

Ciberespaço: vigilância e apropriação de dados¹

Luis Gustavo Varela²

RESUMO

Este estudo tem o objetivo de entender os mecanismos pelos quais os provedores de serviços na internet se apropriam das informações e dados publicados na rede para fins comerciais de personalização de produtos ofertados aos internautas em suas redes sociais. A compreensão da vigilância e da punição de Michel Foucault e seus escritos sobre o panóptico auxiliaram bibliograficamente esta produção. Assim como as ideias de tecnologia de controle, privacidade virtual e sociedade em rede de Manuel Castells. E as ideias do filtro invisível e a personalização da internet para cada usuário de Eli Pariser. Isso estabelece a interferência que o controle, vigilância e monitoramento dos perfis podem exercer no futuro do jornalismo que, cada vez menos, faz a intermediação das marcas. Os dados que servem para anúncios podem auxiliar a apuração jornalística.

PALAVRAS-CHAVE: vigilância; perfis; ciberespaço; jornalismo pós-industrial

INTRODUÇÃO

A Web 2.0 torna-se um ambiente que sobrevive dos ideais de compartilhamento, de liberdade; a facilitação de acesso às informações, de transação de dados e a ideia de troca com o fim da propriedade intelectual. Nesse sentido, muitas empresas que operavam as mesmas funções por outros meios de comunicação que não fossem através do computador, viram na rede mais um espaço para se apropriar.

Logo, um espaço que é público pode estar sendo desenhado para cercar territórios virtuais. A privacidade na rede é uma questão delicada, pois ao mesmo tempo que as informações e dados postados são de caráter pessoal, estão disponíveis para uma determinada rede de perfis que pode se apropriar, monitorar, visualizar. E, por um

¹ Artigo apresentado no Eixo Temático de Jornalismo, Mídia livre e Arquiteturas da Informação no 7º Simpósio Nacional da Associação Brasileira de Ciberultura (2013) – Curitiba (PR)

² Estudante do curso de graduação em Comunicação Social – habilitação em Jornalismo do Instituto Superior e Centro Educacional Luterano Bom Jesus Ielusc (Joinville, SC). E-mail: varela.luisgustavo@gmail.com

momento, pensamos na segurança desse sistema de compartilhamento, que se desenha na Web 2.0. Mas se nos privilegiarmos de segurança, teremos que abrir mão da liberdade da publicação de conteúdo, que vai totalmente contra os princípios e funcionalidades fundamentais da Internet. Afinal, aparenta-me uma reivindicação de lugares privados em um espaço que é e nasceu público.

Assim, Manuel Castells colabora na discussão ao evidenciar que a transformação da liberdade e da privacidade na internet é um resultado direto de sua comercialização. A necessidade de assegurar e identificar a comunicação na internet para ganhar dinheiro com ela, e a necessidade de proteger direitos de propriedade intelectual nela, levaram ao desenvolvimento de novas arquiteturas de software que permitem o controle da comunicação por computador. (CASTELLS, 2003, 140-1)

Dentro do contexto de produção de informações, controle de vigilância e como esse controle tem influenciado comercialmente irá determinar a maneira como o internauta interage na rede e definir o comportamento do algoritmo, que se torna dispositivo de controle e vigilância. Desta forma, o objetivo desse estudo propõe entender os mecanismos pelos quais os provedores de serviços na internet se apropriam das informações e dados publicados na rede para fins comerciais de personalização de produtos ofertados aos internautas em suas redes sociais.

Podemos discutir também como as redes sociais transformam a ideia do panóptico, criando situações onde não mais um vigia todos, mas onde todos vigiam todos. Dados pessoais servem para fins comerciais, por exemplo. E os internautas produzem essas informações sem ter consciência de que suas postagens podem servir para uma vigilância, seja de sua própria rede de amigos ou para uma rede corporativa que adquire serviços virtuais de servidores que fornecem dados com combinação de perfis.

Monitoramento de perfis e mapeamento de características

Se existem ordem e disciplina para não ser punido na sociedade comum das relações pessoais, na sociedade em rede não é diferente. Existe o “passo-a-passo”, por exemplo, pra o novo internauta fazer parte da rede. Primeiro, o indivíduo deve fornecer suas informações pessoais como nome, senhas, região, foto. Uma série dessas informações primeiras direcionarão os caminhos da navegação na rede. É uma forma de

troca e um momento em que se sede para usufruir de um serviço gratuito. As conta no Facebook, por exemplo, ainda são consideradas legítimas, já que elas se constituem de uma seriedade nas informações, partindo do pressuposto de que os perfis são verdadeiros. Ou seja, minimamente, o perfil do internauta por trás da máquina se expõe como sujeito. Diferente do que acontece no Orkut, por exemplo, rede social onde é mais comum perfis falsos.

Até mesmo para se tornar um usuário dos serviços do Google essas informações são cruzadas. Por exemplo, ao enviar emails para os quais você cria uma lista breve de contatos para a mesma mensagem. Em um dado momento a discussão se encerra, por qualquer motivo. E, na criação de uma nova mensagem de email, se você citar um contato que estivesse naquela pequena lista, o Gmail (serviço de correio eletrônico do Google) te aconselha a considerar a inserção daquelas pessoas, sendo que, às vezes, é uma coisa específica para aquele contato.

O que se quer propor é que existe uma vigilância, mesmo que por parte de comandos algorítmicos, mas que acessa esses conteúdos e tem permissão legitimada para se apropriar deles. O acesso aos dados pessoais dos internautas facilitou o monitoramento dessas empresas para saber dos gostos de cada perfil. Seguindo o pensamento de Foucault, podemos tomar a rede social como um espaço, onde as divisões, se é que existem, são envidraçadas, permitindo o monitoramento do ambiente.

Fundamentação teórica: a adoção do panóptico foucaultiano

A revisão bibliográfica da obra Vigiar e Punir, de Foucault, pretende problematizar a ideia do Panóptico na estrutura das redes sociais, onde não mais um vigia a todos, mas onde todos vigiam a todos com muito mais artifícios do que os utilizados nos campos periféricos e torres do pensamento elaborado pelo autor.

À medida que o aparelho de produção se torna mais importante e mais complexo, à medida que aumentam o número de operários e a divisão do trabalho, as tarefas de controle se fazem mais necessárias e mais difíceis. Vigiar torna-se, então, uma função definida, mas deve fazer parte integrante do processo de produção; deve duplicá-lo em todo o seu comprimento. A vigilância torna-se um operador econômico

decisivo, na medida em que é, ao mesmo tempo, uma peça interna no aparelho de produção e uma engrenagem específica do poder disciplinar (FOUCAULT, 2002, p. 146-7).

O poder disciplinar está em toda a parte e sempre alerta, pois em princípio não deixa nenhuma parte às escuras e controla continuamente os mesmos que estão encarregados de controlar; é absolutamente “discreto”, pois funciona permanentemente e em grande parte em silêncio (FOUCAULT, 2002, p. 148). Foucault exemplifica a definição da conduta ameaçada por punições:

“na oficina, na escola, no exército funciona como repressora toda uma micropenalidade do tempo (atrasos, ausências, interrupções das tarefas), da atividade, (desatenção, negligência, falta de zelo), dos discursos (tagarelice, insolência), do corpo (atitudes “incorretas”, gestos não conformes, sujeira), da sexualidade (imodéstia, indecência). Ao mesmo tempo é utilizada, a título de punição, toda uma série de processos sutis, que vão do castigo leve a privações ligeiras e a pequenas humilhações. Trata-se ao mesmo tempo de tornar penalizáveis as frações mais tênues da conduta, e de dar uma função punitiva aos aparelhos aparentemente indiferentes do aparelho disciplinar: levando ao extremo, que tudo possa servir para punir a mínima coisa; que cada indivíduo se encontre preso numa universalidade punível-punidora” (FOUCAULT, 2002, p. 149).

A forma como o autor propõe leva-nos a refletir que quando publicamos informações ou geramos conteúdo na rede, estamos cientes de que tais atividades virtuais podem gerar medidas punitivas. Isso pode ser identificado tanto em represálias da rede de contatos com a qual compartilho informações como do próprio sistema da rede, em suas camadas mais profundas, que podem bloquear as atividades por determinado tempo.

Diante disso, podemos nos apropriar da ideia de Foucault quando se adota o Panoptismo. Por isso, Bentham, citado por Foucault, colocou o princípio de que o poder devia ser visível e inverificável. Visível: sem cessar, o detento terá diante dos olhos a alta silhueta da torre central de onde é espionado. Inverificável: o detento nunca deve saber se está sendo observado; mas deve ter certeza de que sempre pode sê-lo. (...) O Panóptico é uma máquina de dissociar o ver-ser visto: no anel periférico se é totalmente visto, sem nunca ver; na torre central vê-se tudo, sem nunca ser visto. O Panóptico é um lugar privilegiado por se tornar possível a experiência com homens, e para analisar com toda a certeza as transformações que se pode obter neles. O Panóptico

pode até constituir-se em aparelho de controle sobre seus próprios mecanismos. (FOUCAULT, 2002, p. 167-9)

A disciplina de oficina, sem deixar de ser uma maneira de fazer respeitar os regulamentos e as autoridades, de impedir os roubos ou a dissipação, tende a fazer crescer as aptidões, as velocidades, os rendimentos e, portanto, os lucros; ele continua a moralizar as condutas, mas cada vez mais ela modela os comportamentos e faz os corpos entrar numa máquina, as forças numa economia. (FOUCAULT, 2002, p. 173-4)

Desta forma, a disciplina também está inserida no contexto do ciberespaço ao definir certos tipos de conduta dos usuários, ainda pouco esclarecidos sobre as penalidades da interação social em rede. Embora isso seja mais uma implicação para que ele promova seu próprio policiamento no que diz respeito a seus percursos na rede. O internauta sabe que está público ao divulgar, por exemplo: “Boa noite, Brasil”. Mesmo que ele não tenha uma lista superior a de mil conexões de perfis, esse número pode se expandir em progressão geométrica, sendo potencializado dependendo dos tipos de perfis que estão conectados à sua rede e da prolongação da interação e exposição da mensagem. O que, certamente, não representa um país inteiro visualizando a mensagem, mas dá o tom de que os perfis se percebem projetados publicamente.

Interação nas redes: a vigilância desejada

Partimos do princípio que a vigilância é esperada pelos internautas. Uma vez que a produção de conteúdos é pensada em atingir determinado público na rede e obter determinada “audiência”.

Existe, portanto, uma racionalidade em se expor que talvez não calcule certas consequências que estão por trás desse monitoramento e vigilância que se apropria de conteúdos para estabelecer características de perfis. Existe, por parte do internauta criador de conteúdos e fornecedor de informações, um desejo em ser vigiado.

Conseguimos enxergar, com a leitura de Manuel Castells, o surgimento de uma sociedade em rede que também possui suas normas de conduta, mecanismos de vigilância e métodos de punição que são ostensivamente utilizados para alavancar mercadologicamente os produtos designados para determinados perfis na rede.

Questionamos, por exemplo, a maneira como se configura a *time line* de um perfil no Facebook. Temos as opções da conta nos dois lados do menu, a linha de

informações e ao seu lado sugestões de compras, lojas, marcas. E, o mais interessante, os anúncios são sempre personalizados de acordo com cada perfil. Ou seja, são raras as ofertas pelas quais o perfil não se interesse. Uma coisa é eu sair para procurar as ofertas e/ou anúncios. Outra é receber, sem que se peça, na *time line*.

A preocupação em se expor nem sempre é medida no ato diário da interação na rede social. O que nos chama a atenção é que deva existir uma porção da rede com a qual o internauta se relaciona diretamente, mas que, ao mesmo tempo, esse perfil não enxergue outras camadas mais profundas da rede que tem livre apropriação dessas informações para fins comerciais.

Isso nos leva a duas possíveis reflexões: i) existe uma naturalização com a interface, por parte do internauta, que acham comum que os gostos sugeridos se personifiquem em anúncios, ou; ii) o internauta pensa essa interface como uma perversidade de mecanismos mais profundos da rede.

Conforme já evidencia Castells, aplicações de software podem ser superpostas em camadas e protocolos da internet, tornando possível identificar rotas de comunicação e conteúdo. Com o uso dessas tecnologias, é possível violar a privacidade, e uma vez que se torna possível relacionar indivíduos com processos específicos de comunicação em contextos institucionais específicos, todas as formas tradicionais de controle político e organizacional podem ser lançados sobre o indivíduo em rede.

Manuel Castells explica o que acontece nas camadas mais profundas da rede:

“as tecnologias de identificação incluem o uso de senhas, “cookies” e procedimento de autenticação. Os “cookies” são marcadores digitais automaticamente inseridos por websites nos discos rígidos computadores que se conectam com eles. Uma vez que um cookie foi inserido num computador, este passa a ter todos os seus movimentos online automaticamente registrado pelo servidor do website que fez a inserção. Procedimentos de autenticação usam assinaturas digitais para permitir que outros computadores verifiquem a origem e as características dos correspondentes que interagem com eles. Baseiam-se frequentemente em tecnologia de criptografia. A autenticação opera muitas vezes em camadas, com usuários individuais sendo identificados por servidores que são eles próprios identificados por redes. Um dos primeiros exemplos de protocolos de segurança na internet foi a ‘camada de soquetes segura’ (SSL, de Secure Socket Layer) introduzida pela Netscape” (CASTELLS, 2003, 141).

Uma vez que os dados são coletados em forma digital, todos os itens de informação contidos no banco de dados podem ser agregados, desagregados, combinados e identificados de acordo com o objetivo e o poder legal. Por vezes, trata-se

simplesmente de fazer perfis agregados, como em pesquisa de mercado, seja para o comércio ou para a política. (CASTELLS, 2003, 142)

Essas tecnologias operam seus controles sob duas condições básicas. Primeiro, os controladores conhecem os códigos da rede, o controlado, não. O software é confidencial e patenteado, só podendo ser modificado por seu dono. Uma vez na rede, o usuário médio torna-se prisioneiro de uma arquitetura que não conhece. Segundo, os controles são exercidos com base num espaço definido na rede, por exemplo a rede em torno de um provedor de serviços da internet, ou a intra-rede de uma companhia, uma universidade ou uma agência governamental. Sim, a internet é uma rede global, mas os pontos de acesso a ela não o são. Se há filtros instalados nesse acesso, o preço da liberdade global é a submissão local (CASTELLS, 2003, 142). Mesmo assim, cabe a ressalva de não subestimar o internauta que, em muitos casos também pode saber operar sistemas e entender como funcionam as camadas de filtro e processamento de dados por trás da interface da internet.

Nos Estados Unidos, 92% dos websites coletam dados pessoais de seus usuários e os processam segundo seus interesses comerciais (Lessig, 1999, p.153 apud Castells, 2003, p.143)

Contudo, valendo-me da afirmativa de Manuel Castells, o problema passa a ser, então, a troca de dados pelo privilégio de acesso aos serviços online. “A maioria das pessoas abre mão de seus direitos à privacidade para ter condições de usar a internet. Uma vez que se renunciou a esse direito à proteção da privacidade, os dados pessoais tornam-se propriedade legítima das firmas de internet e de seus clientes” (CASTELLS, 2003, 144). E, nesse sentido, é contraditório reivindicar uma privacidade num espaço que é público para o compartilhamento de dados. E, parece que nunca vamos nos equilibrar na linha tênue entre liberdade e segurança. Ora, quando desejo que haja segurança, estou cobrando vigilância dos conteúdos e informações. Mas a segurança que se tem é que ao invés das informações estarem sob posse de uns, estarão sob posse de outros. De qualquer forma, andamos desarmados. Se desejamos liberdade, também haverá a liberdade de visualizar conteúdos de terceiros, abrindo mão também da minha privacidade. Me lembra até uma opção de configuração de segurança da rede social nos tempos de Orkut: “para visualizar quem te procurou você deve permitir que terceiros também possam ver que perfis você acessou”.

A criação potencial de um sistema de vigilância está no horizonte. A ironia é que, em geral, foram as firmas da internet, de ideologia ardorosamente libertária, que forneceram a tecnologia para a quebra do anonimato e a redução da privacidade, e foram as primeiras usá-la. Assim fazendo, deixaram a vigilância do governo voltar a rugir com furor redobrado no espaço de liberdade que fora laboriosamente construído pelos pioneiros da internet, tirando proveito da indiferença ignorante das burocracias tradicionais. (CASTELLS, 2003, 145)

A comunicação continuará fluindo imperturbável porque essa é arquitetura da internet. Mas redefinir o espaço de acesso, através do controle dos provedores de serviços da internet e ao estabelecer protocolos especiais de vigilância dispostos em camadas sobre a internet para redes específicas, permite o exercício de controle (e da punição) *ex post facto*. A nova arquitetura da internet, o novo código, torna-se a ferramenta fundamental de controle, possibilitando o exercício da regulação e do policiamento por formas tradicionais do poder do Estado (CASTELLS, 2003, 147).

Identidade: construção de perfis e interações

O que aparece do sujeito é só uma parte. Mas é uma parte performática. O sujeito edita seus conteúdos para que as pessoas o vejam e compreendam de uma determinada maneira, a medida que o perfil se constrói.

E isso vale para todo o tipo de relação social. As informações que eu compartilho nas páginas têm uma forma mais consciente, uma racionalidade de um conjunto de relações que eu estabeleço ali. A identidade precisa ser coerente, precisa ter coesão. Quando nos posicionamos ou nos caricaturamos de alguma maneira, isso não significa dizer que é assim só nas redes sociais.

No monitoramento de perfis que englobam nossa rede social na internet, geralmente amigos, pessoas próximas, existe a curiosidade de acompanhar seus posicionamentos, posturas, postagens. Mas quando um determinado perfil compartilha conteúdos inesperados, que não são comuns aquele sujeito, a reação da rede que os liga é de estranhamento. Ou, no mínimo a cogitação de uma invasão no perfil.

A liberdade de expressão era a essência do direito à comunicação irrestrita na época em que a maior parte das atividades diárias não era relacionada à expressão na esfera pública. Mas em nosso tempo, uma proporção significativa da vida cotidiana,

inclusive o trabalho, o lazer, a interação pessoal, tem lugar na rede. A maior parte da atividade econômica, social e política é de fato um híbrido de interação online e física. Em muitos casos, uma não pode existir sem a outra. Assim, viver num panóptico eletrônico equivale a ter metade das nossas vidas permanentemente expostas a monitoramento. Como vivemos existências compósitas, essa exposição pode nos levar a um eu esquizofrênico, dividido entre o que somos offline e a imagem que temos de nós mesmo online, que assim internaliza a censura (CASTELLS, 2003, 148).

Deste modo, as interações na rede online deixam de ser uma prática marcada pelo anonimato, como sugerem muitos autores. Sobre isto, Hermílio Santos argumenta que “embora as formas interativas mediadas pela internet pareçam ser propícias à tentativa de falsificação da identidade, seu sucesso é apenas parcial, uma vez que não é capaz de encobrir os elementos fundamentais caracterizadores da identidade, já que a interação no ciberespaço depende de uma habilidade bastante reveladora: a linguagem escrita” (SANTOS, 2005, p. 45). Portanto, ainda que os perfis estejam disfarçados sob um pseudônimo ou uma “falsa” identidade, ele é visto por um grupo mais ou menos delimitado que legitima sua prática e que compartilha com ele de um sistema de linguagem específico.

Por que as empresas de tecnologia da informação colaboram com tanto entusiasmo na reconstrução do velho mundo de controle e da repressão? Há duas razões principais, afora atitudes oportunistas ocasionais. A primeira que diz respeito sobretudo às firmas ponto.com, é que elas precisam quebrar a privacidade de seus clientes para poder vender os dados deles. A segunda é que elas precisam de apoio do governo para preservar seus direitos de propriedade na economia baseada na internet. (CASTELLS, 2003, 149)

Para impor essa proteção, o negócio da produção de informação precisa controlar o acesso e a identidade na internet, onde a maior parte da informação é distribuída. Assim, tem especial interesse em apoiar os esforços governamentais para restaurar o controle, construindo uma casa de vidro com base numa arquitetura de software controlado (CASTELLS, 2003, 150).

Espaço de troca ou ceder para ter: quando só uma parte sai ganhando

Para Eli Pariser, autor de O filtro invisível – o que a internet está escondendo de você, a preocupação além da vigilância está na personalização dos perfis e das buscas e a customização das informações de acordo com cada usuário. Pariser exemplifica a partir de navegações corriqueiras:

“A maior parte das pessoas imagina que, ao procurar um termo no Google, todos obtemos os mesmos resultados – aqueles que o PageRank, famoso algoritmo da companhia, classifica como mais relevantes, com base nos links feitos por outras páginas. No entanto, desde dezembro de 2009, isso já não é verdade. Agora, obtemos o resultado que o algoritmo do Google sugere ser melhor para cada usuário específico – e outra pessoa poderá encontrar resultados completamente diferentes. Em outras palavras, já não existe Google único. Se compartilharmos um artigo sobre culinária na ABC News, seremos perseguidos por toda a rede por anúncios de panelas revestidas de Teflon. Se abrirmos – por um mero instante – uma página que liste sinais para identificar se nosso conjugue está nos traindo, logo seremos assombrados por anúncios de testes de paternidade por DNA. A nova internet não só já sabe que você é um cachorro – ela conhece a sua raça e quer lhe vender um saco de ração *premium*” (PARISER, 2012, p.08-12).

Como explica Chris Palmer, da Electronic Frontier Foundation a Pariser: “Recebemos um serviço gratuito, e o custo são informações sobre nós mesmos. E o Google e o Facebook transformam essas informações em dinheiro de uma forma bastante direta”. Embora o Gmail e o Facebook sejam ferramentas úteis e gratuitas, também são mecanismos extremamente eficazes e vorazes de extração de dados, nos quais despejamos os detalhes mais íntimos de nossas vidas. O nosso belo iPhone novo sabe exatamente aonde estamos, para quem ligamos, o que lemos; com seu microfone, giroscópio e GPS embutidos, sabe se estamos caminhando, se estamos no carro ou numa festa. (PARISER, 2012, p.12)

Se analisarmos que a apropriação das informações que os internautas inserem na rede, sejam elas de conteúdos publicados, a fotos, endereços, pessoas ou compartilhamentos pode ser utilizada para fins comerciais de empresas que compram serviços da Google para ter acesso ao monitoramento, ou vigilância, vamos de encontro ao fator que desperta o interesse das empresas de produção. Por exemplo, uma empresa quer vender seus produtos e não pagar para anunciá-los em grandes veículos de mídia que chegam até as massas. A internet é um meio que as empresas conseguiram para falar diretamente com o cliente, sem que haja a mediatização de um veículo, ou a intermediação.

Compartilhando do pensamento de Chris Anderson, desde 2000 existe um enfraquecimento do monopólio de produtos que vendem muito no grande mercado. Esses são os chamados “hits” que irão disputar o mercado do século XXI com milhares de produtos de nicho. Se já não interessa às empresas que vendem produtos de massa investir em um veículo para anunciar sua marca, imagina para as empresas de produtos segmentados. E é, desde então, que o jornalismo vem perdendo seu principal financiamento. As empresas criam sites, fan pages, aplicativos, contratam jornalistas e essas medidas, possibilitadas pelas benesses da internet, impactam em uma nova reformulação de financiamento do jornalismo. Seja ele ainda por meio impresso e, agora, pelo digital. Claro que as pessoas não abrem mão das informações noticiadas pela imprensa, mas exigem, cada vez mais, o acesso gratuito às notícias.

A fórmula dos gigantes da internet para essa estratégia de negócios é simples: quanto mais personalizadas forem suas ofertas de informação, mais anúncios eles conseguirão vender e maior será a chance de que você compre os produtos oferecidos. E a fórmula funciona. A Amazon vende bilhões de dólares em produtos prevendo o que cada cliente procura e colocando esses produtos na página principal de sua loja virtual. Até 60% dos filmes alugados pela Netflix vêm de palpites personalizados feitos pelo site sobre as preferências dos clientes – a esta altura, a Netflix consegue prever o quanto iremos gostar de certo filme com margem de erro de aproximadamente meia estrela. A personalização é uma estratégia fundamental para os cinco maiores sites da internet – Yahoo, Google, Facebook, YouTube e Microsoft Live – e também para muitos outros. (PARISER, 2012, p.13)

O vice-presidente do Yahoo, Tapan Bhat, em declaração a Pariser, afirma que o futuro da internet é a personalização. O Google Instant, funcionalidade lançada no outono de 2010, que adivinha o que estamos procurando enquanto digitamos, é apenas o começo. O presidente do Google, Eric Schmidt, acredita que o que os clientes esperam do Google é que o site lhes diga o que deverão fazer a seguir.

Talvez, os internautas também já percebiam essa perseguição de seus passos na rede, ao sempre se deparar com ofertas ou promoções de gostos pessoais que, antes, nunca foram anunciados. Talvez os usuários dos serviços gratuitos já se atentem para uma possível perversidade da rede por parte dessa apropriação de dados. Eli Pariser aponta algumas consequências:

“Na melhor das hipóteses, se uma empresa souber que artigos você lê ou que ânimo está, poderá apresentar anúncios relacionados aos seus interesses. Na pior, poderá tomar decisões que afetem negativamente a sua vida. Se você visitar uma página para mochileiros sobre viagens em países de terceiro mundo, uma companhia de seguros que tenha acesso ao seu histórico online poderá decidir aumentar a sua franquia, como sugere o professor de direito Jonathan Zittrain a Pariser” (PARISER, 2012, p.20).

Considerações finais e apontamentos para estudos futuros

Contudo, as reflexões levantadas nessa produção nos munem de mais entendimento sobre como se configuram a troca de informações e, nesse sentido, revelam uma aproximação com a prática do jornalismo. Em que essas informações e dados podem contribuir para a transformação das apurações e produções de notícias e como o profissional repórter deve se comportar no ciberespaço. Mesmo com a cogitação de que o sistema de vigilância e apropriação de dados na rede seja perverso, ainda assim não conseguimos medir sua real interferência, tanto benéfica quanto prejudicial na interação social online. Mas se a publicidade e propaganda e o marketing se aproveitam desse sistema, o questionamento proposto é de que maneira o jornalismo também pode se reconfigurar na forma em que obtém informações por meio desse novo canal de interação, tornando-se um sistema de monitoramento que auxilia a apuração jornalística e possibilita novos métodos para o exercício da profissão. Um estudo levantado pela Columbia University e publicado na edição especial da Revista ESPM Jornalismo (mai/2013), e escrito por C. W. Anderson, Emily Bell e Clay Shirky aponta reflexões sobre o jornalismo pós-industrial.

O relatório aponta que a máquina é capaz de garimpar com rapidez grandes volumes de dados melhor que o homem. A automação de processos e conteúdos é o território mais subaproveitado para derrubar o custo do jornalismo e melhorar a produção editorial. E profetizam que no prazo de cinco a dez anos, teremos informações produzidas a baixo custo e monitoradas em redes de aparelhos sem fio. Vão servir para várias coisas – informar às pessoas qual o melhor momento de usar a água para evitar a poluição dos rios, por exemplo, ou quando atravessar a rua – e levantam questões de ética, posse e uso da informação.

Nesse sentido, as possibilidades infinitas abertas pela coleta de dados já permitem a empresas do setor de tecnologia, como por exemplo a Narrative Science, a

automatização da produção de textos padronizados como resultados financeiros de empresas e resultados de competições esportivas.

Khris Hammond, diretor de tecnologia da empresa explica em entrevista à revista Wired que, no futuro, algo como 80% a 90% das matérias sejam geradas por algum algoritmo. As matérias poderão ser produzidas por máquinas à medida que mais dados de caráter local e pessoal forem sendo coletados e lançados na rede. Esse tipo de reportagem será viável sempre e quando houver dados disponíveis nesse formato digital. E sempre e quando não houver dados nesse formato, como em uma audiência pública realizada por algum poder da União, será preciso um repórter para registrar os dados.

Essa previsão pode ser consolidada já em nossa contemporaneidade por meio dos apontamentos de Eli Pariser quando destaca que a personalização está moldando os fluxos de informação muito além do Facebook, pois sites como o Yahoo Notícias ou o News.me – financiado pelo New York Times – estão passando a nos fornecer manchetes segundo nossos interesses e desejos pessoais. A personalização influencia os vídeos a que assistimos no YouTube e numa dúzia de concorrentes menores, além das postagens de blogs que acompanhamos. Podemos observar que não só matérias podem ser produzidas pelos filtros, mas como também a sua seleção editorial e definição de qual conteúdo é do interesse público personalizado.

No fim das contas, Pariser manifesta-se no sentido de que os defensores da personalização nos oferecem um mundo feito sob medida, adaptado à perfeição para cada um de nós.

Na verdade, somos aprisionados dentro de uma rede personificada que não nos permite conhecer outros gostos, acessar outros conteúdos. Aproprio-me do pensamento da socióloga Danah Boyd citada em Pariser quando menciona uma dieta de informações, não no sentido de que vamos acabar consumindo um conteúdo nada benéfico para nós mesmos e para a sociedade como um todo. Mas, sim, que deixamos de consumir esse conteúdo. É uma dieta que limita nosso acesso aos conteúdos, por exemplo, artigos em outras línguas. Nessas buscas, o idioma é filtrado e podemos deixar de obter conhecimentos mais avançados ou mais recentes porque os filtros atuam para nos trazer o que mais se enquadra ao perfil do internauta perseguindo seus passos na rede.

Como diz Pariser, se a Amazon pensar que estou interessado em livros de culinária, é pouco provável que me mostre livros de metalurgia. Com isso o ciberespaço se caracteriza ainda pelo ambiente de troca e compartilhamento, mesmo que surjam as tentativas de se demarcar territórios ou domínios tecnológicos. Nesse sentido, o jornalismo e as interações na rede se reconfiguram na tentativa de se fortalecerem na utilização dos recursos virtuais que hoje interferem na vida social, na forma de se comunicar, lançar dados na internet e receber informações.

Ryan Calo, professor de Direito em Stanfor, disse a Pariser que toda a tecnologia tem uma interface, um ponto em que nós terminamos e a tecnologia começa. E quando a tecnologia passa a nos mostrar o mundo, acaba por se colocar entre nós e a realidade, como a lente de uma câmera. São muitas maneiras pelas quais ela pode deformar a nossa percepção do mundo. E é exatamente o que faz a bolha dos filtros.

Os filtros impedem que nossas ideias se confrontem com outras opiniões e conteúdos, por isso nos apresentam informações homogêneas com as quais o perfil se identifica, impedindo novas percepções e aprendizagens. Isso, em parte, iniciou com a navegação “logada” a um perfil, a um endereço de email, a um sistema de validação das características do usuário. Impedem até a inclusão de usuários à rede pessoal do perfil que não tenham contatos ou características em comum. Em uma reflexão mais distante, o que se percebe é uma ilusão ao acesso de conteúdos dos mais diversos e a concentração do perfil em um circuito vicioso que o mantém sempre no mesmo limite de acessos e contatos. A bolha dos filtros, como sugere Pariser, pode ser um caminho sem volta. E a internet se torna, a cada dia, um espaço onde os atores não são mais meros usuários e, sim, potenciais consumidores.

REFERÊNCIAS BIBLIOGRÁFICAS

ANDERSON, C. W. et al. **Jornalismo pós-industrial, adaptação aos novos tempos.** In: Revista de Jornalismo ESPM, n. 5, ano 2, p. 30-90.

ANDERSON, Chris. **Íntegra da entrevista com Chris Anderson.** Época Online, 9 de Nov. 2006. Entrevista concedida a Guilherma Ravache. Disponível em <<http://revistaepoca.globo.com/Revista/Epoca/0,,EDG75221-5856-433,00.html>>. Acesso em 13 junho

BRUNO, Fernanda. **Dispositivos de vigilância no ciberespaço: duplos digitais e identidades simuladas.** In: Revista Fronteiras – estudos midiáticos, Ano VIII, Ed. 02, maio/agosto 2006, Unisinos

CASTELLS, Manuel. **A galáxia da internet.** Rio de Janeiro: Jorge Zahar Ed., 2003

_____. **A sociedade em rede** (volume 1). A era da informação: economia, sociedade e cultura. São Paulo: Paz e Terra, 2ª edição, 1999.

FOUCAULT, Michel. **Vigiar e punir: nascimento da prisão.** Petrópolis: Vozes, 25ª Edição, 1987.

PARISER, Eli. **O filtro invisível: o que a internet está escondendo de você.** Rio de Janeiro: Zahar, 2012

SANTOS, Hermílio. **Alteridade, decepção e estigma no ciberespaço: desdobramentos da interação social mediada.** In: Revista Famecos, Porto Alegre, n. 26, abril de 2005. Disponível em <<http://www.revistas.uni-verciencia.org/index.php/famecos/article/viewArticle/418>>. Acesso em 28 de mar. 2012