Vigilância e seu sentido de In/Segurança: a ressignificação das novas formas de controle e os riscos para a autonomia e a privacidade na rede

Surveillance and their sense of In / Security: the reinterpretation of new forms of control and the threats to autonomy and privacy online

Emanuella Santos[1]
Claudio Cardoso de Paiva[2]

Resumo

O percurso histórico anterior aos eventos que possibilitaram o atual estado de vigilância, potencializado pelo uso das tecnologias, foram determinantes no aumento do monitoramento e da espionagem na esfera individual e coletiva das sociedades globalizadas. Seja qual for o procedimento utilizado na vigilância, tal prática é comum desde que o *homo sapiens* percebeu ser preciso conhecer as intenções e as forças das tribos vizinhas para garantir sua segurança. Há séculos se espionou, monitorou e vigiou, resultando em guerras vencidas, inimigos dizimados, e governos derrubados. A realidade do mundo pós-11/09 têm como bandeira a máxima: "guerra contra o terror", fortalecendo a investida de vigilância em massa por serviços privados oferecidos na internet, por empresas como Google e Facebook, somada aos interesses das instituições governamentais. Porém, depois da divulgação dos arquivos secretos pelo ex-analista da NSA, Edward Snowden, uma série de discussões acadêmicas, jurídicas e políticas vem se fortalecendo e promovendo condições para a luta e fiscalização contra esse sistema pervasivo e complexo. O objetivo do artigo é investigar o percurso histórico da vigilância e sua ressignificação na sociedade em rede, analisando o que está por trás do discurso moderno de segurança, como suas implicações para a liberdade e a privacidade nesse contexto.

Palavras-chave:

Vigilância; espionagem; terrorismo; controle; privacidade

Abstract

The previous historical background to the events that made possible the current state of alertness, enhanced by the use of technology, were instrumental in increasing surveillance and spying on individual and collective sphere of globalized societies. Whatever the procedure used in surveillance, this practice is common, as homo sapiens perceive as necessary to know the intentions and the forces of the neighboring tribes to ensure their safety. For centuries to spy, watch and see, resulting in overdue wars,

[1] Mestre em Comunicação pelo Programa de Pós-Graduação em Comunicação. PPGC/UFPB. Pesquisadora do Grupo de Pesquisa em Linguagens e Processos Midiáticos. E-mail: emanuellassrp@hotmail.com.
[2] Professor Associado IV, Departamento de Comunicação UFPB, PPGC/UFPB; PPJ/UFPB. E-mail: claudiocpaiva@yahoo.com.br

decimated enemies and toppled governments. The reality of the world post-11/09 is to flag the maxim "war on terror", strengthening mass surveillance invested by private Internet services, for companies like Google and Facebook, plus interest of government institutions. However, after the disclosure of secret files by former NSA analyst, Edward Snowden, a number of academic, legal and political debates come to strengthen and promote the conditions for the control and execution against this widespread system complex. The aim of this study is to investigate the historical background of monitoring and reinterpretation in the network society, the analysis of what is behind the discourse of modern security and its implications for the freedom and privacy in this context.
Keywords:

Surveillance; espionage; terrorism; control; privacy

Introdução

A internet, em seus primeiros anos, gerou tanto fascínio que foi difícil enxergar o que de negativo ela poderia acarretar às relações sociais. O fim das amarras que por décadas fez todos reféns dos meios de comunicação tradicional anunciava um novo momento histórico da humanidade, em que a tão desejada liberdade e a informação livre enfim se instaurariam como parte das dinâmicas sociais.

Porém, como toda história tem pelo menos dois lados, assim aconteceu com a internet. Dentre as inúmeras possibilidades de uso, não tardou para que determinados usos gerassem certas implicações para os seus usuários. Se os meios de comunicação de massa tinham perdido domínio sobre nossas vidas, novos modelos de negócios, que contribuíram para a estruturação da internet que conhecemos hoje, passariam a ocupar os seus lugares.

O controle pelo governo, que pareceu ter se encerrado, continuou de forma muito mais intrusiva e sem amarras. A internet se tornou, ao passar dos anos, uma das principais ferramentas através da qual o governo utiliza para garantir seu poder. Diante de suas várias funcionalidades, nos debruçaremos sobre os regimes de espionagem e vigilância na internet, na qual empresas e governos se aproveitam para exercer seus domínios.

A partir da revolução tecnológica e contextualizada no impacto de dois eventos que se mostraram determinantes para o estado de vigilância atual, o atentado terrorista no dia 11 de setembro de 2001 e o vazamento de informações sigilosas da NSA, por Edward Snowden em 2013, nossa pesquisa compreende esses dois momentos como sendo balizadores para os estudos das práticas modernos da vigilância.

A nossa proposta do trabalho é analisar as reconfigurações que a vigilância perpassou no decorrer da história da humanidade e seu atual estado de ressignificação na sociedade em rede. O estudo é parte de uma linha de pesquisa que entende a crítica das práticas de controle e o descaso com os direitos individuais, como de necessidade ininterrupta, gerando a reflexão coletiva e social.

1 A prática da espionagem na História

O filósofo general Sun Tzu, no ano 500 a.C, em sua famosa obra "A arte da guerra" já dizia:

> O que possibilita ao soberano inteligente e seu comandante conquistar o inimigo e realizar façanhas fora do comum é a previsão, conhecimento que só pode ser adquirido através de homens que estejam a par de toda movimentação do inimigo (2007, p. 135).

Para Tzu, um bom sistema de espionagem é o maior tesouro de qualquer governante, pois é possível vencer uma guerra sem precisar ir para o conflito armado, a partir apenas da informação sobre o adversário - quais são suas fraquezas, suas armas, seus homens e seus generais. A espionagem é assim, essencial em qualquer batalha.

Quando nos referimos a estratégias de guerra a espionagem é vital para a vitória e consequentemente, a derrota do inimigo. Tal prática existe desde a história das primeiras civilizações humanas, o que lhes garantiu muitas de suas conquistas e vitórias. O Coronel Allison Hind (1967, p. 11) afirma que "Nações que não fizeram uso da espionagem caíram na poeira do esquecimento; outras, antigas e modernas, cresceram e se fortificaram com seus frutos". O que mudou no decorrer dos anos foi a sistemática das formas de espionagem e como as informações passaram a ser obtidas e utilizadas.

Desde que o homem percebeu que para ficar em vantagem sobre o seu inimigo era preciso obter todas as informações possíveis para tal, ele fez uso da vigilância e espionagem para poder se defender e atacar com precisão, caso fosse necessário. Ernest Volkman afirma que "A espionagem nasceu ao mesmo tempo em que emergiu outro componente vital na história da humanidade, a luta armada" (2013, p. 6), o que veio a intensificar e aprimorar certos sistemas de espionagem.

Mas o que de fato é considerado espionagem? Segundo Volkman (2013, p.7) "a espionagem é o ato de obter informações secretas militares, políticas, econômicas e

outras de uma nação-estado, através do uso de espiões, furto, monitoramento ou outros meios". Mesmo a espionagem sendo uma tática antiga, utilizada em tempos de paz ou de guerra, para a Convenção de Genebra[3], a espionagem não é reconhecida como ato legal de guerra, não existindo assim leis que regule tal prática.[4] E é ainda, para a maioria das nações, um crime imperdoável.

As transformações e avanços sobre as estratégias de espionagem foram gradativas e tiveram como precursoras muitos erros de administração. Por volta dos acontecimentos que precederam a Primeira Guerra Mundial, enquanto a Alemanha escolhia a escória da sociedade para serem seus espiões, a Rússia usou seus serviços de inteligência para repressão interna (VOLKMAN, 2013). Erros desse tipo foram cometidos por anos, tanto entre os dois países como por outras nações.

Dois grandes momentos foram marcantes na história da espionagem, ocorridos no período da Segunda Guerra Mundial. A primeira foi a decodificação da máquina alemã Enigma, que para decifrá-la os governos da França, da Polónia, dos EUA e da Grã-Bretanha atuaram de forma colaborativa na busca pela decodificação da máquina. Contudo, foi principalmente Alan Turing, um matemático britânico, que criou o que veio a ser chamado do primeiro computador do mundo, que serviu para decifrar os códigos criptografados alemães, antecipando com isso o fim da guerra, sendo esse, uma das principais causas da derrota alemã.

A segunda foi a corrida para o desenvolvimento de armas nucleares. Em 1938, foi publicado um trabalho de cunho científico de dois químicos alemães que descreviam a divisão do núcleo do átomo (VOLKMAN, 2013). Tal publicação gerou preocupação em vários governos e intensificou o uso de espionagem, principalmente entre Estados unidos e União Soviética. Desde então, a espionagem tornou-se indispensável entre as nações, visto o poder destruidor das armas nucleares nos ataques de Hiroshima e Nagasaki, o que disseminou a sensação de incerteza diante do mundo.

Um dos grandes responsáveis por trazer à tona à existência e a atuação secreta dos espiões foi o cinema. O filme de Hitchcock "Secret Agent", de 1936, por exemplo,

[3] Disponível em: < http://migre.me/sJwG7 >. Acessado em: 13 nov. 2015.
[4] Na Convenção de Genebra o artigo 46º faz referência ao ato de espionagem, ressaltando que se um membro das forças armadas estiver uniformizado ele deve ser tratado como prisioneiro de guerra, visto que ele está fazendo um ato legítimo no campo militar, o reconhecimento da parte adversa do conflito.

e também os do espião mais conhecido da franquia "007", James Bond, apresentou ao público geral a figura do espião e tirou do anonimato uma das profissões mais secretas de toda a história. Para Hind (1967), a negação das atividades do serviço secreto por diversos governos, reluz a hipocrisia destes e só consegue de fato enganar os ingênuos.

A partir do desenvolvimento tecnológico, a prática de espionagem se especializou e ganhou novas ferramentas. Se os únicos recursos que a prática da espionagem dispunha era a passagem de informações a partir de espiões, a intercepção de correspondências postais, a decodificação de criptografia através do telégrafo e do rádio, o surgimento de novos sistemas tecnológicos contribuíram para o aprimoramento da espionagem, acelerando o estado atual de vigilância.

Vale acrescentar que a vigilância e a espionagem possuem suas diferenças conceituais e práticas. Enquanto o ato de espionagem usa diversas técnicas com o objetivo de conseguir obter determinadas informações, a vigilância se enquadra como uma dessas técnicas, que atualmente, a partir das tecnologias digitais, por exemplo, recolhe o maior número de dados dos usuários da internet e os transformam em informação estratégica, utilizando-a em diferentes situações e contextos.

2 Implicações do 11 de Setembro de 2001 para a vigilância

O surgimento da internet e sua popularização da década de 1990 quebraram as barreiras territoriais e temporais e possibilitaram que a comunicação acontecesse de muitos com muitos. Tal aspecto descaracterizou o sistema unidirecional dos meios tradicionais de comunicação de massa e permitiu aos novos usuários da rede o poder da livre comunicação e maior autonomia.

> Criada como um meio para a liberdade, nos primeiros anos de sua existência mundial a Internet pareceu prenunciar uma nova era. Os governos pouco podiam fazer para controlar o fluxo de comunicação capazes de burlar a geografia e, assim, as fronteiras políticas. A liberdade de expressão podia se difundir através do planeta, sem depender da mídia de massa, uma vez que muitos podiam interagir com muitos de maneira irrestrita. A propriedade intelectual (na música, em publicações, em ideias, em tecnologia, em software) tinha de ser partilhada, já que dificilmente podia ser limitada a partir do momento em que essas criações eram introduzidas na Net. A privacidade era protegida pelo anonimato da comunicação na Internet e pela dificuldade de investir as origens e identificar o conteúdo de mensagens transmitidas com o uso de protocolos da Internet (CASTELLS, 2003, p. 139).

A cultura da internet (CASTELLS, 2003), desde seu surgimento foi alicerçada pelo discurso de liberdade e pela participação de forma colaborativa de seus usuários. A chegada da Web 2.0 deu base tecnológica à cultura da participação (SHIRKY, 2011), promovendo e facilitando os processos criativos. Visto como um otimista desta era, Levy (1999) anunciou a necessidade de se estar aberto às mudanças que a internet e a tecnologia proporcionavam. O autor assegurava que é preciso aceitar as novas condições que surgiam e aprender a utilizá-las de forma proveitosa.

Contudo, esse cenário aos poucos foi se mostrando enganoso. A livre comunicação prometida estava longe de ser perfeita, organizações aprimoraram seus códigos para que toda troca e uso dos seus serviços fossem arquivados e classificados, gerando uma quantidade incalculável de dados sobre determinado usuário e utilizando-os para diferentes fins.

Castells (2003, p. 140) afirmou que "A transformação da liberdade e privacidade na Internet é um resultado direto de sua comercialização". A publicidade passou a ser a maior fonte de rendimento das empresas da internet, e seu principal produto eram de fato os seus usuários. Todo simples clique ganhou um valor precioso, devido à venda dos dados de tais usuários para seus verdadeiros clientes, as empresas de marketing.

Os governos se aproveitaram dessas tecnologias privadas para voltar a ter o controle que estava fragilizado devido à natureza aberta e livre da internet. Por vários anos o usuário foi cego sobre os processos que estavam por trás dos serviços e ferramentas que eles utilizavam. À medida que a internet se alastrava em volta dos vários aspectos da vida humana, os usuários viam-se prisioneiros de uma arquitetura desconhecida.

Entretanto, um evento em particular contribuiu para a internet se tornar um lugar de vigilância em massa e de monitoramento ininterrupto, os atentados terroristas de 11 de Setembro de 2001. Se antes, os EUA e as empresas americanas trabalhavam em parceria espionando e utilizando a internet para monitorar comunicações específicas, depois dos atentados terroristas ao *World Trade Center* e ao Pentágono, tal processo foi intensificado violentamente.

> Ficou claro após o 11 de Setembro que várias formas de vigilância tornaram-se cada vez mais aceitas como parte da vida cotidiana. Desde então, isso se tornou ainda mais óbvio na medida em que inúmeros esquemas de vigilância,

> com exceção apenas dos exemplos mais absurdos, têm sido aceitos sem resistência, especialmente pela população norte-americana. É possível que, de uma forma geral, cidadãos aceitem que a perda da privacidade seja o preço a ser pago pela segurança – como a mídia tem reiterado *ad nauseam* desde o 11 de Setembro (LYON, 2010, p. 116).

O *Patriot Act*, assinado pelo ex-presidente George W. Bush logo após os atentados e em 2011, sancionada por mais quatro anos pelo presidente Barack Obama, deu poder ao Estado de atuar contra possíveis ameaças sem necessitar da intervenção judicial. Tendo como justificativa a guerra contra o terrorismo, muitas políticas legais e técnicas postas em prática, jamais teriam sido aceitas e aprovadas antes dos atentados de 11 de Setembro(CHOMSKY,2013).

O discurso construído de "Guerra ao terror" foi legitimado pela narrativa da TV que vitimou os norte-americanos e convenceu a opinião pública que tudo era permitido dentro dessa guerra, sendo os seus inimigos tão cruéis e violentos. A invasão do Iraque, assim, foi mais uma vez justificada e aceita pela população, revestida do discurso de "guerra ao terror", e segundo Chomsky (2015) foi uma das raízes do grupo terrorista Estado Islâmico e também é considerado pelo autor como um dos maiores crimes do milênio.

Por ser um ambiente de livre circulação e por ter um uso diversificado, sejam eles lícitos ou ilícitos, a internet tornou-se um dos principais meios de comunicação utilizados pelos terroristas para propagar suas ideias e recrutar seguidores. O professor israelense Gabriel Weimann[5] pesquisa há vários anos sobre o uso da internet por grupos terroristas e traz como resultado, a sofisticação das redes online montadas por tais grupos, possibilitando que façam uso de várias plataformas e criem novas estratégias de recrutamento e de propaganda.

Desde os atentados de 11 de Setembro e também pelo grande uso da internet pelos terroristas, as redes de comunicação online vêm sendo amplamente vigiadas e monitoradas, com o discurso principal, de que outros atentados sejam evitados. Como afirmamos anteriormente, embora não exista nenhuma novidade em se encontrar nações vigiando seus cidadãos e espionando outras nações, sejam estes parceiros ou não, aspectos importantes voltados à privacidade e a liberdade de expressão dos usuários da

[5] Entrevista para Revista Veja em 2011. Matéria disponibilizada no site: < http://migre.me/sJwE1 >. Acessado em: 27 nov. 2015.

rede ganha novas implicações na era digital, visto que tanto governos como empresas, usam a arquitetura da rede como mecanismos de imposição de poder.

3 As revelações de Edward Snowden

A Agência de Segurança Nacional (National Security Agency – NSA) dos EUA foi criada em 1952, com o objetivo, em princípio, de enfrentar os desafios da Guerra Fria. A agência faz parte do Departamento de defesa e uma das suas funções primordiais é proteger as comunicações e informações voltadas à segurança nacional norte-americana.

Para muitos, o que a NSA representa é sinônimo de poder e vigilância, mas também de mistério e segredos. Durante anos a sua existência foi negada pelos órgãos do governo, entretanto a sua história é marcada por denúncias e por vazamentos de informações contra a própria instituição. A primeira dessas histórias aconteceu ainda na década de 1960, por dois funcionários da NSA, Bernon F. Mitchell e William Martin, que descontentes com a politica dos EUA, se juntaram ao governo soviético e descreveram em detalhes as operações da NSA (NSA, 2012).

Desde sua fundação, a NSA tentou passar despercebida e ocultar seu trabalho de espionagem dentro da sociedade norte-americana. Contudo, acusações contra a organização impossibilitaram sua tentativa de ocultamento. Em 2013, aconteceu um dos maiores vazamentos da instituição, quando o ex-analista da NSA Edward Snowden revelou para o jornalista Glenn Greenwald e a documentarista Laura Poitras, um grande número de arquivos altamente secretos pertencentes à NSA e suas práticas modernas de espionagem. Suas ações se voltavam tanto para seus inimigos (como é o caso de grupos terroristas, por exemplo), como também para seus aliados e seus próprios cidadãos americanos, incluindo governos de outras partes do mundo.

As principais informações contidas nos documentos vazados se referiam às práticas sigilosas de espionagem e vigilância realizadas pela agência como as escutas e registros telefônicos, a coleta de dados da internet, a invasão de e-mail de políticos de outros países, como Brasil e Alemanha, a violação da criptografia utilizada pelos serviços de internet, dentre outras[6]. Tais revelações se tornaram o marco do despertar de

[6] Matéria do site Último segundo, disponível em: < http://migre.me/sJwCt >. Acessado em 12 dez. 2015.

nações e da sociedade civil sobre a falta de limites que o uso da internet possibilita a esses tipos de agências e governos.

Amparadas pelas possibilidades trazidas pela tecnologia e após os atentados de 11 de setembro, a NSA iniciou secretamente o trabalho de vigilância em massa. O objetivo final da agência era "coletar tudo, de todos, em todos os lugares, e armazenar por prazo indefinido" (HARDING, p. 14, 2014). A suspeita de suas práticas, mas a falta de mecanismos de comprovação durante anos impediu que a instituição fosse desmascarada.

Nesse entremeio, um ponto de virada ocorre com a apropriação tecnológica pelos *hackers*, com a sofisticação das suas habilidades técnicas e de programação no mundo virtual. Seguidores de um ideal de cultura livre, Julian Assange, criador da Wikileaks, os criadores do *The Pirate Bay*, o grupo *Anonymous*, Aaron Swartz, assim como Edward Snowden, são parte de uma geração de delatores e que acreditam que "a informação deve ser livre". Com o uso da tecnologia, esses indivíduos burlaram os esquemas blindados de empresas e governos e tornara-os visíveis para o mundo.

O que antes só era compreendido pelos *hackers* (e alguns poucos grupos com conhecimentos sobre o funcionamento da tecnologia) as revelações de Snowden possibilitaram que a maioria dos usuários da internet pudesse tomar conhecimento sobre o que pode ser feito com seus dados e a partir das suas informações. Embora, seja característico da cibercultura, publicar informações pessoais e compartilhar fotos e opiniões em redes de relacionamento, abertas ou "privadas", e a maioria das pessoas sente prazer nisso.

Contudo, desde 2013, inúmeros grupos de todos os continentes, lutam e exigem que práticas como a da NSA possam ser impedidas e proibidas. Pois, apesar dos riscos, o discurso desejoso de convencer que a privacidade é coisa do passado, ainda incomoda e não é aceita por muita gente. O fenômeno ultrapassa a dimensão do discurso que tenta usar a segurança como justificativa para espionar, vigiar e recolher dados de qualquer indivíduo sem medir as consequências para o escopo social, que depende da naturalidade de suas ações para se desenvolverem e relacionarem, sem colocar em risco as liberdades individuais.

4 Sociedade em rede vigiada

As tecnologias comunicacionais que surgiram no final do século XX e início do século XXI foram preponderantes no processo de globalização (SANTAELLA, 2002). A popularização da internet e a comercialização das tecnologias digitais aceleraram tal processo, quebrando barreiras territoriais e possibilitando a interconexão planetária.

Segundo Santaella (2002), duas tendências principais surgiram com as infovias que a cibercultura possibilitou, a tendência dos eufóricos e a tendência dos disfóricos. Para a autora, os eufóricos enxergavam as liberdades abertas pela nova cultura cibernética de forma utópica, acreditando numa reviravolta nas formas de poder social e nas tradicionais formas de propriedade. Enquanto os disfóricos, que seriam os impacientes críticos, sem nem ao menos esperar por resultados práticos, já foram lançando suas descrenças, comparando a cibercultura aos fatos críticos ocorridos na cultura de massa e na indústria cultural.

Categorizar as transformações da cibercultura como positiva ou negativa soa de forma imatura, devido principalmente à complexidade e velocidade do fenômeno. Desde o início, a quantidade de pessoas que queriam fazer parte dessa cultura só crescia, utilizando os chats das salas do Uol, criando perfis na rede social Orkut, ou Twitter, ou mais recentemente no Facebook, realizando pesquisas nos motores de busca do Yahoo ou do Google, o que contribuía para facilitar o uso da tecnologia e também para encontrar informações e notícias de forma rápida. A internet, assim, parecia ter sido a melhor invenção de todos os tempos.

> A cultura que se cria na web é fascinante e, ao mesmo tempo, miserável. Fascinante porque nos envolve em seus tentáculos, tornando-nos servos desse novo grande senhor dos tempos eletrônicos. A técnica, já dizia o velho Heidegger, não só realiza plenamente aquilo que nenhuma religião conseguiu, a saber, o envolvimento de todo o planeta em sua rede, mas também funda uma época, impões um único modo de pensar, coloca tudo a seu serviço (VIANA, 2012, p. 9).

Porém, enxergar na internet somente um espaço aberto, livre e sem limites de uso, fez com que se ignorassem aqueles que estavam estruturando e formatando os serviços que conquistavam cada vez mais usuários. O que muitos não compreendiam, e nem passava pela cabeça ser uma preocupação, era como a tecnologia e seus serviços funcionavam. Quando a TV surgiu, com quase um aparelho por residência, os

telespectadores não sentiram necessidade de entender o que significava estar assistindo a um canal ou outro, e o que aquilo representava para o mercado capitalista que investia naquele tipo de serviço.

Assim foi com a internet. Seus usuários só se preocuparam em saber quais passos seguir para ligar o computador, como se conectar à rede e o que fazer para navegar de forma mais rápida e fácil. O que significava está conectado em uma rede, acessando determinado site e clicando em certos anúncios, nem de longe pareceu ser um problema, ao contrário, nunca as pessoas tiveram tanta autonomia para escolher as noticias que queriam ler, nem na busca de informação e conhecimento. O que seria feito dos seus dados obtidos a partir das suas navegações, não era uma pergunta que se consideraria fazer naquele momento. A maioria não sabia nem o que essa pergunta representava dentro do contexto socioinformacional.

Diante de tal grau de inocência, ou mesmo de ignorância, as empresas passaram a construir uma arquitetura da rede seguindo suas próprias regras e necessidades. Não se fazia ideia como o ciberespaço poderia ser regulado, e a omissão do Estado fez com que os interesses comerciais fossem sobrepostos aos interesses públicos. Para Cleland (2012), "o que nós não vimos – o que nos recusamos a ver – era a dinâmica de 'o vencedor leva tudo' da internet".

O romance de George Orwell, escrito na década de 1940, alertava como no futuro a tecnologia seria utilizada como mecanismo de dominação e controle. Na obra, o autor traz a televisão, (ou a teletela, como ele chamou), como a responsável por tal controle e espionagem de toda população, "A teletela recebia e transmitia simultaneamente. Todo som produzido por Winston que ultrapassasse o nível de um sussurro muito discreto seria captado por ela" (ORWELL, 2009, p. 13). No contexto do ciberespaço, a narrativa de Orwell tornou-se bastante atual, embora potencialmente mais poderosa. Ao invés de só escutar e assistir a qualquer coisa, como fazia as teletelas, a internet é usada para coletar milhões de dados de qualquer pessoa que utilize as redes sociais, os motores de busca e os sites espalhados pela Web. Todas as conversas são arquivadas em um lugar que ninguém conhece ao certo, todos os cliques são registrados e a partir de tais informações as empresas constroem um perfil detalhado sobre os gostos, as preferências e o modo de pensar de cada usuário.

> A tentativa de saber o máximo possível sobre seus usuários tornou-se a batalha fundamental da nossa era entre gigantes da internet como Google, Facebook, Apple e Microsoft. Como me explicou Chris Palmer, da Eletronic Frontier Foudation: "Recebemos um serviço gratuito, e o custo são informações sobre nós mesmos. E o Google e o Facebook transformam essas informações em dinheiro de 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 das nossas vidas. O nosso belo Iphone novo sabe exatamente onde 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).

Pariser (2012) ainda retrata em sua tese os perigos que o formato de negócios dessas empresas pode acarretar. Os serviços personalizados separam cada vez mais as pessoas, e as tornam incapazes de decidirem por si mesmas, pois os algoritmos criam "filtros bolhas", diminuindo suas perspectivas e percepção do mundo. Tal personalização também faz com que os padrões de uso de cada um sejam mais facilmente submetidos à inspeção e a vigilância.

Essa configuração da rede tornou-se o principal meio de controle das pessoas. A vigilância, que como já vimos, sempre existiu, atualmente tem sua mais eficaz e eficiente ferramenta. Agora, o problema não é mais se pensar em estratégias para se obter determinadas informações, mas sim em como conseguir monitorar os milhões de dados gerados o tempo todo na internet. A diversidade das práticas de vigilância torna-as comuns e presentes no cotidiano da vida social, e ampliam-se à medida que tais práticas não são questionadas.

Bruno (2013) nos alerta que devemos abrir mão dos modelos grandes e acabados de compreensão da vigilância, devido à singularidade das práticas e processos que se desenrolam atualmente. Mas, também percebe que à medida que tentamos entender a atualização da vigilância, corre-se o risco de sermos ultrapassados pela velocidade do fluxo das dinâmicas em curso. O que se deve estar atento segundo a autora (2013, p. 19), é que "as atuais práticas de vigilância contam com uma imensa e crescente diversidade de tecnologias, discursos, medidas legais e administrativas, instituições e corporações, enunciados e empreendimentos científicos, midiáticos, comerciais, políticos etc". A partir disso, percebe-se a diversidades de interesses e como está distribuído nos processos sociais, mas por fim, envolve os jogos de poder de quem

controla quem, afetando diretamente a individualidade e também as relações coletivas existentes.

Não é novidade que a pesquisa cientifica se especializa e traz grandes contribuições aos vários setores sociais, sendo a tecnologia na maioria do caso a base para muitos avanços e descobertas. As técnicas de espionagem e vigilância tendem a se aprimorar num continuo de melhorias e especificidades, como acontece desde seus primeiros usos na história da humanidade. O discurso de segurança que tenta justificar práticas invasivas, em princípio para proteger, parece gerar mais in/segurança atualmente (BAUMAN; LYON, 2013). Se antes a vigilância era voltada para possíveis suspeitos, hoje qualquer um pode ser foco de vigilância, e mesmo sendo inocente de qualquer suspeita, o medo e a in/segurança gerados pelo controle excessivo de suas ações paralisam e infringem as leis que garantem as liberdades de expressão dos indivíduos.

Considerações finais

Apesar de não ser possível datar com exatidão quando a prática de espionagem iniciou, tal estratégia passou a ser um recurso básico e indispensável para a segurança das tribos, dos estados e das nações. O objetivo do nosso artigo foi investigar como a vigilância se reconfigurou no cenário digital contemporâneo, e quais sãos as implicações para os usuários comuns da rede.

Dois acontecimentos foram propulsores para o estado de vigilância atual, os atentados de 11 de Setembro de 2001e as revelações dos arquivos secretos da NSA, por Edward Snowden. Percebemos em nossa análise que os fatos não são intrinsicamente dependentes um do outro, pois como podemos observar a espionagem sempre existiu entre nações e sobre seus cidadãos. O que mudou com o primeiro evento, e o que é comprovado pelo segundo, foi a intensificação das práticas de vigilância e as novas ferramentas utilizadas para este fim.

Paralelamente, as ações de espionagem que acontecem pelos governos e pelo mercado corporativo, grupos de *hackers* em defesa da maioria dos usuários da rede denunciam e tornam público o que é feito de forma mascarada. A partir de suas habilidades de programação e com os computadores, utilizando as próprias tecnologias que vigiam e monitoram a todos na web, tais indivíduos, por um despertar de uma

centelha ética, confrontam o poder e enfrentam as duras consequências de suas revelações.

A justificativa de "segurança nacional" acalma, mas não convence aqueles que hoje têm suas vidas rastreadas e vigiadas pelas empresas, que em troca de seus serviços exigem a transparência total. Ocorre o mesmo com os governos, que trabalham em parceria com tais empresas, e a partir da criação de leis que os resguardam, como foi o caso do *Patriot Act*, lançam uma "guerra contra o terror" sem limites e sem se preocupar com as consequências.

O excesso de segurança, que ainda assim não impede que atos terroristas matem e firam centenas de pessoas em vários países, além de não garantir a segurança prometida, causa no interior dos usuários das tecnologias digitais, que é base das relações sociais do século XXI, um alto grau de in/segurança. Saber que suas trocas de mensagens, suas pesquisas feitas nos buscadores e que cada clique seu é classificado e registrado, definindo o perfil de pessoa que se é, pode causar tanta in/segurança em um indivíduo, como paralisar suas ações e as tornarem ações automáticas, sem nenhuma consciência crítica em seus usos.

Se falharmos em reconhecer as implicações que a vigilância acarreta, poderemos nos deparar com o que os gregos chamam de *hybris*, a arrogância em ignorar a causa de um problema que visivelmente pode gerar resultados catastróficos. Por isso, devemos estar voltando sempre aos acontecimentos e fatos que balizaram o estado atual de vigilância. Se compreendermos as consequências geradas, talvez a nossa reflexão possa servir para que no futuro as decisões sejam tomadas de maneira mais responsável e assertiva.

Referências

BAUMAN, Zygmunt; LYON, David. **Vigilância líquida**: diálogos com David Lyon. Rio de Janeiro: Zahar, 2013.

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

CASTELLS, Manuel. **A galáxia da internet**: reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Zahar, 2003.

CHOMSKY, Noam. **Mídia**: propaganda política e manipulação. São Paulo: Editora WMF Martins Fontes, 2013.

_____. Disponível em: <https://www.youtube.com/watch?v=YTqeP6B9pvE>. Acessado em: 15 dez. 2015.

CLELAND, Scott. **Busque e destrua**: por que você não pode confiar no Google Inc. São Paulo: Matrix, 2012.

HARDING, Luke. **Os arquivos Snowden**: a história secreta do homem mais procurado do mundo. Rio de Janeiro: LeYa, 2014.

HIND, Cel. Allison. **História da espionagem**. Rio de Janeiro: Edições Bloch, 1967.

LÉVY, Pierre. **Cibercultura**. São Paulo: Ed 34, 1999.

LYON, David. 11 de setembro, sinóptico e escopofilia: observando e sendo observado. (org.) Bruno, Fernanda; KANASHIRO, Marta; FIRMINO, Rodrigo. **Vigilância e visibilidade**: espaço, tecnologia e identificação. Porto Alegre: Sulina, 2010.

NSA. **60 Years of defending our nation**. Disponível em: < http://migre.me/sJwym >. Acessado em: 17 nov. 2015.

ORWELL, George. **1984**. São Paulo: Companhia das Letras, 2009.

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

SANTAELLA, Lúcia. A crítica das mídias na entrada do século XXI. In: PRADO, Jóse Luiz Aidar (org.). **Crítica das práticas midiáticas**: da sociedade de massa às ciberculturas. São Paulo: Hacker Editores, 2002.

SHIRKY, Clay. **A cultura da participação**: criatividade e generosidade no mundo conectado. Rio de Janeiro: Zahar, 2011.

TZU, Su. **A arte da Guerra**: os trezes capítulos originais. São Paulo: Jardim dos livros, 2007.

VIANA, Granja. FILHO, (org.) Ciro Marcondes. **Fascinação e miséria da comunicação na cibercultura**. Porto Alegre: Sulina, 2012.

VOLKMAN, Ernest. **A história da espionagem**: o mundo clandestino da vigilância, espionagem e inteligência, desde os tempos antigos até o mundo pós-9/11. São Paulo: Editora Escala Ltda, 2013.