rastreia-o-v%C3%ADrus/a-53442196
https://www.tsf.pt/mundo/policia-de-marrocos-cria-aplicacao-para-rastrear-movimentos-dos-cidadaos-12100780

Tabela 1- Vigilância digital: medidas obrigatórias

Medidas adotadas	Países
Localização de doentes por telemóvel como medida de rastreio obrigatória	China, Singapura, Coreia do Sul
Software de reconhecimento facial associado ao registo criminal do cidadão (atribuição de um código QR)	China
Pulseiras eletrónicas para quem viole quarentena obrigatória	Coreia do Sul Hong Kong
A *app* não voluntária para milhões de utilizadores e sem limitar o uso dos dados recolhidos	India
Ferramentas de geolocalização para monitorização de doentes (as usadas na luta antiterrorista)	Paquistão
App móvel da polícia permite rastrear os movimentos dos cidadãos e identificar quem desobedece às regras do estado de emergência	Marrocos
App criada pelo Governo que pede, aleatoriamente, *selfies* aos cidadãos em quarentena obrigatória (o utilizador tem 20 minutos para publicar um selfie no local onde está)	Polónia
Tecnologias digitais iguais às utilizadas pela ISA (Israel *Securities Authority*) para monitorizar grupos terroristas (ex: a autorização do governo para vigilância dos telefones dos cidadãos).	Israel

Fonte: Elaboração própria

Tabela 2- Utilização massiva de vigilância digital

Tecnologias e práticas	Países
• Câmaras de vigilância (200 milhões) • Câmaras de infravermelhos • Capacetes de inteligência artificial para medir a temperatura • Drones para reconhecimento facial (para alertar quem não usava máscaras em público) • Recolha de dados de localização dos telemóveis ou das redes sociais • Aplicações móveis para controlar as viagens	China
• Câmaras de vigilância • Acesso a dados de cartões de crédito	Coreia do Sul
• Publicitação de informação do contaminado (ex: identidade das pessoas com quem privou)	Singapura
• Uso de bases de dados para acompanhamento do histórico de viagens; informações de saúde ligadas ao cartão de identificação	Taiwan
• Reforço do uso de tecnologia para o escrutínio em massa	Rússia
• Câmaras térmicas para medir a temperatura de uma multidão • Algoritmos ligados a grandes bases de dados para determinar as novas fontes de contágio em tempo real	Israel

Fonte: Elaboração própria

Tabela 3 - *Apps* de rastreio

Tecnologia utilizada	Países
• *App* com tecnologia *Bluetooth*	Alemanha, Itália, Irlanda, Espanha, Áustria e República Checa e Portugal.
• *App* tecnologia de geolocalização combina dados recolhidos via *Bluetooth* e GPS	Noruega Espanha
• *App* de rastreio de contactos com tecnologia de *Bluetooth* e GPS (localização de pessoas anonimizada)	Chipre
• Tecnologia *Bluetooth* (mas Estado quis partilhar informação de localização dos telemóveis do utilizador com as autoridades de saúde	França
• *App* com modelo centralizado (mas foi abandonada em favor do uso do sistema *Apple-Google).*	Reino Unido
• Os métodos mudam de acordo com os Estados • O Governo Federal explora o uso de dados de geolocalização fornecidos pelas grandes empresas tecnológicas	EUA
• *App* inspirada no modelo se Singapura, mas não permitindo a geolocalização.	Austrália
• A *app* tem um código QR através da sua digitalização (no autocarro, no supermercado, etc.) é recebido um 'recibo de geolocalização' (a identidade dos utilizadores é verificada via *blockchain*, mas não armazenada num servidor central)	Africa do Sul
• A *app* revelou uma vulnerabilidade: enviava dados de saúde pessoais e informações de identificação (foi substituída por *app* com tecnologia *blockchain* que permite que os cidadãos partilhem dados sobre o coronavírus, mas sem expor sua privacidade)	Colômbia[12]

Fonte: Elaboração própria

Por fim, sublinhe-se que existem países onde o uso de tecnologias (e a própria a pandemia) estão a ser usadas de modo explicito para corroer a democracia. É disso exemplo Israel, onde se utilizaram tecnologias avançadas para combater uma segunda onda de contaminação (câmaras térmicas para medir a temperatura de uma multidão ou algoritmos ligados a grandes bases de dados para determinar as novas fontes de contágio em tempo real). Em março, foram anunciados planos de utilizar as mesmas tecnologias digitais normalmente utilizadas pela ISA (Israel Securities Authority) para monitorizar grupos terroristas, entre elas a autorização do governo para vigilância dos telefones dos cidadãos. Os defensores dos direitos humanos denunciaram a medida e a justiça anulou a autorização em abril, tendo deixado a porta aberta: se o método fosse aprovado por uma lei, poderia ser utilizado, o que o Parlamento viria a fazer em maio. Note-se ainda que o partido Likud, que conquistou a maioria dos assentos nas últimas eleições, usou a emergência sanitária para impedir a oposição de assumir o controlo dos procedimentos parlamentares [13].

[12] Governos de vários países América do Sul disponibilizaram *apps* próprias sem problemas de privacidade. Para além dos países referidos, também encontrámos a utilização de app de rastreamento em: Brunei (BruHealth); COCOA – COVID-19 Contact App; Cazaquistão (eGov bizbirgemiz); Filipinas (StaySafe PH); Arábia Saudita (Tabaud); Guam (Guam Covid Alert)

[13] https://www.em.com.br/app/noticia/internacional/2020/05/30/interna_internacional,1152197/panorama-dos-metodos-de-rastreamento-contra-a-covid-19-no-mundo.shtml
https://www.uol.com.br/tilt/noticias/afp/2020/06/26/israel-recorre-a-inteligencia-artificial-para-impedir-segunda-onda-de-covid-19.htm

Mas também na Rússia se observaram atropelos à democracia: para além do reforço do uso de tecnologia para o escrutínio em massa, foram aprovadas novas regras contra as notícias falsas sobre o vírus, que poderiam refletir-se numa crescente perseguição aos meios de comunicação independentes (o que também está a acontecer na Sérvia e na Turquia). Na Hungria, a luta contra o coronavírus inclui a detenção dos críticos de Viktor Orbán que se opuseram através das plataformas das redes sociais (nomeadamente criticando o governo). Na Polónia, o primeiro país europeu a usar uma app destas para telemóvel, o governo criou uma aplicação que pede, aleatoriamente, selfies aos cidadãos em quarentena obrigatória (o utilizador tem 20 minutos para publicar um selfie no local onde está, caso não o faça recebe uma visita da polícia em casa)[14]. Observou-se que em 2020, à escala global, as medidas de emergência destinadas a conter a pandemia, ao limitarem direitos e liberdades, agravaram o declínio da democracia em pelo menos 82 países (Edgell et al, 2020).

Apps de rastreio de contactos: uma quase desilusão

Vários países viram-se confrontados com os problemas e a controvérsia suscitados pelas *apps* de rastreamento automático de pessoas em contato com infetados: receios e resistência dos defensores da privacidade, dúvidas quanto à sua eficácia no controlo da doença, problemas técnicos, dificuldade em ativar o sistema de alerta automático das *apps*, incompatibilidades de *software*, etc.

Estima-se que mais de 40 países tenham apostado em *apps* do mesmo género, em 2020, embora com funcionamentos ligeiramente diferentes entre si. Em outubro desse ano previa-se que existisse entre 60 e 80 por cento de potenciais utilizadores destas aplicações, mas as taxas de *download* a nível mundial, nessa altura, rondavam apenas os 20 por cento. Mesmo nos casos mais bem-sucedidos, como Singapura e Islândia, a taxa não ultrapassava os 40 por cento. A Universidade de Oxford apontava para uma taxa de 56 por cento como o valor capaz de travar a pandemia [15].

Apesar do número de *downloads* em relação ao tamanho de uma população representar uma métrica-chave - uma baixa taxa de instalação apresenta baixa eficácia- os problemas de funcionalidade e de confiabilidade são igualmente determinantes no sucesso. Mesmo onde não houve fracasso, a eficácia das *apps* permanece uma incógnita. O Conselho da Europa colocou mesmo a questão de saber se as promessas feitas sobre essas *apps* "valem os previsíveis riscos sociais e legais"[16].

Em França, a *app* StopCovid, lançada em junho de 2020 pelo governo francês, em meados de agosto tinha apenas 2,3 milhões *downloads* (de uma população de 67 milhões). Permitiu a notificação de apenas 72 contatos de risco, apesar de 1.169 utilizadores se declararem positivos. Baseada num protocolo "centralizado", incompatível com a maioria das *apps* de rastreamento europeus ("descentralizadas") foi amplamente criticada devido aos riscos para a proteção de dados[17].

---

https://expresso.pt/coronavirus/2020-03-21-Israel-vai-monitorizar-telemoveis-para-combater-o-coronavirus.-Nem-toda-a-gente-considera-que-isso-faz-bem-a-saude--democratica...
https://www.reuters.com/article/us-health-coronavirus-israel/israel-to-use-anti-terror-tech-to-counter-coronavirus-invisible-enemy-idUSKBN21113V
https://www.lawfareblog.com/israeli-supreme-court-checks-covid-19-electronic-surveillance?fbclid=IwAR1h2gJi1JzWN25A2RDAHa8Uzozm2OXQB-5rNj-bjfaVTX5quxWcyhwAGgQ

[14] https://brasil.elpais.com/internacional/2020-03-31/coronavirus-poe-a-democracia-de-quarentena.html
https://www.euronews.com/2020/05/14/hungary-critics-silenced-in-social-media-arrests-as-eu-debates-orban-s-powers

[15] https://newinoeiras.nit.pt/fit/stayaway-covid-a-historia-desastrosa-da-app-que-nos-ia-salvar-a-todos/

[16] https://zap.aeiou.pt/apps-rastreio-ajudar-travar-covid-354719

[17] https://istoe.com.br/os-aplicativos-de-rastreamento-do-coronavirus-na-europa/

Na Alemanha, a Corona-Warn-App começou por ser bem recebida até por defensores da proteção de dados (em 24 de julho já tinha 16,2 milhões de downloads, o equivalente a 20% da população), mas deixou de o ser quando o jornal tabloide Bild revelar que a *app* provavelmente não tinha funcionado adequadamente para milhões de utilizadores (pois para economizar energia, alguns sistemas operacionais Android bloquearam a execução da *app* em 2º plano, o que significa que sua principal função – enviar um alerta ao utilizador que encontrasse alguém que testou positivo para o vírus – pode não ter funcionado) [18]

Em Portugal, chegou a ser anunciada pelo primeiro-ministro a obrigatoriedade da utilização aplicação Stayaway Covid, mas a contestação pública (nomeadamente pela anti constitucionalidade da medida) e os pareceres de organismos públicos levaram ao abandono da ideia. A *app* foi criticada por associações de defesa do consumidor pela possibilidade de utilização indevida de dados pessoais e pelo papel central de gigantes digitais na definição de protocolos de saúde. Note-se que já anteriormente a CNPD, no parecer que emitiu no final de junho, havia sinalizado alguns aspetos críticos, nomeadamente o recurso à interface da Google e da Apple, na medida em que há uma parte crucial da execução da aplicação que não é controlada pelos autores; referindo também o facto de nem todos os telefones inteligentes poderem utilizar a *app*, pois requere sistemas operativos muito recentes (para ser eficaz no rastreio a *app* tem de ser instalada por 60 por cento de utilizadores de smartphones). Também a Associação D3 – Defesa dos Direitos Digitais em relação à Stayaway Covid, já havia destacado, em julho, a sua profunda preocupação e apreensão pela falta de transparência no desenvolvimento da *app* e pelas consequências implicadas pelo uso generalizado de uma solução tecnológica, com eficácia não comprovada[19]. Desde o lançamento (setembro) até janeiro de 2021 quase 1,8 milhões de pessoas desistiram da *app*, isto é apenas 39 por cento das quase três milhões de pessoas que instalaram a aplicação a continuam a usar. Outra das razões que explica a desinstalação é a sua ineficácia: no pico de utilização, após 38 mil novos casos detetados durante o período de vigência da aplicação, apenas foram emitidos 730 códigos (aquilo que torna a aplicação útil). Mais: desses códigos gerados pelo sistema e entregues pelos médicos, apenas 300 foram inseridos pelos pacientes na aplicação[20].

Em Espanha, a Radar Covid, lançada no final de julho, em setembro tinha obtido mais de 17,8 de download (numa população estimada de 83 milhões de pessoas).

O Reino Unido e a Noruega começaram por ter que abandonar (em junho) as primeiras versões das *apps.* O primeiro, por ter uma app de abordagem "centralizada" considerada ineficaz (o governo atribuiu o fracasso às restrições impostas pela Apple), substituindo-a por uma "descentralizada". A Noruega por ter visto a *app* suspensa pelas autoridades nacionais, após ser considerada pela Amnistia Internacional profundamente invasiva. O facto de recolher o sinal GPS do utilizador, para além dos contactos de proximidade por *Bluetooth*, e de o transmitir a um servidor central, fazia da app um potencial perigo para os seus utilizadores, recolhendo e concentrando dados sensíveis que podia ser utilizado para outros fins ou intercetados por quem comprometesse o servidor central de operações da aplicação[21].

A fraca adesão às *apps* dos diferentes países é notória em muitos lugares. Veja-se o caso do Brasil, onde a Coronavírus-SUS teve 61,5 milhões de downloads desde o seu lançamento, em março do ano passado, sendo que em fevereiro deste ano eram apenas 2,3 milhões de utilizadores ativos (o equivalente a menos

[18] https://www.msn.com/pt-br/noticias/ciencia-e-tecnologia/apps-para-rastrear-covid-19-apresentam-problemas-e-causam-controv%C3%A9rsia/ar-BB17thZM
[19] https://shifter.sapo.pt/2020/07/stayway-covid-aplicacao/
[20] https://www.publico.pt/2021/01/15/tecnologia/noticia/60-ja-apagaram-stayaway-covid-sao-18-milhoes-portugueses-1946366
[21] https://shifter.sapo.pt/2020/06/app-norueguesa-rastreamento-covid19/

de 1 por cento da população brasileira.)[22]. Uma das principais causas para a fraca adesão das *apps* revelados pela investigação de Toussaert (2021) foi mesmo o problema da privacidade. Existem, contudo, países onde esta tecnologia foi bem recebida, como é o caso da Islândia (a *app* é utilizada por cerca de que de 40 por cento dos islandeses); ou, de um modo menos expressivo, a Suíça, onde a *app* teve 2,3 milhões de *downloads* (numa população de 8,5 milhões), sendo utilizada ativamente por 1,6 milhão de suíços[23]. Indagando sobre a aceitação da *app* alemã, Munzert et al (2021) concluem que é entre os mais velhos e as pessoas com condições pré-mórbidas que nesse país a aceitação é maior, ao contrário do que seria de esperar, dada a maior familiaridade dos mais jovens com o digital.

Considerações finais

Esta pandemia trouxe um surto de "solucionismo" tecnológico, assente na crença de que para todo o problema existe uma resposta tecnológica. A tecnologia fornece-nos ferramentas poderosas, mas nem todas as soluções terão de ser tecnológicas, como lembra Naughton (2020, 25 de abril). Ao longo do texto observámos como foi grande a esperança depositada nas *apps* de rastreio de contactos e inúmeros os países que as desenvolveram e adotaram. Mas também constatámos quantas resistências encontraram junto dos cidadãos e organizações de defesa de direitos humanos de alguns países, e quanta ineficácia demostraram no controlo da pandemia. Nas sociedades democráticas o poder nunca está todo nos governantes. E a tecnologia também não tem todo o poder. A relação entre esta e a sociedade é um processo de condicionamento recíproco (Baym, 2010), pois todo o desenvolvimento tecnológico é produto de relações culturais, sociais, políticas…

A utilização de meios técnicos ampliou enormemente a quantidade de dados recolhidos, conduzindo ao Big Data - conceito que remete para a capacidade de procurar, agregar e efetuar referências cruzadas entre conjuntos de grande dimensão de dados, utilizando uma série de práticas, técnicas e softwares. Mas os riscos da vigilância eletrónica já estão além da recolha de dados e da falta de transparência deste processo, pois passaram a advir também da sua subsequente acumulação e da incerteza quanto aos fins a que se destinam (nomeadamente por parte de atores privados como a Google, a Amazon ou a Apple).

Os tempos atuais impõem, inelutavelmente, que saibamos lidar com a tecnologia. Para tal, a literacia – a digital, mas também os outros tipos de literacia que lhe são indissociáveis - poderá desempenhar um importante papel, na medida em que permite escolhas mais informadas, seja no plano da relação dos cidadãos com os recursos digitais ou no exercício da cidadania. Tudo indica que nos tempos mais próximos a tecnologia (incluindo aquela que no vigia)", já omnipresente na atualidade, desempenhe um papel importante na proteção da saúde pública (é até expectável que se incremente um forte entusiasmo por "tecnologias sem contacto", que não passam pelo humano, já que este representa um risco biológico"). Não obstante o fim ou a virtude, torna-se sempre imprescindível que os seus usos estejam sujeitos ao escrutínio das instituições democráticas e à avaliação dos cidadãos.

Na verdade, e em síntese, podemos dizer sobre a vigilância o que Kranzberg disse sobre a tecnologia: "não é boa, nem má, mas também não é neutra" (1986, citado em Boyd & Crawford, 2012: 662). A vigilância,

[22] https://www.uol.com.br/tilt/noticias/redacao/2021/04/14/falta-de-politica-nacional-faz-app-do-sus-flopar-no-rastreamento-de-contato.htm

[23] https://istoe.com.br/os-aplicativos-de-rastreamento-do-coronavirus-na-europa/

produto social que utiliza a tecnologia como meio, tem hoje novos e múltiplos contornos. Reinventam-se e emergem e inúmeros panóticos, porém alguns revelam-se imperfeitos.

Referências bibliográficas

Barriga, A. C., Martins, A.F., Simões, M.J., Faustino, D. (2020). The COVID-19 pandemic: Yet another catalyst for governamental mass surveillance? *Social Sciences & Humanities Open*. Volume 2, Issue 1

Barriga, A. C. (2015). Uma exploração à opinião na twittosfera: entre e discussão política e a privatização do público. In J. R. Carvalheiro (Org.), *Público e Privado nas Comunicações Móveis* (159-180). Coimbra: Minerva Coimbra.

Bartlett, J. (2018). *The People Vs Tech: How the internet is killing democracy (and how we save it).* New York: Dutton.

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

Baym, N.K. (2010). *Personal connections in the digital age*. Cambridge: Polity Press.

Boyd, D., Crawford, K. (2012). Critical Questions for Big Data. *Information, Communication & Society*, 15, pp. 662–679.

Caluya, G. (2010). The Post-Panoptic Society? Reassessing Foucault in Surveillance Studies. *Social Identities*, 16(5), pp. 621–633.

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

Dijck, J. (2014). Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology. *Surveillance and Society*, 12(2), pp.197–208.

Edgell, A., Grahn, S., Lachapelle, J., Lührmann, A., Maerz, S. (2020). An Update on Pandemic Backsliding: Democracy Four Months After the Beginning of the Covid-19 Pandemic, Policy Brief, V-DEM Institute. Available at: https://www.v-dem.net/media/filer_public/13/1a/131a6ef5-4602-4746-a907-8f549a5518b2/v-dem_policybrief-26_201214_v31.pdf

Finn, R., Watson, H., & Wadhwa, K. (2018). Mining social media for effective crisis response: Machine learning and disaster response. In Boersma, K. & Fonio C. (Eds.), *Big data, surveillance and crisis management* (38–56). New York: Routledge.

Foucault, M. (1998). Vigiar e Punir. Petrópolis: Vozes.

Fuchs, C. (2011). New Media, Web 2.0 and Surveillance. *Sociology Compass*, 5(2), pp.134–147.

Garcia, J.L. (June 28, 2020). A pandemia e os perigos de uma distopia digital: colonizando pelo algoritmo? Público. Available at: https://www.publico.pt/2020/06/28/tecnologia/noticia/pandemia-perigos-distopia-digital-colonizando-algoritmo-1921806

Haggerty, K. (2006). Tear down the walls: on demolishing the panopticon. In Lyon, David (Ed.), *Theorizing Surveillance: The panopticon and beyond* (pp.23-45). Devon: Willan Publishing.

Haggerty, K. e Ericson, R. (2006). The New Politics of Surveillance and Visibility. In Keven Haggerty e Richard Ericson (eds) *The New Politics of Surveillance and Visibility*. Toronto: University of Toronto Press.

Harding, L. (2014). *The Snowden Files: The Inside Story of the Worlds Most Wanted Man*. New York: Vintage Books.

Jansson, A. (2012). Perceptions of surveillance: Reflexivity and trust in a mediatized world (the case of Sweden). *European Journal of Communication*, 27(4), pp. 410–427.

Lessig, L. (1999). *Code and other laws of cyberspace*. New York: Basic Books.

Lyon, D. (2001). *Surveillance Society: Monitoring Everyday Life*. Buckingham and Philadelphia: Open University Press.

Lyon, D. (2007). *Surveillance Studies: An Overview*. Polity: Cambridge.

Lyon, D. (2014). Surveillance, Snowden, and big data: Capacities, consequences, critique. *Big Data & Society*, pp.1-13.

Lyon, D. (2018). *The Culture of Surveillance: Watching as a Way of Life*. Cambridge: Polity Press.

Marx, G. (2015). Surveillance studies. *International encyclopedia of the social & behavorial sciences*, 23(2), pp.733-741.

Menárguez. A. (November 21, 2018). Os privilegiados são analisados por pessoas; as massas, por máquinas. *El País Brasil.* Available at:https://brasil.elpais.com/brasil/2018/11/12/tecnologia/1542018368_03500 0.html

Moura, M.G. (April 16, 2019). Uma abominação que estranhamente parece não estar a incomodar por aí além. *Diário de Notícias*. Available at: https://www.dn.pt/opiniao/opiniao-dn/convidados/uma-abominacao-que-estranhamente-parece-nao-estar-a-incomodar-por-ai-alem-10804651.html

Munzert, S., Selb, P., Gohdes, A., Stoetzer, L. & Lowe, W. (2021). Tracking and promoting the usage of a COVID-19 contact tracing app. Nature Human Behavioir.

Naughton, J. (April 25, 2020). Contact apps won't end lockdown. But they might kill off democracy. *The Guardian*. Available at:https://www.theguardian.com/commentisfree/2020/apr/25/contact-apps-wont-end-lockdown-but-they-might-kill-off-democracy

Rheingold, H. (2002). *Smart mobs: the e Next Social Revolution*. Cambridge, MA: Perseurs Publishing.

Shapiro, A.L. (1999). *The Control Revolution*. New York: Public Affairs.

Steeves, V. (2009). Reclaiming the Social Value of Privacy. In Ian Kerr, Valerie M. Steeves e Carole Lucock (orgs.) *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*. Oxford: Oxford University Press.

Soguel, D. (March 21, 2020). Pandemic dilemma: Emergency surveillance won't be easy to unplug. The Christian Science Monitor. Available at: https://www.csmonitor.com/Technology/2020/0330/Pandemic-dilemma-Emergency-surveillance-won-t-be-easy-to-unplug

Toussaert, S. (2021). Upping uptake of COVID contact tracing apps. *Nature Humain Behavioir.*

Tufekci, Z. (April 21, 2019). Think You're Discreet Online? Think Again. *The New York Times.* Available at: https://www.nytimes.com/2019/04/21/opinion/computational-inference.html

Warren, S. D., Brandeis, L.D. The Right to Privacy, *Harvard Law Review*, 4(5), (Dec. 15, 1890), pp. 193-220.

Zureik, E. (2007). Surveillance Studies: From Metaphors to Regulation to Subjectivity. *Contemporary Sociology*, 36 (2), pp.112-115.