Novos modelos de negócio, vigilância ubíqua e as transformações no desenvolvimento da internet

New business models, ubiquitous vigilance and transformations in internet development

Leonardo Ribeiro da Cruz *

RESUMO

Estamos acompanhando o crescimento em importância de um modelo de negócio assente na captura, processamento e comercialização de dados de navegação dos usuários de serviços na internet. Esse modelo tem se tornado hegemônico na valorização do acesso às informações e serviços na rede e está cada vez mais presente na nossa experiência cotidiana de navegação. Esse artigo tem como objetivo analisar como essa hegemonização pressupõe a imposição de um modelo centralizado de topologia de rede ao favorecer o controle do fluxo de dados que nela trafega, e como isso amplia as possibilidades de vigilância na vida cotidiana.

Palavras-chave: Internet; Vigilância; Privacidade; Marketing Comportamental; Controle.

ABSTRACT

We're now seeing the growth of a business model based on capturing, processing and commercialization of the user's navigation data on the internet. This model has become hegemonic in the valuation of access to information and services on the network and is increasingly present in our everyday experience in the internet. This article aims to analyze how this hegemony requires the imposition of a centralized model of network topology to facilitate the control of the flow of data that circulates in it and how it expands the possibilities of surveillance in everyday life.

Keywords: Internet; Surveillance; Privacy; Behavioral Marketing.

INTRODUÇÃO

Hoje, na internet, podemos observar o crescimento de um tipo específico de modelo de negócio que busca valorizar serviços e acessos a informações cedidas de forma gratuita (FUCHS, 2011; GOLDHABBER, 2012; DOCTOROW, 2012) aos usuários. Esse novo modelo é o do *marketing* comportamental, que, por meio da mineração e comercialização de dados de navegação para empresas de prospecção, consegue valorizar a gratuidade e a abundância de informações na internet. A oferta de serviços gratuitos na rede funciona de fato a partir da troca dos dados de acesso dos usuários – conseguidos via rastreamento de seus hábitos na rede – e representa um grande salto em importância das ações de *marketing online*, assim como a

* Doutor em Sociologia. Bolsista de pós-doutorado do Laboratório de Estudos Avançados em Jornalismo da Universidade Estadual de Campinas (LabJor/Unicamp). Endereço: Rua Seis de agosto, 50, 3° piso, CEP: 13083-873, Campinas, SP. E-mail: leocruz.0@gmail.com.

implementação de uma nova abordagem na relação empresa/consumidor ao transformar os hábitos registrados de seus "clientes" em mercadoria.

Para que esse modelo se realize na internet, é preciso um investimento em um tipo de rede que possibilite o controle do fluxo de dados que nela trafega. Esse modelo topológico de rede – o de redes centralizadas e descentralizadas – pode permitir que o acesso e a transmissão de informações possa ser controlada, captada, tratada e transformada em produto no lucrativo mercado de dados informacionais. Contudo, o investimento nesse modelo de rede pressupõe o desinvestimento em um outro: o de redes distribuídas. Isso porque esse modelo horizontal de comunicação impede o controle e a captação dos dados que trafegam na rede, dificultando um modelo de negócio que se baseia na comercialização dos dados dos usuários e, em última instância, na criação de um modelo de vigilância econômica e política.

Este artigo tem como objetivo apresentar e problematizar a rivalização entre esses modelos de rede. Pretendo analisar como a hegemonização dos serviços valorizados por intermédio do *marketing* comportamental pressupõe a imposição de um modelo centralizado e controlativo de rede sobre outra, e como tal modelo, ao favorecer o controle do fluxo de dados que nela trafega e ao agregar cada vez mais ambientes digitais agindo sob sua lógica, amplia as possibilidades de vigilância na vida cotidiana.

A HEGEMONIZAÇÃO DO *MARKETING* COMPORTAMENTAL

A possibilidade de geração de valor sobre a atenção gera um mercado em que o "consumidor" concorda em receber tipos de serviços informacionais em troca do seu tempo de atenção. Quanto mais consumidores-usuários, maior seu estoque de atenção. Contudo, baseado em um mercado concorrencial, quanto mais empresas funcionam nesse tipo de economia, mais escassa se torna a atenção do usuário. Nesse sentido, há duas medidas de concorrência: agregar mais informação dentro de um mesmo espaço de valorização ou apresentar informações com maior relevância – ou ao menos com maior atratividade – ao consumidor-usuário. É nesse momento que se torna importante a segunda mercadoria criada por essa economia da atenção online: a possibilidade de aquisição, via termos de uso, dos dados de navegação dos usuários da rede. Quanto mais informações as empresas tiverem sobre os usuários, mais relevantes e atrativos poderão se tornar os ambientes de captura de atenção. Esse é o maior salto qualitativo desse tipo de estratégia de *marketing*: a atratividade não precisa mais ser massiva, ela pode ser mais ou menos personalizável e individualizada.

O que ocorre é que todas as formas de gerenciamento de informações digitais na rede estão sendo organizadas na internet para esse fim: o da maximização das ações de marketing e sua maior efetividade, ou seja, a possibilidade de que todo o investimento em *marketing* retorne de fato como lucro. O *marketing* é uma forma de antecipação do futuro – e, na internet, isso ocorre via prospecção dos dados de navegação dos usuários. Essa economia da gratuidade é financiada por uma atividade que aposta que aquilo que ela financia voltará a se tornar valor econômico capitalizado. Mas a evolução do marketing é justamente tornar mais real essa antecipação. O *marketing* massivo, vinculado em mídias de *broadcast* – como o rádio ou a televisão – tem muito menos chances de se efetivar do que as estratégias prospectivas personalizadas da internet. Aproveitando-se da característica da comunicação difusiva do *broadcast* – de poucos para muitos

–, o *marketing* vinculado nas chamadas "grandes mídias" está voltado para a venda de poucos produtos para muitas pessoas. Porém, atualmente, segundo os consultores de *marketing* Don Peppers e Martha Rogers, citados por Jeremy Rifkin em A era do acesso (2001), o objetivo é justamente tentar vender para um único consumidor o maior número de produtos possível. Para isso, devem-se elaborar estratégias capazes de definir, com a maior exatidão possível, o que o usuário quer, para lhe oferecer a melhor experiência de *marketing* que ele possa ter, e, para isso, as empresas de marketing encontraram na internet o espaço de excelência.

Esse movimento voltado à valorização acaba por transformar nós mesmos em informação e, como tal, tornamo-nos mercadoria. Nessa economia do acesso digital, somos acessados, nós e nossos dados, que são a propriedade retida e ofertada como leasing em uma rede que envolve empresas de *marketing online* e empresas de venda de produtos. Entramos aqui como produto e como consumidores. Somos matéria-prima e público-alvo de um complexo mercado de *marketing*.

A transformação do consumidor em produto é a maior façanha desse novo modelo de negócio digital, e isso ocorre via digitalização dos nossos gostos e via mercantilização de nossa atenção e nosso tempo de navegação. Essa é a maior tendência à valorização da internet e é a base da economia da gratuidade na rede. Esse modelo é aplicado em praticamente todos os serviços oferecidos: desde o serviço gratuito de webmail ou o site de notícias de um grande veículo de comunicação até os sites voltados ao compartilhamento de arquivos. De alguma forma, estamos sendo acessados, seja na comercialização dos nossos dados, do nosso tempo de acesso ou em ambos.

Christian Fuchs analisa, em seu artigo intitulado "Web 2.0: prosumption, and surveillance" (2011), que os modelos de negócio inaugurados com a invenção do conceito de *web* 2.0 – que tendem a se tornar hegemônicos – têm, como objetivo econômico, a geração de lucro por meio da comercialização dos dados dos usuários. Sob essa lógica, todas as informações que possam ser registradas através do monitoramento do usuário podem ser utilizadas pelas empresas para fins econômicos, e quanto mais pessoas utilizarem os serviços disponíveis para esse fim, mais lucrativa essa empresa será. Usando a empresa Google como exemplo, o autor resume bem essa estratégia:

> A estratégia econômica da Google é coletar dados sobre os usuários que utilizam diferentes aplicativos da Google em diferentes situações cotidianas. Quanto mais situações comuns forem suportadas por aplicativos da Google, mais tempo os usuários vão gastar *online* com a Google, e mais dados do usuário estarão disponíveis para a Google, o que permite a empresa analisar melhor o uso e comportamento do consumidor. Como resultado, dados cada vez mais precisos sobre os usuários e dados agregados podem ser vendidos para clientes publicitários que, armados com as informações sobre escolhas de consumo em potencial, fornecem aos usuários publicidade personalizada que os atinge em todas essas situações cotidianas (FUCHS, 2011, p. 291, tradução minha).

A Google é um ótimo exemplo para caracterizar o funcionamento desse novo modelo assente na publicidade comportamental justamente por ser um dos maiores atores dentro desse mercado. Segundo Fuchs, em dezembro de 2008, a Google controlava 57% do mercado de publicidade digital (ATTRIBUTOR, 2008 apud FUCHS, 2011). Já, conforme o estudo produzido pela empresa Evidon em setembro de 2013 – publicado

pela revista *online* Ad Age e que contabilizou o número de anúncios publicitários em toda a internet naquele mês –, o serviço de publicidade DoubleClick,1 da Google, aparece com cerca de 300 bilhões de anúncios, aproximadamente 30% do total. Outros dois produtos da Google aparecem na lista: Google AdSense2 aparece em quarto lugar, com 59 bilhões de anúncios; e o DoubleClick Bid Manager,3 em décimo segundo, com cerca de 27 bilhões (KANTROWITZ, 2013). Portanto, a empresa Google, com todos os seus serviços listados, detinha, em setembro de 2013, o direito de comercializar quase 40% de todos os espaços publicitários da internet.

Fuchs alerta que a dimensão econômica e política das empresas e das transações de dados que envolvem esse novo modelo de negócio são enormes. Essa importância deve ser observada em todas as decisões que envolvem a utilização desses tipos de serviço, pois o que está em jogo é a segurança e a integridade das comunicações quando inseridas em um modelo que se valoriza através de sua prospecção. Portanto, por envolver um tipo específico de vigilância econômica e política consequentes de um modelo de negócio, a adesão a esses tipos de serviços de gestão informacional demanda atenção, pois se trata da possibilidade de prospecção e análise de todas as formas de comunicação que envolve os usuários desses serviços, e a discussão deve ser realizada por intermédio de termos que envolvem a segurança informacional e a sensibilidade dos dados que trafegam nessas redes vigiadas.

MODELOS DE REDE E O CONTROLE DO FLUXO DE DADOS

Bruce Schneier (2013), programador e especialista em criptografia e segurança digital, ao analisar o momento atual da internet e das forças que estão atuando sobre ela, afirma que estamos vivenciando uma batalha épica pelo domínio do ciberespaço. De um lado, temos um tipo de agir minoritário, ágil, descentralizado e desorganizado, como os dos grupos dissidentes, dos *hackers* e das ações criminosas. De outro lado, temos os poderes institucionais, tradicionais e organizados, como o poder governamental e o das grandes corporações multinacionais. Se por muito tempo a internet pôde favorecer a coordenação, a eficiência e o empoderamento de grupos minoritários por meio da possibilidade de criação de redes livres de comunicação horizontal e sem mediação, atualmente, o poder institucional, centralizado e voltado ao controle e/ou à valorização, está vencendo, e o desdobrar dessa disputa é o que vai definir o futuro da internet. O crescimento do poder corporativo na rede, portanto, é resultado de uma disputa que tem a internet não mais como campo de batalha – como nos embates relacionados aos direitos autorais na internet –, mas

1 DoubleClick (Disponível em: <www.google.com/doubleclick/>.) é uma agência de *marketing online* especializada em mídia eletrônica. Comprada pela Google em 2007, ela oferece diversas ferramentas de publicidade comportamental para anunciantes e para editores de websites.

2 Google AdSense é um serviço oferecido gratuitamente pela Google que permite a um editor valorizar seu website por meio da venda de espaço publicitário.

3 DoubleClick Bid Manager é um serviço de comercialização de demandas publicitárias em tempo real da Google, um serviço chamado de DSP, *demand-side-plataform*. A DSP cria um mercado de oferta e demanda de publicidade digital que inclui anunciantes e editores. Nele, os espaços publicitários dos editores são valorizados por meio da análise dos dados de navegação de seus usuários. Eles são compilados em perfis e comercializados em tempo real na forma de leilão aos anunciantes. Em poucas palavras, um DSP é um leilão de perfis de usuários, materializados em espaços publicitários oferecidos por editores.

como o próprio objeto em disputa. Segundo Schneier, essa disputa coloca em oposição não mais dois atores, mas duas forças: o rápido *versus* o forte.

O rápido, por seu desprendimento, foi o primeiro a se beneficiar da estrutura descentralizada de troca de informações, e levou essa estrutura a um limite. O forte e pesado, com seu aparato institucional e seu investimento em ambientes pretensamente seguros, está atualmente vencendo, e o resultado dessa disputa se reflete no próprio desenvolvimento da rede. Essa disputa analisada por Schneier nos faz lembrar outras oposições, de mesmo teor, cunhadas por Deleuze e Guattari em "Tratado de nomadologia" (1997): o rápido e o grave; o liso e o estriado; o nômade e o sedentário; a máquina de guerra e o Estado. De certa forma, essas são as forças que se opõem na rede: de um lado, há os poderes minoritários e descentralizados, que se movimentam em fluxos de velocidades heterogêneas e que se beneficiam do anonimato, do livre fluxo de informações e da desterritorialização da internet. São nômades por utilizar a rede pelo seu movimento, não pelo seu território. Movimentam-se em um espaço liso, sem barreiras, e o fazem sem estabelecer um território. Do outro lado, há os poderes institucionais que se movimentam de forma grave, centralizada, e são sedentários por ocupar a rede pelos seus nós – espaços de passagem do fluxo-informação – e por sua territorialização. Movimentam-se em um espaço estriado, construindo dutos e canais por onde escoa o fluxo de informação. O que está em disputa aqui, portanto, não é só a possibilidade de movimento, e sim o lugar onde os dois termos se movimentam. A oposição dos termos pressupõe a oposição do uso do espaço em disputa. De certa forma, na internet, essa oposição diz respeito a dois modelos distintos de rede.

Para ilustrar essa questão, basta opor os dois termos extremos que estão em disputa em relação ao modelo de distribuição de produtos culturais digitalizados, em especial a música e os produtos audiovisuais: a rede P2P e os serviços de *streaming*. Cada um desses dois termos se baseia em um modelo e um objetivo distinto de rede. Seu modo de funcionamento, as entradas e saídas, os modos de distribuição do fluxo de informações, o papel dado aos usuários das redes, as características dos objetos que nela circulam e sua estrutura reticular não só se opõem, mas também rivalizam entre si.

As redes dos serviços de *streaming* de música ou de vídeo que se baseiam no já citado "novo modelo de negócio" do *marketing* comportamental – como os serviços Youtube, Spotify e Netflix – são do tipo centralizada. As empresas que prestam esse serviço devem se fixar em um nó da rede, um lugar, um site, um ambiente, e devem fazer passar todo o fluxo de informações por ele, pois é controlando esse fluxo que elas conseguem se valorizar. É a sujeição do *link* ao nó. Nesse sentido, as empresas fazem estriar o espaço, criando barreiras que impedem e controlam o fluxo. Mesmo a criação de *links* entre os nós menores da rede – os usuários – deve e é realizada dentro do nó central, impedindo a criação periférica de *links*.

Alexander Galloway (2004) – com base na categorização criada pelo desenvolvedor de redes da Rand Corporation, Paul Baran, no texto seminal chamado *Introduction to distributed communications networks* (1964), primeiro volume da série On Distributed Communications – apresenta, em seu livro Protocol, uma descrição bem apropriada sobre as redes centralizadas:

> Redes centralizadas são hierárquicas. Elas operam com um único *hub* autoritário. Cada nó radial, ou ramo da hierarquia, é subordinado ao *hub* central. Toda a atividade viaja do centro para a periferia. Nenhum nó periférico está ligado a qualquer outro nó. Redes centralizadas podem ter mais de um ramo que se estende

> para fora do centro, mas a cada nível da hierarquia o poder é exercido de cima para baixo (GALLOWAY, 2004, p. 30, tradução minha).

A rede centralizada tem, portanto, um formato de estrela. Nela, o nó central – chamado de *hub* por Alexander Galloway – aglomera a função de receptor e difusor de informações, e os nós periféricos dependem do nó central para participarem da rede. Todos os *links* de fluxo de informação estão subordinados ao nó e só circulam com autorização. Quem controla o nó controla o que pode circular na rede.

Galloway faz uma interessante analogia da rede centralizada com a metáfora criada por Foucault em *Vigiar e punir* (1987) a partir da imagem do panóptico. Para ele, o panóptico é uma rede centralizada onde o vigia habita o nó central cercado de celas periféricas. As únicas relações possíveis são os links entre o centro e a periferia da rede, sempre controlada pelo poder de vigilância. É uma arquitetura de pleno exercício de poder, projetada de forma hierárquica para favorecer a vigilância de muitos por poucos.

Já Paul Baran (1964), em seu artigo sobre arquiteturas de rede – cujo objetivo era apresentar ao Departamento de Defesa dos Estados Unidos da América um modelo de rede de comunicação eficiente e invulnerável– aponta para a fragilidade das arquiteturas radiais. Para ele, a comunicação baseada em redes centralizadas é muito vulnerável, pois a destruição do nó central significa o fim de toda a comunicação. Pensando nessa vulnerabilidade, Baran apresenta um segundo tipo de rede, chamada de "rede descentralizada". Segundo o autor, a rede descentralizada é um conjunto não hierárquico de redes centralizadas. Nelas, vários nós centrais – cada um cercado de seus nós periféricos – se ligam uns aos outros por meio de diversas formas de comunicação.

Nas redes descentralizadas descritas por Paul Baran, os nós ainda subordinam os *links*. A horizontalidade entre pontos, quando existem, acontece apenas entre os nós centrais. Os fluxos de informação entre os nós ainda são controlados e canalizados, e a topologia da rede continua a ser baseada no paradigma da territorialização e do sedentarismo.

Alexander Galloway afirma que o modelo de redes descentralizadas apresentado por Paul Baran "é o diagrama mais comum da era moderna" (GALLOWAY, 2004, p. 31). Ele permite que fluxos de informação circulem por grandes territórios de forma controlada, por dutos e canais construídos através das ligações entre os nós centrais. É uma codificação controlada do domínio territorial por meio de uma reticulação virtual.

As redes de comunicação telefônica, dos correios, as redes de tráfego terrestre e aéreo são exemplos desse tipo de topografia de rede. Nelas, aquilo que circula – informações, cartas, carros, pessoas, etc. – deve passar necessariamente por um número reduzido de nós – antenas de transmissão de dados, agências postais de distribuição, cidades de grande circulação de veículos, etc. – para chegar ao seu destino. Não é possível que um nó periférico de uma rede descentralizada se ligue a outro nó sem passar pelos centros, que mediam o fluxo de informações.

Se caracterizei aqui as redes dos serviços de *streaming* como de modelo centralizado, o tipo de rede imposta pelo modelo de negócio aqui abordado – que inclui, além dos serviços de *streaming* e redes sociais, os serviços de busca e notícia, as agências de publicidade digital, as redes de troca de informação do *marketing* comportamental, agências governamentais de segurança, etc. – é o descentralizado. São todas uma série de redes centralizadas interligadas, voltadas para o controle dos dados que

circulam por elas e entre elas, que se emponderam quanto mais informações circulem em seus dutos. Esse modelo de rede é voltado para a valorização dos nós centrais em detrimento dos periféricos e dos *links* entre eles. Faz com que toda a movimentação nesses espaços vá sempre "de um ponto a outro", pois são justamente os pontos, e não as linhas, que se valorizam.

O artigo escrito por Paul Baran, e enviado ao Departamento de Defesa dos Estados Unidos da América, propunha uma solução para a troca de informações militares dentro de uma rede de comunicação. A questão principal era a eficiência e a segurança da comunicação em uma rede que deveria ser, de alguma forma, invulnerável. No contexto da Guerra Fria, Baran estava interessado em propor uma rede de troca de informações que resistisse a um ataque bélico de grandes proporções.

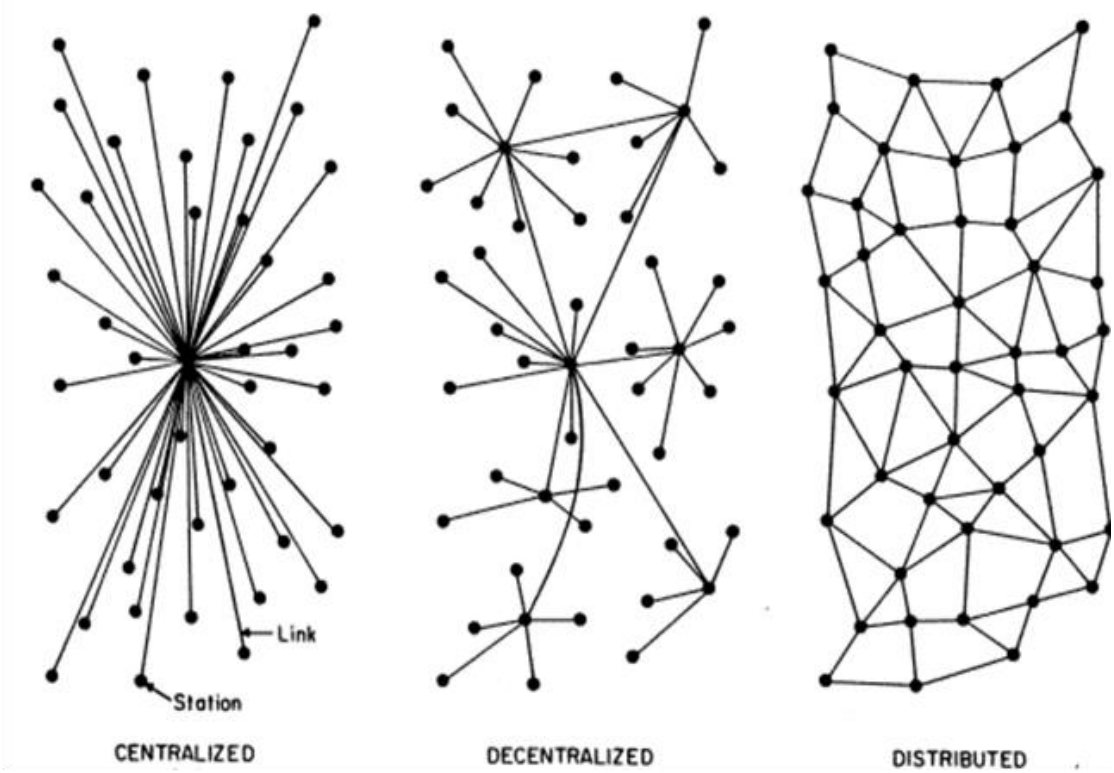
Para o autor, a rede descentralizada, embora apresentasse vantagens em relação à rede centralizada, ainda não era invulnerável. A destruição de um pequeno número de nós pode ocasionar a irrupção de toda a comunicação. Destarte, para sanar essa vulnerabilidade, Paul Baran apresenta um terceiro tipo de rede: a rede de comunicação distribuída.

As redes distribuídas são aquelas que horizontalizam o papel de recepção e emissão de informação entre todos os nós. Nela, cada nó é uma entidade autônoma na rede e de igual valor aos outros em relação à sua atuação. Por isso, cada nó pode, potencialmente, conectar-se e produzir *links* com qualquer outro, se isso corresponder a um aumento na eficácia e na segurança da comunicação.

Nas redes distribuídas, não há nós centrais. Os nós que compõem a rede são sempre circunstanciais e só fazem parte da comunicação se facilitarem o tráfego de informação, visto como um fluxo genérico de dados. Não há um caminho comum para um fluxo de informação. Portanto, não há dutos, somente um espaço aberto para a criação de *links*.

A horizontalidade dos nós faz com que sua importância se reduza. Se não há uma quantidade de nós centrais e não há previsibilidade de espaços por onde a informação deve trafegar, o controle do nó sobre o fluxo se torna muito mais difícil. É por isso que a rede distribuída é um modelo que privilegia o link, o fluxo de informação, em detrimento do nó, da territorialização e do controle sobre os dados. Podemos compreender a diferença entre esses os paradigmas de rede por meios da oposição dos diagramas de rede centralizada, descentralizada e distribuída apresentados por Paul Baran.

Figura 1 – Tipologias de redes.



Fonte: Baran (1964, p. 3).

Galloway afirma que a emergência das redes distribuídas "é parte de uma mudança maior na vida social [...] que inclui um movimento que se afasta das burocracias centrais e hierarquias verticais em direção a uma ampla rede de atores sociais autônomos" (GALLOWAY, 2004, p. 33). Como um modelo de rede da pós-modernidade, Galloway sugere que a rede distribuída se assemelhe com o conceito de rizoma apresentado por Deleuze e Guattari na introdução de Mil platôs (1996). A metáfora do rizoma – a estrutura botânica das raízes de algumas plantas onde não há uma núcleo central, podendo se ramificar de qualquer ponto, assim como se transformar em uma rede descentralizada compostas por diversos pontos autônomos, como bulbos ou tubérculos – é utilizada para explicar, em um primeiro momento, o modelo de organização dos elementos e conceitos que os autores apresentam no livro, e serviu para exemplificar uma estrutura epistemológica múltipla, sem raízes centrais, hierárquicas e dicotômicas.

O rizoma foi apresentado pelos autores para denunciar e propor uma alternativa aos modelos hierárquicos de sistematização do conhecimento. Segundo eles, as estruturas convencionais de organização são resultados de uma distribuição de poder na edificação da explicação científica. No modelo rizomático, qualquer elemento pode ser conectado ou incidir em qualquer outro, mesmo sendo de natureza ou campos do conhecimento distintos, sem a necessidade de posições ou afirmações mais fundamentais ou subordináveis que as outras. Para eles, a estrutura do conhecimento não parte de um conjunto de conceitos fundamentais, mas surge em todos os pontos relacionados e baseados em distintos argumentos e conceitualizações. Trata-se de um modelo que pretende dar conta da explicação da multiplicidade sem prendê-la em uma estrutura que possa reduzi-la a leis determinadas de combinação ou atribuí-la a uma unidade hierarquicamente superior.

As redes distribuídas, portanto, são redes não hierárquicas. Sua topologia não só difere daquela das redes centralizadas ou descentralizadas, mas se opõe a elas. O papel de cada nó é sempre contingente, assim como cada caminho que a informação pega para chegar de A a B. A única coisa em jogo é a eficiência e a segurança do envio.

As redes P2P são redes distribuídas. Sua maior característica é repartir as funções da rede entre seus pares de forma não hierárquica. Cada par pode ser, potencialmente, emissor e receptor de informação, dependendo da demanda da rede. Não há nós centrais nas redes P2P, pois eles não têm função. As informações que circulam na rede são armazenadas pelos pares, e quanto mais a rede cresce, mais informação é distribuída e de forma eficiente.

As redes P2P priorizam o fluxo de informações em detrimento de seus nós. O nó só é importante enquanto possui uma função no fluxo (emissor ou receptor), e desaparece depois disso. E, para toda a rede, ele é considerado apenas isso: emissor ou receptor. Qualquer informação adicional sobre o nó – a sua localização, sua identificação ou sua movimentação na rede – é, em um primeiro momento, irrelevante.

As características das redes P2P fazem com que ela seja bastante eficiente na transmissão de informações e no compartilhamento de arquivos. Por não haver um nó central onde as informações são armazenadas e por elas estarem distribuídas nos computadores de vários usuários conectados, a velocidade da transmissão de informações é substancialmente mais rápida (se houver uma boa oferta do arquivo na rede). Uma rede centralizada sempre tende a sobrecarregar o nó central, impedindo-a de atingir a velocidade ideal.

Pelo mesmo motivo, em uma rede distribuída fica muito difícil restringir a circulação de informações e controlar o que está circulando, já que ela pode surgir de qualquer ponto e chegar a qualquer outro sem passar por centros controlados. A distribuição horizontal das funções entre os pares e seu cariz circunstancial impedem a formação de redes centralizadas e sua sedentarização, da mesma forma que a autonomia de cada par em relação à formação de *links* impede que se criem dutos e canais de circulação de informação e, consequentemente, seu controle.

Esses dois tipos de rede são, portanto, rivais. Em relação à distribuição de produtos culturais digitalizados, eles representam duas formas distintas de empoderamento: dos usuários, nas redes P2P, e das grandes corporações, nos serviços de *streaming*. Se, como sugeriu Bruce Schneier, o poder corporativo na rede está se tornando hegemônico, seu modelo de rede também está, e, como tendência, esse crescimento atinge todo o desenvolvimento da internet.

Em síntese, vimos até aqui que há um crescimento em importância de um modelo de negócio baseado na gratuidade e na abundância da informação, e que comercializa, através de diversas redes de produtores de *marketing*, os dados de rastreamento da navegação do usuário e seu tempo de atenção. Esse novo modelo é visto como a maior possibilidade de valorização de produtos midiáticos digitalizados e distribuídos na internet. Mas tal valorização só é possível com a imposição de um modelo de rede centralizado em detrimento de um modelo distribuído. Isso porque as operações de controle da distribuição de informação – músicas e vídeos em *streaming*, notícias, ferramentas de busca, redes sociais, etc. – e de captura dos dados e da atenção do usuário só são possíveis por meio da criação de uma arquitetura de controle instalada entre os nós da rede.

REDES CENTRALIZADAS E A VIGILÂNCIA UBÍQUA

Segundo Bruce Schneier (2012), a vigilância ubíqua possibilitada pelos protocolos de controle na internet é algo desejado tanto pelas corporações na rede quanto pelos governos, e baseados em novos dispositivos de controle, o poder corporativo e o poder governamental sobre os usuários da rede estão em ascensão e mais fortes do que nunca. O poder corporativo é consolidado por intermédio do mercado de dados de navegação dos usuários de seus ambientes, que podem ser trocados por capital pelas empresas de *marketing online*. Já o poder governamental se consolida, segundo Schneier, ao mobilizar os dispositivos de controle social para a vigilância, a censura, a propaganda e para o controle sobre o uso da rede. Segundo o autor, "Em muitos casos, os interesses dos poderes corporativos e governamentais estão alinhados" (SCHNEIER, 2013, tradução minha).

Em 2013, houve um caso que evidenciou de maneira inequívoca a aliança entre o poder corporativo na internet e a atuação do poder governamental em relação à vigilância dos usuários e controle de seus movimentos na rede: o caso Snowden. Edward Joseph Snowden é um ex-analista de inteligência estadunidense que trabalhou, como colaborador terceirizado, para a Agência de Segurança Nacional (NSA – National Security Agency) e para a Agência Central de Inteligência (CIA – Central Intelligence Agency) dos Estados Unidos da América. Ele foi o responsável pelo vazamento de informações e de documentos da NSA que provavam a existência de um grande programa de espionagem dentro e fora dos EUA.

Entre os dias 5 e 7 de junho de 2013, o jornal britânico *The Guardian*[4] e o estadunidense *The Washington Post*[5] noticiaram que a NSA, o FBI e o serviço de inteligência britânico GCHC (Government Communications Headquarters) tinham acesso, desde 2007, aos servidores das principais empresas de tecnologia de informação dos EUA – nominalmente: Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube e Apple – e utilizavam esse acesso para realizar um tipo de espionagem massiva em alvos dentro e fora dos EUA, a partir da interceptação e processamento dos dados de navegação, dados pessoais, do monitoramento de mensagens pessoais, de conversas em salas de bate-papo *online*, chamadas de voz e de vídeo, transferência de arquivos, metadados usados para publicidade, dados de redes sociais e do conteúdo de conversas por *e-mail*. Além disso, as agências de inteligência dos EUA, a partir de um acordo com empresas de telecomunicações estadunidenses, monitoravam massivamente chamadas telefônicas dentro e fora do país.[6] Como prova, os veículos de comunicação apresentaram uma série de documentos secretos da NSA que continham detalhes do programa e que foram entregues por Edward Snowden.

Segundo notícia do *The Guardian* intitulada "The top secret rules that allow NSA to use US data without a warrant", o programa de espionagem foi aprovado pela Foreign Intelligence Surveillance Court – uma corte federal estadunidense, também

---

4 "NSA Prism program taps in to user data of Apple, Google and others". Disponível em: <http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>.

5 "U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program". Disponível em: <http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html> .

6 "Verizon providing all call records to U.S. under court order". Disponível em <http://www.washingtonpost.com/world/national-security/verizon-providing-all-call-records-to-us-under-court-order/2013/06/05/98656606-ce47-11e2-8845-d970ccb04497_story.html >.

conhecida como Fisa Court, que atua sob as regras do Foreign Intelligence Surveillance Act (FISA), de 1978, e que analisa pedidos de mandato de vigilância a alvos estrangeiros suspeitos fora do território estadunidense. Contudo, o programa de espionagem *online* da NSA foi autorizado não só a perseguir os rastros de pessoas, empresas ou governos suspeitos, mas também a filtrar e processar uma quantidade enorme de dados de diversas localidades em busca de atividades suspeitas, e que às vezes eram voltadas para dentro do país. A diferença substancial é que não houve suspeitos de antemão e nem provas de atividades terroristas, e sim a possibilidade de monitorar o tráfego de informação de uma quantidade enorme de cidadãos, empresas e governos estrangeiros não suspeitos por meio de seus dados de navegação.[7] Essa ampliação das possibilidades de espionagem descritas na FISA ocorreu com a aprovação, pelo congresso estadunidense, da lei temporária Protect America Act (PAA), em 2007, e, em 2008, de uma série de alterações da FISA com a FISA Amendments Act (FAA). Segundo a organização Electronic Frontier Foundation, essas duas leis "indiscutivelmente autorizaram a vigilância programática massiva e não particularizada das comunicações internacionais de qualquer americano, abrindo as portas para o poder executivo interceptar seus *e-mails* e telefonemas internacionais praticamente sem controle" (EFF, 2013, tradução minha). Todas as empresas listadas nos documentos oficiais entregues por Snowden negaram ter dado à NSA acesso aos seus servidores centrais, e alegaram desconhecer o programa de espionagem estadunidense, mesmo quando os documentos das agências de segurança apontam o contrário.[8]

O vazamento dos documentos da NSA que provam a existência de um programa massivo de vigilância eletrônica e informacional é um alerta sobre os rumos do desenvolvimento da rede e a realização de sua potência de ultravigilância política. Entretanto, ampliando nosso campo de visão, podemos perceber uma convergência em relação ao controle das informações na rede que engloba tanto a vigilância política como a vigilância econômica, e que ambas compartilham as mesmas fontes. Dessa vez, é a permissividade da vigilância ubíqua implementada por um modelo de negócio que possibilita a formação de um aparato de controle político. A estrutura de captação e processamento de informações já está pronta, atuando de forma eficiente e largamente estabelecida pelas empresas do mercado digital. Basta aos mecanismos de vigilância política acessá-las.

---

[7] Em 31 de julho de 2013, o jornal *The Guardian* publicou um artigo intitulado "XKeyscore: NSA tool collects 'nearly everything a user does on the internet'" , que detalhava, a partir da análise dos documentos cedidos por Snowden, um *software* utilizado pela NSA chamado XKeyscore e que possibilitava aos analistas de dados da agência de segurança buscar, por meio de filtros e de palavras-chave, qualquer conteúdo em um vasto banco de dados que incluía conversas privadas *online* de milhões de usuários de internet. Disponível em: <http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data> .

[8] Os documentos enviados por Snowden sustentam categoricamente que a NSA tinha autorização das empresas citadas para acessar seus servidores. Segundo documento da agência de segurança, publicada na primeira notícia do *The Washington Post* sobre o caso, a primeira empresa a colaborar com o programa de espionagem foi a Microsoft, em 2007. Esta foi seguida pela Yahoo em 2008, Google, Facebook e PalTalk em 2009, YouTube em 2010, Skype e AOL em 2011 e Apple em 2012. A mesma matéria aponta a dificuldade de se conseguir o acesso aos dados citados sem a conivência das empresas, e que elas podem ter sido obrigadas a abrirem seus servidores por meio de diretrizes emitidas pela corte da FISA em troca de imunidade em relação a processos jurídicos sobre o assunto.

A partir de uma certa estruturação da rede e da situação de importância da internet em nossa sociedade, estamos convergindo, tanto a política quanto a economia, para o paradigma da vigilância ubíqua. O espectro do fim da privacidade a partir de um tipo específico do desenvolvimento tecnológico se tornou a base da produção econômica e de uma certa prática política. Como bem aponta Evgeny Morozov (2014), as revelações de Snowden representam um marco não somente por apresentar provas de que podemos ser constantemente vigiados por governos de qualquer tipo, mas por enfatizar que o escândalo da vigilância política e a aceitação da vigilância econômica em troca de serviços cada vez mais essenciais na rede evidenciam a importância dos dispositivos de controle e o papel por eles desempenhados no capitalismo hoje.

Evgeny Morozov defende que as discussões acerca da importância das revelações de Edward Snowden para restabelecer a democracia devem ultrapassar a questão das relações governamentais e ser capazes de problematizar o papel da vigilância para o capitalismo digital, os limites da tendência de acúmulo de dados relacionados aos usuários de internet ou a realocação do poder para as grandes empresas do Vale do Silício. Estamos assistindo à permeabilidade de um tipo específico de desenvolvimento tecnológico baseado no paradigma da vigilância em nossa vida cotidiana, no funcionamento de nossas instituições, nas comunicações governamentais ou de movimentos sociais diversos. Estamos aceitando o paradigma da vigilância, da perda da privacidade e do controle da estrutura e do conteúdo dos espaços (privados) de discussão em troca da eficiência dos serviços *online*. Como esses serviços tendem ao oligopólio – como bem apontou Fuchs (2011)

–, não há espaço para discutir outras alternativas de desenvolvimento de rede ou para popularizar ambientes livres e não controlativos.

CONSIDERAÇÕES FINAS

Dos serviços Google aos novos modelos de negócio, do mercado fonográfico aos programas de vigilância das agências de segurança dos EUA e do Reino Unido: tudo representa a tendência do desenvolvimento das tecnologias de informação e de comunicação que, mesmo em seu desenvolvimento econômico, cumprem uma função militar: a vigilância e o controle. É como se a internet finalmente cumprisse sua potência à militarização, fechando o ciclo iniciado nos primórdios do seu desenvolvimento, quando a ideia de estruturar uma rede de troca de informações digitais surgiu dentro do Departamento de Defesa dos EUA, depois de ter sua permeabilidade expandida no capitalismo informacional, quando a vigilância se tornou toque de caixa para a obtenção de lucro. É aqui que se encaixa a crítica de Morozov (2014): se temos que nos preocupar com o uso político da vigilância, é porque ela é também técnica, econômica e social. É a permeabilidade dos dispositivos de vigilância e de controle no tecido social – conquistada através da mudança de paradigma do capitalismo contemporâneo – e sua potência à militarização que deveriam ser discutidas.

Paul Virilio, nas conversas que compõem o livro *Guerra pura* (1984), analisa precisamente a militarização do cotidiano realizada por meio de um tipo específico de desenvolvimento técnico, discurso político e práticas econômicas. Para ele, houve um alargamento e uma difusão da chamada "classe militar" por intermédio de uma ordem específica de crença em uma lógica tecnológica voltada puramente à eficiência.

A diferença de topologia de rede – sedentária ou nômade, centralizada ou distribuída – que determina o tipo de acumulação e a estrutura política é o ponto-chave da militarização do cotidiano. Como aponta Laymert Garcia dos Santos, na introdução à *Guerra pura*, esse movimento é a "passagem do heterogêneo ao homogêneo, desaparecimento do diverso no princípio propulsor da Guerra Pura" (VIRILIO, 1984, p. 11). É dessa forma que a convergência da vigilância ubíqua é mobilizada, tanto pelas agências de segurança governamentais, quanto pelas empresas de internet. A topografia de rede centralizada, sedentária e homogênea é sua estrutura de controle. É a logística da informação, como ela trafega, por onde ela deve passar, que determina seu controle.

Artigo recebido em 08/07/2016 e aprovado em 04/11/2016.

REFERÊNCIAS

BARAN, Paul. Introduction to distributed communications networks. Santa Monica, CA: RAND, 1964. (On Distributed Communications, 1).

CRARY, Jonathan. *Suspensões da percepção*: atenção, espetáculo e cultura moderna. São Paulo: Cosac Naify, 2013

DELEUZE, Gilles. *Conversações*. São Paulo: Ed. 34, 1994.

DELEUZE, Gilles; GUATTARI, Felix. *Mil Platôs:* capitalismo e esquizofrenia. São Paulo: Ed. 34, 1996. v. 1.

_____. *Mil platôs:* capitalismo e esquizofrenia. São Paulo: Ed. 34, 1997. v. 5.

_____. Tratado de nomadologia: a máquina de guerra. In: _____. *Mil platôs*: capitalismo e esquizofrenia. São Paulo: Ed. 34, 1997. v. 5.

DOCTOROW, Cory. *Music*: The internet's original sin. *Locus Online*, jul. 2012. Disponível em: <http://www.locusmag.com/Perspectives/2012/07/cory-doctorow-music-the-internets-original-sin/>. Acesso em: 9 mar. 2016.

EFF [Electronic Frontier Foundation]. *Beyond FISA*. [EFF report]. 2013. Disponível em

<https://web.archive.org/web/20130614054118/https://ssd.eff.org/foreign/beyond-

fisa>. Acesso em: 23 nov. 2016.

FOUCAULT, Michel. *Vigiar e punir:* nascimento da prisão. Petrópolis: Vozes, 1987.

FREIRE, Emerson. *Da sensação ausente à sensação como potência*: tema e variações sobre a relação arte-tecnologia. Campinas, 2012. Tese (Doutorado em Sociologia) – Instituto de Filosofia e Ciências Humanas, Unicamp.

FUCHS, Christian. Web 2.0: prosumption, and surveillance. *Surveillance & Society*, v. 8, n. 3, 2011.

GALLOWAY, Alexander. *Protocol*: how control exists after decentralization. Cambridge, MA: The MIT Press, 2004.

GOLDHABER, Michel H. The attention economy and the net. *First Monday*, v. 2, n. 4, abr. 1997. Disponível em <http://firstmonday.org/article/view/519/440>. Acesso em: 12 mar. 2012.

KANTROWITZ, Alex. *Just look at how Google dominates ad tech*. 2013. Disponível em <http://adage.com/article/digital/google-dominates-ad- tech/244824/>. Acesso em 12 fev. 2014

MOROZOV, Evgeny. A segunda morte do *flâneur*. O Estado de São Paulo, 19 fev. 2012. Caderno Link. Disponível em: <http://link.estadao.com.br/noticias/geral,a-segunda-morte-do-flaneur,10000036432>. Acesso em: 2 jun. 2016.

_____. Como sanar o déficit de democracia exposto por Snowden. *Folha de São Paulo*, 20 jan. 2014. Seção Colunistas. Disponível em: <http://www1.folha.uol.com.br/colunas/evgenymorozov/2014/01/1398996-como-sanar-o-deficit-de-democracia-exposto-por-snowden.shtml>. Acesso em: 2 jun. 2016.

RIFKIN, Jeremy. *A era do acesso*. São Paulo: Makron Books, 2001.

SANTOS, Laymert Garcia dos. A informação após a virada cibernética. In: SANTOS, Laymert Garcia dos et al. *Revolução tecnológica e socialismo*. São Paulo: Perseu Abramo, 2003a.

_____. Paradoxos da propriedade intelectual. In: VILLARES, Fábio (Org.). *Propriedade intelectual*: tensões entre o capital e a sociedade. São Paulo: Paz e Terra, 2007. p. 41-57. Disponível em: <http://www.ifch.unicamp.br/cteme/txt/propriedade.pdf>. Acesso em: 3 maio 2009.

_____. *Politizar as novas tecnologias*. São Paulo: Ed. 34, 2003b.

SCHNEIER, Bruce. *The battle for power on the internet*. 2013. Disponível em <http://www.theatlantic.com/technology/archive/2013/10/the-battle-for-power-on-the-internet/280824/>. Acesso em: 12 jan. 2014

SENRA, Stella. Crary e as transformações do observador. In: CRARY, Jonathan. *Suspensões da percepção*: atenção, espetáculo e cultura moderna. São Paulo: Cosac Naify, 2013, p. 9-19.

SIMON, Herbert. *Designing organizations for an information-rich world*. Baltimore: John Hopkins University Press, 1969

VIRILIO, Paul. *A bomba informática*. São Paulo: Estação Liberdade, 1999.

_____. Guerra pura: a militarização do cotidiano. São Paulo: Brasiliense, 1984.