AS APOSTAS DE SNOWDEN: DESAFIOS PARA ENTENDIMENTO DE VIGILÂNCIA HOJE*

David Lyon

> "*1984* é um livro importante, mas não devemos nos limitar à imaginação do autor. O tempo demonstrou que o mundo é muito mais imprevisível e perigoso do que isso" (1) (Edward Snowden)

As revelações sobre a vigilância em massa, feitas por Edward Snowden, oferecem inúmeros *insights* sobre a funcionamento interno da Agência de Segurança Nacional (NSA). Uma das primeiras coisas que se destacaram em termos de notícias foi que a chamada vigilância em massa é realizada sobre as "pessoas dos EUA" assim como sobre os "estrangeiros", que podem incluir aliados próximos. Enquanto alguns detalhes são instigantemente incompletos, a maior parte do grande volume de arquivos e a ampla gama de áreas a que se referem são nada menos que incompreensíveis. E embora as revelações tenham começado a gotejar em junho de 2013, elas continuam a ser lançadas, e consequentemente qualquer comentário está aberto a uma nova alteração.

Além disso, o impacto do vazamento das denúncias de Snowden está agora, [em 2015], sendo sentido mais profundamente em um nível político nacional, e em mais de um contexto. Primeiro, o Freedom Act – aprovado em 2 de junho de 2015, e recuperado com alterações de alguns aspectos do Patriot Act pós 11 de setembro – abrange fundamentalmente a maior parte da coleta de metadados de telefones de cidadãos estadunidenses. Em segundo lugar, em 11 de junho, um importante relatório encomendado pelo governo sobre medidas contra o terrorismo – intitulado *Uma questão de confiança*, de autoria de David Anderson – solicitou restrições na Agência de Espionagem do Reino Unido (GCHQ). Em particular, isso é altamente crítico do sistema de supervisão das agências de inteligência existentes. Nada disso teria sido possível sem Snowden.

Tanto o que pode ser apreendido a partir dos documentos divulgados, quanto o que pode ser visto de seus impactos diretos fornecem a base para revisões sérias de algumas suposições sobre a vigilância no século XXI. Para dar um exemplo, o próprio termo "vigilância" pode exigir algumas novas qualificações. O que se sabe sobre as práticas da NSA levanta questões sobre a suposta clara distinção entre "vigilância de massa" e "vigilância orientada", e o uso indiscriminado de "metadados" que coloca em primeiro plano debates de longa data sobre como definir "dados pessoais" (ou "informações pessoalmente identificáveis"). O que vale para o "sujeito" da vigilância aplica-se à "privacidade" também. Cada qual requer alguma reflexão séria.

Sobre essas questões, vistas como controversas pelos próprios defensores das práticas da NSA, existem ainda poucas opiniões equilibradas. Se os dados são procurados em uma base de "massa", a partir de vastas faixas de uma dada população, com vistas a identificar algoritmicamente através de correlações quem poderia ser uma "pessoa de interesse", o ponto em que a "vigilância de massa" se torna "vigilância orientada" tem, na melhor das hipóteses, um limiar indeterminado. E se o tipo de dado obtido for, de fato, metadado, como o endereço IP, a duração de chamada, os amigos que foram contatados? – então eles compreendem exatamente os tipos de informação que um detetive pode procurar: quem falou com quem, quando e por quanto tempo? Apesar dos protestos contrários, é difícil negar que tais metadados sejam estritamente "pessoais", especialmente agora que o Freedom Act dos EUA limita explicitamente essa coleta.

Que as atividades da NSA e suas agências parceiras ao redor do mundo são controversas está bastante claro nos esforços do governo em mais de um país para usar o termo *bulk collection* (coleta de massa) de dados em vez de "vigilância em massa" (2). Em um caso, em 2000, o Tribunal Europeu de Direitos Humanos concluiu que até mesmo o armazenamento de dados relacionados à "vida privada" de um indivíduo se enquadra na aplicação do artigo 8.1 da Convenção Europeia dos Direitos Humanos (3). Mas os debates sobre isso são ferozes em países como o Reino Unido e Estados Unidos. Este artigo argumenta que a coleta e análise de metadados, incluindo conteúdo das comunicações, é melhor pensado como "vigilância de massa", mesmo que, como mencionado acima, a localização de "suspeitos" seja o objetivo principal.

Estudos de vigilância, o campo multidisciplinar de pesquisa dedicado à compreensão, no contexto contemporâneo, de práticas tais como monitoramento, rastreamento e identificação, está bem posicionado para responder aos novos desafios colocados pelos arquivos de Snowden. No entanto, o caso aqui é que, enquanto alguns desafios são diretos, para a nossa compreensão de aspectos substantivos dos processos de vigilância, outros são indiretos. Ainda que não se pretenda fazer aqui uma análise exaustiva, sugere-se que os estudos de vigilância podem fazer contribuições significativas para considerar cada tipo de desafio.

Os próprios comentários de Snowden acerca de Orwell seguem também nessa direção. Levando em conta que, para muitas pessoas, o espectro do *big brother* ainda é o que alimenta a imaginação sobre a vigilância em massa, existe a necessidade de colocar o conto distópico e preventivo de Orwell no contexto. Para Snowden, isso é principalmente um questão tecnológica; "exóticos" microfones escondidos em arbustos e a tela que pode nos observar deu lugar a webcams e microfones em rede em telefones celulares. Mas enquanto Orwell não pode ser culpado por não prever as consequências da chamada revolução da informação, vale a pena recordar que, como Max Weber ou Hannah Arendt (4), Orwell também viu a vigilância em parte como um resultado de uma racionalidade implacável expressa em procedimentos burocráticos. Essa condição cultural limitante sem dúvida ajuda a explicar por que a vigilância é, em certo sentido, retrolimentada. Mas mais do

que isso é necessário para indicar, em especial, a diferença que é feita através do digital.

A convicção de Snowden é que, devido à vigilância, "(...) o mundo de hoje é muito mais imprevisível e perigoso" do que Orwell poderia ter adivinhado. Isso representa também um verdadeiro desafio lançado por Snowden, não só para atualizar nossa compreensão de novas tecnologias, mas também para colocar todo e qualquer sistema tecnológico, em seus devidos contextos social, político-econômico e cultural. O uso de metadados, por exemplo, não é um simples resultado do potencial tecnológico, como a expansão exponencial da capacidade de armazenamento, mas de abordagens específicas como a gestão de risco nas indústrias de segurança e de clusterização do consumidor no marketing, cada um dos quais tem aumentado em importância em contextos onde a globalização – entendida como o neoliberalismo – reina.

A seguir, três tipos de desafios são identificados e discutidos. O primeiro, "pesquisa negligenciada" em um sentido histórico: por que as revelações de Snowden causaram respostas tão chocantes e indignadas, como se fosse a primeira vez que ouvíamos algo sobre vigilância em larga escala no início do século XXI ou mesmo no final do século XX? O segundo tem mais a ver com desafios substanciais e atuais que emergiram das próprias revelações. Eu o nomeei "déficit de investigação". Indico algumas áreas que exigem alguma reavaliação séria para nossa compreensão da vigilância hoje. O terceiro, "direção de pesquisa", apontamentos para o futuro, sugere que o contexto mais amplo das revelações Snowden é o destino da internet. Vigilância nunca deveria ser pensada como uma dimensão discreta do mundo moderno. Hoje, ela não pode ser entendida sem investigar informações e seu canal corrente, a internet. Finalmente, eu retorno para as questões de como repensar a "vigilância" e a "privacidade" hoje.

Essas, então, são as apostas Snowden. As revelações têm sido mantidas vivas nas manchetes, exatamente porque muita coisa está "em jogo", não apenas para os estudos de vigilância ou para o futuro da internet, mas de forma mais significativa, para a privacidade, os direitos humanos, as liberdades civis, para a liberdade e a justiça.

PESQUISA NEGLIGENCIADA As revelações de Snowden continuam a ser manchete e vários eventos diplomáticos importantes foram provocados por eles. Angela Merkel, chanceler da Alemanha, e Dilma Roussef, a presidente brasileira, por exemplo, expressaram que estavam chocadas com a descoberta que suas conversas feitas por telefone celular foram monitoradas (5). Da mesma forma, populações fora dos EUA reagiram negativamente ao descobrir que a NSA tem sido ativa de formas inesperadas no seu território nacional. No Canadá, por exemplo, foi divulgado que a NSA tinha se estabelecido na capital, Ottawa, a fim de monitorar o G8, a reunião do G20 em junho de 2010 (6).

Em termos gerais, pelo menos três elementos das práticas de vigilância tornaram-se notadamente evidentes durante e após 2013. Primeiro, os governos se envolveram em vigilância em massa sobre os seus próprios cidadãos. A NSA trabalha em estreita colaboração com o "Five Eyes", Austrália, Canadá, Nova Zelândia e Reino Unido, e suas atividades também são replicadas em muitos outros países. Segundo, corporações partilham seus "próprios" dados com o governo, para benefício mútuo. Isso acontece em especial com empresas de internet que, conscientemente ou não, tornam-se coniventes com o governo para fornecer dados pessoais. Terceiro, os cidadãos comuns também participam através de suas interações – especialmente no uso de redes sociais e de telefonia celular. Sem necessariamente estarmos cientes disso, todos nós fornecemos dados para a NSA e suas agências cognatas, apenas entrando em contato com os outros por via eletrônica (7).

Apesar das revelações grandiosas, deve ser ser dito que havia pouco que fosse completamente novo sobre os três elementos de vigilância mencionados aqui. A importação maciça das divulgações feitas por Snowden assentada sobre um estoque substancial de provas claras apontando para a realidade presente e vindoura da vgilância de massa, foi o fato indubitavelmente novo. Quando as notícias surgiram pela primeira vez no jornal *The Guardian*, em 5 de junho de 2013, vários fatores foram surpreendentes. Verizon, a gigante das telecomunicações, foi obrigada pela NSA a dar informações sobre todas as ligações telefônicas dentro dos EUA e entre os EUA e outros países, entre abril e julho daquele ano. Espionagem secreta e doméstica, em uma escala espantosa, estava acontecendo sob a presidência de Obama (8). Mas o alvoroço internacional contra as realidades reveladas sobre a vigilância em massa deu a impressão que os cidadãos estavam bastante inconscientes e despreparados para o que eles estavam ouvindo.

Isso sugere que a vigilância não estava de fato no radar da maioria dos cidadãos comuns. Mas ainda assim, para aqueles envolvidos no exame de vigilância e na proposição de respostas legais, técnicas e políticas, a sensação de inconsciência dessa realidade pode ter vindo como uma espécie de decepção; é fácil superestimar a recepção de nosso próprio trabalho. Além disso, a maioria das respostas se preocupavam com o ataque à privacidade, interpretado como um problema pessoal – entendido como individual –, que demonstra pouco entendimento sobre as formas que a vigilância também funciona como classificação social, visando principalmente grupos populacionais antes de indivíduos, ou sobre como a privacidade diz respeito também a questões relativas a direitos humanos e justiça social. A principal exceção ao foco individualizante sobre a privacidade está entre aqueles cuja preocupação é que a privacidade das comunicações tenha sido flagrantemente violada, o que traz, em especial, questões importantes sobre a confiança.

O debate popular e na mídia sobre Snowden se concentrou, muito frequentemente, em estado de vigilância, principalmente como uma ameaça para os indivíduos, exceto quando o desafio a uma internet livre e aberta foi reconhecido. Além disso, as evidências mostram que o poder arbitrário é usado contra todos os cidadãos quando a vigilância em massa é praticada. Como um bom número de advogados têm argumentado, já há algum tempo (9-11), a privacidade não é apenas uma questão individual. Vigilância e privacidade podem ser consideradas ao longo de um espectro de relações,

desde a mônada até a multidão. Por definição, a vigilância em massa significa que toda e qualquer pessoa pode ser apanhada na rede de vigilância e quanto maior a escala de vigilância, mais provável é que falsos positivos surjam na busca de "pessoas de interesse". Essas questões são trazidas abaixo.

Apesar de duas décadas de crescimento dos estudos de vigilância, parece haver pouca compreensão pública sobre como a vigilância é praticada hoje. Os tipos de práticas descobertas por Snowden são aquelas que têm um longa história, não apenas nos anais de coleta da inteligência e das agências nacionais de segurança, mas em esferas que vão desde o policiamento e a administração pública, até o marketing de consumo. Isso deveria ser salutar para aqueles envolvidos no estudo acadêmico da vigilância e, na verdade, para qualquer um que se preocupa com liberdade, democracia e justiça no século XXI (para uma crítica sem tabus ver 12). Vale a pena rever brevemente esse desenvolvimento.

Na década de 1980, os interessados no estudo da vigilância estavam preocupados principalmente, por um lado, com a vigilância do Estado (13-14), e por outro, com a vigilância no local de trabalho (15-16). Mais amplamente, a vigilância a serviço do "controle social" foi discutida em relação ao policiamento e à gestão de infratores (17-18), e essa dimensão já foi objeto de fusão, em parte, com questões de "segurança nacional". No entanto, pesquisa sobre vigilância sobre o consumidor – e suas ligações com os sistemas de administração pública também estavam disponíveis nessa época (ver o trabalho pioneiro de Rule em 19), mas a vigilância sobre o consumidor não seria reconhecida como parte da corrente principal dos desenvolvimentos da vigilância até os anos 1990 (ver principalmente Gandy em 20). Sem exceção, esses autores salientaram o impacto da informatização sobre os rumos que essas formas existentes de vigilância, incluindo câmeras públicas de vídeo, iriam se desenvolver.

PARECE HAVER POUCA COMPREENSÃO PÚBLICA SOBRE COMO A VIGILÂNCIA É PRATICADA HOJE

Na década de 1990, no entanto, o termo "sociedade da vigilância" estava muito mais em uso como um termo que indicava que as formas que antes pareciam estar restritas às atividades de governo, relativas ao policiamento ou ao trabalho foi transportado para a vida cotidiana (21). Este termo, de forma alguma minimizava a importância da vigilância de Estado, mas indicava que a vigilância sistemática de muitos tipos poderia ser esperada simplesmente como resultado da realização de assuntos diários. Cada vez mais, a vigilância tornou-se visível através de câmeras onipresentes em vias públicas e locais, tais como centros comerciais, no uso de cartões de crédito e, progressivamente, cartões de fidelidade, além de, em alguns aspectos rudimentares, por meio de interações online que se expandiram após o desenvolvimento da World Wide Web, em 1994, e a subsequente comercialização da internet, a partir de 1995.

No início de 2000, ocorreram dois eventos que moldaram decisivamente a direção da vigilância, embora as potenciais conexões entre eles não se tornaram públicas até 2010. Um deles foram os ataques de 11 de setembro de 2001, e também os atentados em Londres de 7 de julho de 2005, e em Madrid, que consequentemente impulsionaram muito a vigilância relacionada com a segurança, pelo menos, no norte global. Curiosamente, as atividades do Departamento de Segurança Interna (DHS), formado às pressas, recebeu algumas sugestões do Gerenciamento de Relações com o Consumidor (CRM) na formulação do programa anti-terrorista Total Information Awareness (TIA) (7). O outro foi o aparecimento definitivo das mídias sociais, simbolizadas pela invenção do Facebook em 2004, que rapidamente se estabeleceu como a principal dimensão da internet, facilitando simultaneamente novos níveis de vigilância do consumidor (para não mencionar a vigilância social Marwick, ver 22-23), agora baseada na auto-expressão de preferências e gostos. Na posse do presidente Obama, em 2009, o Departamento de Segurança Interna desenvolveu um Centro de Monitoramento de Redes Sociais para buscar "itens de interesse" (24).

Em certo sentido, então, as revelações de Snowden podem estar funcionando como uma chamada para que públicos ainda inconscientes acordem para a vigilância em massa dos cidadãos comuns, que já raiou. Se já não fosse clara, depois de 11/9 a lógica da já intensificada "segurança nacional" (25) tornou-se proeminente, assim como o uso de análise de dados (agora geralmente referidos como *big data*, ver 26). O programa TIA era dependente de um amplo banco de dados utilizando "novos algoritmos para mineração, combinando e refinando os dados" (27) que incluía o uso da máquina bancária, rastros de cartão de crédito, cookies de navegação na internet, arquivos médicos – qualquer coisa, de fato, que pudesse produzir correlações interessantes, que pudessem indicar relações significativas entre os registros. Os arquivos que Snowden publicizou estão exatamente entre os métodos utilizados pela NSA para sua vigilância tanto nacional e internacional.

Sem dúvida, Snowden está certo em levantar questões sobre privacidade, liberdades civis, incluindo a liberdade de expressão, de comunicação e de reunião de pessoas – e direitos humanos na relação para as quais suas descobertas sobre a NSA e suas agências cognatas foram expostas em todo o mundo. Mas o que muitos estudos de vigilância, ao longo das últimas duas décadas, têm mostrado é que questões mais profundas são levantadas e que desafiam muitas suposições convencionais sobre as sociedades contemporâneas, suas atuais formas de poder, suas políticas e os seus processos e instituições democráticas. Conforme a análise apresentada acima mostra, esta não é apenas uma questão de poder burocrático eletronicamente aprimorado indo para cima de cidadãos desafortunados. Ele também tem a ver com a forma como os cidadãos se envolvem com o cotidiano, na comunicação, interação e troca, muito do que ocorre com dispositivos digitais. Discutivelmente, então, isso também é

uma questão de uma cultura de vigilância (28), na qual uma crescente proporção da população mundial vive e na qual, por inúmeras razões, muitos estão se acostumando.

Bem como as mais fundamentais questões socioculturais suscitadas pelas descobertas de Snowden, as questões chave da vigilância contemporânea também podem ser discernidas através da consideração de algumas das principais tendências que têm se tornado cada vez mais evidentes por volta da última década (e que na seção seguinte, vamos explorar como alguns delas se cruzam com três questões centrais e específicas de Snowden). Além do crescimento exponencial da vigilância, como isso tem se tornado crescentemente um modo básico de prática organizacional, muitas outras tendências significativas podem ser identificadas (29-30).

Como mencionado anteriormente, a segurança está se tornando um fator-chave da vigilância, não só em nível "nacional", mas também em tipos gerais de policiamento, segurança urbana e em locais de trabalho, sistemas de trânsito e escolas (31). Essa é, obviamente, uma questão chave e repleta de problemas básicos de definição, que também se relacionam a seu status como uma racionalidade política amplamente utilizada para uma série de medidas controversas. O tipo de "segurança nacional" que pede aumento da vigilância, sem dúvida, tem pouco em comum com os tipos de segurança – de coisas como escassez, medo, até mesmo a liberdade – que muitos podem pensar que beneficiaria suas comunidades e famílias. Além disso, na prática, muitas tentativas atuais de obter a segurança nacional parecem colocar em perigo as liberdades civis e os direitos humanos básicos para a prática democrática (32).

Ao mesmo tempo, deve-se reconhecer que não apenas "segurança", mas também alguns motivos muito mais mundanos são significativos no desenvolvimento de vigilância hoje. Um deles é a "eficiência", que incentiva o uso de políticas de redução de custos e soluções de tecnologia intensiva; e o outro é a "conveniência" que domina grande parte do apelo do marketing para os consumidores. Sob tais motivos tão ordinários a vigilância se expande em ritmo acelerado, como as tecnologias de produção de provas (como Josh Lauer os chama) que são adotadas por razões que são rotineiras e cotidianas.

"Segurança", por outro lado, ainda é um motivo superior entre esses "condutores". Para o filósofo Giorgio Agamben, a segurança como um motivo oculto da vigilância contemporânea pode estar superando não só a democracia, mas a própria política (33) e essa percepção pode pelo menos servir como um teorema a ser explorado. Ao mesmo tempo, esta tendência deve ser vista ao lado de outra, o entrelaçamento – e, em alguns aspectos, a integração – de órgãos públicos e agências privadas. O governamental e o corporativo sempre trabalharam em conjunto nos tempos modernos, mas a ideia de que eles habitam essencialmente esferas diferentes, com diferentes encargos, está atualmente se desfazendo. Como revelou Snowden, empresas de telefonia como a Verizon e empresas de internet tais como a Microsoft trabalham em conjunto com as agências estatais, como a NSA, em formas que ainda não foram totalmente compreendidas.

Várias outras tendências importantes também merecem menção, mesmo que apenas para marcar o quão significativas (29). Vigilância móvel e baseada em localização está se expandindo, o que significa que as coordenadas de tempo e espaço das nossas vidas são cada vez mais monitoradas. A vigilância é cada vez mais incorporada em ambientes do cotidiano, tais como edifícios, veículos e residências. Máquinas reconhecem proprietários e usuários através do deslizamento do cartão ou da ativação de voz. O corpo humano é a própria fonte de dados de vigilância, com registos de DNA, impressões digitais, reconhecimento facial, todos vistos como sendo meios confiáveis de identificação e verificação. Além disso, todas essas tendências estão sendo rapidamente globalizadas, o que é em si mesma uma tendência de importação da vigilância. Como mencionado acima, vigilância social através de sites de redes sociais está aumentando, um tópico que nós retomaremos abaixo. E, em tudo isso, torna-se cada vez mais difícil saber exatamente o que conta como "dados pessoais". Placas de veículos, presença em fotos de grupo postadas em mídias sociais e, claro, metadados tornam difícil a definição.

Todo o ponto de vista acima surge como desafio para os estudos de vigilância, em particular, e para todo e qualquer cidadão de democracias liberais contemporâneas em geral. Há, contudo, algumas perguntas mais específicas para as quais eu agora chamo a atenção. Estas são áreas que, depois de Snowden, somos obrigados a dizer que a atual pesquisa sobre vigilância simplesmente ainda não sabe o suficiente.

DÉFICIT DE PESQUISA Se o problema histórico é a aparente indiferença às pesquisas sobre a vigilância, permitindo uma sensação de surpresa, em vez de expectativa sóbria, então o problema contemporâneo é que a pesquisa atual ainda não alcançou alguns desenvolvimentos vitais da vigilância. Em cada caso – infraestruturas digitais, redes profissionais e práticas das mídias sociais – a dificuldade de identificar o objeto da pesquisa é agravada pela linguagem enganosa, suposições dúbias e teoria inadequada. Não há nenhuma conspiração aqui, apenas um nevoeiro analítico que tem que ser limpo antes que os contornos de cada situação possam ser vistos de forma mais acentuada.

A primeira questão é aquela que pode ser vista de forma mais dramática em relação à computação em nuvem (névoa de novo?) e a transferência eletrônica de dados de um lugar a outro. A metáfora da nuvem, originada dos diagramas, destina-se a demonstrar como as informações são movimentadas (34). A impressão dada – reforçada através do marketing da nuvem – é de que, de alguma forma, os dados voam levemente através do éter, quando de fato os canais reais são cabos de fibra óptica. Existe um elemento geográfico material para a nuvem que desmente a imagem afável, macia e flutuante. Esse elemento geográfico e material é crucial para as configurações do poder. Parte disso tem a ver com o papel de liderança dos EUA, através da NSA. Como Andrew Clemente mostra, arquivos de dados enviados pela Universidade de Toronto para o governo de Ontário (a alguns quarteirões de distância, também em Toronto) realmente viajam por cabos

de fibra ótica em um padrão de *boomerang* para tratamento e troca de dados nos EUA, antes de chegarem ao seu destino no Canadá (35). Eles, assim, viajam, embora em um regime de dados completamente diferente do Canadá. Mas novas configurações de poder também são geradas pela capacidade de acessar dados digitais, o que depende da cooperação entre os países participantes, a fim de adotar um posicionamento geral do funcionamento da internet.

Os programas da NSA usam esses cabos para coletar (Upstream, Quantuminsert – ver também versões comerciais tais como programas para hackear, 36) e para interceptar (Tempora) dados. Interceptadores são colocados estrategicamente ao longo das rotas de cabos, uma prática realizada por muitos países, como mostra o trabalho de Snowden, e através de acordos de segurança da Global Crossing com empresas privadas, muitos dos cabos de fibra óptica do mundo ficam acessíveis para os EUA (37). Vigilância mais direcionada ocorre usando sistemas como Xkeyscore, que está ligado ao programa Prisma. Xkeyscore também armazena o material em *caches* de dados espalhados ao redor do mundo em locais específicos (38). O Prisma, por sua vez, depende dos dados do consumidor obtidos de empresas de internet através de redes sociais e plataformas em nuvem (como o Dropbox, ver 39).

A segunda questão é que é difícil definir exatamente quem está realizando vigilância. Embora o termo vigilância de "Estado" seja comum na linguagem cotidiana, aqueles que substituem funcionários do "Estado" são muitos e variados, e isso decorre do ponto acima sobre a indefinição entre os setores público e privado. A própria posição de Snowden antes de sua partida com os documentos ilustra isso. Ele trabalhou para a Booz Allen Hamilton, cuja expertise foi subcontratada pela NSA. Didier Bigo (40-43) já há algum tempo chamou a atenção para as formas em que "os profissionais de segurança" agora formam uma rede internacional, operando em diferentes países, mas com ampla cooperação. Esses agentes da inteligência, especialistas técnicos, polícia (tanto públicos, quanto privados), consultores e outros – cuja gênese reside na cooperação internacional contra o terrorismo pós-11/9 – , agora se expandiram em uma rede claramente discernível de considerável influência.

É importante ressaltar que as distinções mais velhas se decompõem conforme essa rede de "gestores da inquietação" (como as chama Bigo) se desenvolve. Eles conectam órgãos públicos e privados, segurança interna e externa, interesses nacionais e internacionais e assim por diante. Este desenvolvimento cresce junto com a digitalização da segurança e da vigilância de tal forma que, paradoxalmente, a segurança "nacional" não é mais "nacional" "(...) na sua aquisição ou até mesmo na sua análise de dados (...)", que ajudam a borrar "(...) as linhas do que é nacional, bem como os limites entre a aplicação da lei e inteligência" (44). Esse problema está relacionado com outro, mencionado acima, sobre a incerteza de quem realmente exerce a vigilância, embora o ponto adicional aqui seja uma afiliação frouxa de organizações profissionais que podem ser identificadas. Eles trabalham juntos, aprendendo uns com os outros e desenvolvem os seus próprios protocolos, justificativas e práticas de vigilância.

Como mostram os exemplos dos Estados Unidos, práticas de vigilância semelhantes ocorrem em todos os domínios, seja na DHS, CIA, FBI ou a NSA (ou, para essa questão, no GCHQ do Reino Unido ou no CSEC do Canadá). Esses "acrônimos" de organizações policiais e de inteligência também contam com organizações similares e subcontratadas que também exibirão atividades técnicas, estatísticas e político-econômicas semelhantes (41). Ambos, policiamento e as agências de inteligência, têm conexões militares que também influenciam as suas práticas, assim como o tráfego é bidirecional: a manipulação da informação é fundamental para cada um, de tal forma que o policiamento se torna mais pesado (45) e também mais flexionado pelo método militar (46). Em todos os casos, também é claro que tais organizações não apenas reagem à percepção de ameaças para a segurança nacional ou a atos criminosos. Elas constroem ativamente as populações-alvo e refinam as razões para fazê-lo-. Este é o lugar onde as ligações comerciais com empresas de tecnologia também se tornam centralmente significativas, em conjunto com atores governamentais. Políticas influenciam e são influenciadas por abordagens e práticas técnicas e corporativas. Em nível organizacional e de rede, então, essas relações são múltiplas e complexas.

A terceira questão "déficit de pesquisa" tem a ver com os tecidos que conectam essas redes organizacionais e suas práticas com os temas de vigilância ou, mais propriamente, com populações-alvo. A internet e, acima de tudo, as mídias sociais, são cruciais aqui, embora o uso do celular seja uma outra dimensão vinculada a mesma questão. É importante lembrar que mídia social é um fenômeno do século XXI, de proveniência bem recente. No entanto, tem crescido a uma velocidade espantosa e com alcance global tão incrível que é agora um dos aspectos dominantes da utilização da internet. Enquanto muita pesquisa social significativa tem sido realizada nessa área – particularmente com a ajuda de instituições como Oxford Internet Institute, no Reino Unido, ou o programa Pew Internet and American Life –, compreender como os usuários de mídias sociais operam em relação a práticas e conceitos relativos a vigilância e privacidade ainda é um subcampo incipiente e uma prioridade vital de investigação (47-49).

Em um quadro histórico mais amplo, pode parecer estranho que os usuários de mídias sociais permitam a circulação livre, ampla e promíscua de dados pessoais online, tornando-os vulneráveis à intensa vigilância tanto das corporações que buscam os seus dados para fins de marketing, como pelo policiamento e pelas agências de inteligência. Tal disposição e submissão certamente teriam intrigado e incomodado um Orwell, sintonizado como ele era com o uso de novas tecnologias para conseguir subserviência popular ao Estado. Mas existe uma sensação forte de que a situação de hoje é decididamente pós-orwelliana. Não apenas as tecnologias de vigilância foram extremamente atualizadas, mas as práticas de vigilância são comuns a todas as organizações, o que equivale a "regimes" de vigilância (50) e, como já referido anteriormente, uma cultura de vigilância. Dentro de tal cultura, a vigilância não é apenas uma forma de entretenimento, mas também algo encontrado na vida cotidiana

e na qual muitos, conscientemente e ativamente, envolvem-se. Vidas são vividas, em parte, online.

A questão de pesquisa que se apresenta aqui é o impacto, a longo prazo, das revelações Snowden e suas consequências futuras no sentido de informar e, talvez, reorientar as práticas de usuários de mídias sociais. Isso envolve análises cuidadosas de como os usuários percebem as situações em que se encontram e as práticas que eles desenvolvem online. Por exemplo, pesquisadores do Pew descobriram que os usuários de redes sociais não estão dispostos a discutir sobre Snowden online – e offline também – preferindo ambientes mais seguros, como uma mesa de jantar para tal conversas (51). Assim este é um desafio para a pesquisa de políticas e de defesa que esteja disposta a ir além dos entendimentos convencionais de vigilância e, principalmente, de privacidade (52).

Isso também envolve novas investigações sobre o potencial de comunicação da internet para problematização e resistência a formas de vigilância consideradas excessivas, desnecessárias ou ilegais. Por um lado, numerosas ONGs e grupos de lobby e pressão relacionados com a internet formaram um movimento social diferente para exigir a responsabilização por e transparência sobre as práticas de vigilância expostas por Snowden (53). Por outro lado, o engajamento cotidiano dos usuários com as mídias sociais pode ser reflexivamente informado pelo conhecimento crescente de como a vigilância funciona no mundo após Snowden. Conceitos como "exposição" (54) encontram novo significado crítico para a compreensão de como, quanto, e sob quais circunstâncias os usuários revelam dados pessoais para os outros.

Essas questões levam a um questionamento mais geral sobre o futuro da pesquisa sobre vigilância relacionada com internet, que, como argumento na próxima seção, cresceu em importância para se firmar hoje como uma área-chave – no sentido de que isso informa muitas outras áreas – nas pesquisas sobre vigilância.

DIREÇÃO DE PESQUISA

> Liberdade na internet – a capacidade de usar a rede sem constrangimentos institucionais, de controle estatal ou social, e sem medo difuso – é fundamental para a concretização da [sua] promessa. Convertendo a internet em um sistema de vigilância esvazia-se então seu principal potencial. (55)

Qualquer campo de estudo, incluindo o de vigilância, é obrigado a avaliar, de tempos em tempos, os principais campos de força que moldam o objeto de análise. Hoje, a internet está ligada à vigilância em diversos níveis e, portanto, merece uma atenção especial. Esta seção argumenta que a direção dos estudos de vigilância deveria ser fortemente flexionada por questões da informação e da internet. Os tipos de vigilância desenvolvidos ao longo de várias décadas são fortemente dependentes do digital e, cada vez mais, no que é agora rotulado como *big data* – mas também se estendem para além disso. Como Greenwald indica, as revelações Snowden levantam como questão-chave o futuro da internet. Embora seja verdade que as sociedades modernas têm sido "sociedades da informação" – e, portanto, "sociedades da vigilância" – desde seu princípio (56), hoje, informação e seus canais centrais tornaram-se uma arena sem precedentes de luta política, centrada na vigilância. Isso sugere que tanto analiticamente, em termos de direção de pesquisa, como politicamente, em termos de prática e política, internet e vigilância estão vinculadas em uma relação mutuamente informante.

O uso da internet para a vigilância não é novo, mas o seu alcance nunca foi tão grande. Para muitos, como Greenwald e o próprio Snowden, esta é uma grande traição da onda inicial de otimismo sobre o potencial democrático com o qual a internet nasceu. O esperado benefício humano é pré comercialização da internet, mas versões disso também foram tecidas em muitas aspirações corporativas no Vale do Silício e em outros lugares a partir dos anos 1990. Alguns escritores populares e prescientes como Ithiel de Sola Pool (57) previram o desenvolvimento do que hoje chamamos de internet, argumentando que era uma chave para liberdade tecnológica. Ele insistiu que a liberdade de expressão se tornou uma questão vital. Como regulação e acesso forem organizados iria determinar se as novas comunicações reforçariam a democracia como plataforma política e como a imprensa escrita tinha feito antes.

O que aconteceu com os sonhos utópicos dos filósofos da "Revolução da Informação" da década de 1980? Afinal, eles haviam observado corretamente as possibilidades emancipatórias e democratizantes oferecidas pelas novas tecnologias. Mas Ithiel de Sola Pool e outros da sua ala talvez tenham prestado pouca atenção à economia política já existente sobre tecnologias de informação – sem mencionar a abrangente crença cultural no poder da tecnologia. Juntos, eles falharam em notar que as novas tecnologias deveriam ser consideradas eficazes, a despeito das evidências em contrário, e para ver as falhas na análise que enxerga o conhecimento como um fator novo e independente de produção. Seguindo Karl Polanyi (1944-2001), pode-se pensar o conhecimento informacional como de fato uma "mercadoria fictícia" que tem sido destacada de suas origens sociais no trabalho criativo, como uma forma "independente" em sistemas especializados ou serviços virtuais (58), integrado em um sistema econômico de mercantilização geral, onde o lucro é a base, e é atribuído pelo mercado, em que a reciprocidade ou a justiça social têm pouco ou nada a dizer (59-60). A mercantilização da internet em 1995 foi um momento crítico no desenvolvimento mais geral da informação como mercadoria fictícia.

No entanto, trinta anos de comentários de De Sola Pool sobre a liberdade de expressão chegaram dramaticamente na figura dos documentos liberados por Snowden. A essa altura, as questões se tornaram polarizadas. No encalço das notícias sobre o acesso da NSA aos dados de assiantes da Verizon vieram as revelações sobre o programa Prisma que implicava diretamente sobre as grandes empresas da internet, como Microsoft, Yahoo, Google e Facebook. Intercâmbios urgentes ocorreram, alguns dos quais envolveram alguma perplexidade por parte do empresas: sim, elas tinham cedido alguns dados,

mas as revelações pareciam sugerir que quantidades muito maiores do que elas próprias haviam autorizado estavam envolvidas. Como transpareceu, além do acesso autorizado aos dados (FISA) mantidos pelas empresas de internet, a NSA também havia encontrado maneiras para interceptar um montante no fluxo de dados, usando sistemas como Muscular, desenvolvido pela NSA, junto com o parceiro do Five Eyes, o GCHQ do Reino Unido (61).

Como Steven Levy observou em um artigo da *Wired* (62), as "revelações" de Snowden expuseram um "(...) conflito aparentemente insolúvel. Enquanto o Vale do Silício deve ser transparente em muitos aspectos, as agências de espionagem operaram sob um manto de ofuscação".

As descobertas de Snowden jogaram um holofote sobre uma questão que as empresas da internet já estavam conscientes há alguns anos. Empresas como Google, Yahoo e Twitter tinham lutado para se manter fora das tentativas do governo, através do tribunal do Ato de Vigilância de Inteligência Estrangeira (FISA), que as obrigava a entregar dados dos consumidores. Para seu crédito, as empresas parecem ter tentado afastar tais esforços (63), mas a combinação do poder do governo e o fato de que as empresas também tinham contratos e compromissos com o governo comprometeu um pouco a luta. O Prisma focalizou o embate, mas o segredo envolvendo a NSA dificulta saber exatamente o que está acontecendo. Eles estão lutando em uma névoa. Isso também apresenta problemas para aqueles que tentam pesquisar as relações de vigilância entre governo e corporaçoes.

Os detalhes das controvérsias e batalhas em curso pode ser encontrado em vários sites (64), mas o tema que os une é a vigilância e o futuro da internet. Isso tem várias implicações para as análises e para a ação.

Um resultado importante é que aqueles que estudam vigilância perceberam que aqueles que pesquisam as comunicações têm muito a oferecer. Desde o trabalho pioneiro de Oscar Gandy ou Joseph Turow sobre vigilância do consumidor, até as explorações de Mark Andrejevic ou Alice Marwick sobre vigilância online (20; 65-68), para não mencionar os trabalhos em curso sobre vigilância das comunicações, as conexões são claras. Aqueles cujo conhecimento de vigilância está na criminologia ou em política pública, em especial, podem precisar reforçar suas análises examinando, mais de perto, a forma como a internet se cruza com a sua compreensão sobre vigilância. Do mesmo modo, aqueles que abordam a vigilância na internet fariam bem em olhar para as bibliografias sobre vigilância e privacidade, concebidas mais amplamente (69).

A segunda área é explorar ainda mais as possibilidades analíticas para considerar a informação como uma *commodity* fictícia. Pode-se argumentar, por exemplo, com o forte impulso na direção do chamado *big data*, que a separação das conexões entre a informação e as suas raízes sociais está agora ainda mais pronunciada. Na análise de Katherine Hayles a informação perde o seu corpo desde a década de 1950, nas Conferências Macey sobre a teoria da comunicação. Mas eu argumentaria que agora os chamados dados pessoais progressivamente perdem a sua "pessoa" (26). Quando os dados coletados para fins comerciais (marketing) propõe – o que já estende as ligações entre dados e indivíduos – que sejam ressignificados para objetivos de segurança, muitos novos problemas sociais e legais aparecem (70). Com demasiada frequência, afirmações inadequadas de "dados como matéria-prima dão a impressão de que eles são meios técnicos inofensivos para conectar os pontos através de algoritmos. As práticas e políticas de algoritmos são profundas, mas pouco exploradas (71-72).

Uma terceira área de preocupação tem a ver com as políticas da internet na era de vigilância de "massa". Obviamente, esse tem sido um aspecto chave das controvérsias de Snowden desde o início. Os governos, incluindo a administração dos EUA, foram obrigados a responder aos contínuos debates sobre o poder do Estado e seu entrelaçamento com as redes comerciais, especialmente as empresas da internet (73). Mas as políticas de vigilância da internet são também uma forte corrente transpassando as empresas da internet – elas devem se manter distantes da NSA, enquanto ao mesmo tempo reconhecem que cooperam extensivamente com o governo. Paralelamente a essas áreas de turbulência, há a resistência ativa de numerosas ONGs que estão envolvidas tanto com as liberdades civis como com as dimensões da privacidade da vigilância em massa e, mais uma vez, o futuro da própria internet. As novas coalizões que têm se formado desde Snowden, entre EPIC, EFF e ACLU nos EUA, por exemplo, ou sob a bandeira da OpenMedia no Canadá, estão fazendo algo novo de forma estimulante construindo criativamente consensos sobre cada nova revelação de Snowden. Esta poderia ser a resposta mais planejada para vigilância que Colin Bennett concluiu que ainda estava faltando, quando publicou seu livro *The privacy advocates?,* em 2008.

O futuro da internet ainda está na balança conforme as revelações sobre a vigilância em massa continuam. Como Ron Deibert indica no livro *Black code* (2013), amplas questões de cercamento, sigilo e a corrida armamentista estão todos implicados aqui. E como Jonathan Zittrain (74) nos lembra, a partir de um ponto de vista diferente, a internet nunca teve uma época de ouro. Os problemas, bem como o potencial estavam embutidos desde o início. Análises sobre a disseminação da vigilância nunca foram tão significativas, desde as ameaças para pessoas individuais até as consequências para a guerra e a paz, riqueza e pobreza, em um nível global.

CODA: SNOWDEN, VIGILÂNCIA E PRIVACIDADE Este artigo investigou algumas das implicações mais marcantes do que, graças a Snowden, nós agora sabemos sobre a vigilância e "segurança nacional" no início do século XXI. A questão histórica é, por que, quando sociedade de vigilância já está bem desenvolvida, as "revelações" de Snowden foram lidas na mídia como uma completa surpresa? Esta questão demanda quais os aspectos chave da vigilância hoje que exigem novas formas de análise, junto a respostas políticas e de políticas públicas? A questão futura considera o que a internet significa agora, e como ela deve ser recuperada na direção da sua promessa original, dado que é o local chave para as práticas de vigilância em vários níveis?

No início, no entanto, observamos que as revelações de Snowden levantaram questões sobre a própria linguagem comumente usada

para discutir o monitoramento e rastreamento da vida diária e responde a essas práticas: vigilância e privacidade. Os conceitos são sempre contestados, alguns mais do que outros. E as definições são sempre difíceis porque revelam o tempo, lugar e pressupostos culturais de suas origens. Mais uma vez, essas questões foram levantadas antes, mas talvez não tão acentuadamente como no cenário pós-Snowden. Outrora, a distinção entre vigilância orientada e de massa parecia bastante claro. Não mais. As linhas borradas com o tráfego entre ambos: é a pessoa ou o perfil que está sendo vigiado? Antes, privacidade foi construída principalmente como uma questão relativa aos interesses, ou direitos, de um indivíduo identificável específico. Não mais.

Quando perfilização é "antecipação" e palpites sobre um possível "nexo" com o terrorismo são as bases da suspeição, como exatamente a privacidade faz para lidar com isso?

Tem sido argumentado aqui que os tipos de vigilância destacadas pelas revelações Snowden são de um lado informação-intensiva, muitas vezes relacionada com a internet e, de outro, orientada pela segurança nacional. O conceito de "segurança" também requer uma problematização nesse contexto, que é mais uma tarefa para a pesquisa multidisciplinar que hoje é claramente urgente. Tal como a vigilância ou a privacidade, a definição de segurança é difícil, especialmente sob as condições atuais, onde a segurança "nacional" foi elevada à categoria de prioridade por muitos governos. É um conceito altamente contestado (ver 32), muitas vezes erroneamente supõe-se estar em conflito (75) com reivindicações de direito à privacidade ou às liberdades civis. Compreensões muito mais matizadas de segurança são necessárias se o termo é reter qualquer ligação com os desejos, aspirações e, de fato, o bem-estar dos cidadãos. E esses devem ser considerados em relação ao outro conceitos – vigilância e privacidade – afetados pelas apostas de Snowden e discutido aqui (ver 40; 76-77).

As apostas Snowden são muitas e variadas e diferem de país para país. Mas essa complexidade não deveria obscurecer o fato de que em todos os casos esses riscos são altos. As divulgações desafiam algumas suposições dada como certas e expõem as lacunas reais no conhecimento atual. Mas isso não é apenas uma questão para aqueles envolvidos na pesquisa sobre vigilância – de qualquer disciplina; este é um empreendimento multidisciplinar envolvendo não apenas as ciências sociais, mas jornalistas investigativos e profissionais de informática também (78). Está particularmente em jogo o futuro da internet e das comunicações digitais em geral. Este artigo tenta salientar a magnitude desse desafio e sugere algumas maneiras nas quais isso pode, pelo menos, ser descrito e analisado, que não se conformam com alguns dos pressupostos perigosamente dominantes e atualmente disponíveis. Mas as apostas são ainda maiores e incluem o próprio caráter e as possibilidades da política, democracia e justiça social em um momento de vigilância do *big data* pós-orwelliana.

***David Lyon** é sociólogo, professor da Queen's University, no Canadá e diretor do Centro de Estudos de Vigilância dessa mesma universidade. Há mais de 20 anos vem se dedicando aos estudos de vigilância e publicou inúmeros livros e artigos sobre o tema.*

*Este artigo foi originalmente publicado em inglês na revista *Surveillance & Society.* Lyon, D. "The Snowden stakes: challenges for understanding surveillance today. *Surveillance & Society*, vol.13 (2): pp.139-152. 2015. Esta tradução foi feita por Marta Kanashiro.

NOTAS E REFERÊNCIAS

1. Entrevista com Edward Snowden, por Alan Rusbridger e Ewen MacAskill, 18 de julho de 2014, jornal *The Guardian*. Acesse em: http://www.theguardian.com/world/2014/jul/18/-sp-edward-snowden-nsa-whistleblower-interview-transcript
2. Em maio de 2015, a Corte de Apelações dos Estados Unidos decidiu que a coleta em massa de metadados de telefones feita pela NSA nunca foi legal.
3. Bowden citado por Greenwald, G. "The Orwellian re-branding of mass surveillance as merely bulk collection". *The Intercept*. Março, 2015. Disponível online em https://firstlook.org/theintercept/2015/03/13/orwellian-re-branding-mass-surveillance-merely-bulk-collection/.
4. Weber e Arendt têm muito a dizer sobre o que é hoje conhecido como vigilância, em relação à manutenção de registros burocráticos sobre indivíduos (Weber) ou como poder é gerado em "espaços de aparência" (Arendt). Ver Dandeker, C. *Surveillance power and modernity*. Cambridge: Polity, 1990; e Marquez, Xavier. *Spaces of appearance and spaces of surveillance*. Cambridge: Polity 44: 6-31, 2012.
5. É sintomático da cultura de celebridades de hoje que a vigilância de perfis de figuras públicas recebem muito mais interesse da mídia de massa do que a vigilância em massa do que é comum - neste caso alemão-cidadãos. Ao mesmo tempo, não é apenas a NSA que espiona líderes de outros países: Alemanha também manteve o controle sobre os americanos proeminentes tais como John Kerry e Hillary Clinton. Acesse em: http://www.theguardian.com/world/2014/aug/16/germany-spied-john-kerry-hillary-clinton-der-spiegel/
6. Weston, P.; Greenwald, G.; Gallagher, R. "New Snowden docs show US spied during G20 in Toronto". *CBC News*. Nov 27. Acesse em: http://www.cbc.ca/m/touch/news/story/1.2442448/.
7. Lyon, D. "Can citizens roll back silent army of watchers? The Toronto Star". Setembro, 2013. Acesse em: http://www.thestar.com/opinion/commentary/2013/09/23/can_citizens_roll_back_silent_army_of_watchers.html/.
8. Greenwald, G. "NSA collecting phone records of millions of Verizon customers daily". *The Guardian*. Junho 2013. Acesse em:http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order/
9. Regan, P. *Legislating privacy: technology, social values and public policy*. Durham, NC: University of North Carolina Press, 1995.
10. Bennett, C. J.; Raab, C.D. *The governance of privacy: policy instruments in global perspective*. Cambridge, MA: MIT Press, 2006.
11. Steeves, V. *Reclaiming the social value of privacy. In lessons from the identity trail: anonymity, privacy and identity in a networked age*. New York: Oxford University Press, 2009.
12. Giroux, H. "Totalitarian paranoia in the post-Orwellian surveillance state". *Cultural Studies*. Vol.29, no.2, pp.108-140. Maio, 2014.
13. Burnham, D. *The rise of the computer state*. New York: Vintage, 1983.
14. Campbell, D.; Connor, S. *On the record: surveillance, computers and privacy*. London: Michael Joseph, 1986.

15. Webster, F.; Robins, K. *Information technology: A luddite analysis*. NJ: Ablex. 1986.
16. Zuboff, S. *In the age of the smart machine: the future of work and power*. New York: Basic Books, 1988.
17. Cohen, S. *Visions of social control.* Cambridge: Polity Press, 1985.
18. Marx, G. *Undercover: police surveillance in America.* Berkeley, CA: University of California Press, 1988.
19. Rule, J. *Private lives, public surveillance: social control in the computer age.* New York: Schocken Books, 1974.
20. Gandy, O. *The panoptic sort: a political economy of personal information*. Boulder, CO: Westview Press, 1993.
21. Lyon, D. *Surveillance society: monitoring everyday life.* Buckingham: Open University Press, 2001.
22. Marwick, A. "The public domain: surveillance in everyday life". *Surveillance & Society* 9 (4): 378-393, 2012.
23. Trottier, D. *Social media as surveillance*. London: Ashgate, 2012.
24. Lynch, J. "New FOIA documents reveal DHS social media monitoring during Obama inauguration", 2010 Acesse em: https://www.eff.org/deeplinks/2010/10/new-foia-documents-reveal-dhs-social-media/.
25. Ball, K. S.; Webster, F (org). *The intensification of surveillance.* London: Pluto Press, 2003.
26. Lyon, D. "Surveillance, Snowden and big data: capacities, consequences, critique". *Big Data & Society* 1 (1), 2014a Acesse em: http://bds.sagepub.com/content/1/2/2053951714541861.abstract/.
27. Acesse o link: www.darpa.mil/iao/TIAsystems.htm
28. Lyon, D. "The emerging surveillance culture". *Media, surveillance and identity.* Jansson e Christensen (org). New York: Peter Lang, 2014b.
29. Bennett, C.; Haggerty,K.; Lyon, D.; Steeves, V. (org). *Transparent lives: surveillance in Canada.* Edmonton AB: Athabasca University Press, 2014. Acesse em: www.surveillanceinacanada.org
30. Brown, I. "The challenges to European data protection laws and principles". Working paper #1 of the Directorate General Justice Freedom and Security, 2010. Disponível em: http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_working_paper_1_en.pdf
31. Taylor, E. *Surveillance schools: security, discipline and control in contemporary education.* London: Macmillan, 2013.
32. Zedner, L. *Security*. New York and London: Routledge, 2009.
33. Agamben, G. *For a theory of destituent power,* 2013. Chronos. Acesse em: http://www.chronosmag.eu/index.php/g-agamben-for-a-theory-of-destituent-power.html
34. Mosco, V. *To the cloud: big data in a turbulent world*. Boulder, CO and London: Paradigm Publishers, 2014.
35. Clement, A. IXmaps – "Tracking your personal data through the NSA's warrantless wiretapping sites". International Symposium on Technology and Society. (IEEE Explore Digital Library: 216-223, doi: 10.1109/ISTAS.2013.661661322), 2013.
36. Veja link: https://citizenlab.org/2014/08/cat-video-and-the-death-of-clear-text
37. Timberg, C.; Nakashima, E. "Agreements with private companies protect access to cables' data for surveillance". *The Washington Post*, 6 de julho de 2013. Acesse em: http://www.washingtonpost.com/business/technology/agreements-with-private-companies-protect-us-access-to-cables-data-for-surveillance/2013/07/06/aa5d017a-df77-11e2-b2d4-ea6d8f477a01_story.html
38. Ver mapa em Bennett, C.; Haggerty,K.; Lyon, D.; Steeves, V., 2014. *Op. Cit*. p.113.
39. Bauman, Z; Bigo, D. et al. "After: rethinking the impact of surveillance". *International Political Sociology*, Vol.8 (2): 121-144, 2014. p. 113.
40. Bigo, D. 2008. "Globalized (in)security: the field and the ban-opticon". In *Terror, Insecurity and Liberty*. Bigo, D.; Tsouskala, A. (orgs). London and New York: Routledge.
41. Ball, K. S.; Snider, L. (orgs) *The surveillance-industrial complex: a political economy of surveillance*. London and New York: Routledge. 2013.
42. Bauman, Z; Bigo, D. et al. (2014). *Op Cit.* p.124-131
43. Lyon, D.; Topak, O. Promoting global identification: corporations, IGOs and ID card systems. *In:* Ball; Snider,. *Op Cit*. pp.27-43.
44. Bauman; Bigo; et al. 2014. *Op Cit.* p.125.
45. Haggerty, K.; Ericson, R. V. *Policing the risk society.* Toronto: University of Toronto Press, 1997.
46. Brodeur, J. *The policing web.* Oxford and New York: Oxford University Press, 2010.
47. Fuchs, C. *Social media: a critical introduction.* London: Sage. 2014.
48. Marwick, A. "The public domain: surveillance in everyday life". *Surveillance & Society*, vol.9 (4): 378-393, 2012.
49. Trottier, D. *Social media as surveillance*. London: Ashgate. 2012.
50. Giroux, H. "Totalitarian paranoia in the post-Orwellian surveillance state". *Cultural Studies*. Maio, 2014. p.7. Acesse em: http://dx.doi.org/10.1080/09502386.2014.917118
51. Veja link: http://techcrunch.com/2014/08/26/social-media-is-silencing-personal-opinion-even-in-the-offline-world
52. Cohen, J. *Configuring the networked self.* New Haven, CN: Yale University Press. 2012.
53. Coligações contra a vigilância em massa se envolveram em vários eventos globais organizados desde que as revelações de Snowden começaram. Por exemplo, https://blog.wikimedia.org/2014/06/05/global-action-against-mass-surveillance-snowden-revelações A questão da "transparência", no entanto, está em tensão com a necessidade legítima, mas limitada por sigilo dentro das agências de inteligência. Pesquisas sobre essa questão polêmica poderiam ser frutíferas.
54. Ball, K.S. "Exposure: exploring the subject of surveillance". *Information, Communication & Society*,vol.12 (5): 639-657, 2009.
55. Greenwald, G.. *No place to hide: Edward Snowden, the NSA, and the US surveillance State.* New York: Metropolitan Books,Toronto: McClelland and Stewart. 2014.
56. Lyon, D. "A sociology of information". *In*: *The Sage handbook of Sociology,* Calhoun, C; Rojek, C; Turner, B. (org). London and New York: Sage, 2005.
57. De Sola Pool, I. *Technologies of freedom: on free speech in an electronic age.* Cambridge, MA: The Belknap Press.1983.
58. Hayles, K. How we became posthuman: virtual bodies in cybernetics, literature, and informatics. Chicago: University of Chicago Press, 1999.
59. Jessop, B. "Knowledge as a fictitious commodity: insights and limits of a Polanyian analysis". In: *Reading Karl Polanyi for the 21 st Century: market economy as a political project*, Bugra, A.; Agartan, K (org), Basingstoke: Palgrave, 2007. p. 115-134.
60. Schiller, D. "How to think about information". *In*: *The political economy of information*, eds Mosco, V.; Wasko, J. Madison: University of Wisconsin Press,1988. p. 27-44.

61. Gellman, B.; Soltani, A. "NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say". *The Washington Post*. 30 de outubro de 2013. Acesse em: http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html/.
62. Levy, S. "How the NSA almost killed the internet". *Wired*. J)1 de julho de 2014. Acesse em: http://www.wired.com/2014/01/how-the-us-almost-killed-the-internet/all/.
63. Documentos do Centro para Democracia e Tecnologia norte-americano. Setembro de 2014: "Yahoo v. U.S. Prism documents", disponível em https://cdt.org/insight/yahoo-v-u-s-prism-documents
64. Veja, por exemplo, http://america.aljazeera.com/articles/multimedia/timeline-edward-snowden-revelations.html ou http://www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline
65. Gandy, O. *Coming the terms with chance: engaging rational discrimination and cumulative disadvantage*. London: Ashgate. 2012.
66. Turow, J. *The daily you: how the new advertising industry is defining your identity and your worth*. New Haven, CT: Yale University Press, 2012.
67. Andrejevic, M. *Infoglut: how too much information is changing the way we think and know*. London: Routledge, 2012. Veja também Andrejevic, M. *iSpy: surveillance and power in the interactive Era*. Lawrence: University of Kansas Press, 2007.
68. Marwick, A. *Status update: celebrity, publicity and branding in the social media age*. New Haven, CT: Yale University Press 2013.
69. Por exemplo, Raab, Charles e Benjamin Goold. Protecting information privacy. Equality and human rights Commission Research Report 69, 2011. Acesse em: http://www.equalityhumanrights.com/sites/default/files/documents/research/rr69.pdf
70. Amoore, L. "Security and the claim to privacy". *International Political Sociology*, vol.8 (1): 108-112. 2014.
71. Kitchin, R. *The data revolution: big data, open data, data infrastructures and their consequences*. London: Sage, 2014.
72. Morozov, E. "The real privacy problem". *MIT Technology Review*. Outubro, 2011. Acesse em: http://www.technologyreview.com/featuredstory/520426/the-real-privacy-problem
73. Clarke, R.; Morrell, M.; Stone, G.; Sunstein, C.; Swire, P. *The NSA Report: Liberty and Security in a Changing World*. Princeton, NJ and Oxford: Princeton University Press. 2014.
74. Zittrain, J. *The future of the internet*. New Haven, CT: Yale University Press, 2014.
75. A frase "(...) encontrar um equilíbrio entre privacidade e segurança" é rotineiramente entoada por governos e mídia, mas isso é na melhor das hipóteses, vazia, e, na pior, um disfarce para minar um e reforçar o outro.
76. Raab, C. "Privacy as a security value". *In*: *Jon Bing: En Hyllest / A Tribute*, Schartum, D. W.; Bygrave, L.; Bekken, A.G.B. (org) Oslo: Gyldendal, 2014. p. 39-58.
77. Lyon, D. *Surveillance after Snowden*. Cambridge: Polity, 2015.
78. Veja, por exemplo, a chamada do cientista político Charles D. Raab em 2013. Raab, C. "Studying surveillance: the contribution of political science?" *Political Insight*. October 29. 2013. Acesse em: http://www.psa.ac.uk/insight-plus/blog/studying-surveillance-contribution-political-science/.

RASTREAR, CLASSIFICAR, PERFORMAR*

Fernanda Bruno

No ano de 2010, o *Wall Street Journal* (WSJ) lançou une série de matérias e documentos revelando que inúmeros sites da internet utilizam quantidades expressivas de rastreadores das navegações e ações de seus visitantes. O *dictionary.com*, por exemplo, figura no topo da lista divulgada pelo *WSJ* (1), utilizando 234 tipos de rastreadores. A série, intitulada *What they know* (O que eles sabem) (2), mostra ainda como inúmeras corporações coletam e categorizam os rastros que deixamos na web, constituindo perfis de hábito, consumo, empregabilidade, longevidade, periculosidade etc. Em pesquisa realizada no mesmo ano no Brasil, identificamos a presença de 362 rastreadores de dados de usuários (cookies, flash cookies e web beacons) em apenas cinco sites da internet brasileira (Terra, UOL, Yahoo, Globo.com, YouTube) e de 295 rastreadores nas duas redes sociais mais populares no Brasil na ocasião (Orkut e Facebook). Cerca de 68% desses rastreadores atuam no campo do marketing online (3;4). Entretanto, ainda que habitualmente se enfatize o papel e os interesses do marketing neste contexto, é fundamental ressaltar que, além do marketing e da publicidade direcionada, o monitoramento de rastros pessoais na internet é de interesse comum a diferentes domínios: segurança, entretenimento, saúde, gestão do trabalho e recrutamento de pessoal, consultoria e propaganda política, desenvolvimento de produtos e serviços, vigilância e controle, inspeção policial e estatal etc.

Tecnicamente, o rastreamento e arquivamento das ações cotidianas na internet é possível graças à própria estrutura desta rede de comunicação distribuída e de seus navegadores, onde toda ação deixa um rastro potencialmente recuperável, constituindo um vasto, dinâmico e polifônico arquivo de nossas ações, escolhas, interesses, hábitos, opiniões etc. (3). Na série de matérias do WSJ, encontramos diversos exemplos de empresas cujo negócio consiste na coleta de rastros pessoais na internet e sua correlata categorização em bancos de dados e sistemas de *profiling*, visando orientar tanto escolhas de clientes de seguro de vida quanto ofertas de crédito e alvos de propaganda política, por exemplo.

A Acxiom Corp. (5), uma das maiores empresas de comércio e tratamento de dados da internet, monitora e categoriza diversas informações provenientes do comportamento online de milhões de americanos, cruzando-as com suas bases de dados offline. Tais dados, combinados a outros de natureza diversa, orientam, por exemplo, definições de bons e maus candidatos a seguros de vida. Os convencionais exames de sangue, considerados pouco amigáveis e explicitamente invasivos, dão lugar a análises preditivas que levam em conta