



ANOTAÇÕES SOBRE INFRAESTRUTURA DE INTERNET 5G, DATAFICAÇÃO E COLONIALISMO DE DADOS

NOTES ON 5G INTERNET INFRASTRUCTURE, DATAFICATION AND DATA COLONIALISM

Mauricio de Souza Fanfa¹

RESUMO

Objetivamos apresentar três tópicos de estudo que podem contribuir para o debate acerca de comércio internacional, tecnologias digitais e políticas públicas. Primeiro, o enquadramento teórico da mediação, especialmente o conceito de dataficação. Depois, o conceito de colonialismo de dados. Por último, os estudos de infraestrutura. O texto trata-se de um ensaio e, teórico-metodologicamente, propomos o que tem se chamado de inversão infraestrutural. Também analisamos uma sessão da Comissão de Ciência e Tecnologia, Comunicação e Informática (CCTCI) da Câmara dos Deputados sobre a Internet 5G; uma entrevista dada pelo vice-presidente Hamilton Mourão sobre a relação entre o Brasil e a empresa chinesa Huawei; e o documento lançado pelo Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC) declarando estratégias para a implementação do 5G (MCTIC, 2019). Exploramos questões acerca da segurança da informação e as vulnerabilidades da infraestrutura de Internet. Por fim, reiteramos a importância de auditoria das tecnologias de comunicação e de investimentos em segurança da informação.

Palavras-chave: 5G; infraestrutura de Internet; mediação; segurança da informação.

ABSTRACT

We aim to present three topics of study that can contribute to the debate about international commerce, digital technologies and public policies. First, the theoretical framework of mediatization, especially the concept of datafication. Secondly, the concept of data colonialism. Last, infrastructure studies. The present text is an essay and, methodologically, we propose what is being called infrastructure inversion. We also analyse a session of the Committee on Science and Technology, Communication and Information of the Brazilian Chamber of Deputies on 5G Internet; an interview given by vice-president Hamilton Mourão on the relation of Brazil and the Chinese company Huawei; and a document by the Ministry of Science, Technology, Innovation and Communication declaring strategies for 5G implementation. We explore questions about information security and vulnerabilities of Internet infrastructure. Finally, we reaffirm the importance of communication technology audit and investments in information security.

Keywords: 5G; information security; Internet infrastructure; mediatization.

¹ Doutorando em Comunicação (POSCOM UFSM). Mestre em Comunicação (POSCOM UFSM). Bacharel em Comunicação, hab. em Produção Editorial (UFSM). mauriciofanfa@mail.ufsm.br



INTRODUÇÃO

O presente trabalho tem como objetivo refletir acerca do enquadramento teórico da midiatização – especialmente os conceitos de digitalização e dataficação como postos por Nick Couldry e Andreas Hepp² – como forma de pensar o momento contemporâneo da construção de infraestrutura de Internet 5G e Internet das Coisas (IdC). Pensar a dataficação no contexto da infraestrutura de Internet envolve pensar também questões de vigilância, espionagem industrial, privacidade, entre outros.

Produzimos nosso texto como um ensaio e, teórico-metodologicamente, propomos uma inversão infraestrutural, nos termos de Bowker e Star³: “inversão infraestrutural é reconhecer as profundidades da interdependência dos sistemas e padrões técnicos, por um lado, e o real trabalho das políticas e da produção de conhecimento, por outro”⁴. Trata-se de uma tentativa de valer-se das infraestruturas, tecnologias e sistemas de larga escala em geral para colher considerações e dados empíricos sobre questões sociais anteriores, compreensão que marca os Estudos de Infraestrutura.

Complementamos empiricamente este trabalho com três materiais para análise e consideração. Primeiro, de arquivo em vídeo de sessão da Comissão de Ciência e Tecnologia, Comunicação e Informática (CCTCI) da Câmara dos Deputados no dia 15/05/2019, quando a comissão discutiu a implementação da tecnologia 5G.⁵ Depois, de uma entrevista dada pelo vice-presidente Hamilton Mourão defendendo a presença no Brasil da empresa chinesa Huawei – líder mundial em tecnologia 5G e alvo de sanções estratégicas nos Estados Unidos.⁶ Enfim, o documento lançado pelo Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC) declarando estratégias para a

² COULDRY, N.; HEPP, A. *The Mediated Construction of Reality*. Cambridge: Polity Press, 2016.

³ BOWKER, G. C.; STAR, S. L. *Some Tricks of the Trade in Analyzing Classification*. BOWKER, G. C.; STAR, S. L. *Sorting things out: classification and its consequences*. Cambridge: The MIT Press, 1999.

⁴ No original: “*Infrastructural inversion means recognizing the depths of interdependence of technical networks and standards, on the one hand, and the real work of politics and knowledge production on the other.*”

⁵ Comissão de Ciência e Tecnologia, Comunicação e Informática, Audiência Pública Conjunta das Comissões CCTCI e CDU, Tema: “A tecnologia 5G”. Câmara dos Deputados. Brasília: Câmara dos Deputados, 15 mai. 2019. Disponível em: <https://www.camara.leg.br/evento-legislativo/55263>. Acesso em: 19 jun. 2019.

⁶ ARAÚJO, C.; RITTNER, D.; MURAKAWA, F. Brasil descarta vetar presença da Huawei em 5G, avisa Mourão. *Valor Econômico*, [s.l.], [s.n.], 7 jun. 2019. Disponível em: <https://www.valor.com.br/brasil/6296401/brasil-descarta-vetar-presenca-da-huawei-em-5g-avisa-mourao>. Acesso em: 19 jun. 2019.



implementação do 5G.⁷

Buscamos, neste trabalho, fazer coro com outras pesquisas e análises – que serão devidamente apresentadas e comentadas – acerca da possibilidade, no cenário que se desenha, de espionagem industrial no nível do que se tem chamado de *big data*. Em linhas gerais, se antes as corporações e agências de inteligência tinham acesso a dados pessoais, mensagens e e-mails – como sugerem as revelações de Edward Snowden em 2013^{8, 9} –, com a 5G e a IdC, especula-se que tais corporações e agências terão acesso direto e antecipado a dados gerados por sensores e demais processos de automação e conectividade.

Na seção seguinte, apresentamos o conceito de mediatização e dataficação. Na outra seção, apresentamos o Estudo de Infraestruturas como forma de pensar a relação entre tecnologia e sociedade. Depois, apresentamos algumas considerações sobre como o debate acerca da Internet 5G apresenta-se no Brasil. Concluimos o texto reiterando a importância de auditoria das tecnologias de comunicação e de investimentos em segurança da informação e em pesquisas na área.

1 A DATAFICAÇÃO COMO UMA ONDA DA MEDIATIZAÇÃO

A mediatização apresenta-se como um arcabouço teórico para se pensar a relação entre a mídia e outras transformações e processos sociais ao longo da história e contemporaneamente. Para Couldry e Hepp¹⁰, são três as ondas da mediatização: mecanização, eletrificação e digitalização. De acordo com o argumento dos autores, a mecanização é marcada pela industrialização e pela prensa de tipos móveis; a eletrificação é marcada pela eletricidade e pelas tecnologias de radiotransmissão e televisão; e a

⁷ MCTIC. Estratégia brasileira de redes de quinta geração (5G): versão para consulta pública, 2019. Disponível em:

<https://www.mctic.gov.br/mctic/export/sites/institucional/sessaoPublica/arquivos/estrategia5g/Documento-base-da-Estrategia-Brasileira-de-5G.pdf>. Acesso em: 4 jul. 2019.

⁸ GREENWALD, G. *Sem lugar para se esconder*: Edward Snowden, a NSA e a espionagem do governo americano. Rio de Janeiro: Sextante, 2014.

⁹ BAUMAN, Z. et al. Após Snowden: Repensando o Impacto da Vigilância. *Revista ECO-Pós*, Rio de Janeiro, v. 18, n. 2, p. 8-35, 2015. DOI: <https://doi.org/10.29146/eco-pos.v18i2.2660>

¹⁰ COULDRY, N.; HEPP, A. *Op. cit.*



digitalização é marcada pelo armazenamento e processamento de informação em sistemas binários e conectados.

A partir da leitura de Couldry e Hepp¹¹, podemos dizer que tais ondas não são momentos estanques na história da relação entre mídia e sociedade: elas se afetam mutuamente, correlacionam-se, sobrepõem-se, resolvem algumas contradições ao mesmo tempo que criam outras. Também não são forças de simples determinação tecnológica: pelo contrário, são momentos onde os diversos agentes sociais constroem paisagens midiáticas diferentes para determinados fins.

A midiatização, aqui, é um conceito que preza pela contextualização social e histórica da relação entre mídia, tecnologia e sociedade como um processo. A expressão busca chamar atenção para o crescente lugar de destaque das mídias nas diversas relações sociais. Friedrich Krotz¹² conceitua a midiatização como um metaprocesso, um processo em relação com outros processos, tal qual a globalização, a individualização, a comoditização.

Couldry e Hepp¹³ ainda apontam a possibilidade do desdobramento da digitalização em uma quarta onda de midiatização, a dataficação. Tal onda está associada a uma incorporação muito mais intensa da mídia nos processos sociais através da produção e captação massiva de dados, fenômeno comumente chamado de *big data*. Trata-se de coleta massiva de dados para categorização, *marketing*, personalização de *feed* de *sites* de mídias sociais, automação, tomadas de decisão, entre outros.

Em outro texto, Nick Couldry e Ulises Mejias¹⁴ expõem a questão colonial na problemática da dataficação. De acordo com os autores, os movimentos recentes de empresas, indústrias, governos e outras organizações pela extração e gerenciamento de dados visa o lucro capitalista e se organiza de forma colonial. “Colonialismo de dados combina as práticas predatórias de extração do colonialismo histórico com os métodos abstratos de quantificação da computação”^{15, 16}.

¹¹ *Ibid.*

¹² KROTZ, F. The meta-process of “mediatization” as a conceptual frame. *Global Media and Communication*, v. 3, n. 3, p. 256-260, 2007. Disponível em:

<http://journals.sagepub.com/doi/10.1177/17427665070030030103>. Acesso em: 4 jul. 2019.

¹³ COULDRY, N.; HEPP, A., *op. cit.*

¹⁴ COULDRY, N.; MEJIAS, U. A. Data Colonialism: Rethinking Big Data’s Relation to the Contemporary Subject. *Television & New Media*, v. 20, n. 4, p. 336-349, 2018. DOI:

<https://doi.org/10.1177/1527476418796632>

¹⁵ *Ibid.*, p. 2



A ideia de colonialismo de dados envolve uma nova forma de pensar as práticas conhecidas como *big data*. Não se tratam, apenas, de dados sendo massivamente gerados, extraídos e analisados, mas sim de uma apropriação em função do capital – e, portanto, do lucro das corporações – análoga à condição colonial histórica. Segundo Couldry e Mejias¹⁷, tais fluxos de dados acontecem de maneira global, em relações de desigualdade. Para os autores, o epicentro do fenômeno não é mais um único polo de poder colonial europeu, mas sim os Estados Unidos e a China.

Para Couldry e Mejias¹⁸, parte desse processo envolve a concentração econômica no mercado das plataformas digitais, como Facebook, Amazon e Google. A relação entre usuários e plataformas baseia-se em rastreamento e produção de dados. E tal lógica espalha-se para outros setores, como a logística industrial, onde estas e outras plataformas protagonizam processos de concentração nas aplicações de IdC.

Couldry e Mejias¹⁹ guiam-se pela noção de que angariar dados e usá-los para extrair lucro não é usar uma forma natural de conhecimento, mas uma “forma de extração motivada comercialmente que promove determinados interesses econômicos ou governamentais”^{20, 21}. Os métodos quantitativos de gerar dados abstratos empregados pelos sistemas dessas plataformas servem a tais interesses predatórios.

No mercado de *smartphones*, por exemplo, diversos desenvolvedores de aplicativos e fabricantes de celulares coletam dados de maneira abusiva, fenômeno documentado por Gamba *et al.*²² e Razaghpanah *et al.*²³. Frequentemente os dados coletados de pessoas em um país terminam em servidores de rastreamento e gerenciamento de anúncios em outros países, principalmente nos Estados Unidos²⁴. Além da possibilidade de *backdoors*, quebras

¹⁶ No original: “*Data colonialism combines the predatory extractive practices of historical colonialism with the abstract quantification methods of computing*”.

¹⁷ *Ibid.*

¹⁸ *Ibid.*

¹⁹ *Ibid.*

²⁰ *Ibid.*, p. 11.

²¹ No original: “*a commercially motivated form of extraction that advances particular economic and/or governance interests*”.

²² GAMBA, J. *et al.* *An Analysis of Pre-installed Android Software*. arXiv:1905.02713, 2019. Disponível em: <http://arxiv.org/abs/1905.02713>. Acesso em: 1 jul. 2019.

²³ RAZAGHPANAH, A. *et al.* *Apps, Trackers, Privacy, and Regulators: A Global Study of the Mobile Tracking Ecosystem*. In: *PROCEEDINGS 2018 NETWORK AND DISTRIBUTED SYSTEM SECURITY SYMPOSIUM 2018*, San Diego, CA. Anais... Disponível em: https://www.ndss-symposium.org/wp-content/uploads/2018/02/ndss2018_05B-3_Razaghpanah_paper.pdf. Acesso em: 1 jul. 2019.

²⁴ *Ibid.*, p. 10.



de segurança ou acesso remoto sem consentimento. Se tratam de vulnerabilidades de fábrica, implementadas pelos fabricantes ou por terceiros no processo de fabricação.

Além dos dados gerados pelos nossos hábitos de consumo ou socialização *online*, há também a preocupação com os dados gerados por aplicações industriais de IdC. Isabelle Carbonell²⁵, por exemplo, denuncia um possível abuso da coleta de dados pelos fabricantes de *software* e dispositivos para especulação no mercado de commodities e desenvolvimento de tecnologias proprietárias.

Por exemplo, o *Climate FieldViewPro* da Monsanto, serviço digital que utiliza IdC – sensores, GPS e computadores de bordo em tratores e outras máquinas rurais – para levantamento de dados à serviço do contratante. Tal relação coloca certas empresas em posições privilegiadas de inteligência, pois teriam acesso aos dados gerados por todos os seus clientes²⁶. Tal relação se repete em vários outros setores industriais onde há empresas prestadoras de serviços de automação digital.

Para Couldry e Mejias, tais aplicações industriais de IdC tem como objetivo “instalar em cada ferramenta da vida humana a capacidade de continuamente e autonomamente coletar e transmitir dados através de sistemas controlados em instâncias privadas e de segurança incerta”^{27, 28}. Daí que, de acordo com os estudos de midiaticização e de colonialismo de dados, o momento atual tem uma tendência a buscar, incentivar, aceitar e explorar a geração de dados sobre as atividades humanas.

2 QUESTÕES DE INFRAESTRUTURA MIDIÁTICA

A IdC exige conexões à Internet de velocidade considerável e baixa latência, como é a tecnologia 5G. A tecnologia 5G, em linhas gerais, utiliza frequências eletromagnéticas específicas que possibilitam conexões mais estáveis e exigem equipamentos diferentes dos que estamos acostumados: no lugar de grandes antenas distantes, teremos pequenas

²⁵ CARBONELL, I. M. The ethics of big data in big agriculture. *Internet Policy Review*, v. 5, n. 1, 2016. Disponível em: <https://policyreview.info/articles/analysis/ethics-big-data-big-agriculture>. Acesso em: 19 jun. 2019.

²⁶ *Ibid.*

²⁷ COULDRY, N.; MEJIAS, U. A., *op. cit.*, p. 9.

²⁸ No original: “Consider the fast-growing “Internet of Things.” The goal is clear: to install into every tool for human living the capacity to continuously and autonomously collect and transmit data within privately controlled systems of uncertain security.”



antenas mais próximas dos dispositivos. No Brasil, a expectativa é que os leilões dos espectros eletromagnéticos relativos à 5G aconteçam no ano de 2020.

Susan Leigh Star²⁹ comenta sobre como as infraestruturas são comumente vistas como o substrato de outras coisas: um espaço já pronto, quase invisível e desconsiderável. A autora propõe “ver infraestrutura como parte da organização humana, e tão problemática quanto qualquer outra”^{30, 31}. Assim, o que se torna objeto de estudo é a relação da infraestrutura com outros contextos sociais que se dão a partir dela.

Lisa Parks e Nicole Starosielski³² – no âmbito do que as autoras chamam de estudos críticos de infraestruturas midiáticas – argumentam que “nossas atuais paisagens midiáticas não poderiam existir não fosse pelas nossas atuais infraestruturas midiáticas”^{33, 34}. Podemos entender, assim, uma relação condicional entre o que Couldry e Mejias³⁵ chamam de colonialismo de dados e o desenho de sua infraestrutura midiática.

A velocidade da conexão, a capacidade dos servidores e a capacidade dos processadores, sensores e dispositivos móveis são detalhes do processo de dataficação e dos diversos interesses envolvidos. Seja coletar dados industriais para vantagens competitivas, estratégicas ou coletar dados pessoais para *marketing*, a infraestrutura de Internet é questão crítica.

Assim como comentamos sobre as vulnerabilidades de *software*, vulnerabilidades de *hardware* são uma questão especialmente crítica quando se trata da construção de infraestruturas. Xiao *et al.*³⁶ realizam uma revisão dos estudos sobre *trojans* em peças de *hardware* e apontam como uma das principais preocupações está justamente no fato da produção envolver uma cadeia de suprimentos muito complexa e com a participação de muitas empresas diferentes, assim, com muitos pontos críticos.

²⁹ STAR, S. L. The Ethnography of Infrastructure. *American Behavioral Scientist*, v. 43, n. 3, p. 377-391, 1999. Disponível em: <https://doi.org/10.1177/00027649921955326>. Acesso em: 1 jul. 2019.

³⁰ *Ibid.*, p. 380.

³¹ No original: “We began to see infrastructure as part of human organization, and as problematic as any other.”

³² PARKS, L.; STAROSIELSKI, N. *Signal Traffic: Critical Studies of Media Infrastructures*. Springfield, Illinois: University of Illinois Press, 2015.

³³ *Ibid.*, p. 1.

³⁴ No original: “our current mediascapes would not exist without our current media infrastructures.”

³⁵ COULDRY, N.; MEJIAS, U. A., *op. cit.*

³⁶ XIAO, K. et al. Hardware Trojans: Lessons Learned After One Decade of Research. *ACM Trans. Des. Autom. Electron. Syst.*, v. 22, n. 1, p. 6:1-6:23, 2016. Disponível em: <https://dl.acm.org/citation.cfm?id=2906147>. Acesso em: 1 jul. 2019.



Por tal motivo, a fabricação de *hardware* não é totalmente confiável, exige cautela e auditoria. Além disso, o uso de grampos em cabos submarinos de Internet, manobra até 2013 realizada principalmente por países como Estados Unidos e Reino Unido em diferentes atividades ou programas de inteligência como *Upstream collection* ou *Tempora*, como mencionam Bauman *et al.*³⁷.

Uma das várias disputas geopolíticas neste cenário é a relação entre as sanções econômicas dos Estados Unidos e a empresa chinesa de telecomunicações Huawei³⁸. A preocupação estadunidense – e de organizações em outros países como Canadá, Alemanha e Polônia – é que o *hardware* produzido pela Huawei possibilite espionagem por parte do governo chinês.

Sendo a Huawei uma das principais fornecedoras de equipamentos para tecnologia 5G, especula-se que ela se tornará uma das principais empresas no setor de tecnologia para telefonia móvel, atualmente dominado por empresas norte-americanas e europeias. Trata-se de uma disputa econômica acerca da possibilidade de coletar e processar dados.

As vulnerabilidades de segurança são reais – como já comentamos, de acordo com Xiao *et al.*³⁹, Gamba *et al.*⁴⁰, Razaghpahan *et al.*⁴¹, entre outros – e a preocupação com espionagem e uso indevido de dados também. A construção da infraestrutura é, então, questão de inteligência e segurança da informação.

Para Star⁴², uma das características da infraestrutura é sua invisibilidade, ou transparência: quando está a funcionar normalmente, passa despercebida. No entanto, se não funciona como esperado – por exemplo, servindo como entrada para vulnerabilidades – ela torna-se visível e de interesse crítico.

Como qualquer momento de reestruturação, a implementação da 5G e as controvérsias que dela se desdobram são momentos excepcionais para o estudo de infraestrutura. Aparecem os agentes políticos e econômicos que a constroem e dela se valem, são obrigados se posicionar. As controvérsias convidam os outros agentes a

³⁷ BAUMAN, Z. *et al.*, *op. cit.*

³⁸ CILLUFFO, F. J.; CARDASH, S. L. What's wrong with Huawei, and why are countries banning the Chinese telecommunications firm? *The Conversation*, [s.l.], 19 dez. 2018. Disponível em: <http://theconversation.com/whats-wrong-with-huawei-and-why-are-countries-banning-the-chinese-telecommunications-firm-109036>. Acesso em: 19 jun. 2019.

³⁹ XIAO, K. *et al.*, *op. cit.*

⁴⁰ GAMBA, J. *et al.*, *op. cit.*

⁴¹ RAZAGHPANAH, A. *et al.*, *op. cit.*

⁴² STAR, S. L., *op. cit.*



tomarem posições. “Mudanças levam tempo e negociação, e envolve ajustes com outros aspectos dos sistemas”^{43, 44}.

3 O BRASIL MONTANDO INFRAESTRUTURA DE 5G

As preocupações até aqui elencadas pouco aparecem nas falas dos representantes das empresas, das agências reguladoras ou do poder público na sessão da CCTCI na Câmara dos Deputados.⁴⁵ Na ocasião, a Comissão ouviu nove representantes de empresas, governo e agências reguladoras. Em geral, as manifestações trataram das possibilidades que a tecnologia traz para desburocratização e vigilância.

Apenas um dos seis deputados que se manifestaram elencou dúvidas acerca da capacidade de auditoria das tecnologias e verificação de *backdoors*: “qual a real possibilidade, e alguns trataram do tema, de auditoria dessas tecnologias e a verificação da existência de possíveis *backdoors*? O Brasil possui capacidade para tal verificação?”, perguntou o deputado Gustavo Fruet.⁴⁶ Quem responde é Alberto Paradisi, vice-presidente de Pesquisa e Desenvolvimento do Centro de Pesquisa e Desenvolvimento em Telecomunicações (CPqD):

É imperativo que os governos desenvolvam uma gestão de riscos cibernéticos [...] eu não tenho dúvida que as universidades e as empresas têm competências e eu acho que falta o estabelecimento de uma prioridade nesse tema específico e da mobilização de recursos para fazer isso acontecer.⁴⁷

Ainda que o representante do CPqD sugira a participação de empresas, infelizmente, repete-se aqui uma postura comum nesse tipo de investimento: propor que o governo e o setor público assumam os riscos. Na auditoria de tecnologias de conectividade e Internet, é imprescindível a participação plural de setores. As universidades brasileiras,

⁴³ *Ibid.*, p. 382.

⁴⁴ No original: “*Changes take time and negotiation, and adjustment with other aspects of the systems are involved*”.

⁴⁵ Comissão de Ciência e Tecnologia, Comunicação e Informática, Audiência Pública Conjunta das Comissões CCTCI e CDU, Tema: “A tecnologia 5G”. Câmara dos Deputados. Brasília: Câmara dos Deputados, 15 mai. 2019. Disponível em: <https://www.camara.leg.br/evento-legislativo/55263>. Acesso em: 19 jun. 2019.

⁴⁶ *Ibid.*, 2h00min37s.

⁴⁷ *Ibid.*, 2h26min47s.



por exemplo, tanto por serem relativamente neutras na disputa de interesses quanto por terem condições e competências específicas, devem ter um papel central em tais auditorias de segurança e outras atividades de contrainteligência.

Tornar política pública a auditoria de segurança da informação em parceria com as universidades é um cenário ideal, porém um desafio de compatibilidade com o cenário de crescente desincentivo às universidades, redução de investimentos e de autonomia. O desenvolvimento sustentável e responsável de tecnologias de infraestrutura, especialmente de conectividade e de *Internet*, provoca os limites e as contradições de políticas de austeridade. Não estaríamos errados em inferir – ao menos frente às falas de deputada, deputados e palestrantes na sessão da CCTCI – que é baixo o interesse do setor público na questão de segurança da informação.

O vice-presidente Hamilton Mourão, ao retornar de viagem oficial à China, em entrevista à *Valor Econômico*, afirmou que o governo brasileiro não tem intenção de banir a Huawei.⁴⁸ Mourão disse também ter aconselhado o presidente da Huawei a criar um ambiente de confiança. A postura de Hamilton Mourão, ao menos de acordo com a entrevista, tem caráter mercadológico: resolvem-se as controvérsias nos termos do mercado, da livre concorrência, e do estabelecimento de confiança na marca.

O documento base de *Estratégia Brasileira de Redes de Quinta Geração 5G*, lançado pelo MCTIC no contexto da consulta pública sobre tecnologia 5G, discute, entre outros assuntos, políticas para Pesquisa, Desenvolvimento & Inovação (PD&I) para tecnologia 5G e segurança da informação.⁴⁹ Em termos propositivos, o documento elenca referências, objetivos e oportunidades por parte do governo brasileiro na gestão de tal tecnologia.

Segundo o documento do MCTIC a PD&I em 5G são, atualmente, fomentadas pelo Fundo para o Desenvolvimento Tecnológico das Telecomunicações (FUNTTEL), pela Lei de Informática e pela Lei do Bem.⁵⁰ A Lei de Informática e a Lei do Bem tratam de incentivos e isenções fiscais para empresas que invistam em Pesquisa, Desenvolvimento e Inovação

⁴⁸ ARAÚJO, C.; RITTNER, D.; MURAKAWA, F. Brasil descarta vetar presença da Huawei em 5G, avisa Mourão. *Valor Econômico*, [s.l.], [s.n.], 7 jun. 2019. Disponível em: <https://www.valor.com.br/brasil/6296401/brasil-descarta-vetar-presenca-da-huawei-em-5g-avisa-mourao>. Acesso em: 19 jun. 2019.

⁴⁹ MCTIC. *Estratégia brasileira de redes de quinta geração (5G): versão para consulta pública*, 2019. Disponível em: <https://www.mctic.gov.br/mctic/export/sites/institucional/sessaoPublica/arquivos/estrategia5g/Documento-base-da-Estrategia-Brasileira-de-5G.pdf>. Acesso em: 4 jul. 2019.

⁵⁰ *Ibid.*, p. 22-23.



(PD&I). O FUNTTEL recebe 0,5% sobre o faturamento líquido das empresas prestadoras de serviços de telecomunicações e gere fomento a projetos, bolsas de capacitação, eventos, entre outros.

O FUNTTEL é gerido por um conselho composto por diferentes organizações como o MCTIC e a Agência Nacional de Telecomunicações (ANATEL). Não há participação popular no conselho. A pesquisa em comunicações estratégicas e segurança da informação é uma das quatro áreas definidas como prioridade pelo FUNTTEL, o que indica uma disposição a tratar do assunto.

Tornando ao documento base, a discussão sobre segurança da informação tem como modelo bem-sucedido o sistema de certificações, e traz como exemplo a certificação realizada pela ANATEL de dispositivos móveis como celulares. Menciona também investimento em equipamentos e capacitação, principalmente em articulação com órgãos como o Centro de Estudos, Resposta e Tratamentos de Incidentes de Segurança no Brasil (CERT.br) e o Centro de Tratamento e Resposta a Incidentes Cibernéticos do Governo (CTIR Gov).

Em tal questão, o documento também menciona estar em desenvolvimento desde o ano passado, por parte do Governo Federal, políticas como a Política Nacional de Segurança da Informação, instituída por decreto pelo então presidente Michel Temer. Os meandros e detalhes da implementação dessa política ainda carecem de mais estudos e observação, assim como sua efetividade.

A principal preocupação, aqui pontualmente e nas preocupações com segurança da informação a nível nacional, é a mudança da relação entre estrangeiro-doméstico para a forma de uma fita de Moebius, como mencionam Bauman *et al.*⁵¹ – a partir de leituras de Didier Bigo. Segundo as autoras e autores, a coleta em grande volume de dados é um fenômeno cuja transnacionalidade desfaz os limites do que é nacional, diminui a soberania dos Estados e mina a possibilidade de proteção ao interesse público.

Dado isso, Bauman *et al.* alertam que “enquanto lutam contra a vigilância em massa, Estados podem criar as condições adequadas para que eles mesmos a pratiquem”.⁵² Daí o caráter sensível e crítico dessa questão e de questões de tecnologia e de infraestruturas em geral. Explicitar tal caráter deve ser um convite à reflexão, ao debate e

⁵¹ BAUMAN, Z. *et al.*, *op. cit.*, p. 16-19.

⁵² *Ibid.*, p. 19.



a criação de consensos que defendam o interesse público, os direitos humanos, as liberdades civis, entre outros valores.

CONCLUSÃO

Cada vez mais é possível registrar os fenômenos cotidianos da vida humana, do comércio, da agricultura, das indústrias. Tais registros são o que compreendemos como dados e metadados. A apropriação de tais registros para alimentação de bancos de dados, de algoritmos de inteligência artificial, e aplicações similares, gera um tipo de conhecimento e informação que coloca certos agentes em posições privilegiadas em operações e relações financeiras, trabalhistas, de segurança e vigilância, nos negócios, nos interesses nacionais e militares, entre outros.

Couldry e Meijas comentam que “uma vida continuamente rastreável é uma vida despossuída, não importa como se olhe para ela. Reconhecer essa desapropriação é o começo da resistência ao colonialismo de dados”^{53, 54}. Concordamos, e por tal motivo este trabalho buscou lançar luz a esse fenômeno associando-o aos estudos sobre midiatização e aos estudos sobre infraestruturas.

No cenário da dataficação, do colonialismo de dados, das tecnologias de conectividade e infraestrutura, existem duas questões diferentes. Podemos descrevê-las assim: 1) dados sendo apropriados e comercializados por prestadoras de serviço (legal ou ilegalmente); 2) dados sendo apropriados por agências de inteligência (corporativas ou governamentais). Em certos momentos, tais questões são bastante distintas; em outros, são inter-relacionadas.

A primeira questão diz respeito a corporações como a Monsanto utilizando secretamente os dados coletados através de seu serviço de tecnologia digital para construir posição privilegiada na negociação com seus clientes e com outras empresas. A segunda questão trata de dados de todo tipo coletados através de *backdoors* em tecnologias de telecomunicações em geral sendo utilizados para construir posições privilegiadas de todo tipo, inclusive interferir na soberania nacional.

⁵³ COULDRY, N.; MEJIAS, U. A, *op. cit.*, p. 10.

⁵⁴ No original: “A continuously trackable life is a dispossessed life, no matter how one looks at it. Recognizing this dispossession is the start of resistance to data colonialism.”



Frente a tais desafios, compete ao poder público, às universidades, aos institutos de pesquisa, entre outras organizações, a tarefa de realizar a auditoria desses equipamentos e criar tecnologias de contrainteligência. Por exemplo, incentivar o uso de *software* livre e de código aberto, de criptografias eficientes e auditáveis. Além de, a longo prazo, desenvolver tecnologias alternativas e resistentes a tais vulnerabilidades.

O enquadramento teórico da midiatização, como exposto ao longo do texto, corrobora para pensarmos o que significam as relações entre infraestrutura, políticas públicas, governos, prestadoras de serviços de telecomunicação, entre outros agentes sociais. O presente debate pode agregar-se a um cenário mais abrangente: das ondas de midiatização contemporâneas, da dataficação, do colonialismo de dados.

REFERÊNCIAS

- ARAÚJO, C.; RITTNER, D.; MURAKAWA, F. Brasil descarta vetar presença da Huawei em 5G, avisa Mourão. *Valor Econômico*, [s.l.], [s.n.], 7 jun. 2019. Disponível em: <https://www.valor.com.br/brasil/6296401/brasil-descarta-vetar-presenca-da-huawei-em-5g-avisa-mourao>. Acesso em: 19 jun. 2019.
- BAUMAN, Z. et al. Após Snowden: Repensando o Impacto da Vigilância. *Revista ECO-Pós*, Rio de Janeiro, v. 18, n. 2, p. 8-35, 2015. DOI: <https://doi.org/10.29146/eco-pos.v18i2.2660>
- BOWKER, G. C.; STAR, S. L. Some Tricks of the Trade in Analyzing Classification. BOWKER, G. C.; STAR, S. L. *Sorting things out: classification and its consequences*. Cambridge: The MIT Press, 1999.
- CARBONELL, I. M. The ethics of big data in big agriculture. *Internet Policy Review*, v. 5, n. 1, 2016. Disponível em: <https://policyreview.info/articles/analysis/ethics-big-data-big-agriculture>. Acesso em: 19 jun. 2019.
- CILLUFFO, F. J.; CARDASH, S. L. What's wrong with Huawei, and why are countries banning the Chinese telecommunications firm? *The Conversation*, [s.l.], 19 dez. 2018. Disponível em: <http://theconversation.com/whats-wrong-with-huawei-and-why-are-countries-banning-the-chinese-telecommunications-firm-109036>. Acesso em: 19 jun. 2019.
- COMISSÃO de Ciência e Tecnologia, Comunicação e Informática, Audiência Pública Conjunta das Comissões CCTCI e CDU, Tema: "A tecnologia 5G". Câmara dos Deputados. Brasília: Câmara dos Deputados, 15 mai. 2019. Disponível em: <https://www.camara.leg.br/evento-legislativo/55263>. Acesso em: 19 jun. 2019.
- COULDRY, N.; HEPP, A. *The Mediated Construction of Reality*. Cambridge: Polity Press, 2016.
- COULDRY, N.; MEJIAS, U. A. Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject. *Television & New Media*, v. 20, n. 4, p. 336-349, 2018. DOI: <https://doi.org/10.1177/1527476418796632>



GAMBA, J. et al. *An Analysis of Pre-installed Android Software*. arXiv:1905.02713, 2019. Disponível em: <http://arxiv.org/abs/1905.02713>. Acesso em: 1 jul. 2019.

GREENWALD, G. *Sem lugar para se esconder: Edward Snowden, a NSA e a espionagem do governo americano*. Rio de Janeiro: Sextante, 2014.

KROTZ, F. The meta-process of “mediatization” as a conceptual frame. *Global Media and Communication*, v. 3, n. 3, p. 256-260, 2007. Disponível em: <http://journals.sagepub.com/doi/10.1177/17427665070030030103>. Acesso em: 4 jul. 2019.

MCTIC. *Estratégia brasileira de redes de quinta geração (5G): versão para consulta pública*, 2019. Disponível em: <https://www.mctic.gov.br/mctic/export/sites/institucional/sessaoPublica/arquivos/estrategia5g/Documento-base-da-Estrategia-Brasileira-de-5G.pdf>. Acesso em: 4 jul. 2019.

PARKS, L.; STAROSIELSKI, N. *Signal Traffic: Critical Studies of Media Infrastructures*. Springfield, Illinois: University of Illinois Press, 2015.

RAZAGHPANAH, A. et al. Apps, Trackers, Privacy, and Regulators: A Global Study of the Mobile Tracking Ecosystem. In: *PROCEEDINGS 2018 NETWORK AND DISTRIBUTED SYSTEM SECURITY SYMPOSIUM 2018*, San Diego, CA. Anais... Disponível em: https://www.ndss-symposium.org/wp-content/uploads/2018/02/ndss2018_05B-3_Razaghpanah_paper.pdf. Acesso em: 1 jul. 2019.

STAR, S. L. The Ethnography of Infrastructure. *American Behavioral Scientist*, v. 43, n. 3, p. 377-391, 1999. Disponível em: <https://doi.org/10.1177/00027649921955326>. Acesso em: 1 jul. 2019.

XIAO, K. et al. Hardware Trojans: Lessons Learned After One Decade of Research. *ACM Trans. Des. Autom. Electron. Syst.*, v. 22, n. 1, p. 6:1-6:23, 2016. Disponível em: <https://dl.acm.org/citation.cfm?id=2906147>. Acesso em: 1 jul. 2019.