

APRESENTAÇÃO

VIGIAR E RESISTIR: A CONSTITUIÇÃO DE PRÁTICAS E SABERES EM TORNO DA INFORMAÇÃO

Marta M. Kanashiro

Os estudos e pesquisas que tratam sobre vigilância de pessoas, de dados e monitoramento têm sido realizados por diferentes áreas do saber e abordando aspectos diversos. Aproximadamente nos últimos vinte anos, alguns desses trabalhos vêm sendo reunidos numa área interdisciplinar conhecida como estudos de vigilância (*surveillance studies*), em especial em países da América do Norte e da Europa(1).

Abordando a constituição dessa área, Gary T. Marx (2), afirma que os estudos de vigilância não se voltam exclusivamente para questões urbanas, por exemplo, ou outros assuntos das ciências sociais tidos como clássicos, como estudos de gênero ou questões étnicas. Da mesma forma, esses estudos também não se baseiam numa perspectiva disciplinar, teórica ou metodológica únicas. Ainda na tentativa de definir essa área, o autor indica que eles compartilham com as pesquisas sobre tecnologia e sociedade o interesse pelos impactos sociais, econômicos e culturais daquelas tecnologias que se voltam para a informação, e dedicam-se a compreender um conjunto de ações e comportamentos que lidam com informações sobre indivíduos ou grupos.

Assim, apesar dos esforços para delimitar a área e reunir pesquisas sob o nome estudos de vigilância, há muitos trabalhos dispersos em áreas como comunicação, ciências sociais, arquitetura e urbanismo, geografia, direito, história, ciência da informação, psicologia, criminologia, filosofia, artes, computação. A Rede Latino-americana de Estudos sobre Vigilância, Tecnologia e Sociedade (Lavits) (3), fundada em 2009, espelha em seu nome exatamente a tentativa de abrir o intercâmbio entre pesquisas dispersas que tematizam direta ou indiretamente a vigilância, mas sem aderir exclusivamente ao

nome estudos de vigilância, como é o caso do Surveillance Studies Centre (Canadá) que influenciou sua criação.

Independente da nomeação da área, e dos exemplos que buscam não se restringir a determinadas definições, é certo que os estudos que tratam do tema vigilância são emergentes, encontram-se hoje em franca expansão, e precisam ser reunidos e dialogar entre si. Numa concepção ampliada, eles podem ser compreendidos como aqueles que têm problematizado as práticas de captura contínua e rotineira de dados, processamento, armazenamento, análise, cruzamento, apropriação e gerenciamento de informações. Dedicam-se a analisar discursos e práticas que atravessam a construção e utilização de tecnologias que permitem essas ações e que incluem também o controle de acesso, a vigilância, o monitoramento e a identificação de pessoas, a construção de bancos de dados e perfis sobre a população.

De forma geral, as tecnologias de informação e comunicação (TICs) e o aumento da capacidade computacional figuram como centrais nesses estudos. Assim, as câmeras para monitoramento, os controles de acesso (incluindo a biometria ou não), as etiquetas RFID (identificação por rádio frequência) (4) (e a internet das coisas), utilização da internet para as mais variadas finalidades, o uso de celulares, de *smartphones*, de dispositivos de geolocalização, e a constituição e exploração do *big data* são objetos recorrentes das pesquisas. No entanto, ainda que se observe essa recorrência, o estudo de determinadas tecnologias não é definidor exclusivo desse campo que volta-se para pensar, em especial (mas não somente), as transformações contemporâneas que incluem as mudanças no capitalismo, nas racionalidades governamentais, no exercício do poder, nos modos de ver, de pensar, de sentir, de conhecer. Assim, esses

estudos procuram refletir sobre a contemporaneidade, mirando as transformações atravessadas por e constituidoras dessas tecnologias, mas sem recair no determinismo tecnológico ou na afirmação de que a tecnologia é razão ou causa explicativa suficiente para as mudanças.

Quando Gary T. Marx afirma que os estudos de vigilância não se voltam exclusivamente para determinados temas, é exatamente porque eles podem ser mesclados com os mais variados assuntos que, nas ciências sociais, são considerados clássicos. Por exemplo, os estudos de gênero podem ser contemplados em pesquisas que se desdobrem também sobre o uso de TICs, as constituições de bancos de dados, de perfis e as mudanças no capitalismo, na cultura. No mesmo sentido, há inúmeros estudos que se mesclam, dentre muitos outros temas, com cidades, segurança, trabalho, lazer, consumo, saúde, democracia, cidadania, legislação, público e privado, privacidade, movimentos sociais, resistência, poder, estética etc.

O debate político e acadêmico sobre o tema foi impulsionado, nos últimos anos, por alguns acontecimentos (que também alteraram a própria forma como se realiza a vigilância) como o ataque ao World Trade Center, em 2001 e, a partir de então, o recrudescimento e reelaboração das práticas e discursos da vigilância. Nessa mesma década, assistimos ainda a expansão e consolidação do uso de redes sociais e de empresas como Google e Facebook; a reformulação de termos de privacidade e condições de uso de serviços baseados na internet (apontando uma nova relação de acesso e utilização de informações de usuários por parte de empresas); a ampliação de ferramentas de marketing e de comércio eletrônico; o acirramento das tensões em torno de propriedade intelectual, direito autoral, acesso e compartilhamento de informação. Na década seguinte, a organização Wikileaks vazou uma série de documentos confidenciais e, em seguida, Edward Snowden tornou públicas as informações sobre programas de vigilância dos Estados Unidos e as formas de atuação da Agência Nacional de Segurança estadunidense em conexão com empresas de internet e telefonia.

Esses acontecimentos que impulsionaram as pesquisas apontam a centralidade da informação e as tensões e disputas que a atravessam (e que incluem acesso, vigilância e propriedade) e sua intensificação nos últimos anos. Esses processos tornaram-se mais claros com os casos emblemáticos de Julian Assange e Edward Snowden, os quais, ao mesmo tempo, podem ser vistos apenas como a precipitação de muitos aspectos já anunciados por estudiosos – quer sejam aqueles que compreendem a contemporaneidade como “sociedade da informação” (5), como “sociedade de vigilância” (6), ou “sociedade de controle” (7) entre muitas possibilidades.

A captura da informação, armazenamento, cruzamento e recombinção de dados são movimentos que atravessam as comunicações e inúmeras práticas cotidianas, a constituição de saberes, a criação de conhecimento, os processos de invenção, e os modos de produção.

São aspectos que estão no cerne das tensões e disputas contemporâneas, envolvendo muitos atores diferentes. A transformação da informação em valor e motor de acumulação das sociedades contemporâneas, ou a centralidade da informação (8) na atualidade nos leva a compreender a informação como questão tática e estratégica crucial para as mais diversas esferas.

Nesse panorama, um caminho que nos permite compreender uma parte das tensões e conexões entre os atores é seguir a trilha apontada por Foucault (9). Vale retomar que, para o filósofo, na passagem da soberania (na Idade Média) para a disciplina e para o biopoder (a partir do século XVIII), o direito à morte – realizado pelo soberano – foi deslocado para um poder que gerencia a vida, e tornou-se uma administração eficaz dos corpos e uma gestão calculada da vida pelo Estado. As taxas de nascimento e morte, as taxas de saúde, longevidade aparecem como uma série de intervenções regulatórias e controles de Estado que atravessam o corpo, caracterizando o que Foucault chamou de biopolítica da população. “A estatística como a ciência do Estado” estava ligada à captura e detenção de informações sobre as pessoas por parte do Estado e seus técnicos, e por parte das instituições disciplinares como hospitais, escolas, exércitos e prisões.

Quando hoje nos voltamos para a centralidade da informação, podemos notar que a capacidade de coletar dados, arquivar, monitorar, entender, reconhecer, identificar e classificar já não é mais uma prerrogativa do Estado (10). Redes sociais como Facebook, corporações como Google, empresas de telefonia, têm uma capacidade de coleta de informações que atravessa uma dimensão da vida não capturada pelos mecanismos de Estado durante a era industrial.

Enquanto o Estado herdou sua coleta de informações das instituições disciplinares (no exercício da biopolítica), voltando-se para dimensões e esferas da vida como saúde, ensino, segurança, punição e defesa nacional, o mercado das TICs voltou-se para uma captura de dados que pode incluir todos esses aspectos, somando um nível de informações que não se relaciona mais à figura identitária do indivíduo, mas a uma dimensão fragmentada dos dados que habita as visões de mundo, as dúvidas e incertezas, os desejos e as aspirações muitas vezes ainda não realizados.

Haggerty e Ericsson (11) ajudam a compreender melhor essa dimensão fragmentada, a partir da ideia de *data double* (duplo de dados) que se refere a uma operação realizada pela computação e pela internet. Nela o corpo humano passa a ter uma composição híbrida, na medida em que aos olhos desses sistemas ele é desmembrado em informações, e então reagrupado em diferentes configurações por meio de uma série de fluxos de dados. O resultado é um corpo “*decorporealized*” ou um “duplo de dados” (*data double*) de pura virtualidade.

Em suma, esses sistemas não estão olhando para o indivíduo, mas para o fluxo de dados e de metadados (12). A perfilização que

**ESSES SISTEMAS
NÃO ESTÃO
OLHANDO PARA
O INDIVÍDUO
MAS PARA O
FLUXO DE DADOS
E DE METADADOS**

é realizada a partir disso opera fragmentos, por exemplo, para realização de marketing. Nesse caso, o que interessa é o fragmento que revela a potencialidade de realização de determinado consumo. Como lembra Fernanda Bruno, a partir de autores como Didier Bigo e Oscar Gandy (13).

Certamente o Estado também investe na captura dessa dimensão dos rastros fragmentados (o risco potencial apontado pelos dados), amparando-se na defesa nacional e na segurança, ou em questões estratégicas e comerciais, para se apropriar dessas informações, mas realiza seu monitoramento e requer informações das empresas de comunicação e telefonia (como nos mostrou Snowden), para reunir rastros e reconstituir o indivíduo passível de punição ou encarceramento (dada sua herança disciplinar), e para obter informações que podem ser politicamente ou comercialmente vantajosas, como nos lembram Assange e Schmidt (14). Trata-se de uma coleta que precisa recorrer aos canais de prospecção de dados das empresas de comunicação e telefonia, mas que se volta para objetivos que, muitas vezes, se ligam ao indivíduo, à nação, à soberania, à competição comercial e à algo que ainda reconhecemos como um todo, talvez mais objetivo. Nesse sentido, ainda que os mecanismos disciplinares e do biopoder estejam ativos, o exercício do poder ocorre de maneira mais incisiva pela via do controle que imprime as táticas, estratégias e que constitui os saberes de nossa época.

A partir dessa perspectiva, a captura de informações realizada pelo mercado libertou-se do indivíduo e das fronteiras, e apenas joga com esses velhos limites. Joga, por exemplo, ao reativar a figura individual que concorda com termos de acesso, de serviço e de privacidade, ao reafirmar essa figura do direito que pouco lhe interessa, ao estimular a constituição identitária e a figura egóica

das redes sociais, ao mesmo tempo em que opera a diluição do indivíduo e da identidade, para extração de valor, para troca de informações que são apenas fragmentos de desejos ou aspirações, pura subjetividade, virtualidade, potencialidade. Aos olhos dos sistemas o que emerge como objeto é o dividuo e não mais o indivíduo.

Ainda que sejam apontadas aqui duas perspectivas para a captura de dados, essa divisão deve ser compreendida como um esforço de desconstrução de algo muito mais complexo, para tornar visíveis os elementos mobilizados a partir de um determinado ângulo, as tensões e conexões entre diferentes atores e as formas como são equacionadas. O cenário caracterizado pelo amálgama entre o Estado e o mercado embaralham as peças desse jogo que Edward Snowden desvelou. Nesse caso, os dados que a Agência Nacional de Segurança acessou, sem conhecimento dos usuários, foram capturados por empresas de serviço de internet e de telefonia como a Verizon, Microsoft, Yahoo, AOL, Facebook, Google, Apple, Skype, dentre outras (15).

A essa altura é importante sublinhar o surgimento de novas formas de resistência e a contestação do que foi exposto. Por um lado, ela pode ser observada em organizações que debatem e atuam sobre

o direito à privacidade; e nos movimentos que buscam problematizar os mesmos dispositivos e sistemas que servem à captura de dados, a partir de sua reapropriação. São muitas as possibilidades emergentes, mas em muitos casos esse movimento de reapropriação passa pela cultura do faça você mesmo, em geral, mencionada como DIY (sigla em inglês para *do it yourself*), pela utilização de software e hardware livres, pela proliferação de laboratórios experimentais em rede (16), por propostas de desviar a função original de determinada tecnologia e pela ideia da contravigilância.

Ainda destacando essas possibilidades de resistência, vale mencionar que questões relativas à privacidade têm sido discutidas por grupos ativistas que realizam oficinas para fazer proliferar o uso de ferramentas que protejam a privacidade dos usuários, como as que possibilitam navegação anônima e troca de mensagens criptografadas. Tanto os laboratórios experimentais como as oficinas surgem nesse cenário como produtores de conhecimento e de novas alternativas e possibilidades de relacionamento com as tecnologias, em especial de informação e comunicação. Apesar disso, no Brasil, ainda é muito incomum que ocorram no ambiente acadêmico (17), em especial, porque a forma como está estruturado esse espaço restringe a incorporação de formas diversas de produção do conhecimento.

Reconhecendo a importância dessa produção, que inclui ainda artistas que problematizam o tema, a Rede Lavits, mencionada anteriormente, tem buscado, promover o intercâmbio de conhecimento e o diálogo entre as produções que ocorrem no meio acadêmico, entre artistas e ativistas. Assim, como dito antes, a rede soma à tentativa de não se restringir a definições de área do saber, a ampliação das vozes e saberes visíveis no debate.

Essas experiências caminham na contramão de falsas e simplistas opções que advogam, por exemplo, a não utilização de redes sociais ou de determinados serviços de email que praticariam uma vigilância de dados mais pesada e não respeitariam a privacidade. Isso porque não há fora desse modo de prospecção de informações, não é possível nos ausentarmos dos sistemas de comunicação e todos estamos incluídos, ainda que não utilizemos determinados serviços. David Golumbia (2015), pesquisador de novas mídias e professor na Universidade da Virgínia (Estados Unidos), em seu texto *Crowdforcing: when what I share is yours* (18) aponta como exemplos dessa lógica a constituição de um banco de dados genético da população da Islândia, que acaba envolvendo mesmo aqueles que não tiveram seus dados genéticos mapeados. Isso porque o mapeamento de parte da população islandesa pode guiar valores de planos de saúde para todos, “premiando” com descontos aqueles mapeados ou, melhor dizendo, “punindo” com valores maiores aqueles não mapeados. Isso ocorre no Brasil, por exemplo, com seguros de carros que diferenciam aqueles usuários que aceitam instalar no carro um localizador (que rastreia por geolocalização o carro e pode extrair daí inúmeras informações) e aqueles que não aceitam.

**A CAPTURA DE
INFORMAÇÕES
REALIZADA
PELO MERCADO
LIBERTOU-SE DO
INDIVÍDUO E DAS
FRONTEIRAS**

Algo similar – em termos de inserção nesse sistema, mesmo sem aderir a algumas opções – serve para aqueles que não utilizam serviços de email do Google, mas que se comunicam com usuários desse serviço. Afinal, basta isso para que o Google possa coletar informações. O termo *crowdfunding* realça, dentre outros, esse sentido de pressão coletiva que torna falsa a opção de estar fora de um determinado sistema.

As formas de resistência e construção de alternativas são muitas, indo desde o uso de câmeras de celulares para denúncia, até os laboratórios experimentais, sendo mais ricas e frutíferas aquelas que buscam as respostas sem se deslocar de onde já estamos inseridos. É a partir da reapropriação da tecnologia e da construção e proliferação de saberes que se pode propor alternativas e não negando a tecnologia ou falsamente se ausentando de alguns sistemas de comunicação.

Este Núcleo Temático da revista *Ciência e Cultura* foi elaborado com o intuito de trazer algumas abordagens sobre o tema da vigilância, mas sem a pretensão de trazer um panorama completo da área. O sociólogo David Lyon, que desde 1992 trabalha com o tema da vigilância na contemporaneidade e com uma série de temas correlatos, como privacidade, transparência, direitos e é coordenador do Surveillance Studies Centre (Canadá), problematiza em seu artigo aspectos da vigilância que se tornaram visíveis a partir das revelações de Edward Snowden. Dentre eles, o artigo explora a indeterminação do limiar entre “vigilância de massa” sobre uma ampla gama de metadados e a “vigilância orientada” que distingue determinadas pessoas em meio às informações, e o uso indiscriminado de “metadados” que coloca em primeiro plano a definição de “dados pessoais”. O autor busca apontar a vigilância também como resultado de uma racionalidade que se expressa em procedimentos burocráticos (e cotidianos) e mais do que o resultado de um potencial tecnológico, observa-a a partir de suas vinculações com uma gestão de riscos e da segurança e com uma clusterização do consumidor no marketing.

Considerando as revelações de Snowden como um marco importante no cenário da vigilância, Lyon ainda problematiza o que já existia em termos de pesquisa quando esse caso emblemático veio à tona, balizando e avaliando as contribuições e o alcance das pesquisas realizadas no campo dos estudos de vigilância até então. Além disso, o autor ainda aponta os desafios para pesquisa e a direção que novas contribuições podem tomar após Snowden.

A seguir, o artigo de Fernanda Bruno se volta para os rastreadores de dados presentes na navegação na internet, na utilização de cartões de créditos e outros sistemas digitais para explorar como funcionam os processos de coleta, categorização e perfilização (*profiling*). Para isso, a autora pesquisou empresas que se dedicam exclusivamente à coleta de dados pessoais na internet e à construção de categorias em bancos de dados e de perfis, com intuito de explorar potenciais desejos e capacidade de consumo ou intenções de voto. A autora vislumbra nesse cenário a constituição de saberes que buscam legitimar-se com base na afirmação da objetividade da coleta de dados e na atribuição do estatuto de evidência aos rastros digitais, elevando a categorização e a construção de perfis ao patamar de ferramenta ideal para revelar verdades, prever e antecipar futuros. Mineração de dados (*data*

mining) e perfilização e *profiling* funcionam assim como os *precogs* de Philip K. Dick em *Minority report* (1956), prevendo o futuro e deslocando-o para o presente não apenas tornam mais provável o que é antecipado, como limitam outros futuros e alternativas possíveis.

Henrique Parra também problematiza a antecipação do futuro e a prospecção de dados, mas o faz a partir da tensão presente na atualidade entre abertura e controle. Nesse cenário, o enorme fluxo informacional (ou *big data*) encontra-se no centro da disputa entre o aumento do dinamismo da economia, a capacidade de inovação e desenvolvimento da ciência e da tecnologia (que muitas vezes pressupõe a abertura de informações) e a apropriação e fechamento das informações pela via dos sistemas de propriedade intelectual. Esse mesmo fluxo é central tanto para a participação cidadã e para a avaliação das ações estatais, como para o exercício do controle social e de uma lógica securitária. Por meio de três eixos que se relacionam com a economia e o modo de produção de riquezas, com a ciência e o modo de produção do conhecimento, com o Estado e a capacidade de gestão, controle e cidadania, o autor traz para o primeiro plano os pontos de contato e tensão entre diferentes atores no embate acerca da informação hoje, ao mesmo tempo que problematiza questões contemporâneas cruciais sobre: participação, transparência, acesso à informação e controle social. Parra ainda faz emergir em seu artigo tanto a racionalidade política, ao explorar questões relativas à governamentalidade, como as demandas que esse cenário de vigilância da informação apresenta no que concerne à privacidade, ao anonimato.

A extração de valor das informações, por meio de sofisticados mecanismos de vigilância e análise dos dados, é retomada no artigo de Rafael Evangelista a partir de uma pesquisa sobre sites de pôquer. O instigante objeto de pesquisa permite trazer a tona de forma mais explícita os paradoxos, ambiguidades e confusões de fronteira (entre lazer e trabalho) que delinham esses ambientes de extração de valor. Ao mesmo tempo que esses espaços e a atividade de jogar pôquer se define como local de lazer, também é um ambiente de trabalho mas na perspectiva, cada vez mais comum na atualidade, que descarta relações salariais e direitos trabalhistas. As práticas de mineração de dados, constituição de perfis, antecipação de cenários futuros e auto-exposição encontram-se, nesse artigo, no centro de decisões de investimento e apostas caracterizando uma espécie de vigilância mercantil, mas acionada dentro dos sentidos de diversão e jogo.

Finalmente, Rosa Pedro, Luciana Albuquerque e Ulisses dos Anjos Carvalho discutem algumas das possibilidades de resistência e anonimato da atualidade que podem ser analisadas na relação entre as redes e as ruas. Se, por um lado, grupos hackerativistas exploram as possibilidades de resistência pela via do anonimato nas redes (tendo como exemplo o grupo Anonymous), outros grupos o fazem pela via do anonimato nas ruas com o uso de máscaras (como fazem os Black Blocs). Não está em questão no artigo a validade ou uma avaliação da atuação desses grupos, mas sim a análise dos sentidos de visibilidade e invisibilidade hoje, temas fundamentais quando se trata de problematizar a vigilância hoje.

Os artigos deste dossiê apontam, em conjunto, para alguns dos principais aspectos e elementos que vêm sendo problematizados quando o tema é vigilância de informações. Incluindo diferentes abordagens teóricas e perspectivas analíticas, os artigos procuram explorar desde os modos de funcionamento, constituição de práticas e saberes, tensões e conflitos, exercício da vigilância ou das formas de captura de informação até a constituição de novas formas de resistência: todos temas fundamentais na contemporaneidade.

Marta M. Kanashiro é socióloga, pesquisadora e professora do Laboratório de Estudos Avançados em Jornalismo da Universidade Estadual de Campinas (Lajor/Unicamp) e líder de pesquisa da Rede Lavits junto ao CNPq. Em 2015, realizou uma pesquisa de pós-doutorado junto ao Surveillance Studies Centre (Canadá).

NOTAS E REFERÊNCIAS

1. Uma publicação bastante representativa dessa área é a *Surveillance and Society*, uma revista científica publicada em acesso aberto, desde 2002: <http://library.queensu.ca/ojs/index.php/surveillance-and-society>. Dentre os vários livros e artigos sobre o tema, um panorama geral sobre as pesquisas que têm sido realizadas pode ser encontrado no *Routledge handbook of surveillance studies* Lyon, D.; Ball, K., Haggerty, K (org.), Nova Iorque e Abingdon: Routledge, 2012. O livro reúne 51 pesquisadores atuando na área, em países como Brasil, Canadá, Estados Unidos, México, Austrália, Israel, Alemanha, Finlândia, França, Holanda e Reino Unido. O Surveillance Studies Centre, do Departamento de Sociologia, na Universidade de Queen's (Canadá) representa, por sua vez, um esforço institucional de reunião das pesquisas sobre o tema <http://www.sscqueens.org/>
2. Marx, G. T. "Your papers please": personal and professional encounters with surveillance". In: *Routledge handbook of surveillance studies*. Lyon, D.; Ball, K., Haggerty, K (org.), Nova Iorque e Abingdon: Routledge, 2012.
3. <http://www.lavits.org>
4. RFID é a sigla em inglês para identificação por rádio frequência. As etiquetas ou *tags* RFID respondem a sinais de rádio enviados por uma base transmissora e podem ter diferentes usos, como localização de animais, implantes humanos (para uso médico ou hospitalar, existem implantes que contêm toda a informação de um paciente que pode ser lida por um médico), em automóveis (para serem localizados), em etiquetas de produtos, medicamentos e livros de bibliotecas para serem administrados, ou em celulares, para *check in* em aviões e hotéis, ou para a compra de produtos pelo celular. Existem *smart cards* que possuem RFID. Neste caso, a leitura de informações do cartão pode ser feita sem contato físico do cartão com a máquina leitora, bastando a aproximação do cartão do equipamento.
5. Castells, M. "A era da informação: economia, sociedade e cultura". In: *A sociedade em rede*. São Paulo: Paz e Terra, 2000. vol. 1
6. Lyon, D. *Surveillance as social sorting: privacy, risk, and digital discrimination*. Psychology Press, 2003.
7. Deleuze, G. "Post-scriptum das sociedades de controle". In: *Conversações*. Rio de Janeiro, Editora 34, 2000.
8. Santos, L.G. "A informação após a virada cibernética". In: *Revolução tecnológica, internet e socialismo*. São Paulo, SP: Editora Fundação Perseu Abramo, 2003.
9. Foucault, M. *Vigiar e punir, história da violência nas prisões*. Petrópolis: Vozes, 2000. Foucault, M. *História da sexualidade I: A vontade de saber. História da sexualidade*. (14a ed.) Rio de Janeiro: Graal, 2001. Foucault, M. *Em defesa da sociedade*. Curso no Collège de France (1975-1976). São Paulo: Martins Fontes, 2002. Foucault, M. *Segurança, território e população*. Curso no Collège de France (1977-1978). São Paulo: Martins Fontes, 2006.
10. É importante notar que a história da criação dos documentos de identidade ajudam a trazer a tona o entrelaçamento entre processos de identificação e de captura de informação sobre a população com o exercício da cidadania, a possibilidade do voto, o uso de sistemas públicos de saúde e de educação. Nesse sentido, é importante afastar aqui qualquer tipo de análise que recaia sobre usos positivos ou negativos, maléficis ou benéficos seja da estatística das populações, dos processos de identificação, ou das possibilidades de coleta de informação. Distante de uma análise que seja maniqueísta, tecnofóbica ou tecnofílica, o objetivo aqui é vislumbrar a construção das relações de poder.
11. Haggerty, K.; Ericsson, V. "The surveillant assemblage". In: *British Journal of Sociology*. Vol. 51, no. 4, december, 2000. p. 605-622.
12. Kanashiro, M.; Bruno, F.; Evangelista, R.; Firmino, R. "Máquina da privacidade". In: *Revista Rua, no. 19. Volume 2, 2013*. Disponível online <http://www.labeurb.unicamp.br/rua/pages/home/lerArtigo.rua?pdf=1&id=211>
13. Bigo, D. (2009) e Gandy, O. (2002) *Apud Bruno, F. Máquinas de ver, modos de ser: vigilância, tecnologia e subjetividade*. Porto Alegre: Sulina, 2013.
14. Assange, J.; Schmidt, E. *Quando o Google encontrou o Wikileaks*. São Paulo: Boitempo, 2015.
15. Destaca-se aqui que os usos das TICs não são únicos, e que os mesmos serviços de empresas de internet podem ser reelaborados pelos usuários. Também várias formas de resistência e construção coletiva de propostas e alternativas têm se dado exatamente vinculadas à utilização das TICs. Ainda assim, a perspectiva aqui assumida tem como intuito perscrutar o *modus operandi* que tensiona esse cenário no sentido de construir um movimento dominante, muitas vezes ligado à criação de oligopólios e de um modo de produção do capitalismo informacional.
16. Fonseca (2014) atribui a denominação "laboratórios experimentais em rede" para uma série de experiências diferentes que abrigam laboratórios comunitários, a cultura DIY (makerspaces), a cultura do conserto e da gambiarra, os hacklabs (laboratórios de cultura hacker), os fablabs (laboratórios de fabricação digital), os medialabs (laboratórios de mídia), a cultura do empreendedorismo e da inovação, a cultura do *open science*, dentre outros. Fonseca, F. S. "Redelabs: laboratórios experimentais em rede" / Felipe Schmidt Fonseca. - Campinas, SP : [Dissertação Unicamp], 2014.
17. É importante destacar aqui que existem exceções nas quais esses laboratórios são desenvolvidos em universidades, como é o caso do Medialab da Universidade Federal do Rio de Janeiro e do Labics da Universidade Federal do Espírito Santo.
18. Golumbia, D. *Crowdforcing: when what I share is yours*, [online] 2015 (disponível online <http://www.uncomputing.org/?p=1658>)