



Dados digitais no espaço público: visibilidade e vigilância distribuída em cidades brasileiras

Lucia Meneghetti, Universidade de São Paulo, Brasil
luciameneghetti@usp.br

PALAVRAS-CHAVE:

Espaço público; visibilidade; vigilância; TICs; dados digitais.

RESUMO

Apoiado no conceito teórico de vigilância de Foucault (1983), atualizado principalmente por Bruno (2013), o presente artigo enfoca o tema das relações entre as práticas de visibilidade e vigilância de indivíduos, potencializadas pelas tecnologias de informação e comunicação (TICs), em espaços híbridos e ampliados da cidade contemporânea. A partir do entendimento das TICs como catalizadoras das interações humanas no espaço urbano, investiga-se narrativas empregadas e formas de subjetividades nutridas pela lógica do compartilhamento de dados digitais, e procura-se identificar situações em que a vigilância distribuída se mostra inserida no cotidiano de cidadãos brasileiros, com objetivo de compreender como as práticas de visibilidade alimentam sistemas vigilantes em territórios urbanos, e como esses fenômenos podem interferir nas noções de espaço e esfera pública.

TICs, visibilidade, e os espaços híbridos e ampliados da cidade contemporânea

Nas últimas décadas, tanto os espaços em que vivemos quanto nossas práticas cotidianas vêm sofrendo profundas transformações, especialmente por conta do desenvolvimento e difusão das tecnologias de informação e comunicação (TICs), cuja ascensão se deu principalmente a partir dos anos de 1970, (Girard, 2017). TICs são constituídas por dispositivos, métodos e mídias cujo objetivo é comunicar, tais como: computadores; internet; telefonia móvel; vídeo, TV, cinema e fotografia digitais entre outros. À medida que possibilitam interações entre pessoas que podem estar distantes fisicamente, estas tecnologias potencializam uma das práticas humanas cotidianas e fundamentais para vida em sociedade: as práticas de visibilidade – capacidade do indivíduo ver, se expor e ser visto – para além de limites estritamente humanos. Viabilizada geralmente por uma câmera fotográfica digital embutida em um dispositivo de telefonia móvel, a prática da *selfie*¹ é hoje exercida nos mais diversos cenários urbanos e não urbanos:

Milhares, milhões de fotografias serão produzidas a partir do mesmo gesto: o braço esticado, a câmera voltada para o próprio rosto, a cidade às costas. O ato do sujeito que vai a lugares distantes e fotografa a si mesmo, ou que fotografa coisas sem nunca vê-las, é um fenômeno-chave, me parece, para entendermos o século XXI. (Vieira, 2018).

As *selfies* são responsáveis por trazer popularidade e contribuir na disputa por visibilidade entre os usuários das atuais redes sociais digitais, que são baseadas fundamentalmente em imagens. Sob este aspecto, a prática da *selfie* pode ser encarada como um dos indícios da “reordenação dos regimes de visibilidade que está em curso nas sociedades contemporâneas, o que implica uma reorientação da experiência dos espaços em que vivemos e das tecnologias com as quais lidamos cotidianamente”. (Bruno et al., 2010, p.7).

Segundo Crary (2016, p.30) “uma corrente da teoria política contemporânea afirma que expor-se é uma característica constitutiva fundamental, ou trans-histórica, do indivíduo”. Ainda neste sentido, Brighenti (2007) e Feldman (2011), afirmam que o indivíduo contemporâneo se expõe e produz sua visibilidade de maneira incansável. Por sua vez, Bruno (2013, p. 47) analisa que “a visibilidade e a exposição deliberada do eu, da intimidade, da vida banal e quotidiana em reality shows, blogs, redes sociais são aí vetores de prazer, entretenimento e sociabilidade”, o que, segundo a autora, faz com que a prática de exposição pessoal passe a ser voluntária por parte dos indivíduos que desejam a visibilidade. Ao tratar das condições de visibilidade entendidas enquanto regime, Bruno (2013, p.15) baseada principalmente em Foucault (1983), entende que “participam máquinas, práticas, regras, discursos que estão articulados a formações de saber e jogos de poder”. Desta maneira, compreendemos que “a visibilidade está na intersecção dos domínios da estética (relações de percepção) e da política (relações de poder)”. Brighenti (2007, p.324, tradução nossa)².

1 O termo selfie (língua inglesa), diz respeito a um autorretrato geralmente tirado com objetivo de ser compartilhado na internet, principalmente em redes sociais digitais.

2 “Visibility lies at the intersection of the two domains of aesthetics (relations of perception) and politics (relations of power)”.

Ao potencializar as práticas de visibilidade, no momento em que possibilitam que pessoas fisicamente distantes interajam, as TICs acabam também por modificar nossa percepção de tempo e de espaço. Diversos autores apontam maneiras pelas quais a tecnologia tem interferido nas noções do espaço físico. Santos (2006) considera o espaço geográfico do mundo atual como um meio técnico-científico-informacional, e afirma que:

A informação não apenas está presente nas coisas, nos objetos técnicos, que formam o espaço, como ela é necessária à ação realizada sobre essas coisas. A informação é o vetor fundamental do processo social e os territórios são, desse modo, equipados para facilitar a sua circulação. (Santos, 2006, p.160).

O autor considera o espaço um híbrido de materialidades e relações sociais. Por sua vez, Ferrara (2000, p.22), diz que “a cidade virtual não substitui a real, mas ambas convivem por meio dos veículos ou canais que reproduzem, nas suas torres, a força da comunicação planetária, ao mesmo tempo, em que é capaz de estimular o imaginário na idealização de outras cidades possíveis”. Assim como estes dois autores, o presente artigo considera que os aspectos físicos e sociais do espaço são indissociáveis.

Mais recentemente, nesta mesma chave, Beiguelman (2016) defende que diferentes dispositivos tecnológicos suplementam nosso cotidiano físico com informações, fazendo com que coexistam no mesmo espaço objetos virtuais e reais. Segundo a autora, esta condição de coexistência acaba por borrar a oposição entre espaço real e espaço virtual, proporcionando o entendimento da cidade como conjuntos de territórios híbridos configurados a partir da superposição de fisicalidades e redes informacionais diversas. Lemos (2010) afirma que quando dispositivos eletrônicos criam, a partir de bancos de dados, funções informacionais no espaço físico, configurando o que ele chama de “territórios informacionais”, o que entra em disputa é o controle das informações e por consequência uma nova função dos espaços.

Paradoxalmente, as tecnologias que propiciam e potencializam a exposição do indivíduo e sua visibilidade, passam frequentemente despercebidas no cotidiano das cidades, devido a sua própria invisibilidade, Duarte e Firmino (2010, p.102) esclarecem: “[...] fibras ópticas são subterâneas, as ondas de rádio são invisíveis e os satélites estão além do alcance de nossa percepção”. Girard (2017) também aponta para a invisibilidade das mídias eletrônicas, afirmando que seus efeitos “atuam sobre a percepção da cidade ao modificar os tempos da experiência pela implementação de sistemas de tempo real à velocidade da luz. O impacto das tecnologias de comunicação de massa não é tão perceptível no espaço da cidade quanto no tempo”. (Girard, 2017, p.35). Para o autor, percebe-se mais a instantaneidade das interações humanas que as TICs propiciam do que a presença física delas em nosso meio ambiente.

Bruno et al. (2010), entende que os chamados espaços ampliados se formam à medida que sensores tecnológicos que monitoram o espaço físico e informacional, tornam sensíveis processos usualmente despercebidos como maneiras discretas de vigilância de dados. Assim, entendemos que as TICs ampliam as possibilidades de interações humanas – antes limitadas ao

meio físico – principalmente ao adicionarem camadas informacionais no espaço híbrido de materialidades e relações sociais, constituindo desta forma o que entendemos por espaços híbridos e ampliados da cidade contemporânea.

Territorialização e vigilância: plataformas que orientam a participação de pessoas para monitoramento de espaços urbanos

A maneira como passamos a usar aplicativos como *Waze* e *Google Maps*³ em dispositivos móveis, para apreender e nos deslocar pelas cidades, pode ser considerada como evidência do impacto das TICs na reorganização da mobilidade e dos espaços. Porém, ao usarmos esses aplicativos, que através de GPS (tecnologia de localização por satélite) registram os lugares pelos quais passamos, estaríamos contribuindo para um tipo específico de vigilância. Chamada por Bruno (2013) de vigilância distribuída e tratada por Lemos (2010), Koskella (2010) e Virilio (2012) como nova vigilância ou vigilância atual, contemporânea, em que muitos vigiam muitos, é aquela que é espalhada, heterogênea, diversificada e se caracteriza por seu caráter reticular – em rede. De acordo com Virilio (2012), diferente da vigilância do século XIX, que dependia do sujeito encarcerado, preso, sob a vigilância do cárcere, a vigilância atual depende de um estado de ocupação permanente. Esse sujeito contemporâneo, ocupado, atuante, produz registros físicos e digitais de suas atividades e consequentemente deixa rastros (informações passíveis de serem monitoradas). Por exemplo, de acordo com Bioni e Machado (2016), desde que o programa Nota Fiscal Paulista foi implantado no Brasil, ao informar seu CPF no ato da compra em um estabelecimento comercial das cidades brasileiras participantes do programa, corre-se o risco de compartilhar com o Estado – e com as empresas para as quais ele cede seus dados – nosso perfil de compras e a lista de lugares que costumamos frequentar. Portanto, participar deste programa do governo brasileiro, pode também ser considerado como uma maneira de contribuímos para a vigilância distribuída. Bruno (2013) atualiza os conceitos de Foucault (1983), e define o conceito de vigilância no qual este artigo se baseia:

[...] em linhas gerais, uma atividade de vigilância pode ser definida como a observação sistemática e focalizada de indivíduos, populações ou informações relativas a eles, tendo em vista produzir conhecimento e intervir sobre os mesmos, de modo a conduzir suas condutas. [...] As atuais práticas de vigilância contam com uma imensa e crescente diversidade de tecnologias, discursos, medidas legais e administrativas, instituições e corporações, enunciados e empreendimentos científicos, midiáticos, comerciais, políticos etc. Tais elementos não são apenas diversos, mas também distribuídos. Muitos deles só podem ser definidos, quanto às suas propriedades vigilantes, pelas relações que mantêm uns com os outros, e não por suas características intrínsecas, sendo portanto constituídos pelas redes segundo as quais se articulam. (Bruno, 2013, p. 18-19)

3 Waze e Google Maps são aplicativos para dispositivos móveis baseados em navegação por satélite, que disponibilizam mapas e rotas, e monitoram o trânsito. Ambos permitem compartilhamento de informações de seus usuários. Segundo seus sites, Waze possuía mais de 65 milhões e Google Maps mais de 1 bilhão de usuários ativos ao redor do mundo entre 2016 e 2017. Disponível em: <<https://www.waze.com/pt-BR/>> e em: <<https://cloud.google.com/maps-platform/?hl=pt>>. Acessos em: 25/07/2017.

Vale esclarecer a diferença entre ver e vigiar, ou entre vigilância e visibilidade, de acordo com a definição citada: se não houver a intenção de intervir sobre os indivíduos ou populações em foco, não se trata de vigilância, e sim de práticas de visibilidade. O ver, o ser visto, ou a exposição pessoal, como as *selfies* comentadas anteriormente, são práticas de visibilidade. Porém, ao usarmos a internet para postar registros fotográficos e consequentemente ceder informações relacionadas aos lugares por onde passamos, haveria possibilidade de também estarmos contribuindo com a vigilância distribuída, o que faz com que espaços de visibilidade e exposição de indivíduos se tornem também potenciais espaços de vigilância.

A vigilância distribuída possui um caráter multifacetado que pode englobar não só: a vigilância exercida por um cidadão, com foco em um outro indivíduo, e em sua vida comum – geralmente por meio de monitoramento de atividades online de colegas e familiares em redes sociais, por exemplo –; mas também a vigilância exercida por um dispositivo construído para vigiar – que pode agenciar grande número de pessoas, com foco em grupos específicos de indivíduos. (Bruno, 2013). Para exemplificar esta segunda situação, Bruno (2013) cita o caso da plataforma que orientou a participação de indivíduos para o monitoramento de espaços urbanos, e convidou pessoas a atuarem como vigias colaborativos a partir de seus computadores pessoais de 2008 a 2012 na fronteira entre México e Estados Unidos. A artista espanhola Joana Moll e o antropólogo francês Cédric Parizot acompanharam entre 2010 e 2013 as atividades de um grupo formado de maneira espontânea no *Facebook*⁴, por cidadãos na maioria americanos, com perfis públicos, que vigiavam voluntariamente trechos da fronteira entre México e Estados Unidos através de 200 câmeras em um circuito fechado de televisão⁵. Os vigilantes voluntários podiam acessar gratuitamente as transmissões em seus computadores pessoais, em um website disponibilizado em 2008 pelo governo dos Estados Unidos em parceria com a empresa BlueServo⁶ que pertencia ao *Texas Virtual Border Watch Program*.⁷ O site transmitia 24 horas por dia e 7 dias por semana, e permitia que os usuários informassem anonimamente se percebessem atividades suspeitas na fronteira, (Moll; Parizot, 2016). A plataforma online de vigilância chegou a ter mais de 200 mil usuários voluntários e resultou em mais de 5 mil interdições, que representou quase 1 milhão de horas de trabalho gratuito para as autoridades. O objetivo declarado desta iniciativa era levar os cidadãos americanos a participar na redução do crime fronteiriço por meio de *crowdsourcing*,⁸ (Moll; Parizot, 2016). A artista Joana Moll se inscreveu no programa com uma identidade falsa, foi aceita no grupo de vigilantes voluntários do *Facebook* e narrou sua experiência:

4 Facebook é atualmente a maior rede social online do planeta. A adesão é gratuita e sua operação e propriedade são privadas. De acordo com dados divulgados em seu site, possuía mais de 1,9 bilhões de usuários ativos ao redor do mundo entre 2016 e 2017. Disponível em: <<https://www.facebook.com/>> Acesso em: 25/07/2017.

5 Constituído basicamente por câmeras, meios de transmissão e monitores, o circuito fechado de televisão é aquele cujos sinais provenientes de câmeras são transmitidos para particulares, não estando disponíveis abertamente.

6 Disponível em: <<http://blueservo.com/>>. Acesso em: 25/07/2017.

7 “Programa de monitoramento virtual da fronteira do Texas” (tradução nossa)

8 O termo crowdsourcing (língua inglesa), diz respeito a um tipo de atividade desenvolvida por meio de colaboração, conhecimento e/ou ações coletivos.

Os usuários de *RedServant*⁹ eram um exemplo muito bom de *gamification*¹⁰, e eu não era nenhuma exceção. Mesmo que estivesse moralmente contra os propósitos do site, quando algo se movesse, ou a atividade humana pudesse aparecer, eu sentia necessidade de pressionar o botão vermelho. Uma vez imersa na lógica – e, por extensão – às regras do site, sentia-me como a coisa certa a fazer. Refletir não parecia ser uma opção, não pelo menos antes de tomar uma ação. A interface, juntamente com os feeds da câmera, permitiu a descontextualização física da fronteira ao trazê-la para a esfera privada do usuário na forma de um jogo, além disso, o site se assemelhava a um videogame, onde qualquer ação tomada seria sem consequência. [...] (Moll; Parizot, 2016, tradução nossa)¹¹

A descontextualização e desmaterialização que suprimem o espaço-tempo do pensar de que fala Moll e Parizot (2016), também podem ser observadas nas reflexões de Virilio (2012), que acredita que o espaço real da geografia está conectado com o tempo real da ação humana. O autor acredita que a perda de lugar é acompanhada pela perda do corpo e que por isso as pessoas são obrigadas a transferir seu poder de decisão para respostas automáticas. À medida que as TICs viabilizam fenômenos de interação instantânea, que resultam em uma supressão do tempo reservado para a reflexão, em favor de respostas prontas produzidas pela emoção, acabam por provocar uma desestabilização na relação das interações humanas (Virilio, 2012).

Em sua análise sobre o *Texas Virtual Border Watch Program*, Koskella (2010, p.184) afirma que embora o objetivo oficialmente declarado pelas autoridades dessa iniciativa era de que o projeto não havia sido criado para controlar a imigração, na prática ele acabava por fazê-lo de uma maneira perversa, uma vez que nele “a vigilância era usada para lidar com o medo ligado a uma população vista como diferente ou desviante: os vindos do sul, os mexicanos, os ilegais, os sem documentos, os indesejados, os pobres. Vigilância é, assim, usada para gerir e forçar a exclusão”. (Koskella, 2010, p.184). Observa-se desta maneira, o discurso da segurança justificando o emprego de sistemas tecnológicos de vigilância que acabam por gerar exclusão social.

Outra situação em que um dispositivo foi construído para vigilância – usou captura de dados para marketing direcionado –, agenciando grande número de pessoas ocorreu recentemente na cidade de São Paulo e gerou discussão sobre direito à privacidade, e sobre o uso de dados de cidadãos por parte de uma empresa privada aliada ao poder público brasileiro. Trata-se do sistema de reconhecimento facial que foi implantado e permaneceu em funcionamento parcial por curto período de tempo – por volta de abril a setembro de 2018 – inicialmente nas estações: Luz, Paulista e Pinheiros da Linha 4-Amarela do metrô.

9 Na narrativa da artista o nome da empresa BlueServo havia sido alterado para RedServant para proteger a identidade de seus usuários.

10 O termo gamification (língua inglesa), diz respeito a formas de interações relacionadas ao universo dos jogos e videogames.

11 “The users of RedServant were a very good example of gamification, and I was no exception. Even though I was morally against the purposes of the site, when something would move, or human activity would appear, I felt compelled to press the red button. Once immersed in the logic – and by extension – the rules of the site, it felt like the right thing to do. To reflect did not seem to be an option, at least before taking an action. The interface, along with the camera feeds, allowed to physically decontextualize the border and bring it to the user’s private sphere in the shape of a game, moreover, the site resembled a video game, where any action taken would be without consequence”.

Assim como diversos canais da imprensa brasileira, a concessionária ViaQuatro (responsável pela operação e manutenção da Linha 4-Amarela do metrô), noticiou por meio de seu website, o lançamento do sistema e descreveu brevemente seu funcionamento, conforme apresentamos a seguir.

Através dos dispositivos e sistemas implantados nas estações, os usuários do metrô supostamente tiveram suas expressões e imagens faciais capturadas ao assistirem anúncios comerciais ou institucionais que foram transmitidos em monitores instalados ao lado das portas de acesso dos vagões de trens nas estações. Por meio de algoritmos em seu software a tecnologia identifica a presença humana pelas formas dos rostos e corpos, sugere a classificação pessoal em gênero masculino ou feminino, estima se o indivíduo é criança, jovem ou adulto e interpreta, por meio de algoritmos em seu software, algumas expressões faciais, que sugerem quatro tipos de emoções: feliz, insatisfeito, surpreso e neutro, (ViaQuatro, 2018; Affonso, 2018; Eler, 2018).

A partir destas informações, diversos aspectos podem ser debatidos, mas vamos nos deter em dois aspectos relevantes mais óbvios, sendo o primeiro relacionado à discriminação de gênero, cabe a pergunta: se no sistema de reconhecimento facial do metrô é sugerido a classificação pessoal em gênero masculino ou feminino, como seriam classificadas as pessoas transgêneros? Essa questão simples pode evidenciar de forma contundente um possível aspecto excludente deste sistema. Seguindo por esta lógica, não haveria espaço adequado para pessoas transgêneros expressarem seu feedback sobre os anúncios ou serviços prestados pelo metrô, provavelmente, correriam maior risco de terem seus feedbacks classificados de maneira equivocada. Em 2015 a imprensa estadunidense noticiou que um algoritmo do Google classificou pessoas negras como gorilas, (Dougherty, 2015; Kasperkevic, 2015; Zhang, 2015). Estudos recentes apontam para discriminação racial e de gênero em algoritmos, entre eles, Buolamwini e Gebru (2018) afirmam que nos sistemas de classificação algorítmicos que estudaram, a assertividade foi maior para pessoas brancas do sexo masculino e menor para pessoas negras do sexo feminino.

O segundo aspecto, a ser tratado sobre o sistema de reconhecimento facial do metrô, refere-se à privacidade dos usuários e aos reais fins para os quais o sistema foi implantado. Após a publicação de um artigo em abril de 2018 de Carlos Affonso (diretor do Instituto de Tecnologia e Sociedade – ITS Rio e professor da Faculdade de Direito da Universidade do Estado do Rio de Janeiro), em seu blog (Tecfront), a ViaQuatro, concessionária responsável pela operação da Linha 4-Amarela do metrô de São Paulo, alegou que: “A tecnologia não faz recolhimento de dados dos passageiros, nem reconhecimento de identificação pessoal. Além disso, a tecnologia não grava, armazena imagens ou faz cruzamento de dados do indivíduo, uma vez que não tem informações para isso.” (Affonso, 2018). Já a explicação publicada também em abril de 2018 no site oficial da concessionária sobre o assunto dizia:

As portas de plataforma interativas são uma tecnologia inovadora desenvolvida pela Via-Quatro para aprimorar transmissão de informações aos passageiros da Linha 4-Amarela. Essa nova ferramenta na área de comunicação e marketing, com recursos sofisticados, pode colaborar na criação de novas estratégias para públicos específicos, visando mais

efetividade na troca de mensagens importantes ou mesmo o incremento em vendas, explica Harald Zwetkoff, presidente da ViaQuatro. (ViaQuatro, 2018)

Ao analisarmos tais declarações, podemos refletir: se a tecnologia citada acima não faz recolhimento de dados dos passageiros, reconhecimento de identificação pessoal, cruzamento de dados de usuários, nem grava ou armazena imagens dos indivíduos, como ela poderia aprimorar a transmissão de informações aos passageiros da Linha 4-Amarela? Como poderia ser uma nova ferramenta na área de comunicação e marketing, colaborando na criação de novas estratégias para públicos específicos e visar o incremento de vendas com mais efetividade na troca de mensagens importantes? Em outras palavras, pergunta-se: como essa tecnologia poderia atingir tamanha efetividade em comunicação sem uma única análise de cruzamento de dados de feedback dos usuários? Afinal, dados que não são recolhidos, não podem ser analisados. As respostas a essas perguntas são no mínimo contraditórias, e evidenciam a falta de transparência por parte da empresa e dos órgãos públicos responsáveis tanto na questão da coleta e uso dos dados dos cidadãos quanto para qual o fim a que realmente serviriam.

A Concessionária que administra a Linha 4-Amarela foi alvo de ação civil pública pela instalação das câmeras de reconhecimento facial, resultando na determinação do Tribunal de Justiça de São Paulo para que os **sensores que fazem o reconhecimento facial** dos passageiros nas plataformas fossem desativados. Até o presente momento a ViaQuatro está acatando a decisão liminar da justiça em que é cabível recurso¹². O ocorrido foi amplamente noticiado pela imprensa brasileira, (Barros, 2018; Eler, 2018; Farias, 2018; Pelegi, 2018).

Outras situações de coleta de dados por parte do poder público brasileiro

Como vimos até aqui, é também por meio do compartilhamento de informações na internet sobre si mesmo que o usuário contribui para a captura de seus dados de maneira voluntária, (Virilio, 2012; Bruno, 2013; Crary, 2016; Hatuka; Tosh, 2016). Outra maneira relevante pela qual dados de indivíduos são coletados se dá por meio de aplicativos e plataformas que orientam a participação das pessoas para o monitoramento de espaços urbanos, (Bruno, 2013). E ainda de acordo com a autora, a terceira maneira mais relevante de coleta de dados pessoais é feita por cruzamento e mineração de grandes quantidades de dados obtidos na internet – muitas vezes sem consentimento ou consciência do usuário – por parte de governos e principalmente de empresas privadas que lucram com a venda das informações coletadas. Diante disso, Birchall (2017) questiona quanto e que tipo de dados os cidadãos devem compartilhar com seus governos.

12 O processo pode ser consultado em inteiro teor no website do Tribunal de Justiça de São Paulo, com o número do processo: 1090663-42.2018. 8.26. 0100 e código: 4EB5CDC no endereço eletrônico: <<https://esaj.tjsp.jus.br/pastadigital/conferirDocumento.do?conversationId=&instanciaDaConsulta=PG&tipoNuProcesso=UNIFICADO&numeroDigitoAnoUnificado=1090663-42.2018&foroNumeroUnificado=0100&nuProcessoUnificado=1090663-42.2018.8.26.0100&nuProcesso=&cdProtocolo=4EB5CDC&cdServicoConferencia=920101>>. Acesso em: 22/02/2019.

A pesquisa TIC Domicílios 2016, (Comitê Gestor da Internet no Brasil, 2017), que trata sobre o uso das Tecnologias de Informação e Comunicação em domicílios do país, revela que embora os padrões de desigualdade persistam (apenas 23% dos domicílios das classes D e E estão conectados à Internet), o Brasil já atingiu 107,9 milhões usuários. O principal motivo para a falta de Internet nos domicílios no Brasil é o preço da conexão, e apesar disso, 54% dos domicílios brasileiros estão conectados à Internet, o que representa 36,7 milhões de residências – um crescimento de três pontos percentuais em relação a 2015. A pesquisa também confirmou a tendência, já revelada na edição de 2015, do avanço do celular como principal dispositivo de acesso à rede.

Já a postura e tendências de atuação do governo brasileiro podem ser entendidas a partir de outra pesquisa que trata sobre o uso das Tecnologias de Informação e Comunicação no setor público brasileiro, chamada TIC Governo Eletrônico 2017, (Comitê Gestor da Internet no Brasil, 2018). Esta pesquisa mostrou uma presença crescente dos órgãos públicos brasileiros na Internet. Aproximadamente três em cada quatro órgãos públicos federais e estaduais (77%) e prefeituras (75%) do Brasil afirmaram possuir perfis próprios em redes sociais online. A pesquisa também constatou que em 2017, 18% das prefeituras que foram investigadas afirmaram ter algum plano ou projeto de cidades inteligentes. Essa proporção chega a 77% nas capitais e a 70% nos municípios com mais de 500 mil habitantes. A Estratégia Brasileira para a Transformação Digital definida pelo Governo Federal, (Ministério da Ciência, Tecnologia, Inovações e Comunicações, 2018), tem como um de seus eixos temáticos o acompanhamento da transformação digital da economia baseada em dados e entende o mercado de dados como elemento estratégico para o crescimento econômico.

Coletar dados pessoais dos cidadãos faz parte das atividades dos governos, que monitoram e identificam indivíduos para controlar o Estado e atender necessidades de sua população civil. Uma das maneiras mais comuns pela qual compartilhamos dados financeiros pessoais com o governo compulsoriamente se dá por meio da declaração anual de imposto de renda. Outras situações como esta já ocorriam antes da ascensão das TICs. Em 1871, ainda durante o período imperial no Brasil, foi criada a Diretoria Geral de Estatística, que teve suas atividades ampliadas, mudando algumas vezes de nome até tornar-se o *Instituto Brasileiro de Geografia e Estatística (IBGE)*, entidade da administração pública federal, vinculada ao Ministério do Planejamento, Desenvolvimento e Gestão, (IBGE, 2019?a). Responsável pela coleta oficial e disseminação de informações estatísticas, econômicas, demográficas, geográficas, cartográficas, geodésicas e ambientais brasileiras, o IBGE produz informações que procuram retratar a realidade do país. Entre outras atividades, o IBGE realiza um censo nacional a cada 10 anos que coleta informações como idade, ocupação e renda familiar, nível de alfabetização e escolaridade, e condições sanitárias de todos os residentes do Brasil (IBGE, 2019?a). A participação da população se faz obrigatória por meio da Lei nº 5.534 de 14 de novembro de 1968, e o ato de recusar ceder informações ou de ceder informações falsas para o IBGE pode ser punido com multa de até dez vezes o maior salário mínimo vigente no país, e de até o dobro desse limite quando a infração for reincidente. O texto desta Lei ainda define que:

As informações prestadas terão caráter sigiloso, serão usadas exclusivamente para fins estatísticos, e não poderão ser objeto de certidão, nem, em hipótese alguma, servirão de prova em processo administrativo, fiscal ou judicial, excetuado apenas, no que resultar de infração a dispositivos desta lei. (Brasil, 1968).

Além disso, como também é esclarecido nas respostas às dúvidas frequentes identificadas pelo site oficial do governo, “as respostas individualizadas de cada entrevistado não são compartilhadas com outras instituições governamentais, empresas, entidades ou pessoas físicas. O acesso a esses dados é restrito aos profissionais do IBGE que atuam na pesquisa”. (IBGE, 2019?b).

O censo do IBGE é um dos meios mais conhecidos pelos quais o governo brasileiro coleta dados sobre seus habitantes, mas ainda há outras maneiras. Uma delas é através do programa da Secretaria Nacional da Fazenda chamado Nota Fiscal Paulista, cujas informações e descrição de funcionamento podem ser verificadas no website oficial do programa e no próprio portal online da Secretaria da Fazenda, conforme apresentamos brevemente a seguir.

Criado com objetivo de reduzir sonegação fiscal, o Nota Fiscal Paulista impõe participação compulsória para os estabelecimentos comerciais localizados no estado de São Paulo e possui cerca de 19 milhões de participantes cadastrados. O consumidor brasileiro é obrigado por lei a pagar uma porcentagem em impostos sempre que adquire um bem ou serviço, entre eles, o ICMS (imposto sobre circulação de mercadorias e prestação de serviços), porém, se o cidadão não registra a compra, não há como o governo recolher os impostos. Desta maneira, o programa incentiva os consumidores a pedirem o documento fiscal que registra a compra em troca de premiações em dinheiro que podem ser resgatadas periodicamente por meio de solicitação via site oficial do governo. Basta que o usuário faça um cadastro prévio no website do programa e informe seu CPF na hora da compra para que até 30% do ICMS recolhido pelo estabelecimento lhe seja devolvido. Além disso, os participantes também concorrem a prêmios em dinheiro sorteados mensalmente pelo governo, que podem alcançar o valor de até dois milhões de reais nos meses de dezembro. (Nota Fiscal Paulista, 2019?; Governo do Estado de São Paulo, 2019?). Diferente da proteção aplicada aos dados coletados pelo IBGE, cujo sigilo é protegido por lei, os dados dos cidadãos coletados pelo governo por meio do programa da Nota Fiscal Paulista contam com pouca ou quase nenhuma proteção, segundo Bioni e Machado (2016):

Em poucas palavras, o cidadão não tem certeza sobre por quem e como estão sendo utilizados seus dados pessoais. Não só as Secretarias da Fazenda Estaduais, mas, também, os estabelecimentos comerciais e os terceiros por eles autorizados podem ter acesso aos dados. Essa plêiade de atores pode fazer o uso que bem entender deles, pois não há nada determinando que os dados do programa devam ser única e exclusivamente processados para fins de combate à sonegação fiscal e para o cálculo de benefícios tributários por parte dos cidadãos-consumidores. (Bioni; Machado, 2016, p.360).

Os autores também chamam a atenção para o fato de que o programa em questão coleta muito mais dados do que precisaria para combater a sonegação fiscal e para entregar seus bônus e premiações:

[...] como o CNPJ do estabelecimento, o CPF do cidadão, o valor total pago e a data, seguem acompanhados do detalhamento das mercadorias, sua quantidade, preço, hora da transação e, até mesmo, as marcas de produtos, sendo tudo transmitido e armazenado no banco de dados da Secretaria da Fazenda. (Bioni; Machado, 2016, p.358).

E esclarecem que este fato vai contra um dos princípios básicos da proteção de dados pessoais, de acordo com artigo 6º, inciso III, do Projeto de Lei 5.276/2016 de 2016: “necessidade: pelo qual o tratamento deve se limitar ao mínimo necessário para a realização das suas finalidades, abrangendo dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.” (Brasil, 2016).

Com a recente criação do Sistema Estadual de Coleta e Identificação Biométrica Eletrônica, – destinado à identificação pessoal de usuários de serviços públicos – o governo do estado de São Paulo aumenta ainda mais a coleta de dados pessoais de seus cidadãos através do uso da tecnologia. O sistema teve sua criação determinada pelo Decreto Nº 63.299, de 21 de março de 2018, seu objetivo declarado é empregar padrões técnicos, tecnológicos, metodológicos e biométricos para coleta e armazenamento das dez digitais, foto do rosto e assinatura dos cidadãos, de forma a permitir a utilização, reutilização e cruzamento dos dados coletados por todos os órgãos e entidades da Administração Pública direta e indireta em todos os serviços públicos, visando economia de recursos públicos. A coleta dos dados é obrigatória a todos os cidadãos nos postos autorizados pelo governo no ato da emissão ou renovação de documentos como: cédula de identidade (RG), passaporte, carteira nacional de habilitação (CHN) e outros que gradativamente passarão a ser digitais, (Governo do Estado de São Paulo, 2018; São Paulo, 2018).

No mesmo mês da publicação do Decreto que criou o Sistema Estadual de Coleta e Identificação Biométrica Eletrônica do Estado, também foi publicada pela Imprensa Oficial do Estado de São Paulo – IMESP, uma portaria oferecendo às pessoas jurídicas um novo serviço público pago de certificação online. O oferecimento da certificação online de identidade por meio de dados biométricos e biográficos permite que pessoas jurídicas contratem o serviço e verifiquem a identidade dos consumidores, por meio do registro de seus dados biográficos (nome completo; data e cidade de nascimento; nome do pai e da mãe; número, autoridade responsável e data de expedição do RG) e da coleta eletrônica de sua impressão digital, seguidos de comparação online com a base de dados biométricos da IMESP, visando a eliminação de fraudes. (IMESP, 2018). Uma Publicação no Diário Oficial do Estado de São Paulo explica como funciona o Serviço de Certificação online:

A empresa que contrata o serviço de certificação online de identidade registra inicialmente os dados biográficos da pessoa a ser consultada e faz a coleta eletrônica de sua impressão digital. Essas informações serão comparadas às existentes na base de dados da Imprensa Oficial do Estado (Imesp), que é constituída pelos dados biográficos e as impressões digitais oficiais das pessoas físicas registradas civilmente no Estado. A empresa usuária do serviço não tem acesso a essa base de dados. Em seguida, a empresa encaminha as informações que coletou à Imesp, para consulta sobre a identidade do indivíduo. Realizada a comparação entre os dados, o resultado é enviado à empresa. Há duas possibilidades de resposta: “Confirmado”, caso a impressão digital coletada corresponda

à existente no banco de dados da Imesp; ou “Não é possível confirmar”, quando a impressão digital coletada não corresponder à existente, ou não existir o nome ou número do RG inseridos, ou ainda se não for possível realizar a verificação em virtude da qualidade da impressão digital coletada ou da existente na base de dados. Na hipótese de o sistema não confirmar os dados, há a possibilidade de uma nova consulta, feita com a inserção de nome, número de RG e um ou mais dados biográficos adicionais do indivíduo. [...] O sistema será operacionalizado por três secretarias estaduais: Governo (por meio da Prodesp e da Imesp), Planejamento e Gestão (Departamento Estadual de Trânsito – Detran.SP) e Segurança Pública (IIRGD).(IMESP, 2018).

É importante observarmos que embora a portaria publicada pela IMESP busque mitigar os riscos de violabilidade de sua base de dados – por meio da homologação do dispositivo eletrônico inteligente, do servidor de dados e do sistema computacional das pessoas jurídicas contratantes do serviço de certificação online – ela não menciona o que as pessoas jurídicas contratantes autorizadas podem fazer com os dados coletados e informações recebidas da IMESP. Também não fica claro quem poderá contratar o serviço de certificação online – e consequentemente ter acesso aos dados –, uma vez que a portaria também não esclarece quais são os critérios que tais pessoas jurídicas necessitam para terem acesso ao serviço oferecido.

Como também como tem sido apontado em matérias da imprensa e em outras pesquisas citadas neste trabalho, é possível constatar que nas situações identificadas no presente artigo em que o poder público brasileiro (em parceria ou não com empresas privadas) está coletando e usando dados digitais de cidadãos, não fica claro para a população quais dados estão sendo coletados, ou de que maneira estão sendo usados, ou ainda quem tem acesso a eles.

Embora existam diversas críticas relacionadas à ameaça da privacidade do cidadão e à segurança da informação na maioria das situações que apresentamos, ainda há mais uma situação: o caso do SINAN – Sistema de Informação de Agravos de Notificação, que pode ser elogiada. Alimentado por notificações dos profissionais da saúde, foi implantado gradualmente a partir de 1993, e regulamentado em 1998, quando também se definiu que a alimentação regular da base de dados nacional seria obrigatória pelos municípios, estados e Distrito Federal (SINAN, 2016). A maioria das notificações é digitada nas Secretarias municipais de saúde, e na falta delas, as notificações são incluídas nas regionais de Saúde, conforme site oficial:

Sua utilização efetiva permite a realização do diagnóstico dinâmico da ocorrência de um evento na população, podendo fornecer subsídios para explicações causais dos agravos de notificação compulsória, além de vir a indicar riscos aos quais as pessoas estão sujeitas, contribuindo assim, para a identificação da realidade epidemiológica de determinada área geográfica.

O seu uso sistemático, de forma descentralizada, contribui para a democratização da informação, permitindo que todos os profissionais de saúde tenham acesso à informação e as tornem disponíveis para a comunidade. É, portanto, um instrumento relevante para auxiliar o planejamento da saúde, definir prioridades de intervenção, além de permitir que seja avaliado o impacto das intervenções. (SINAN, 2016).

O sigilo das informações pessoais integrantes da notificação compulsória por parte das autoridades de saúde é garantido por Lei,e seu Manual de Normas e Rotinas online alerta para possibilidade de maior precaução diante de situações de vulnerabilidade:

Atitudes de discriminação e frequentes violações dos direitos humanos das pessoas com doenças sujeitas ao preconceito exigem uma atenção especial quanto à confidencialidade dos dados obtidos nas investigações realizadas em todos os níveis. Em decorrência disso, o Sinan permite que se defina o nível de acesso aos diferentes módulos por meio da utilização de senhas. É de suma importância que sejam designadas as pessoas responsáveis pelo gerenciamento, acesso às bases de dados e pela interlocução entre as três esferas de governo. (Brasil, 2007)

Como podemos notar, essa breve apresentação de situações não pretende constituir um catalogo de casos e meios pelos quais o governo brasileiro está coletando informações de seus cidadãos, até porque seria tarefa pouco viável devido à sua abrangência, e ao fato de que novos programas e sistemas de coleta de dados têm sido implementados pelo governo com cada vez mais frequência. Desta maneira, a intenção é apresentar algumas situações de coleta de dados, não só sob o importante aspecto de suas ameaças à privacidade ou à proteção dos dados dos cidadãos, mas também sob outros aspectos, como o histórico e os fins e propósitos para que servem, ampliando assim o foco crítico do presente trabalho.

Recusa da esfera pública e ameaças à urbanidade

A efetividade da vigilância distribuída, segundo Bruno (2013), não se dá somente por mecanismos de repressão, mas também por regimes de legitimação, sendo três as principais vias que podem tornar a vigilância aceitável e até requerida, sendo: a via da segurança (a lógica do risco autoriza a vigilância, pois esta permitiria alcançar alguma evidência que atenderia a um desejo de prevenção de ameaças – seja na segurança pública ou nas relações pessoais, corporativas e sociais); a via da visibilidade (ao exercer a exposição pessoal, os indivíduos consentem e até desejam a vigilância); e por fim, a via da eficácia (que requer o emprego da tecnologia que potencializa a vigilância) (Bruno, 2013). Para a autora, a participação do usuário é um dos princípios da cultura digital, e a internet amplia as possibilidades desta participação dos indivíduos na vigilância. Birchall (2017) aborda a questão do compartilhamento digital também para tratar da participação do usuário na vigilância em rede. A autora emprega o termo *shareveillance*, que criou ao unir os termos *share* (compartilhamento) e *veillance* (vigilância) para, segundo ela, fugir das formas predominantes de se compreender o compartilhamento digital como algo sempre positivo, benéfico e correto. Birchall (2017) entende o compartilhamento digital e suas narrativas como uma forma de subjetividade contemporânea que cria a *shareveillance*, “uma situação na qual estamos sempre já compartilhando, e em que qualquer relacionamento com dados só é possível por meio de uma ideia condicional de compartilhamento”. (Birchall, 2017, p.9, tradução nossa)“.

13 “A state in which we are always already sharing – indeed, in which any relationship with data is only made possible through a conditional idea of sharing”.

A autora diz que os discursos sociais dominantes enfatizam vantagens para indivíduos que compartilham. Estes seriam mais bem aceitos por serem supostamente mais éticos, transparentes, e teriam mais ganhos pois receberiam de volta o compartilhamento de outras pessoas. Com visão relacionada a essas ideias, Brighenti (2007), afirma que:

À medida que as tecnologias de comunicação ampliam o campo do socialmente visível, a visibilidade torna-se um mercado de oferta e demanda. Em qualquer ampliação do campo, surge a questão do que vale a pena ser visto a que preço – juntamente com a questão normativa sobre o que deve e o que não deve ser visto. Essas questões nunca são simplesmente uma questão técnica: são inerentemente práticas e políticas. (Brighenti, 2007, p.327, tradução nossa)¹⁴.

O que Brighenti (2007), Bruno (2013) e Birchall (2017) defendem é que na sociedade contemporânea, os indivíduos podem ser controlados pela quantidade de dados que eles disponibilizam, ou seja, a maior parte da participação na vigilância contemporânea não se dá por coerção e sim por iniciativa própria dos que vigiam e são vigiados. Não só por conta da disputa por visibilidade nas populares e difundidas redes sociais digitais fundamentalmente baseadas em imagens, mas também pelo atual impulso social de sermos colaborativos. Estamos constantemente conectados e durante esse período estamos também compartilhando informações. Estes autores nos mostram que a maioria dos pactos em rede são pactos de doação de dados, e que, o que temos hoje são novos formatos de doação de privacidade.

Porém, embora possamos vir a concordar que o movimento em direção à onipresença da vigilância nos espaços híbridos e ampliados das cidades contemporâneas, seja de fato algo a ser resistido, Birchall (2017) entende que o apelo à privacidade – como por exemplo, o principal motor da já mencionada ação civil pública movida contra a Concessionária que administra a Linha 4-Amarela do metrô de São Paulo –, pode ser superficial. Birchall (2017) defende que o apelo à privacidade pouco compreende a subjetividade implícita nas narrativas do compartilhamento digital. E acredita que incorrer neste erro, pode levar ao lugar-comum da resposta que equivocadamente supõe resolver o problema: *se você não fez nada de errado, você não deve temer a vigilância*. A autora apresenta dois argumentos para justificar sua afirmação, o primeiro de que as queixas sobre privacidade são fracas quando se trata de política coletiva, uma vez que privacidade remete ao individualismo, que é o oposto do que fortalece a esfera pública, para Birchall (2017), este apelo reduz a questão política ao invés de ampliá-la. Fazendo paralelo ao conceito de partilha do sensível de Rancière (2005), a autora diz que o apelo à privacidade não pode redistribuir o sensível digital, mas o fortalecimento da esfera pública pode. O segundo argumento de Birchall (2017) diz respeito aos dados pessoais, segundo os quais a autora acredita que não são as particularidades de cada dado sobre cada indivíduo que importam, nem mesmo o conjunto específico de dados de um único indivíduo em particular – a não ser que seja algo notadamente fora do padrão.

14 “As communication technologies enlarge the field of the socially visible, visibility becomes a supply and demand market. At any enlargement of the field, the question arises of what is worth being seen at which price – along with the normative question of what should and what should not be seen. These questions are never simply a technical matter: they are inherently practical and political”.

Ela esclarece que o importante são os cruzamentos de diversos conjuntos de dados de inúmeros indivíduos que ao serem analisados serão interpretados como novas informações ou maneiras de medição e controle relacionados a um determinado perfil de indivíduos ou a uma ampla varredura em massa. O dado é relacional e isto é o que lhe agrega valor. Desta maneira, a autora afirma:

“Somos ruído, não sinal [...]. A configuração dos cidadãos como ruído, e não como sinal, aponta para o nosso papel delimitado dentro da assembleia da *shareveillant* [...]. A ofensa, sugiro, é menos a intrusão no espaço privado e mais a recusa do público como potencial político. O estado de vigilância imagina seus cidadãos nessa configuração como principalmente um conjunto de dados agregados. Não é que os cidadãos estejam sendo espionados, a menos que suas ações sejam sinalizadas como extremas *outliers*, o que é mais preocupante nessa visão é que eles não são considerados agentes políticos totalmente formados dignos de nada além de reforçar um algoritmo para análise de dados. (Birchall, 2017, p.28, tradução nossa)¹⁵.

A esfera pública se constitui em função do indivíduo, e é reflexo de nossa sociedade. Se as práticas de visibilidade e as relações sociais humanas estão sendo alteradas pelo uso da tecnologia, a esfera pública também será alterada. Para Kuster e Pechman (2014, p.19) o poder da cidade é “de produzir relações, de obrigar à negociação, de acolher o conflito. É o poder de ser o lugar da esfera pública, mas não só o lugar, é a própria condição de existência dela”. Ou seja, para estes autores a cidade deixa de ser cidade à medida que se torna excludente, à medida que não abriga mais a diversidade. Em outras palavras, recusar o público como potencial político, como afirma Birchall (2017) na citação anterior, significa recusar a esfera pública, e ao recusá-la estaríamos, de acordo com Kuster e Pechman (2014), recusando a própria cidade. Assim, ao tratar o indivíduo da maneira que Birchall (2017) afirma – como nada além de reforços de algoritmos para análise de dados –, o Estado vigilante estaria ameaçando não só a esfera pública, mas também a urbanidade.

Morozov (2018), assim como Birchall (2017), também trata das implicações políticas do emprego das TICs em nossa sociedade, criticando principalmente a atuação das empresas de tecnologia do Vale do Silício e a falta de intervenção do estado, para ele: “a escolha efetiva que se tem hoje não é entre o mercado e o Estado, e sim entre a política e não política” (Morozov, 2018, p.51-52). Para exemplificar, o autor comenta sobre o Airbnb¹⁶, meio pelo qual ele entende que os imóveis podem até serem transformados em ativos rentáveis para seus proprietários, mas que não será isso que resolverá o problema do déficit de moradia existente em diversas metrópoles contem-

15 “We are noise, not signal. [...] The configuration of citizens as noise, not signal, points toward our delimited role within the shareveillant assemblage [...]. The offense, I suggest, is less the intrusion into private space and more the disavowal of the public as potentially political. The surveillant state imagines its citizens in this configuration as primarily an aggregated data set. It is not that citizens are being spied on that is of most concern in this view but that unless their actions are flagged up as extreme outliers, they are not considered fully formed political agents worthy of anything more than bolstering an algorithm for data analysis”.

16 Airbnb é uma plataforma online de iniciativa privada, onde as pessoas podem disponibilizar seus imóveis para locação temporária. A plataforma retém uma porcentagem sobre as locações. De acordo com seu site oficial, mais de 81 mil cidades possuem imóveis anunciadas na plataforma em mais de 191 países. Disponível em: <<https://press.airbnb.com/br/fact-facts/>>. Acesso em: 22/02/2019.

porâneas. Morozov (2018) também trata das implicações da adição de camadas informacionais no espaço físico, que de acordo com ele, podem acentuar a mercantilização das cidades:

Uma série de aplicativos, como o *Haystack* e o *MonkeyPrking*, permitiam que, usando apenas os celulares, motoristas leiloassem vagas públicas de estacionamento para outros motoristas em busca de um lugar para guardar o carro. O *Haystack* ainda contava com um recurso, *Make Me Move*, pelo qual os afortunados que encontrassem uma vaga poderiam vendê-la pelo maior lance. Evidentemente, as vagas de estacionamento continuam sendo públicas, o que muda de posse é a informação sobre elas estarem ocupadas ou não. Mas a condição formal, de bem público, significa muito pouco, pois o mercado ilegal da informação o converte em um bem privado dissimuladamente. (Morozov, 2018, p. 67).

A partir desta situação de leilão de vagas públicas para estacionamento de veículos, é possível retomar o conceito de “territórios informacionais” de Lemos (2010), que apresentamos no início deste trabalho. Nesta situação descrita por Morozov (2018) percebe-se como a camada adicional de informação no espaço físico – no caso a disponibilidade de vagas – coloca em disputa o controle das informações e embaralha os limites entre espaço público e espaço privado, onde quem tem mais poder aquisitivo provavelmente sairá ganhando, e em uma situação como esta, ficaria com a vaga.

Considerações finais

Vimos ao longo do presente trabalho que a maneira pela qual as atuais práticas de visibilidade, potencializadas pelas TICs alimentam sistemas vigilantes incorporados ao cotidiano urbano também em nossas cidades, possui como principal característica indivíduos que participam voluntaria e ativamente com sua exposição – consciente ou inconscientemente, assumindo papel de vigilantes e vigiados – por meio principalmente do compartilhamento de dados digitais.

Ainda que estas práticas sejam de algum modo menores e usualmente exercidas de modo relativamente disperso por inúmeros indivíduos, elas não são pouco significativas nem isoladas. Elas compõem um cenário multifacetado, expressando e testemunhando a naturalização e distribuição do olhar e da atenção vigilantes nas cidades e nas redes de comunicação contemporâneas. (Bruno, 2013, p.109)

Catracas eletrônicas presentes em meios de transporte públicos, como ônibus e metrô são exemplos óbvios em que as TICs são usadas para controle de acessos. Devido principalmente a seu caráter atual – cada vez mais ubíquo e pervasivo, (Lemos, 2010) – as TICs também “têm servido de suporte para a intensificação de práticas ligadas ao monitoramento e controle de identificações, movimentos, acessos, ou mesmo características físicas de lugares e territórios na cidade, pelo uso de tecnologias de vigilância e securitização.” (Firmino, 2018, p.69). Conforme observamos, os resultados negativos de determinado emprego destas tecnologias nos territórios urbanos podem ser entre outros: exclusão social e discriminação racial ou de gênero.

Bruno *et al.* (2010, p.7) também aponta para os dispositivos de vigilância presentes em diversas cidades, com ênfase em países americanos como Brasil, México e Estados Unidos e afirma que “tecnologias e procedimentos de vigilância tornaram-se cada vez mais corriqueiros nas arquiteturas urbanas”. Botello (2007) acrescenta que o fenômeno tem ocorrido principalmente nos últimos 25 anos, e em escala global. Desta maneira, apresentou-se a necessidade da adoção de uma noção genérica de cidade para efeito da discussão específica do presente artigo. É importante esclarecer que não se trata de adotar um olhar homogeneizante do espaço, ou um ponto de vista a partir de uma determinada realidade socioeconômica, pois como nos esclarece Bruno (2013) e Lyon (2017), os cenários são multifacetados, complexos e podem sofrer mutações ao longo do tempo. Além disso, se compreende que nem todas as pessoas ou regiões do globo possuem acesso à tecnologia e, portanto, não se enquadrariam no fenômeno mencionado. Porém, argumenta-se que mesmo indivíduos que não possuem acesso à tecnologia, acabam na maioria das vezes sendo afetados justamente pela falta de acesso a ela, como nos mostra Crary (2016) ao afirmar que as inovações tecnológicas operam numa lógica de obsolescência programada, que estimula a demanda por substituição ou aprimoramento de produtos diversos, desempenhando “um papel decisivo na reinvenção do sujeito e na intensificação do controle” (Crary, 2016, p.51). O autor explica que esses produtos (artefatos ou serviços) se tornam o padrão ontológico dominante – ou excludente – em nossa realidade social à medida que inúmeros seres humanos vivem em um nível de subsistência que não lhes permite acessar tais produtos, nem serem integrados às novas exigências dos mercados, fazendo com que se tornem irrelevantes ou dispensáveis.

Como podemos constatar, a investigação do presente artigo não se limita aos aspectos físicos e tecnológicos de sistemas de vigilância nas cidades, mas ao tratar também de seus aspectos sociológicos, históricos e até mesmo econômicos, possibilitou a compreensão de como práticas de visibilidade alimentam sistemas vigilantes em territórios urbanos, e de como estes fenômenos podem interferir nas noções de espaço e esfera pública. Cabe também a nós arquitetos, contribuir para teoria crítica da arquitetura por meio de reflexão multidisciplinar, pois segundo Maluf (2008, p. 82-83):

O arquiteto surge como agente instrumentalizador desse espaço por sua capacidade de compreensão espacial, mais que de representação projetual. É, antes de um agente modificador, um leitor da sociedade em que vive [...] Sozinho, não se configura como instrumento apto a alterar ou dirimir as contradições do espaço inerentes às relações sociais em vigor.

As críticas apresentas neste trabalho não possuem como alvo a tecnologia, e sim sua instrumentalização que pode perpetuar diferentes tipos de discriminação e exclusão social em territórios urbanos. Precisamos buscar empregar a tecnologia a favor do rompimento de lógicas racistas, sexistas e/ou excludentes já vigentes em nossas cidades, e não a favor de acentuá-las. Apontamos para o fato de que não podemos nos tornar reféns passivos do emprego perverso da tecnologia, nem perder a atual oportunidade histórica de apropriação da mesma a favor da urbanidade. É preciso atuar na gênese da questão e praticar uma sociologia da arquitetura

através do questionamento e problematização de seu uso que acentua relações assimétricas de poder. À medida que sistemas de vigilância tem integrado o espaço urbano, a discussão sobre o tema proposto ganha mais relevância, principalmente no que tange às relações entre público e privado, para que se abra possibilidades pela busca de lógicas não excludentes de construção ou (re)apropriação de territórios em nossas cidades, para que, em última instância, de acordo com Kuster e Pechman (2014), seja possível defender a própria urbanidade.

Referências

AFFONSO, C. *A privacidade saiu dos trilhos no metrô de São Paulo*. Tecfront [online], 2018. [Acesso em: 24/04/2018] Disponível em: <<https://tecfront.blogosfera.uol.com.br/2018/04/18/a-privacidade-saiu-dos-trilhos-no-metro-de-sao-paulo/>>.

BARROS, M. *Concessionária do Metrô de SP é processada por painel que faz reconhecimento facial de passageiros*. G1 [online], 2018. [Acesso em: 21/11/2018] Disponível em: <<https://g1.globo.com/sp/sao-paulo/noticia/2018/08/31/concessionaria-do-metro-de-sp-e-processada-por-painel-que-faz-reconhecimento-facil-de-passageiros.ghtml>>.

BEIGUELMAN, G. *Cidades interativas*. In: Beiguelman, G. Da cidade interativa às memórias corrompidas: arte, design e patrimônio histórico na cultura urbana contemporânea. São Paulo: Faculdade de Arquitetura e Urbanismo, Universidade de São Paulo, 2016. 303 p., p. 12-90 Tese de livre docência.

BIONI, B. R; MACHADO, J. *A proteção de dados pessoais nos programas de Nota Fiscal: um estudo de caso do “Nota Fiscal paulista”*. Liinc em Revista [online], 2016, vol.12, nº 2, p. 350-364. [Acesso em: 24/08/2018] Disponível em: <<http://revista.ibict.br/liinc/article/view/3734/3146>>.

BIRCHALL, C. *Shareveillance: The Dangers of Openly Sharing and Covertly Collecting Data*. Minneapolis: University of Minnesota Press, 2017.

BOTELLO, N. *An orchestration of electronic surveillance: a CCTV experience in Mexico*. In: International Criminal Justice Review [online], 2007, vol.17, nº 4, p. 325-335. [Acesso em: 22/02/2019] Disponível em: <<https://journals.sagepub.com/doi/pdf/10.1177/10575677070311566>>.

Brasil. Lei nº 5.534 de 14 de novembro de 1968. [online]. *Dispõe sobre a obrigatoriedade de prestação de informações estatísticas e da outras providências*. Brasília, DF, nov. 1968. [Acesso em: 22/02/2019] Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L5534.htm>.

Brasil. Ministério da Saúde. Secretaria de Vigilância em Saúde. Departamento de Vigilância Epidemiológica. *Sistema de Informação de Agravos de Notificação – SINAN: normas e rotinas* – 2. ed. – Brasília [livro eletrônico]: Editora do Ministério da Saúde, 2007. 68 p. : il.– (Série A. Normas e Manuais Técnicos). [Acesso em: 22/02/2019] Disponível em: <http://portalsinan.saude.gov.br/images/documentos/Aplicativos/sinan_net/Manual_Normas_e_Rotinas_2_edicao.pdf>.

Brasil. Projeto de Lei 5.276/2016 de 2016. [online]. *Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural*. Brasília, DF, 2016. [Acesso em: 22/02/2019] Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?sessionid=62B6CCB8D15F03BD169F7421D3CDB6EE.proposicoesWeb1?codteor=1457971&filename=Avulso+-PL+5276/2016>.

BRIGHENTI, A. *Visibility, a category for the social science*. Current Sociology [online], 2007, vol.55, nº 3, p. 323-342. [Acesso em: 24/08/2018] Disponível em: <<https://journals.sagepub.com/doi/10.1177/0011392107076079>>.

BRUNO, F; KANASHIRO, M; FIRMINO R. (Orgs.). *Vigilância e visibilidade: espaço, tecnologia e identificação*. Porto Alegre: Sulina, 2010.

BRUNO, F. *Máquinas de ver, modos de ser: vigilância, tecnologia e subjetividade*. Porto Alegre: Sulina, 2013.

BUOLAMWINI, J; GEBRU, T. *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*. Proceedings of Machine Learning Research, Conference on Fairness, Accountability, and Transparency [online], 2018, vol. 81, p. 1-15. [Acesso em: 22/02/2019] Disponível em: <<http://proceedings.mlr.press/v81/buolamwini18a.html>>

Comitê Gestor da Internet no Brasil. *TIC domicílios 2016: Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros* [livro eletrônico], São Paulo: Núcleo de Informação e Coordenação do Ponto BR, 2017. [Acesso em: 24/08/2018] Disponível em: <https://www.cetic.br/media/docs/publicacoes/2/TIC_DOM_2016_LivroEletronico.pdf>.

Comitê Gestor da Internet no Brasil. *TIC governo eletrônico 2017: Pesquisa sobre o uso das tecnologias de informação e comunicação no setor público brasileiro* [livro eletrônico], São Paulo: coordenação executiva editorial Alexandre F. Barbosa, 2018. [Acesso em: 24/08/2018] Disponível em: <https://www.cetic.br/media/docs/publicacoes/2/TIC_eGOV_2017_livro_eletronico.pdf>.

CRARY, J. *24/7 Capitalismo tardio e os fins do sono*. São Paulo: Ubu Editora, 2016.

DOUGHERTY, C. *Google Photos Mistakenly Labels Black People 'Gorillas'*. The New York Times [online], 2015. [Acesso em: 22/02/2019] Disponível em: <<https://bits.blogs.nytimes.com/2015/07/01/google-photos-mistakenly-labels-black-people-gorillas/>>.

DUARTE, F; FIRMINO, R. *Espaço, visibilidade e tecnologias: (Re)caracterizando a experiência urbana*. In: Bruno, Fernanda; Kanashiro, Marta e Firmino, Rodrigo. (Org.). *Vigilância e visibilidade: espaço, tecnologia e identificação*. Porto Alegre: Sulina, 2010, p. 94-112.

ELER, G. *A discussão sobre direito à imagem no metrô de SP*. Nexo [online], 2018. [Acesso em: 23/11/2018] Disponível em: <<https://www.nexojornal.com.br/expresso/2018/09/13/A-discuss%C3%A3o-sobre-direito-%C3%A0-imagem-no-metr%C3%B4-de-SP>>.

FARIAS, A. *Justiça proíbe uso de câmeras de reconhecimento facial no Metrô*. Veja São Paulo [online], 2018. [Acesso em: 21/11/2018] Disponível em: <<https://vejasp.abril.com.br/cidades/justica-proibe-uso-de-cameras-de-reconhecimento-facial-no-metro/>>.

FELDMAN, I. *Do declínio da intimidade aos novos regimes de visibilidade* In: Predoso, Marcelo. (Coord.). *Pacific: textos para debate*. Recife: Edição André Antônio, 2011, p. 9-15.

FERRARA, L. *Os significados urbanos*. São Paulo: Editora da Universidade de São Paulo: Fapesp, 2000.

FIRMINO, R. *Securitização, vigilância e territorialização em espaços públicos na cidade neoliberal*. In: Bruno, F; Cardoso, B; Guilhon, L; Kanashiro, M. & Melgaço, L. (Orgs.). *Tecnopolíticas da vigilância: perspectivas periféricas*. São Paulo: Boitempo, 2018, p. 69-90.

FOUCAULT, M. *Vigiar e Punir: nascimento da prisão*. Petrópolis: Vozes, 1983.

GIRARD, L. *A programação total do ambiente: Infraestruturas planetárias da comunicação*. São Paulo: Faculdade de Arquitetura e Urbanismo, Universidade de São Paulo, 2017. 126 p. Dissertação de mestrado em Arquitetura e Urbanismo.

Governo do Estado de São Paulo. *Governo cria identificação biométrica e inicia emissão de CHN digital*. Portal do Governo do Estado de São Paulo [online], 2018. [Acesso em: 24/08/2018] Disponível em: <<http://www.saopaulo.sp.gov.br/spnoticias/com-identificacao-biometrica-eletronica-governo-inicia-emissao-da-cnh-digital/>>.

Governo do Estado de São Paulo. *Sobre a Nota Fiscal Paulista*. Secretaria da Fazenda e Pla-

nejamento [online] 2019? [Acesso em: 22/02/2019] Disponível em: <<https://portal.fazenda.sp.gov.br/servicos/nfp/Paginas/Sobre.aspx>>.

HATUKA, T; TOCH, E. *Being visible in public space: The normalization of asymmetrical visibility*. Urban Studies Journal Limited [online], 2016, p. 1-15. [Acesso em: 24/08/2018] Disponível em: <<https://journals.sagepub.com/doi/10.1177/0042098015624384>>.

IBGE. *O IBGE* [online] 2019?a. [Acesso em: 22/02/2019] Disponível em: <<https://www.ibge.gov.br/institucional/o-ibge.html>>.

IBGE. *Você foi procurado pelo IBGE?: O IBGE protege meus dados?* [online] 2019?b. [Acesso em: 22/02/2019] Disponível em: <<https://respondendo.ibge.gov.br/voce-foi-procurado-pelo-ibge/o-ibge-protege-meus-dados.html>>.

IMESP. *Novo Sistema Biométrico facilita a identificação de cidadãos*. Diário Oficial do Estado de São Paulo [online], Vol. 128, n. 54, março de 2018. [Acesso em: 22/02/2019] Disponível em: <https://www.imprensaoficial.com.br/DO/BuscaDO2001Documento_11_4.aspx?link=/2018/executivo%2520secao%2520i/marco/23/pagnot_0001_7VB6RHHEEV1MKeF4U5FGONMNQP8.pdf&pagina=1&data=23/03/2018&caderno=Executivo%201&paginaordenacao=1>.

KASPERKEVIC, J. *Google says sorry for racist auto-tag in photo app*. The Guardian [online], 2015. [Acesso em: 22/02/2019] Disponível em: <<https://www.theguardian.com/technology/2015/jul/01/google-sorry-racist-auto-tag-photo-app>>.

KOSKELLA, H. *Assista à fronteira 24/7 do seu sofá: o programa de observação virtual da fronteira do Texas e a política do informante*. In: Bruno, F; Kanashiro, M; Firmino, R. (Org.). *Vigilância e visibilidade: espaço, tecnologia e identificação*. Porto Alegre: Sulina, 2010, p. 174-187.

KUSTER, E; PECHMAN, R. *O chamado da cidade*. Belo Horizonte: UFMG, 2014.

LEMOS, A. *Mídias locativas e vigilância. Sujeito inseguro, bolhas digitais, paredes virtuais e territórios informacionais*. In: Bruno, F; Kanashiro, M; Firmino, R. (Org.). *Vigilância e visibilidade: espaço, tecnologia e identificação*. Porto Alegre: Sulina, 2010, p. 61-93.

LYON, D. *Surveillance culture: engagement, exposure, and ethics in digital modernity*. International Journal of Communication [online], 2017, vol.11, p. 824-842. [Acesso em: 22/02/2019] Disponível em: <<https://ijoc.org/index.php/ijoc/article/view/5527/1933>>.

MALUF, C. *Espaço, tempo e lugar*. Pós. Revista do Programa de Pós-Graduação em Arquitetura e Urbanismo da FAUUSP [online], 2018, nº 23, p. 70-83. [Acesso em: 22/02/2019] Disponível em: <<https://doi.org/10.11606/issn.2317-2762.v0i23p70-83>>.

Ministério da Ciência, Tecnologia, Inovações e Comunicações. Secretaria de Política de Informática. Departamento de Políticas e Programas Setoriais em TICs. *Estratégia Brasileira para a Transformação Digital (E-Digital)* [livro eletrônico], Brasília: Ministério da Ciência, Tecnologia, Inovações e Comunicações, 2018. [Acesso em: 22/02/2019] Disponível em: <<http://www.mctic.gov.br/mctic/export/sites/institucional/estrategiadigital.pdf>>.

MOLL, P; PARIZOT, C. *The Virtual Watchers*. Exposing the Invisible [online], 2016. [Acesso em: 25/07/2017] Disponível em: <<https://exposingtheinvisible.org/resources/obtaining-evidence/the-virtual-watchers>>.

MOROZOV, E. *Big tech – A ascensão dos dados e a morte da política*. São Paulo: Ubu Editora, 2018.

Nota Fiscal Paulista. *Como funciona a nota fiscal paulista*. Nota Fiscal Paulista [online], 2019? [Acesso em: 22/02/2019] Disponível em: <<https://www.nfpnotafiscalpaulista.com/como-funciona-nota-fiscal-paulista/>>.

PELEGI, A. *Liminar obriga Via Quatro a suspender coleta de emoções de usuários na Linha 4-Amarela*. Diário do Transporte, [online], 2018. [Acesso em: 21/11/2018] Disponível em: <<https://diariodotransporte.com.br/2018/09/15/liminar-obriga-via-quatro-a-suspender-coleta-de-emocoes-de-usuarios-na-linha-4-amarela/>>.

RANCIÈRE, J. *A partilha do sensível: estética e política*. São Paulo: Editora 34, 2005.

SANTOS, M. *A natureza do espaço: técnica e tempo, razão e emoção*. São Paulo: EDUSP, 2006.

São Paulo (Estado). Decreto N° 63.299, de 21 de março de 2018 [online]. *Institui o Sistema Estadual de Coleta e Identificação Biométrica Eletrônica - Sistema Biométrico, e dá providências correlatas*. São Paulo, SP, mar. 2018. [Acesso em: 22/02/2019] Disponível em: <<https://www.al.sp.gov.br/repositorio/legislacao/decreto/2018/decreto-63299-21.03.2018.html>>.

SINAN. *Sinan: sistema de informação de agravos de notificações*. SINAN [online], 2016. [Acesso em: 22/02/2019] Disponível em: <<http://portalsinan.saude.gov.br/o-sinan>>.

VIEIRA, T. *Hipercidades*. Folha de S. Paulo [online], 2018. [Acesso em: 22/02/2019] Disponível em: <<https://arte.folha.uol.com.br/mundo/2018/hipercidades/>>.

VIRILIO, P. *The administration of fear*. Los Angeles: Semiotext(e), 2012.

VIAQUATRO, *Portas interativas digitais nas plataformas da Linha 4-Amarela*. ViaQuatro. [online], 2018. [Acesso em: 20/04/2018] Disponível em: <<http://www.viaquatro.com.br/imprensa/noticias/Portas-interativas-digitais-nas-plataformas-da-Linha-4-Amarela?releaseld=28601>>.

ZHANG, M. *Google Photos Tags Two African-Americans As Gorillas Through Facial Recognition Software*. Forbes [online], 2015. [Acesso em: 22/02/2019] Disponível em: <<https://www.forbes.com/sites/mzhang/2015/07/01/google-photos-tags-two-african-americans-as-gorillas-through-facial-recognition-software/#38d35cfc713d>>.