A DESINFORMAÇÃO EM TEMPOS DE EXCEÇÃO:

Tecnopolítica, vigilância e literacia digital crítica

Sofia José Santos
Tiago Lapa

Resumo: Este capítulo pretende analisar a relação entre democracia, (des)informação e literacia mediática e digital face às medidas de *biovigilância* que vários Estados implementaram no contexto da sua resposta à propagação do SARS-COV-2, em 2020. Usando como recorte metodológico o contexto do estado de exceção que a pandemia COVID-19 legitimou e cruzando debates teóricos com casos ilustrativos, o capítulo argumenta que a natureza tecnicista dos atuais mecanismos de biovigilância digital, a par de um contexto de securitização, tende a facilitar a normalização de práticas e políticas de vigilância, para além da exceção que as legitima, impactando de forma diferenciada a garantia e proteção dos direitos humanos e, consequentemente, a qualidade democrática das sociedades. Pretende, assim, explorar as implicações do que designamos por "*desinformação tecnopolítica*" para a democracia e a garantia e proteção dos direitos humanos digitais.

Palavras-chave: desinformação; democracia; tecnopolítica; digital; COVID-19.

Introdução

Diferentes autores e autoras têm refletido sobre o tema da democracia, sublinhando a relevância da cidadania instruída, esclarecida e empenhada (DAHL, 2020). O conceito de democracia é, hoje, entendido como indissociável dos de informação e literacia (POLIZZI, 2020), embora a relação entre cidadania e literacia mediática não se mostre direta (LOPES, 2015). Enquanto arena política, a democracia promove a construção coletiva e deliberativa do que se entende como o melhor para estruturar e organizar a sociedade (KARVONEN, 2004). Para que tal debate e construção aconteçam, é fundamental a existência de um cidadão informado, que seria putativamente potenciado pelos novos meios digitais (POSTER, 2000). Ou seja, a democracia pressupõe e exige que cidadãos e cidadãs possam, na sua diversidade e heterogeneidade, participar na tomada de decisões coletivas e tenham acesso, a montante e em paralelo, à informação sobre os diferentes interesses, agendas e possibilidades ao dispor (MCNAIR, 2003; SILVEIRINHA, 2008: 4). Tal deve acontecer num espaço discursivo construído como "esfera pública", não só como definida por Habermas (1989), mas também como entendida de forma mais abrangente e horizontal por abordagens Críticas e Pós-coloniais (FRASER, 1992; POSTER, 2002; SANTOS; ARAÚJO; CRAVO, 2016).

Se a informação é condição essencial para a vida democrática (POLIZZI, 2020), a desinformação pode ser vista, então, como uma das suas vulnerabilidades (MORGAN, 2018; MCKAY; TENOVE, 2020). Como acontece com a moeda, em que os elementos que a compõem são calibráveis, expressando uma importância maior ou menor, uma sociedade que tem demasiada desinformação sofre uma progressiva erosão no seu valor democrático e, por conseguinte, na sua aceitação (democrática). Na senda de dar resposta a este desafio, tem-se depositado na difusão da literacia digital crítica a esperança de uma resposta à (des)informação (HERMAN; CHOMSKY, 1988; MCNAIR, 2003; LIVINGSTONE, 2004; STEINBERG, 2009; POTTER, 2010).

Podemos, assim, dizer que democracia, literacia crítica e (des)informação se articulam numa relação

triangular de alimentação recíproca e em permanente (re)ajuste. Nas cedências e avanços que se vão desenhando, os diferentes contextos e temas em questão ajudam a definir os termos e os limites dessa variação.

A tecnologia – enquanto tema e contexto - tem acrescentado desafios crescentes ao lugar de mudança e atualização onde sempre nos encontramos. No século XXI, as chamadas "novas tecnologias" - *softwares* e dispositivos de informação e comunicação capazes de produzir, reunir, armazenar, analisar e compartilhar informações pelas redes digitais e que assentam em características como a imediatez, intercocnetividade e rastreabilidade (SANTOS, 2021a) - alteraram não só as modalidades de circulação da (des)informação, mas recolocaram no centro do debate a sua dimensão tecnopolítica. Na verdade, desde as revelações de Snowden sobre o programa PRISM, em 2013;[60] os casos *Panama Papers*,[61] em 2016; o referendo sobre o BREXIT e as eleições presidenciais norte-americanas, em 2016; o escândalo da *Cambridge Analytica*[62] e as eleições presidenciais brasileiras, em 2018; ou a "biovigilância" (o que envolve, entre outras medidas, o rastreamento da localização ou a coleta de informação sobre comunicações e saúde) instaurada no âmbito da resposta à COVID-19, em 2020, são ilustrativos destes novos desafios que a tecnologia acrescenta ao já referido triângulo que relaciona em permanente (re)ajuste da democracia, (des)informação e literacia crítica.

Este capítulo pretende, a partir de uma abordagem crítica e dialética, explorar essa relação triangular, analisando a desinformação face a aplicações de rastreamento e vigilância em contextos securitizados, explorando as suas implicações para a democracia e para a garantia e proteção dos direitos humanos e desconstruindo o princípio social e politicamente neutralizante do "universalismo digital" (CHAN, 2013). Partindo dos pressupostos de que as arenas *online* e *offline* não são dissociáveis (KENDALL, 1999), o capítulo argumenta que a natureza tecnicista dos atuais mecanismos de biovigilância digital, a par de um contexto de securitização, tende a facilitar a normalização de práticas e políticas de vigilância, para além da exceção que as legitima, impactando de forma diferenciada a garantia e proteção dos direitos humanos e, consequentemente, a qualidade democrática das sociedades.

Para desenvolver a análise, este capítulo usa como recorte metodológico o contexto do estado de exceção que a pandemia de COVID-19 legitimou, recorrendo a casos ilustrativos. Combinando, por um lado, a atual (des)ordem informativa[63] no contexto de comunicação em rede, que tem sido apelidada de "era da pós-verdade" - i.e., um tempo em que a interpretação de factos acontece não por debates racionais, mas por disputa de crenças pessoais e emoções (ROCHLIN, 2017) - e, por outro, assuntos de grande tecnicidade, a atual resposta por parte de vários Estados ao coronavírus SARS-CoV-2 é um caso em que os (re)ajustes entre democracia, (des)informação e (i)literacia mediática e digital estão em permanente negociação, oscilando entre imposição, contestação e reclamação de políticas e de direitos. A par das medidas expectáveis de âmbito epidemiológico e de saúde pública, vários Estados, numa tentativa de desacelerar a disseminação do vírus, adotaram medidas de rastreamento digital e de "biovigilância", tal como aplicativos de rastreamento de contatos, muitos sem verdadeiras políticas de privacidade (DIGITAL FREEDOM FUND, 2020; WOODHAMS, 2020) e sem um debate político alargado sobre a natureza e o impacto políticos destas "novas tecnologias" -

[60] O caso Snowden remete ao vazamento de informação que Edward Snowden, um agente da CIA, levou a cabo, em 2013, e que revelou vários programas de vigilância global sob alçada do governo norte-americano. Ver mais em: https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.

[61] 'Panama Papers' refere-se ao vazamento de 11,5 milhões de arquivos do quarto maior escritório de advocacia *offshore*, o Mossack Fonseca, que tornou público vários regimes fiscais *offshore* secretos. Ver mais em: https://www.theguardian.com/news/2016/apr/03/what-you-need-to-know-about-the-panama-papers.

[62] O caso Cambridge Analytica refere-se ao escândalo que surgiu depois de se saber que a empresa Cambridge Analytica usou dados obtidos indevidamente do Facebook para construir perfis de eleitores. Ver mais em: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

[63] Já Lyotard (1990) chamava a atenção para a "pós-verdade" ou implosão da verdade no contexto de claro domínio da comunicação de massas. No entanto, podemos argumentar que, num contexto comunicacional em rede (CARDOSO, 2006), as modalidades de circulação de informação e, consequentemente, as pressões sobre a categoria de "verdade" assumem novos contornos.

para a democracia e os direitos humanos , bem como sobre a forma diferenciada, não-linear e não-universal como tal afeta diferentes grupos e sujeitos.

O capítulo encontra-se estruturado em três partes. Na primeira parte, explora as peças centrais do puzzle, ou seja, a articulação triangular entre democracia, cidadania e (des)informação centrada nas práticas tecnopolíticas e na heterogeneidade dos seus impactos; na segunda parte, concentra-se nos *continuums* e ruturas que articulam vigilância e estado de exceção, especificamente, a forma como o estado de exceção legitima a vigilância, e como a normalização da exceção regulariza, em permanência, essa mesma vigilância "excecional"; finalmente, a terceira parte concentra-se no contexto do combate à pandemia de COVID-19, apresentando casos ilustrativos no panorama global.

1. Democracia, cidadania e (des)informação digital

É comummente atribuída a Thomas Jefferson a frase de que "a informação é a moeda da democracia" (TUCHMAN, 2013). Daí que, desde longa data, as noções de democracia, informação e literacia existem lado a lado, sendo a cidadania ativa e informada uma das pedras angulares da inclusão, mobilização e participação democráticas. A importância de uma cidadania informada exige que a política democrática seja precedida e acompanhada por uma esfera pública (JACOBS; TOWNSLEY, 2013), onde a informação sobre a qual cidadãos e cidadãs farão as suas escolhas circule livremente em formulações múltiplas, acessíveis e transparentes (TUCHMAN, 2013). Na combinação de informação e democracia, há a exigência de dois binômios que se alimentam mutuamente: *esfera pública e participação política*, por um lado, e, por outro, (co)*existência do individual e do coletivo*. O primeiro conjunto - *esfera pública e participação política* - visibiliza a articulação que existe entre a livre circulação de informações e pontos de vista, a cidadania bem informada e a participação política, entendida tanto do ponto de vista formal ou institucional, como do ponto de vista informal e que, comumente, a literatura anglo-saxônica sintetiza na expressão "*everyday politics*". O segundo conjunto - (co) *existência do individual e do coletivo* - sublinha que, a par da necessidade de pensamento e ação individuais, o processo político democrático exige que cidadãos e cidadãs ajam coletivamente na tomada de decisões políticas, como momentos eleitorais (MCNAIR, 2003), mas também que tenham em atenção o impacto não-linear e diferenciado que as diferentes agendas e decisões (macro e micro) políticas têm nas heterogeneidades que constituem uma determinada sociedade. Neste sentido, entendimentos *bottom-up* (e.g. LEDERACH, 1997) e interseccionais (e.g. COLLINS, 2017; TERRIQUEZ; BRENES; LOPEZ, 2018) da agenda e ação políticas são fundamentais.

Esta secção pretende ilustrar estas dinâmicas essenciais da articulação informação e democracia, tendo em conta a ecologia digital, explorando, em primeiro lugar, como a desinformação digital pode contribuir para uma maior vulnerabilidade da democracia, uma vez que atualiza, aprofunda e ressignifica dinâmicas de desinformação e, em segundo lugar, concretiza este aprofundamento de vulnerabilidade analisando a forma como, em contextos democráticos e crescentemente digitais, a tecnopolítica impacta a gramática, o reconhecimento e a proteção dos Direitos Humanos e como o reequilíbrio democrático exige uma literacia digital crítica também ela democratizada.

a. A desinformação como vulnerabilidade democrática

A centralidade da informação na vida política é transversal a culturas e opções políticas disseminadas no tempo e no espaço, não sendo menos verdade que a forma como a informação é produzida e acedida acompanha as tendências societais, impactando cada contexto específico de forma certa, mas variável. Por

um lado, olhando para o percurso e críticas à democracia liberal (SOUSA SANTOS, 2007), podemos afirmar que a noção da democracia foi e continua a evoluir, a complexificar-se e a densificar-se na medida em que há não só uma democratização de quem tem acesso legal e real à cidadania, mas também uma audiência cada vez mais informada. Por outro, se a noção de democracia evolui e se complexifica, a forma como entendemos a (des)informação e como esta circula também se tem, do mesmo modo, modificado (QUINTANILHA; DA SILVA; LAPA, 2019).

Na segunda década do século XXI, a perene vulnerabilidade da democracia face à (des)informação tem sido atualizada, em grande medida, com as "novas tecnologias", particularmente, a sua ubiquidade, os padrões de utilização e as dinâmicas específicas que as sustentam, como a internet *das coisas*, a *datificação* ou a *big data* (FLAXMAN; GOEL; RAO, 2016; SANTOS, 2021b). Neste contexto, esta vulnerabilidade tem vindo a enfrentar duas dinâmicas de aprofundamento e que conhecem os seus rostos mais visíveis, por um lado, no terreno fértil para as designadas *fake news* e opções de incivilidade no debate político e, por outro, na descoincidência entre, por um lado, a centralidade do uso da Internet das Coisas e das aplicações informáticas e, por outro, o conhecimento de cidadãos e cidadãs sobre as suas implicações democráticas (WEBER, 2013).

A primeira dinâmica é, em grande medida, justificada pela escolha crescente das redes sociais *online* como fontes preferenciais das dietas informativas (FLAXMAN; GOEL; RAO, 2016), a democratização dos processos de *gatekeeping* (AMARAL; SANTOS, 2019), mas também a lógica de "*facebook disclosure*" (WILLS; REEVES, 2009) e a convergência destes elementos num conhecido contexto de crescente polarização ideológica e de "pós-verdade" (BALL, 2017; NICK, 2017; ROCHLIN, 2017; QUINTANILHA; DA SILVA; LAPA, 2019). Tal, impacta a "veracidade" da informação que circula e que informa debates, assim como os termos dos próprios debates, minando o que deveria ser, nas palavras de McNair (2003), o uso constitucional, racional, deliberativo, transparente e, por isso mesmo, politicamente construtivo da informação na esfera pública, afetando a qualidade das decisões políticas e da interação coletiva e, com isso, impactando a qualidade da democracia (e.g. GIULIANI; GARRAIO; SANTOS, 2020).

A segunda, na qual este capítulo se centra, prende-se com o ritmo, intensidade e diversidade de utilização da Internet, o significado tecnopolítico que esse uso corporiza e o conhecimento empenhado das implicações desses usos e significado. Sublinhando que estes números estão em constante atualização, em finais de 2020, 4,66 biliões de pessoas (STATISTA, 2020a) acediam à *web*, sendo que mais de 60% das pesquisas *google* eram feitas a partir de dispositivos móveis (STATISTA, 2020b). Também o ritmo da interação e da produção de conteúdos na *web* é extremamente acelerado. Por exemplo, diariamente, na rede social Facebook gosta-se, em média, de 4,5 bilhões de publicações, compartilham-se mais de 4,7 biliões de atualizações de estado e assiste-se a mais de 1 bilião de vídeos (WEBFX, 2020). Do mesmo modo, em cada dia, são enviados e recebidos mais de 182,9 biliões de *e-mails*, o que perfaz, em média, mais de 2 milhões de mensagens trocadas a cada segundo (WEBFX, 2020). Estando assim presentes na vida quotidiana, as tecnologias digitais conseguem hoje não apenas uma

> difusão horizontal (i.e., expansão contínua em tamanho, conteúdo, volume, acesso, usuários, etc.) (...) [mas sobretudo] uma profusão vertical (i.e., alterações de formas de socialização, de participação política, de organização económica e laboral, de expressão cultural, etc.). (SANTOS, 2021b).

Porém, apesar disso, a presença das tecnologias digitais e da Internet das Coisas foi, durante muito tempo vista meramente, sobretudo, por quem as utiliza, pelo prisma da eficácia e eficiência técnica, descurando o seu significado e implicações políticas.

Casos como as denúncias de Snowden ou o escândalo da *Cambridge Analitica* agitaram as águas do debate sobre as modalidades de interação *online*, a propriedade dos dados, proteção da privacidade, direitos humanos e respetivas implicações democráticas, despertando maior alerta para a questão (CISCO,

2019; MANAGER, 2020; STATISTA, 2020c). No entanto, é importante também frisar que o resultado de um inquérito levado a cabo na região da Ásia Pacífico (Austrália, China, Índia, Indonésia, Hong Kong, Japão, Singapura e Taiwan), em 2020, conclui que cerca de 96% das pessoas preferem, na utilização das aplicações dos seus dispositivos, comodidade e facilidade em detrimento de segurança e privacidade (F5'S, 2020). Esta preferência não acontece, porém, no vazio e pode ser associada, para além das interpretações psicologizantes de comodismo e de gratificação imediata, essencialmente a dois fenômenos. O primeiro é que a literacia digital *per se*, sem o comando de uma dimensão crítica, não desemboca, necessariamente, no uso crítico continuado da Internet, podendo até gerar aquilo que se designa por *paradoxo da privacidade*. A sobrevalorização das competências próprias de literacia[64], a falta de transparência e de conhecimento aprofundado dos mecanismos internos das plataformas digitais pode levar a uma descoincidência entre, por um lado, a perceção e a realidade quanto ao volume de dados pessoais disponibilizados às aplicações e, por outro, entre as intenções de proteção e preocupações dos utilizadores quanto à privacidade e o comportamento efetivo (muitas vezes, não intencionado) de disponibilização de dados pessoais e privados (NORBERG; HORNE; HORNE, 2007; TADDICKEN, 2014). Estes mesmos fatores podem levar a uma sobrevalorização das competências e capacidades para lidar com a desinformação nas plataformas digitais e a desvalorizar o impacto do contacto com a desinformação no próprio, constituindo um risco para a constituição do exercício de uma cidadania informada.

Na senda de Hallam e Zanella (2016), que partem de uma perspetiva focada nas características individuais, podemos argumentar que fenômenos potencialmente lesivos, como a violação de privacidade ou a exposição à desinformação, quando não experimentados diretamente, constituem-se para os indivíduos como psicologicamente distantes, tendo menos peso e estando menos presentes nas escolhas e práticas diárias do que as atividades nas rede sociais *online* mais concretas, gratificantes e psicologicamente próximas. Ora, isto sugere que para os indivíduos estes fenômenos não são tendencialmente sentidos como problemas do próprio, mas dos outros ou que não há uma suficiente consciência ou perceção da (co)*existência e interligação entre o pessoal e o coletivo (psicologicamente distante)*.

Processos como o paradoxo da privacidade, que explicam, pelo menos em parte, a proliferação da disponibilização de informação pessoal e privada, concorrem para alimentar e informar o funcionamento dos algoritmos com impacto na circulação pública de (des)informação. A personalização, algoritmicamente informada pelos dados pessoais e privados, dos *feed* nas redes sociais *online* e dos resultados de pesquisa nos motores de busca - numa lógica apelidada de *googlização* do conhecimento e da sociedade (VAIDHYANATHAN, 2012) - faz com que cada indivíduo tenha a sua própria dieta informativa e seja cada vez menos exposto à informação contraditória com as suas disposições ideológicas e crenças e mais suscetível a conteúdos (des) informativos confirmatórios dos seus pontos de vista.

Em segundo lugar, podemos apontar uma despolitização da tecnicidade que se joga na aparente "neutralidade" algorítmica das plataformas e serviços digitais, que segue um fetichismo tecnicista que oculta as origens sociais dos artefactos tecnológicos. É através desta aparência que se propõem soluções técnicas para problemas como a desinformação, em que as empresas tecnológicas avançam soluções algorítmicas para os próprios problemas que criam, tentando, assim, esvaziar as pretensões de regulação externa e democrática da indústria e da circulação pública de informação. E muitas soluções de regulação remetem para problemas relacionados com o "normal" funcionamento do mercado, deixando de parte considerações sobre a relação entre modelo econômico e social, a produção e circulação de (des)informação e o funcionamento da democracia, num contexto onde se entende as redes digitais, essencialmente, como espaços de consumo, não como esfera pública e palco de participação política e o usuário como consumidor, não tanto como cidadão.

[64] O que remete ainda para questões metodológicas de como aferir competências de literacia digital dos indivíduos, em particular, quando se usam instrumentos, como o questionário, que assentam no auto-relato dos inquiridos.

Os termos do debate em torno destes fenômenos não se centram tendencialmente sobre os efeitos destes nas instituições societais, mas sobre cada um de nós individualmente, uma vez que as pessoas (e, não raras vezes, a literatura existente) tendem a extrapolar as experiências individuais e o interesse privado como matriz do debate, sem as transpor no coletivo e no valor público. Tal, é insuficiente na medida em que não nos permite ter uma real noção do impacto que estas tecnologias podem criar em termos coletivos e de ação política individual e coletiva. Formulando a discussão apenas nestes termos, o debate sobre o impacto da desinformação na democracia está amputado de uma consideração (coletiva) que é, provavelmente, fundamental.

b. Tecnopolítica, direitos humanos e literacia digital crítica

Na era digital, a tecnologia é entendida como um dos pilares da ligação entre democracia, cidadania e (des)informação. Numa lógica McLuhiana, à medida em que a sociedade moderna se estrutura em torno da tecnologia, esta constitui-se como um dos seus elementos fundamentais (FEENBERG, 2005), em redor do qual debates e conceitos políticos (tradicionais) encontram extensões, declinações ou mesmo ressignificações, visibilizando a tecnologia como braço e corporização do político. Esta simbiose entre tecnologia e política - "cumprir objetivos políticos por meio do suporte de artefatos técnicos" (GAGLIARDONE, 2014: 3) a par da exigência que emana da organização da sociedade em termos tecnológicos - é comumente sintetizado como "tecnopolítica", ou seja, "híbridos de sistemas técnicos e práticas políticas que produziram novas formas de poder e agência [distributiva]" (EDWARDS & HECHT 2010: 619), sendo importante enfatizar que as tecnologias "não são, em si próprias, tecnopolítica; ao invés, a prática de usar tecnologias em processos políticos e / ou para fins políticos é que constitui o que se entende por tecnopolítica" (HECHT, 2001: 257). A tecnologia nunca é menos do que a corporização do político. As hierarquias em que o sistema internacional tem assentado – raça, gênero, orientação sexual, religião, etc. (GROSFOGUEL, 2007), projetam-se e reproduzem-se *online*, permeando a tecnopolítica e mostrando a falibilidade do "universalismo digital" (CHAN, 2013).

No contexto de atualização, adaptação e (res)significação que a tecnopolítica (re)cria nos dias de hoje, os Direitos Humanos, enquanto gramática de dignidade humana, passaram cumulativamente a integrar uma dimensão digital, comumente apelidada de "direitos digitais", que muitos veem como uma adaptação dos Direitos Humanos à era digital (MATHIESEN, 2014: 7) e que impulsionam o ativismo de dados enquanto promotor de mudança social (GUTIÉRREZ, 2018). Entre eles, contam-se o direito à informação e à privacidade. Ambos são reconhecidos em diferentes tratados internacionais e documentos com força de *Jus Cogens* (e.g. Arts.º 12, 19 e 27.2 da DUDH; Artsº 17 e 19.2 do Pacto de Direitos Civis e Político). Porém, apesar de, à primeira vista, os direitos digitais parecerem uma atualização ou adaptação linear dos direitos humanos à realidade digital, a mudança da esfera não significa uma mera transposição, mas uma reequação. A questão da esfera, garantia, proteção e reconhecimento dos direitos digitais, no atual contexto tecnopolítico, exige não só competências individuais de literacia que atendem à especificidade, preconceitos e contradições da esfera *online*, mas também a *democratização* de competências críticas de produção, interpretação e interação com e no digital, numa lógica quer individual, quer coletiva.

Enquanto a literacia informacional gira em torno da capacidade de acessar, localizar e avaliar informações, a literacia digital crítica deve ser entendida numa dimensão como a avaliação de conteúdos *online* em relação a representações dominantes, viés, preconceitos e confiabilidade, num contexto comunicacional em rede, onde a difusão de informação circula de forma potencialmente ubíqua por vários canais. Esta capacidade de avaliação deve estar aliada às habilidades de produzir mídia alternativa e de reescrever conteúdos midiáticos de modo a contrabalançar preconceitos, enviesamentos e deturpações (KELLNER E SHARE, 2007). E, como a mídia digital está sujeita a restrições estruturais e inserida em estruturas de poder mais amplas, deve também incorporar, noutra dimensão, conhecimento sobre questões socioeconômicas

relacionadas à Internet, isto é, como a inserção desta em determinado sistema social, político, econômico e corporativo molda a produção, disseminação, acesso e consumo da informação *online* (GREGORY E HIGGINS, 2013), restringindo os potenciais democratizantes da Internet. Deste modo, a literacia digital crítica tem sido interpretada como intrínseca ao engajamento político ideologicamente crítico (POLIZZI, 2020).

2. Vigilância e estado de exceção

A vigilância configura-se hoje enquanto prática organizativa dominante das sociedades modernas contemporâneas - em grande medida, devido a tecnologias efetivas e emergentes como a Internet das Coisas, os serviços de localização e de reconhecimento facial e a concomitante lógica de datificação. Hoje, a arquitetura da vigilância está cada vez mais presente na vida quotidiana, particularmente, enquanto "*dataveillance*" (uma vigilância de alguma forma desprovida do imaginário do controle dos corpos e centrada antes na coleta e organização de dados). Na nossa relação com o Estado e com o setor privado, por questões legais ou como requisito de acesso a determinados produtos e serviços, de forma consciente ou inconsciente, concedemos a estes atores cada vez mais dados e informação pessoal e privada (GOOLD, 2010). Apesar das dinâmicas novas em que assenta e que, por sua vez, gera nos dias de hoje, a vigilância, enquanto processo social e político, nunca esteve, porém, ausente das "rotinas institucionais" ou da própria "sociabilidade humana" (LYON, HAGGERYTY E BALL, 2012: 1). A metáfora do panóptico apresentada por Bentham e recuperada por Foucault (2013) é uma das melhores sínteses dos processos e dinâmicas que a vigilância integra: uma estrutura que permite que poucos, sem serem vistos, vigiem muitos. Ao ser utilizada para identificar, rastrear e/ou monitorizar através de observação direta ou mediada (CHANDLER E MUNDAY, 2011: 414), a vigilância tem alguma elasticidade, podendo ter conotações positivas e negativas. Por exemplo, o controlo que lhe dá corpo pode ser utilizado tanto para proteger como para reprimir. Porém, no contexto de vigilância de dados, o *panóptico* de Foucault (2013) tem dado lugar ao *panspectron* de Braman (2006), pois este não opera sob as mesmas coordenadas cartesianas de tempo e espaço do primeiro, mas no 'espaço dos fluxos', onde as práticas sociais desterritorializadas podem acontecer simultaneamente (CASTELLS, 2007).

Na atual "sociedade de plataformas", regulada pelas aplicações do ecossistema digital global, majoritariamente, corporativo, algoritmicamente conduzida e alimentada por dados (VAN DIJCK; POELL E DE WAAL, 2018), o *panspectron* reúne informações simultaneamente sobre tudo e toda a gente e, devido a um leque de recursos, entre eles aplicações digitais, para tentar controlar a transmissão do coronavírus entre os corpos, podemos falar de um *panspectron pandêmico*. Neste contexto, em vez de dura e imposta, a vigilância constitui-se como líquida, baseada no conluio dos usuários de aplicações, seduzidos pelo consumo ou, no quadro de "exceção" da pandemia, pelo medo, na geração de um fluxo de dados tão fluido quanto os arranjos sociais contemporâneos, que são de curto prazo, frágeis e fragmentários (BAUMAN E LYON, 2014).

No contexto democrático e face a ameaças que eles próprios reconhecem enquanto tal, cidadãos e cidadãs têm-se mostrado predispostos a ceder alguns dos seus direitos e liberdades se, em retorno, lhes for oferecida proteção, abrindo-se as portas para a construção de um "aparato ideológico assente [e negociado] na realidade da necessidade" (FERREIRA, 2019: 329). A relação entre Estado e cidadãos passa a ser investida da "linguagem de exceção" e as "leituras excecionalistas de desenvolvimentos sociopolíticos passam a enquadrar problemas e soluções políticas de uma forma particular, excluindo o significado político da prática social" (HUYSMANS, 2008: 165), com impacto na democracia.

Isto porque

> "as diferentes modalidades através das quais a flexibilização das normas democráticas e dos princípios do Estado de direito se afirmam como um novo normal em momentos de necessidade (...) põem em causa a separação de poderes e o princípio da produção democrática do direito" (FERREIRA, 2019: 329)

Correndo o risco de se enraizar como o novo normal. As reivindicações de excecionalidade exigem que a governação possa transgredir as normas vigentes, criando normas cuja necessidade é diretamente dependente da circunstância (HUYSMANS, 2008: 171-172). Porém, o estado de exceção tem grande probabilidade de, mesmo quando superada a crise que levou à aprovação de medidas excecionais, se constituir como um "paradigma normal de governo" que, apesar de opressivo, passa a ser normalizado (AGAMBEN, 2020). Para Agamben (2020), o que começa como uma medida extraordinária democraticamente aprovada durante um estado de exceção pode, assim, se tornar uma ferramenta dilatada no tempo ou permanente no arsenal governamental assim que a crise que legitimou a exceção esteja superada, impactando liberdades e garantias. Tal como sintetiza Tim Christaens (2020), o argumento de Agamben é que "os poderes draconianos de hoje podem ser o aparato de opressão de amanhã" com a validação gerada pela "cegueira que emana do medo e da urgência" (TEWARI, 2020). Neste contexto, é fundamental uma literacia mediática crítica, para que haja um controle cidadão informado sobre a ameaça, a exceção e as implicações das medidas (aparentemente) excecionais.

3. COVID-19, vigilância e a desinformação em tempos de exceção

A definição da COVID-19 como uma ameaça, bem como o seu enquadramento securitizado deu legitimidade aos governos para promulgar grande parte destas medidas excecionais que servem para combater a pandemia (ROLLAND, 2020). A retórica bélica e o léxico securitário - "ameaça", "combate", "guerra", "inimigo" - que usualmente a compõem foram usados por variadíssimos líderes, nomeadamente Emmanuel Macron,[65] Boris Johnson,[66] António Guterres,[67] e Tedros Adhanom Ghebreyesus[68], entre outros. Esta opção discursiva securitizadora veio no sentido de enquadrar a situação da pandemia, mas, sobretudo, o tipo de medidas que a situação (assim desenhada) exigia por forma a promover a sua aceitação junto do público/audiência e instituir o *panspectron pandêmico*. Sendo o processo de securitização "uma forma específica de politização que faz um apelo aos profissionais de segurança", ele não aponta só para o fato de que "*temos de resolver o problema*, mas que tal tem de ser feito *de uma forma coerciva*" (ARADAU et al. 2006: 460). Esta lógica de securitização facilitou a aprovação de "estados de exceção" - como aconteceu em 84 Estados, muitos deles democráticos[69], mas também de medidas a granel (i.e., *download* de aplicativos de rastreamento) que, não sendo formalmente enquadradas no estado de exceção, assumem o carácter (e aceitação) excecional da circunstância que os cria e legitima. Assim, e numa tentativa de conter a doença, e a par da proibição ou limitação de mobilidade, as chamadas medidas de "biovigilância" estiveram no centro das abordagens de muitos governos fazendo com que, por exemplo, o *Digital Freedom Fund* equipare 2020 à materialização de "um mundo panótico a uma escala nunca vista". Muitas destas ferramentas equiparam-se às tradicionalmente usadas em contextos militarizados, como o combate ao terrorismo ou à espionagem internacional, mas desta feita dirigias aos seus cidadãos e cidadãs (SCHACHAR, 2020).

Entre o aparato do *panspectron pandêmico*, que emerge da interseção entre o atual contexto de "exceção" da pandemia e a regulação societal do tráfego social e econômico na "sociedade de plataformas" (VAN DIJCK; POELL E DE WAAL, 2018), contam-se aplicativos de rastreamento (e.g. 120 aplicativos estavam disponíveis

[65] Ver: https://www.bbc.com/news/av/51917380

[66] Ver: https://www.theguardian.com/world/2020/mar/17/enemy-deadly-boris-johnson-invokes-wartime-language-coronavirus

[67] Ver: https://unric.org/en/covid-19-we-are-at-war-with-a-virus-un-secretary-general-antonio-guterres/ .

[68] Ver: https://www.npr.org/sections/coronavirus-live-updates/2020/03/26/822123471/we-are-at-war-who-head-says-warning-millions-could-die-from-covid-19?t=1610394220459.

[69] Entre os 84 países de que há registro, contam-se, África do Sul, Arménia, Bolívia, Botsuana, Brasil, Burkina-faso, Estónia, Espanha, EUA, Finlândia, França, Geórgia, Índia, Itália, Japão, Jordânia, Libéria, Letónia, Mali, Marrocos, México, Moldávia, Nova Zelândia, Roménia, Paraguai, Perú, Portugal, Reino Unido, Senegal (Centre for Civil and Political Rights, 2020).

em 71 países em 13 de Outubro de 2020, sendo que 19 desses aplicativos com um total de 4 milhões de *downloads* não tem políticas de privacidade), medidas de rastreamento digital (e.g. 60 foram introduzidas em 38 países), para além de iniciativas de vigilância física (e.g. o recurso a *drones* para vigiar as ruas aquando dos confinamentos foi utilizado em 22 países) (WHOODHAMS, 2020), aplicativos de geolocalização das pessoas com teste positivo à COVID-19 ou algoritmos que, a partir de informações sobre saúde, histórico de viagens e contatos, condicionam os movimentos dos cidadãos (SCHACHAR, 2020). Estas formas através das quais os Estados monitorizam cidadãos e cidadãs e quem reside no seu território são cada vez mais extensas e, não raras vezes, suportados por empresas privadas (DIGITAL FREEDOM FUND, 2020), frequentemente, adquirindo também dados dos seus consumidores e implementando novas tecnologias para vigiar locais de trabalho e clientes (ELECTRONIC FRONTIERS FOUNDATION, 2021).

De acordo com Goodes (2020), a partir de um estudo desenvolvido em finais de 2019 a nível global, há uma desconsideração da ética "*privacy by design*" na construção deste tipo de aplicativos e que encontra eco na biovigilância de resposta à COVID-19. Segundo esse estudo, a grande maioria dos aplicativos construídos e validados por governos não estão suficientemente protegidos contra "*reverse engineering*" e potencial exploração, o que significa que são fáceis de *hackear* e suscetíveis de dar espaço para a criação, por exemplo, de clones falsos, com implicações para a segurança de cidadãos e cidadãs e de confiança na tecnologia e nas instituições. Do lado dos cidadãos e do debate político sobre a matéria, em grande medida devido à tecnicidade, mas também à securitização da pandemia, a ausência de um conhecimento detalhado sobre as condições e implicações desta biovigilância tem sido a tendência mais comum.

No caso do aplicativo *NHS Covid-19*, no Reino Unido, a recolha de informação é muito reduzida, estando encriptada e armazenada com recurso a pseudônimos, mas acessível a terceiros e o *Contact Tracing,* nos EUA, recolhe apenas a geolocalização, de forma não encriptada nem anonimizada, estando acessível a terceiros, o aplicativo *Smittestopp,* na Noruega, tem acesso a uma vasta panóplia de informação anonimizada, mas não encriptada e sendo acessível a terceiros. Já, por exemplo, o aplicativo *SAIYAM - Track & Trace Together,* na Índia, com informação muito detalhada, mas encriptada, não acessível a terceiros e com recurso a pseudônimo, ou o *PeduliLindungi,* na Indonésia, que exige informação pessoal e não garante anonimato, mas é encriptada e não precisa pedir acesso a terceiros têm definições mais consentâneas com os direitos digitais do que o aplicativo Norueguês (WOODHAMS, 2020; TOP10VPN, 2020). Tal, revela que Estados com bons índices de Desenvolvimento Humano, de Internet Inclusiva e de Liberdade de Imprensa não têm necessariamente aplicativos mais consentâneos com a garantia e proteção dos Direitos Humanos digitais, nomeadamente o direito à privacidade, o que visibiliza a novidade, complexidade e não-linearidade da desinformação face à tecnopolítica e à necessidade de literacia digital em contexto democrático.

Em termos de adesão, registou-se uma tendência elevada em termos de número de *downloads*, mas de alguma forma reduzida, tendo em conta a população adulta de cada país. Em Janeiro de 2021 e de acordo com dados da Google Play, no Brasil, o *COVID - SUS* contabilizava mais 5.000.000; no Gana, o *GH Covid-19 Tracker App* contava com mais de 5,000 descargas, na Indonésia, o *PeduliLindungi* tinha mais de 1,000,000; na Noruega, o *Smittestopp* contava com mais de 100,000; na Polónia o *ProteGO Safe* contava com mais de 1,000,000; o *STAYAWAYCOVID*, em Portugal, tinha já 1,000,000 e o *NHS Covid-19*, no Reino Unido, contabilizava mais de 5,000,000 (WOODHAMS, 2020; TOP10VPN, 2020; GOVERNO DE PORTUGAL, 2020). Porém, a contabilização de todas estas descargas perfaz um total de, no mínimo, 11.005.000 corpos, movimentos e/ou pessoas biovigiadas cujas informações são geridas por entidades estatais, mas que podem ser, na sua maioria, acedidas por terceiros e poderão rastrear pessoas em novas (ou renovadas) relações de poder, em espaços políticos de mobilidade/imobilidade (SHACHAR, 2020), de securitização ou des-securitização.

Nos EUA, no atual contexto de luta do movimento *Black Lives Matter* e do combate à pandemia COVID-19, a lei do Estado do Minnesota, por exemplo, não proíbe, especificamente, autoridades estatais de

acessar ou usar a informação recolhida por aplicativos ou outros instrumentos de rastreamento no contexto do combate à pandemia para questões policiais ou judiciais atuais ou futuras (RAHMAN, 2020). Os aplicativos de "biovigilância" afetam de forma distinta as diferentes subjetividades (ELECTRONIC FRONTIERS FOUNDATION, 2021). Não por acaso que o diretor-executivo da OMS, Michael Ryan, alertou, em 25 de março de 2020: que se deve "ter sempre em mente, especialmente quando se trata de coletar informações sobre cidadãos individuais ou rastrear o seu paradeiro ou movimento, uma que há sempre implicações muito sérias ao nível da proteção de dados."[70]A arquitetura da *dataveillance* é uma arquitetura de poder e, como tal, encerra uma lógica de privilégio e de discriminação, de segurança e de insegurança, de hegemonia e de contra-hegemonia A natureza tecnicista dos atuais mecanismos de biovigilância digital, a par de um contexto de securitização, propende para normalizar esta arquitetura para além da exceção que as legitima, negligenciando uma abordagem interseccional às questões da vigilância e impactando de forma diferenciada a garantia e proteção de Direitos Humanos e, com isso, a qualidade democrática das sociedades contemporâneas.

Conclusão

Ainda que o termo vigilância e suas variantes não seja uma característica específica das atuais sociedades de plataformas (VAN DIJCK; POELL E DE WAAL, 2018), com o surgimento da ecologia global de plataformas digitais, essencialmente, controlada por empresas tecnológicas que geram lucro através da monetização dos dados coletados por meio dos aplicativos, geralmente vendendo-os a terceiros (ZUBOFF, 2019), e como as revelações da Wikileaks, de Edward Snowden e o escândalo da Cambridge Analytica demonstraram, a internet fez com o que dispositivo societal panóptico evoluísse para o *panspectron* (BRAMAN, 2006), um aparato de vigilância "datificado", em fluxo, que implode barreiras espácio-temporais. No quadro de exceção dilatada e securitizado da pandemia COVID-19, a emergência do '*panspectron pandêmico*' exige que os debates e as políticas sobre democracia, biovigilância e direitos digitais vão além de uma linear adaptação do que já existe no contexto *offline* à ecologia global e, essencialmente, corporativa das plataformas digitais.

Nestas (re)definições e (re)significações do digital, as questões da privacidade são essenciais. Sendo um valor e princípio essencial na garantia da dignidade e liberdade individuais, a privacidade funciona como um direito e valor *per se*, mas é também relevante na restrição ao exercício e (ab)uso do poder e à garantia (ou violação) de outros direitos humanos: ao garantir que há um limite sobre o que o Estado e empresas podem saber sobre nós, a privacidade permite proteger a autonomia individual, mas também usar a autonomia no exercício de outros direitos fundamentais (GOOLD, 2010: 43), sendo o inverso também verdade. Os casos ilustrativos de aplicativos de rastreamento criados por diversos Estados no contexto de contenção da pandemia COVID-19, mostram essa necessidade, apontando para duas questões que fecham este capítulo, constituindo, ao mesmo tempo, uma agenda de investigação. A primeira questão é o facto de as medidas para gerir o risco epidemiológico e conter a pandemia assentarem, em larga medida, numa dependência de "solucionismo tecnológico" (MOROZOV, 2013), ou seja, uma "crença de que o digital supera o físico e que se consegue resolver qualquer problema através de um *click*" (BIGO, 2020). O que, no caso concreto das respostas governamentais à COVID-19, tem negligenciado que as respostas - mesmo tecnológicas - à pandemia são sempre políticas e, por isso, com implicações societais estruturantes. A segunda tem a ver com o lugar de mudança em que sempre nos encontramos e em que os limites da ação tecnopolítica do presente estipulam as possibilidades e impossibilidades do futuro. Como afirma Buckley (2020), "mesmo no meio da pandemia, sabemos que ela vai acabar, que a política vai retomar e que terá sido moldada pelos argumentos feitos durante este tempo".

[70] Ver: https://www.who.int/docs/default-source/coronaviruse/transcripts/who-audio-emergencies-coronavirus-press-conference-full-25mar2020.pdf

REFERÊNCIAS

AGAMBEN, G. L'invenzione di un'epidemia. **Quodlibet**, fev. 2020. Disponível em: <https://www.quodlibet.it/giorgio-agamben-l-invenzione-di-un-epidemia>.

AMARAL, I.; SANTOS, S. J. Algoritmos e redes sociais: a propagação de fake news na era da pós-verdade. In: FIGUEIRA, J.; SANTOS, S. (Ed.). ***As fake news e a nova ordem (des)informativa na era da pós-verdade***. Coimbra: Imprensa da Universidade de Coimbra, 2019. p. 63–85.

ARADAU, C.; THIERRY, B.; BASARAN, T.; BIGO, D.; BONDITTI, P.; BÜGER, C.; DAVIDSHOFER, S.; GUILLAUME, X.; GUITTET, E. P.; HUYSMANS, J.; JEANDESBOZ, J.; JUTILA, M.; LOBO-GUERRERO, L.; MCCORMACK, T.; MÄLKSOO, M.; NEAL, A.; OLSSON, C.; PETERSEN, K. L.; RAGAZZI, F.; AKILLI, Y. S.; STRITZEL, H.; MUNSTER, H.; STRITZEL, R. Van; VILLUMSEN, T.; WÆVER, O.; WILLIAMS, M. C. Critical approaches to security in Europe: A networked manifesto. **Security Dialogue**, v. 37, n. 4, p. 443–487, 2006.

BALL, J. **Post-truth: How Bullshit Conquered the World**. London: London, Biteback, 2017.

BATESON, G. **Steps to an Ecology of Mind**. [s.l: s.n.]

BAUMAN, Z.; LYON, D. **Vigilância Líquida**. Rio de Janeiro: Zahar, 2014.

BENSON, T., Twitter Bots Are Spreading Massive Amounts of COVID-19 Misinformation. IEEE Spectrum, 2020. Disponível em: <https://spectrum.ieee.org/tech-talk/telecom/internet/twitter-bots-are-spreading-massive-amounts-of-covid-19-misinformation>.

BRAMAN, S. **Change of State: Information, Policy and Power**. Cambridge: The MIT Press, 2006.

BUCKLEY, M. Democracy in the UK How Worried Should We Be? **Byline Times**, n. 8 April 2020, p. 1–8, 8 abr. 2020. Disponível em: <https://bylinetimes.com/2020/04/08/democracy-in-the-uk-how-worried-should-we-be.

CASTELLS, M. **A era da informação: economia, sociedade e cultura**. Lisboa: Fundação Calouste Gulbenkian, 2007.

CHAN, A. S. **Networking Peripheries. Technological Futures and the Myth of Digital Universalism**. Cambridge/London: The MIT Press, 2013.

CHANDLER, D.; MUNDAY, R. **Oxford Dictionary of Media and Communication**. Oxford: Oxford University Press (OUP), 2011.

CHRISTAENS, T. Critical Legal Thinking –. **Critical Legal Thinking**, mar. 2020. Disponível em: <https://criticallegalthinking.com/2020/03/26/must-society-be-defended-from-agambe>.

CISCO. Consumer Privacy Survey: The Growing Imperative of Getting Data Privacy Right. **Cisco**, n. November, p. 1–14, 2019. Disponível em: <https://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-series-2019-cps.pdf>.

CISCO. **Cisco Annual Internet Report (2018–2023) White Paper**. [s.l: s.n.]. Disponível em: <https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.pdf>.

CLARK, A. D.; NICKELS, A. E. Doubling down on austerity: Framing and coronavirus response. **Administrative Theory and Praxis**, v. 0, n. 0, p. 1–8, 2020. Disponível em: <https://doi.org/10.1080/10841806.2020.1771905>.

COLLINS, P. H. The difference that power makes: Intersectionality and participatory democracy. **Investigaciones feministas**, v. 8, n. 1, p. 19-39, 2017.

DAHL, R. **On democracy**. Veritas Paperbacks, 2020.

DIGITAL FREEDOM FUND **Why COVID-19 is a Crisis for Digital Rights**. Disponível em: <https://edri.org/our-work/why-covid-19-is-a-crisis-for-digital-rights/>. Acesso em: 14 nov. 2020.

EDWARDS, P.; HECHT, G.History and the Technopolitics of Identity: The Case of Apartheird South Africa. **Journal of Southern African Studies**, v. 36. n. 3, p. 619-639, 2010.

F5'S. **Curve of Convenience 2020 Report: The Privacy-Convenience Paradox**. [s.l: s.n.]. Disponível em: <https://www.f5.com/c/apcj-2020/asset/gc-rp-curve-of-convenience?utm_medium=press-release&utm_source=pressrelease&utm_campaign=apcj-ap_ap>.

ENLOE, C. The persistence of patriarchy. **New Internationalist**, 2017. Disponível em: <http://newint.org/columns/essays/2017/10/01/patriarchy-persistence>.

FERREIRA, A. C. **Sociologia do Direito: Uma Abordagem Sociopolítica**. Porto: Vida Económica Editorial, Lda., 2019.

FLAXMAN, S.; GOEL, S.; RAO, J. M. Filter bubbles, echo chambers, and online news consumption. **Public Opinion Quarterly**, v. 80, n. Specialissue1, p. 298–320, 2016.

FOUCAULT, M. **Vigiar e punir**. Lisboa: Edições 70, 2013.

FRASER, N. Rethinking the Public Sphere: A contribution to the critique of actually existing democracy. In: C. CALHOUN (Ed.). **Habermas and the Public Sphere**. London: MIT Press, 1992.

FRÈRE, M.-S. **Afrique Centrale, Médias et Conflits: vecteurs de guerre ou acteurs de paix?** Brussels: G R I P., 2005.

GARRAIO, J.; SANTOS, S. J.; AMARAL, I.; CARVALHO, A. de S. The unimaginable rapist and the backlash against #MeToo in Portugal. **Europe Now: a journal of research and art,** p. 1–13, 2020.

GOODES, G. **The Proliferation of COVID-19 Contact Tracing Apps Exposes Significant Security Risks**. [s.l: s.n.]. Disponível em: <https://www.guardsquare.com/en/blog/report-proliferation-covid-19-contact-tracing-apps-exposes-significant-security-risks>.

GOOLD, B. How Much Surveillance is Too Much ? Some Thoughts on Surveillance , Democracy , and the Political Value of Privacy. In: DW SCHARTUM (Ed.). **Overvåkning i en rettsstat – Surveillance in a Constitutional Government**. Bergen: Fagbokforlaget, 2010. p. 38–48.

GOVERNO DE PORTUGAL. **STAYAWAYCOVID**. Disponível em: <https://stayawaycovid.pt/landing-page/>.

GREGORY, L.; HIGGINS, S. Introduction. In Gregory, L. and Higgins, S. (eds) Information Literacy and Social Justice: radical professional praxis, Library Juice Press, 1–11, 2013.

HABERMAS, J. The Structural Transformatin of the Public Sphere. v. 53, p. 160, 1989.

HECHT, G. Technology, Politics, and National identity in France In ALLEN, M.; HECHT, G. (eds) **Technologies of Power: Essays in Honor of Thomas Parke Hughes and Agatha Chipley Hughes.**Cambridge and London: Massachusetts Institute of Trechnology, p. 253-293, 2001.

HUYSMANS, J. The jargon of exception - On Schmitt, Agamben and the absence of political society. **International Political Sociology**, v. 2, n. 2, p. 165–183, jun. 2008.

JACOBS, R. N.; TOWNSLEY, E. T**he space of opinion: Media intellectuals and the public sphere**. Oxford: Oxford University Press, 2011.

KELLNER, D.; SHARE, J. Toward critical media literacy: Core concepts, debates, organizations, and policy. **Discourse**, v. 26, n. 3, p. 369–386, 2005.

KELLNER, D.; SHARE, J. Critical Media Literacy, Democracy, and the Reconstruction of Education. In Macedo, D. and Steinberg, S. R. (eds) Media Literacy: a reader, Peter Lang, p. 3–23, 2007.

KENDALL, L. Recontextualizing "Cyberspace": Methodological Considerations for On-line Research. In: **Doing Internet Research: Critical Issues and Relations for Examining the Net**. [s.l: s.n.]p. 57–74.

LEDERACH, J. P. **Building Peace: Sustainable Reconciliation in Divided Societies**. Washington DC: UNITED STATES INSTITUTE OF PEACE PRESS, 1997.

LYON, D.; HAGGERTY, K. D.; KIRSTIE BALL. Introducing surveillance studies. In: BALL, K.; HAGGERTY, K. D.; LYON, D. (Ed.). **Handbook of Surveillance Studies**. Oxon: Routledge, 2012. p. 1–12.

LYOTARD, J-F. **A condição pós-moderna**. Lisboa: Gradiva, 1990.

LIVINGSTONE, S. Media literacy and the challenge of new information and communication technologies. **Communication Review**, v. 7, n. 1, p. 3–14, 2004.

LOPES, P. Literacia mediática e cidadania: uma relação garantida?. **Análise Social**, 216, p. 546-580, 2015.

MANAGER, D. privacy. **100 Data Privacy and Data Security statistics for 2020**. Disponível em: <https://dataprivacymanager.net/100-data-privacy-and-data-security-statistics-for-2020. Acesso em: 30 dez. 2020.

MATHIESEN, K. Human Rights for the Digital Age. **Journal of Mass Media Ethics: Exploring Questions of Media Morality**, v. 29, n. 1, p. 2–18, 2014.

MCNAIR, B. **An Introduction to Political Communication**. London and New York: Routledge, 2003. v. 03.

MORGAN, S. Fake news, disinformation, manipulation and online tactics to undermine democracy. **Journal of Cyber Policy**, 3.1, p. 39-43, 2018. Disponível em: <https://www.tandfonline.com/doi/full/10.1080/23738871.2018.1462395>.

NICK, R. Fake news: belief in post-truth. **Library Hi Tech**, v. 35, n. 3, p. 386–392, 1 jan. 2017. Disponível em: <https://doi.org/10.1108/LHT-03-2017-0062>.

OMS. Novel Coronavirus (2019-nCoV) Situation Report-13, 2020. Disponível em: <https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200202-sitrep-13-ncov-v3.pdf>.

POLIZZI, G. Information literacy in the digital age: why critical digital literacy matters for democracy. In: Goldstein, Stéphane, (ed.) **Informed societies: why information literacy matters for citizenship, participation and democracy**. Facet Publishing, London, UK, p. 1-23, 2020. Disponível em: <http://eprints.lse.ac.uk/102993/1/Polizzi_information_literacy_in_the_digital_age_published.pdf>.

POSTER, M. **A Segunda Era dos *Media***. Lisboa: Celta, 2000.

POSTER, M. Digital Networks and Citizenship. **PMLA Special Topic: Mobile Citizens, Media States**, v. 117, n. 7, p. 98–103, 2002. Disponível em: <https://www.netsafe.org.nz/digital-citizenship-and-digital-literacy/>.

POTTER, W. J. The state of media literacy. **Journal of Broadcasting and Electronic Media**, v. 54, n. 4, p. 675–696, 2010.

QUINTANILHA, T. L.; DA SILVA, M. T.; LAPA, T. Fake news and its impact on trust in the news. Using the portuguese case to establish lines of differentiation. **Communication and Society**, v. 32, n. 3, p. 17–33, 2019.

RAHIMI, S. **Meaning, Madness and Political Subjectivity**. [s.l.] Routledge, 2015.

RAHMAN, ZARA. Black Lives Matter protesters aren't being tracked with Covid-19 surveillance tech. Not yet. **The Correspondent**. Disponível em: https://thecorrespondent.com/507/black-lives-matter-protesters-arent-being-tracked-with-covid-19-surveillance-tech-not-yet/569187644025-767f5154.

ROCHLIN, N. Fake news: belief in post-truth. **Library Hi Tech**, v. 35, n. 3, p. 386–392, 18 set. 2017. Disponível em: <http://www.emeraldinsight.com/doi/10.1108/LHT-03-2017-0062>.

SANTOS, B. D. S. **Democratizing Democracy: Beyond the Liberal Democratic Canon**. [s.l.] Verso, 2007.

SANTOS, S. J. New Technologies Impact on Conflicts. In: LEAL FILHO, W.; AZUL, A. M.; BRANDLI, L.; LANGE SALVIA, A.; ÖZUYAR, P. G.; WALL, T. (Ed.). **Peace, Justice and Strong Institutions. Encyclopedia of the UN Sustainable Development Goals**. [s.l.] Springer International Publishing, 2021a. p. 1–11.

SANTOS, S. J. Admirável Mundo Velho: os (e-)continuuns do poder nas Relações Internacionais da era digital. In: PUREZA, J. M.; FERREIRA, M. F. (Ed.). **Emancipar o mundo. Teoria crítica e Relações Internacionais**. [s.l.] Almedina, 2021b.

SANTOS, S. J.; ARAÚJO, S.; CRAVO, T. A. MEDIA INTERVENTION IN POST-WAR SETTINGS: INSIGHTS FROM THE EPISTEMOLOGIES OF THE SOUTH. **COMMONS: Revista de Comunicación y Ciudadanía Digital Publicación**, v. 5, n. 2, p. 37–63, 2016.

SHACHAR, A. Bio-surveillance, invisible borders and the dangerous after-effects of COVID-19 measures. **Open Democracy**, n. June 2020, 2020. Disponível em: <https://www.opendemocracy.net/en/pandemic-border/bio-surveillance-invisible-borders-and-dangerous-after-effects-covid-19-measures/>.

SILVEIRINHA, M. J. Democracia deliberativa e reconhecimento: Repensar o espaço público. In: CORREIA, J. C. (Ed.). **Comunicação e Política**. Estudos em ed. Covilhã: LabCom Books, 2008. p. 139–169.

STATISTA. **Active Internet Users**. Disponível em: <https://www.statista.com/statistics/617136/digital-population-worldwide/>. Acesso em: 30 dez. 2020a.

STATISTA. **Mobile share of organic search engine visits in the United States from 4th quarter 2013 to 4th quarter 2019, by platform**. Disponível em: <https://www.statista.com/statistics/275814/mobile-share-of-organic-search-engine-visits/>. Acesso em: 30 dez. 2020b.

STATISTA. **Global opinion on concern about online privacy 2019, by region Published by J. Clement, Sep 11, 2020 This statistic presents the share of global internet users who have some degree of concern about their online privacy compared to a year ago as of Februar**. Disponível em: <https://www.statista.com/statistics/373338/global-opinion-concern-online-privacy/>. Acesso em: 30 dez. 2020c.

STEINBERG, S. R. Reading Media Critically. In: STEINBERG, D. M. S. R. (Ed.). **Media Literacy. A Reader.** New York: Peter Lang, 2009. p. xviii–xv.

TERRIQUEZ, V.; BRENES, T.; LOPEZ, A. Intersectionality as a multipurpose collective action frame: The case of the undocumented youth movement. **Ethnicities**, n. 18, v. 2, p. 260-276, 2018.

TEWARI, A. Critical Legal Thinking –. **Critical Legal Thinking**, abr. 2020. Disponível em: <https://criticallegalthinking.com/2020/04/09/begin-from-the-beginning-revisiting-agamben-critique-in-times-of-corona/>.

TOP10VPN. **COVID-19 Digital Rights Tracker Supporting Data**. Disponível em: <https://docs.google.com/spreadsheets/d/1enCBRLVCo2Dp2B0AB3tEYvLc279i5LUuoGCzoelz8aQ/edit#gid=1023364174.>. Acesso em: 10 jan. 2020.

TUCHMAN, Gaye. The Currency of Democracy: Politics, the Media, and Corporate Control. **Contemporary Sociology: A Journal of Reviews**, v. 42, n. 2, 2013. Disponível em: <https://journals.sagepub.com/doi/full/10.1177/0094306113477380d>.

VAIDHYANATHAN, S. **The Googlization of everything: (and why we should worry)**. University of California Press, 2012.

VAN DIJCK, J.; POELL, T.; DE WAAL, M. **The platform society: Public values in a connective world**. New York, NY: Oxford University Press, 2018.

WEBER, R. H. Internet of things–governance quo vadis?. **Computer Law & Security Review**, v. 29, n. 4, p. 341-347, 2013.

WEBFX. **Internet in Real Time**. Disponível em: <https://www.webfx.com/internet-real-time/>. Acesso em: 30 dez. 2020.

WILLS, D.; REEVES, S. Facebook as a political weapon: Information in social networks. **British Politics**, v. 4, n. 2, p. 265–281, 2009.

WOODHAMS, S. COVID-19 Digital Rights Tracker. **Top10Vpn**, p. 1–35, 2020. Disponível em: <https://www.top10vpn.com/research/investigations/covid-19-digital-rights-tracker/>.

ZUBOFF, S. **The age of surveillance capitalism: The fight for a human future at the new frontier of power.** New York, NY: Public Affairs, 2019.