ESPANHA, Rita; ESTÊVÃO, Tiago (2017), *"A Vigilância Lateral e Participativa na Web 2.0", Sociologia: Revista da Faculdade de Letras da Universidade do Porto,* Vol. XXXIII, pp. 115 - 133 DOI: 10.21747/08723419/soc33a6

A Vigilância Lateral e Participativa na Web 2.0

Rita Espanha
ISCTE - Instituto Universitário de Lisboa
Centro de Investigação e Estudos de Sociologia

Tiago Estêvão
ISCTE - Instituto Universitário de Lisboa
Centro de Investigação e Estudos de Sociologia

Resumo
A vigilância é nos dias de hoje um fenómeno disseminado à escala global. A Sociedade em Rede, a disseminação das ferramentas de Web 2.0 e o advento dos dispositivos móveis com acesso à Internet fomentam o surgimento de novas dinâmicas de interação social e por conseguinte de vigilância em ambiente 2.0. Este ensaio tem como principal objetivo o de apresentar a ainda muito recente e pouco estudada Vigilância Lateral na Web 2.0 na vertente de segurança e policiamento. Com vista à contextualização deste novo fenómeno de vigilância serão analisados dois episódios: os tumultos de Vancouver de 2011 e os atentados de Boston de 2013.

Palavras-Chave: vigilância; vigilância lateral; Web 2.0.

Lateral and Participatory Surveillance on Web 2.0

Abstract
Surveillance is nowadays a widespread phenomenon on a global scale. The Network Society, the spread of Web 2.0 tools and the advent of mobile devices with Internet access foster the emergence of new dynamics of social interaction and therefore surveillance in a 2.0 environment. This article has as main objective to present the still very new and little studied Lateral Surveillance on Web 2.0 in the field of security and policing. In order to contextualize this new phenomenon of surveillance are analyzed two episodes: The 2011 riots in Vancouver and the attacks of Boston 2013.

Keywords: surveillance; lateral surveillance; Web 2.0.

Surveillance latérale et participative sur le Web 2.0

Résumé
La surveillance est aujourd'hui un phénomène très disséminé à l'échelle mondiale. La Société en Réseau,

la propagation des outils Web 2.0 et l'avènement des appareils mobiles avec accès à l´ Internet favorisent l'émergence d'une nouvelle dynamique de l'interaction sociale et en conséquence la surveillance dans un environnement 2.0. Cet article a pour objectif principal la présentation de la très récent et encore très peu étudié Surveillance Latérale sur le Web 2.0 dans le domaine de la sécurité et du contrôle policier. Afin de contextualiser ce nouveau phénomène de la surveillance deux épisodes sont analysées: Les émeutes de 2011 à Vancouver et les attaques de Boston 2013.

Mots-clés: surveillance; surveillance; Web 2.0.

Vigilancia Lateral y participativa en la Web 2.0

Resumen

La vigilancia es hoy en día un fenómeno generalizado en una escala global. La sociedad en red, la difusión de herramientas de la Web 2.0 y el advenimiento de dispositivos móviles con acceso a Internet fomentan la aparición de nuevas dinámicas de interacción social y por lo tanto la vigilancia en ambiente 2.0. Este artículo tiene como objetivo principal presentar el todavía muy nuevo y poco estudiado tema de la Vigilancia lateral en la Web 2.0 en el ámbito de la seguridad y del control policial. Para la contextualización de este nuevo fenómeno de la vigilancia se analizan dos episodios: Los disturbios de 2011 en Vancouver y los ataques de Boston 2013.

Palabras clave: Vigilancia, Vigilancia Lateral, Web 2.0.

Introdução

> "O policiamento das redes sociais é indicativo de um novo paradigma de visibilidade. Os utilizadores de redes sociais produzem quantidades impressionantes de informação, e novas tecnologias e práticas policiais asseguram uma vigilância reforçada desta informação." (Trottier, 2012: 422)[1].

Neste artigo pretende-se discutir o fenómeno de vigilância que ocorre na Web 2.0[2], a chamada Vigilância Lateral, nomeadamente na sua vertente de segurança e policiamento.

Realiza-se, em primeiro lugar, um retrato do panorama complexo que envolve a vigilância na atualidade, das suas principais aplicabilidades no espaço físico e no espaço virtual da Internet, nomeadamente ao nível da monitorização das entidades patronais, de segurança e policiamento e com fins comerciais e *marketing*.

Após uma breve abordagem teórica, são analisados dois casos exemplificativos do fenómeno da Vigilância Lateral na Web 2.0, na sua vertente de segurança e

[1] Tradução livre.

[2] Termo que serve para designar uma segunda geração de comunidades e serviços da *Web*.

policiamento, iniciando uma discussão mais abrangente no campo das Ciências da Comunicação e Estudos de Vigilância.

O Novo Paradigma da Vigilância

Nunca antes a vigilância foi alvo de tanta atenção, tão discutida, tão analisada, criticada ou fomentada, tanto do ponto de vista académico como na informação generalista ou mesmo na ficção (literária, televisiva ou cinematográfica).

A visão de vigilância, enquanto conceito e objeto de estudo, realizada por Michel Foucault, ainda que actual, necessita de contextualização à luz dos novos paradigmas da comunicação. O Panótico de Foucault, que cingia a vigilância a locais onde as pessoas estão confinadas (prisões, asilos, hospitais, escolas ou locais de trabalho) (Foucault, 1977), é atualmente alvo de discussão por parte de autores como Mark Andrejevic (2007) ou Anders Albrechtslund (2008), que defendem que esses espaços fechados de confinamento já não são os únicos ou mesmo os principais locais de vigilância, existindo inúmeros instrumentos e modelos de vigilância contemporâneos em utilização (videovigilância, leituras biométricas, sistemas de algoritmos avançados, entre outros).

Após a abordagem de vigilância por Michel Foucault (Foucault, 1977), emergem vários estudos de vigilância e vários autores conceptualizam distintas interpretações de vigilância. Anthony Giddens, em 1985, define vigilância como a atenção rotineira, focada e sistemática com vista à recolha de dados com o fim de influenciar, gerir, proteger ou dirigir indivíduos. Não é aleatória, nem ocasional, nem espontânea. É deliberada e depende de protocolos e técnicas (Giddens, 1985).

Por sua vez David Lyon, em 2001, interpreta o conceito de vigilância da seguinte forma: "Qualquer recolha e tratamento de dados pessoais, seja identificável ou não, para fins de influenciar ou gerenciar aqueles cujos dados foram acumulados" (Lyon, 2001: 2). Catarina Frois, na sua obra *Vigilância e Poder* (Frois, 2011), realiza um retrato da política de segurança e da implementação da videovigilância em Portugal. Neste trabalho, a autora realiza uma reflexão crítica à interpretação e associação de vigilância como um fator exclusivamente negativo de poder, instigando o controlo e a disciplina, colocando a seguinte questão: "Falamos de vigilância no sentido de controlar com o intuito de penalizar ou falamos de proteger?" (Frois, 2011: 122).

Em resposta a esta questão, a autora evidencia o exemplo da *vigilância médica*, não só no que se refere às interacções entre médico e paciente, como na pória deteção e monitorização de doenças infeciosas. Segundo a autora, controla-se

para identificar determinada doença e argumenta-se que ao mesmo tempo se protege o portador e quem o rodeia. Estamos perante uma argumentação que se deve considerar, também de acordo com Frois, pois o controlo sobre o indivíduo é realizado em prol da proteção do ser colectivo (Frois, 2011). Interpretações antagónicas surgem igualmente referentes à vigilância na Sociedade em Rede. Assim, autores como Manuel Castells (2001), Mark Andrejevic (2002) e Joseph Turow (2005; 2006) defendem nas suas premissas a ideia de vigilância na Internet com base no Panótico. Ou seja, consideram a vigilância *online* negativa, evidenciando, como aspetos inerentes, o seu poder de dominação, controlo e disciplina.

Pelo contrário, autores como David Lyon (1998; 2003), Hille Koskela (2004) e Anders Albrechtslund (2008) defendem a vigilância na Internet como distante das noções do Panótico. Ou seja, a vigilância *online* não possuí um papel coercivo, identificando-se-lhe características positivas ou neutras, evidenciando-se o seu papel funcional e lúdico.

David Lyon na sua obra *The World Wide Web of Surveillance* (Lyon, 1998) distingue três formas principais de vigilância na Internet. A (1) Vigilância pela Entidade Patronal – que se distingue pela monitorização, por parte das entidades empregadoras, dos hábitos *online* dos trabalhadores, com o fim último do aumento da produtividade (Taylorismo) (Fuchs, Boersma, Albrechtslund and Sandoval, 2011). A (2) Vigilância de Segurança e Policiamento – perpetrada pelos Estados-Governo, que proliferou após os ataques terroristas de 11 de setembro de 2001, que privilegia políticas de controlo e supervisão, com vista a reinstalar um sentimento de segurança (Lyon, 2007, Frois, 2011). Por fim, o autor apresenta a (3) Vigilância com Fins Comerciais e *Marketing* – onde surgem as redes sociais *online*, recolhendo de forma massiva dados de utilizadores, analisando, classificando e definindo tipologias de consumidor, avaliando os seus interesses e associando-os a determinados consumos e a campanhas de *marketing* pré-definidas (Fuchs, 2011; Estêvão, 2014, 2014a).

As duas últimas formas de vigilância referenciadas - (2) e (3) - encontram-se nos dias de hoje, e como veremos de seguida, em plena expansão na Web 2.0, tendo sido alvo de grande cobertura mediática. No que concerne à (2) Vigilância de Segurança e Policiamento e com o surgimento das redes sociais, é notório o aparecimento de novas dinâmicas sociais na Internet, que são alvo de interesse por parte de entidades governamentais. Anders Albrechtslund refere-se deste modo à vigilância realizada na Web 2.0:

> "O interesse do governo em redes sociais *online* é fácil de entender. Para a identificação do perfil de potenciais criminosos e terroristas, é necessário combinar uma ampla gama de informações sobre as pessoas. Esta informação inclui as relações sociais, tais como atividades compartilhadas

> e círculos de amigos, bem como dados pessoais sobre opiniões políticas, crenças religiosas, orientação sexual e preferências sobre as atividades da vida diária" (Albrechtslund, 2008:4)[3].

No decorrer dos primeiros dias do mês de junho de 2013, surge a controversa revelação difundida pelo jornal britânico The Guardian e o norte-americano The Washington Post, envolvendo alegadamente um programa de vigilância intitulado - Prism. O referido programa governamental, desenvolvido pelos EUA, envolve a troca de informações entre entidades como a National Security Agency (NSA) e empresas como a Google, a Microsoft, o Facebook, o Yahoo!, o Youtube, o Skipe ou a Apple. As informações partilhadas entre as empresas multinacionais referidas e a agência de segurança nacional norte americana (NSA) envolvem dados de milhões de utilizadores, nomeadamente correio eletrónico, fotos e vídeos. Também referenciado pelo mesmo jornal britânico e referente à mesma agência, a National Security Agency (NSA), está a acusação de alegado envolvimento com a empresa de telecomunicações norte americana Verizon, na recolha de milhões de conversas em chamadas telefónicas (Harding, 2014; Estêvão, 2014, 2014a).

A metodologia de recolha massificada de dados é, segundo Edward Snowden, (antigo assistente técnico da NSA e a principal face no processo de acusações), realizada de forma sistemática, massiva e indiscriminada. O motivo apontado para o procedimento é a maior eficácia de escrutínio que a recolha massiva representa, face à recolha seletiva, fazendo uso de algoritmos avançados que identificam perfis de risco (Harding, 2014).

Os desenvolvimentos, até à data, referentes às declarações de Edward Snowden, apontam para uma crescente instabilidade na política internacional, resultante das periódicas revelações de vigilância em massa perpetrada pela agência de segurança norte-americana NSA e pela sua congénere britânica Government Communications Headquarters (GCHQ) a milhões de cidadãos de todo o mundo e a Estados Governo como a Alemanha, o Reino Unido e o Brasil. A meados do mês de maio de 2014, Edward Snowden, pela mão do autor Glenn Greenwald expõe, na obra não ficcional *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State* (Greenwald, 2014), os meandros do já referenciado programa Prism. A 22 de fevereiro de 2015, a Academia de Artes e Ciências Cinematográficas norte americana agracia, com o Óscar de Melhor Documentário de 2014, o documentário *CitizenFour*[4], da realizadora Laura Poitras, que aborda o escândalo de espionagem perpetrada pela NSA

[3] Tradução livre.

[4] http://www.imdb.com/title/tt4044364/

e os encontros com Edward Snowden, antes e depois de sua identidade ser revelada ao público. Edward Snowden, a 1 de agosto de 2014, viu prolongada por mais três anos a sua autorização de residência na Rússia, cedida pelo presidente russo Vladimir Putin.

Quanto à (3) Vigilância com Fins Comerciais e de *Marketing* na Internet, David Lyon, ainda antes do apogeu da Web 2.0 verificou que:

> "A Internet tornou-se uma indústria multibilionária, onde um conjunto de empresas recolhem e analisam uma grande quantidade de dados de consumo pessoais, a fim de direcionar uma publicidade personalizada" (Lyon, 2003: 162).

As características apontadas pelo autor à Internet são extensivas à Web 2.0, e, atualmente, aplicações como o Facebook ou o Foursquare utilizam a vigilância de forma massificada junto aos seus utilizadores. A vigilância é no entanto personalizada e individual, na medida que compara interesses e comportamentos com outros utilizadores, definindo e classificando tipologias de potenciais consumidores. Esta classificação é realizada com base em mecanismos de comparação e algoritmos de seleção que estipulam perfis e direcionam consumos (Fuchs, Boersma, Albrechtslund and Sandoval, 2011).

Ferramentas de Web 2.0, como o Facebook, fazem uso de configurações de privacidade, onde o fornecimento de dados é exigido ao utilizador a fim de ser capaz de usufruir da aplicação. Aplicações digitais em plataformas móveis (como por exemplo *smartphones*) estão hoje capacitadas para identificar e recolher hábitos *online* dos utilizadores, nomeadamente contatos, ficheiros, localização, e muito mais. Perfis elaborados de utilizadores estão a ser recolhidos por empresas multinacionais com base na coleta de dados de plataformas móveis (Cottrill, 2011).

Também as tecnologias de reconhecimento facial, ficcionadas em filmes como *Minority Report*[5], estão atualmente em pleno desenvolvimento. Empresas como a Google e a Apple estão já a desenvolver bases de dados com impressões faciais, fazendo uso de fotografias e perfis de utilizadores de redes sociais como o Facebook (Estêvão 2014, 2014a).

Nos Estados Unidos da América, a legislação em vigor impõe limitações restritas à utilização de impressões faciais para usos de controlo laboral e de segurança nacional. Contudo, estas limitações legislativas, referentes à utilização das impressões faciais, não contemplam a utilização para fins comerciais e de *marketing* realizadas

[5] Baseado no conto de ficção científica, escrito por Philip K. Dick, publicado em 1956. http://www.imdb.com/title/tt0181689/?ref_=nv_sr_1.

por empresas multinacionais. O controlo e a supervisão empresarial, por parte das multinacionais, estão, pois, salvaguardados pela constituição norte americana (Papacharissi, Gibson, 2011). Na Europa, nomeadamente na União Europeia, a legislação em vigor é mais rigorosa e penalizadora dos usos das impressões faciais para fins comerciais.

Segundo dados recentemente revelados pelo Facebook e divulgados pela imprensa mundial, esta empresa multinacional, líder de mercado no sector das ferramentas digitais detinha, a janeiro de 2015, cerca de 1.39 bilião de utilizadores ativos mensalmente (cerca de 1/7 da população mundial).

Mark Andrejevic acrescentaria às três formas principais de vigilância na Internet, distinguidas por David Lyon, uma nova forma de vigilância que designou como - (4) Vigilância Lateral - e que ocorre essencialmente na Web 2.0 (Andrejevic, 2007).

A Vigilância Lateral e Participativa na Web 2.0

O fenómeno particular da Vigilância Lateral na Web 2.0 é o tema que aprofundamos neste artigo. Antes de abordarmos a Vigilância Lateral na Web 2.0, gostaríamos de realçar que a vigilância é, na sociedade contemporânea, um fenómeno complexo, movido por interesses políticos e económicos difusos. Nos recentes estudos sobre vigilância na Web 2.0, destacam-se autores como Mark Andrejevic (2007), Anders Albrechtslund (2008), Christian Fuchs (2011) ou Daniel Trottier (2012, 2012a, 2012b).

Christian Fuchs, salienta que:

> "Os estudos de vigilância na Web 2.0 estão num estágio inicial de desenvolvimento. O debate sugere, até agora, que se pode distinguir entre uma abordagem de estudo cultural e uma crítica abordagem de política económica, no estudo da vigilância na Web 2.0" (Fuch, 2011: 1)[6].

A Vigilância Lateral que ocorre nas redes sociais, segundo Mark Andrejevic (Andrejevic, 2005), pode ter distintos fins e aplicabilidades, das mais elaboradas prospeções de *marketing* digital, realizadas por entidades empresariais, às mais inofensivas prospeções de cariz sexual, a que o autor designa de - *Online Dating* (Andrejevic, 2005). A nossa análise, no presente artigo, cinge-se unicamente à Vigilância Lateral na Web 2.0, numa vertente específica de segurança e policiamento (Estêvão, 2014). Em rigor, e tendo em conta a focalização e especificidade do tema,

[6] Tradução livre.

seria mais apropriado designar esta tipologia de vigilância como Vigilância Lateral e Participativa na Web 2.0. Mais adiante explicaremos a razão desta afirmação.

Mark Andrejevic, define desta forma o conceito de Vigilância Lateral na Web 2.0:

> "Vigilância Lateral, ou monitoramento entre pares (*peer-to-peer*), entendida como o uso de instrumentos de vigilância por indivíduos, ao invés de por agentes de instituições públicas ou privadas, para manter o controlo de um outro, abrange (mas não se limita a) três categorias principais: interesses românticos, familiares e amigos ou conhecidos" (Andrejevic, 2005: 488)[7].

Outros autores como Daniel Trottier designam esta vigilância na Web 2.0, como Vigilância Interpessoal (Trottier, 2012b).

A vigilância, no seu contexto mais amplo, é um instrumento de poder, profusamente estudado e conceptualizado por autores como o já mencionado Michel Foucault (Foucault, 1977), que definiu o conceito de Panótico, vigente nas Teorias Modernas da Vigilância. As Teorias Pós-Modernas da Vigilância, no caso particular da Web 2.0, caracterizam-se pelo nivelamento do poder da vigilância.

A vigilância deixa de ser um benefício exclusivo de quem detém poder - de poucos a vigiar muitos, e passa cada vez mais a ser um fenómeno descentralizado - de muitos a vigiar muitos. O surgimento e crescimento da Sociedade em Rede e da Web 2.0, a domesticação das tecnologias de informação móveis e uma propensão ao aumento da literacia digital das populações, são hoje condicionantes importantes ao nivelamento do poder da vigilância e por sua vez ao surgimento da Vigilância Lateral na Web 2.0. Steve Mann introduz o conceito de - *Sousveillance* (Mann, 2003), que muito sucintamente identifica um fenómeno em que aqueles que geralmente são alvos de vigilância, passam a vigiar, ou seja, atualmente, as redes sociais são instrumentos de visibilidade, onde as interações quotidianas se assemelham cada vez mais a processos de vigilância. A vigilância interpessoal é aqui mútua, vigiando-se e sendo-se alvo de vigilância, disponibilizando-se no perfil individual da rede social, informações tão privadas como a orientação sexual ou estado civil (Mann, 2003).

A Vigilância Lateral na Web 2.0, nomeadamente a de segurança e policiamento, caracteriza-se pela partilha de informação verídica e pela investigação, condenação pública e divulgação de ações impróprias, através de ferramentas de Web 2.0 (Andrejevic, 2005). Segundo Daniel Trottier, a principal razão para a disseminação deste tipo de vigilância na Web 2.0, diz respeito essencialmente à extensão social crescente na Sociedade em Rede e não aos constantes desenvolvimentos tecnológicos (Trottier, 2012b).

[7] Tradução livre.

Verificado igualmente por Trottier (Trottier, 2012), está a particularidade que envolve a utilização das redes sociais, nomeadamente o caso do Facebook. Tendencialmente as tecnologias de informação desenvolvem-se na esfera militar governamental, estendendo-se posteriormente a sua aplicabilidade ao foro doméstico. No caso do Facebook o processo foi o inverso - numa fase inicial esteve circunscrito ao mundo universitário, numa segunda fase democratizou-se a nível planetário e só numa última fase se evidenciou enquanto ferramenta de vigilância, sendo apropriada para fins governamentais (segurança e policiamento) (Trottier, 2012).

Quanto ao aproveitamento para fins de segurança e policiamento, por parte das autoridades, os novos *media* são atualmente uma ferramenta de eleição nas investigações e pesquisas, devido à exposição pessoal que biliões de utilizadores, voluntariamente ou involuntariamente realizam na Web 2.0.

Os tumultos de Vancouver em 2011 e os atentados de Boston em 2013

O enfoque deste artigo, como referido anteriormente, prende-se essencialmente com a análise de dois acontecimentos: (1) os tumultos em Vancouver em 2011 e (2) os atentados na maratona de Boston em 2013, associando-os e correlacionando-os ao fenómeno da Vigilância Lateral na Web 2.0, na vertente de segurança e policiamento, por serem casos onde é possível identificar o referido fenómeno.

(1) Os tumultos em Vancouver em 2011

A cidade de Vancouver no Canadá foi alvo, por duas vezes, de tumultos com características similares e com resoluções concretas e veementes. Ambos os acontecimentos tiveram como motivação os festejos de eventos desportivos e decorreram com a quase exata distância temporal de 17 anos. O primeiro tumulto ocorreu a 14 de junho de 1994 e o segundo a 15 de junho de 2011. O segundo tumulto, o que ocorreu em 2011, é o primeiro dos dois episódios que referenciámos anteriormente, e que iremos analisar no âmbito do estudo da Vigilância Lateral na Web 2.0. Ainda antes de passarmos à análise deste primeiro caso, gostaríamos de distinguir os dois tumultos decorridos em Vancouver com a separação de 17 anos. Resumidamente, em 1994 e no decorrer de uma fase final de um evento desportivo de hóquei em gelo, referente à National Hockey League (Liga profissional de hóquei em gelo que comporta equipas canadianas e norte americanas), surgiram tumultos e confrontos nas ruas de Vancouver com as forças policiais que envolveram cerca

de 8.300 pessoas e resultaram em dezenas de feridos, centenas de detidos e em avultados custos com estragos. Na altura, no decorrer dos tumultos, os *media* tiveram uma presença notória e primordial, realizando a cobertura integral dos acontecimentos. Numa ação sem precedentes e polémica foram confiscadas, pelas forças policiais, as imagens recolhidas pelas televisões locais e usadas na detenção dos implicados nos acontecimentos. Centenas de pessoas foram detidas, implicadas neste episódio, devido às imagens recolhidas pelos meios de comunicação social (Schneider, Trottier, 2012).

Em 2011, no decorrer de mais um evento desportivo, da mesma fase final da National Hockey League, sucedem-se novos tumultos na baixa da cidade de Vancouver. Cerca de 155.000 pessoas assistem nas ruas, em ecrãs gigantes, ao evento desportivo (Schneider, Trottier, 2012). No seguimento dos festejos, grupos de jovens envolvem-se em tumultos durante horas, vandalizando estabelecimentos comerciais e viaturas automóveis. Os tumultos em Vancouver, de 1994 e 2011, embora se assemelhem em muito, nomeadamente na sua essência, são radicalmente diferentes no que se refere ao envolvimento da população na condenação pública do acontecimento e das tecnologias implicadas.

A principal razão para a referida disparidade deve-se à emergência da Sociedade em Rede e a acessibilidade a dispositivos móveis com câmaras de filmar e fotografar. Destaque-se que, separam os dois episódios 17 anos de avanços tecnológicos.

Passamos de seguida a uma mais exaustiva análise do primeiro episódio de estudo, referente aos tumultos de Vancouver em 2011.

No final da tarde de 15 de junho de 2011, a baixa da cidade de Vancouver era palco de mais uma exibição em ecrãs gigantes do 7º jogo do Stanley Cup Finals da National Hockey League. Com o término do jogo, milhares de jovens presentes na exibição televisiva em ecrãs gigantes, na baixa de Vancouver, encetaram tumultos destruindo e incendiando viaturas automóveis e estabelecimentos comerciais. Presentes no local, como nos acontecimentos de 1994, estavam os mesmos canais televisivos a realizar a cobertura dos acontecimentos. Desta vez, estes canais televisivos, não assumiram o papel primordial na cobertura dos tumultos. Milhares de jovens, no decorrer da tarde, filmaram e fotografaram o acontecimento, identificando indivíduos e implicados nos tumultos. Na baixa de Vancouver, na altura dos acontecimentos e em quase sintonia, milhares de jovens auto implicavam-se, documentando os tumultos e exibindo voluntariamente, irrefletidamente e jocosamente comentários, fotografias e filmes nas redes sociais Facebook e Twitter. Numa ação sem paralelo, e passando horas desta exibição nas redes sociais dos contornos e dos implicados nos tumultos, o Mayor de Vancouver Gregor Robertson e o Vancouver Police Department encetam uma

"caça" aos implicados nas redes sociais referidas. As autoridades locais responsáveis fazem apelos concretos à comunidade local e virtual no auxílio na identificação dos implicados nos tumultos. São criadas páginas nas redes sociais, como a "Vancouver Riot Pics: Post Your Photos", no Facebook, a condenar os acontecimentos e a identificar imagens dos tumultuosos.

Imagem 1
Página do Facebook do "Vancouver Riot Pics: Post Your Photos"

Fonte: Facebook, consultada em junho de 2014

A participação das comunidades locais e virtuais na identificação dos implicados, através de fotos colocadas nas redes sociais por terceiros ou pelos próprios, foram essenciais nos processos de investigação e nas condenações.

(2) Os atentados na maratona de Boston em 2013

O segundo caso considerado refere-se ao episódio dos atentados da maratona de Boston, que decorreram no dia 15 de abril de 2013, na baixa da cidade de Boston. Descrevemos de seguida o referido episódio.

Na tarde de 15 de abril de 2013, junto à linha de chegada da maratona de Boston, duas bombas artesanais deflagraram quase simultaneamente, originando 3 mortos, 264 feridos e realizando avultados danos materiais.

O acontecimento foi prontamente divulgado pelos *media*, que o apelidaram de imediato como o pior atentado terrorista desde o 11 de setembro de 2001 nos EUA, e durante dias avançaram possíveis implicados nos atentados. Também na Sociedade em Rede, nomeadamente nas redes sociais, o tema dos atentados da maratona de Boston foi profusamente comentado. Nos dias subsequentes ao referido atentado de Boston, a agência governamental Federal Bureau of Investigation (FBI) realiza apelos concretos à comunidade local e virtual, difundidos pelos *media* e pelas redes sociais, com vista à participação e auxílio na "caça" aos culpados dos atentados. Resultado deste pedido, o FBI recebeu milhares de registos de vídeo e de fotografia do acontecimento. Em poucos dias o escrutínio, envolvendo a agência governamental FBI e uma comunidade civil mobilizada e digitalmente literata, levou à definição de dois suspeitos principais e a uma consequente "caça" ao homem. As imagens de dois indivíduos suspeitos, a percorrerem por entre a multidão as imediações da linha de chegada da maratona, munidos de mochilas e bonés, são avançadas numa primeira fase pelas redes sociais. Só mais tarde estas imagens viriam a integrar aberturas de boletins noticiosos, de canais televisivos, de todo o mundo.

Um dos atores mais interventivos neste caso em particular, nomeadamente na recolha de imagens, identificação de suspeitos e divulgação das imagens implicadoras, foi a então designada comunidade *online* 4Chan (atualmente designada como "Welcome to the Internet"[8]). Esta comunidade *online,* com presença nas redes sociais Facebook e Twitter, funciona como um fórum de discussão que utiliza imagens e textos (*imageboard*) colocados por usuários de forma anónima. O 4Chan está intimamente relacionado com as comunidades *hacker*, com o *ciberativismo* e com o grupo Anonymous[9].

A página do 4Chan, na rede social Facebook, revelou dezenas de imagens dos dois suspeitos do atentado, cedidas anonimamente por esta comunidade *online* (Imagem 2).

[8] https://www.facebook.com/4funsociety?fref=ts

[9] Comunidade virtual, criada em meados de 2003, com o propósito de ciberativismo e entretenimento.

Imagem 2
Página do Facebook do 4Chan convocando a comunidade *online* a procurar os responsáveis pelos atentados de Boston

Fonte: Facebook, consultada em janeiro de 2015

Todo o tipo de motivações eram na altura avançadas, pela comunicação social, para justificar o atentado perpetrado pelos dois suspeitos, os irmãos de origem chechena Dzhokhar e Tamerlan Tsarnaev, das motivações fundamentalistas religiosas às influências dos conflitos no Iraque ou ainda ao "poder" da Internet. O irmão mais velho, Tamerlan, viria a falecer no dia 19 de abril de 2013 vítima de ferimentos vários, após confrontos com forças policiais. No mesmo dia, Dzhokhar Tsarnaev viria a ser ferido e detido. Ele é, a 15 de maio de 2015, condenado pelo júri federal, à pena de morte. Foi considerado culpado, de 10 das 30 acusações de que era alvo referentes ao atentado de Boston.

Os tumultos de Vancouver e os atentados de Boston – dois casos de Vigilância Lateral

Analisando os tumultos em Vancouver em 2011, é importante salientar que este é um dos poucos episódios referenciados como um evidente exemplo de Vigilância Lateral e Participativa na Web 2.0. Tal evidência levou a que este episódio tenha sido referenciado por Christopher Schneider e Daniel Trottier, no seu artigo "*The 2011 Vancouver Riot and the Role of Facebook in Crowd-Sourced Policing*" (Schneider, Trottier, 2012).

Essencialmente, foi através das redes sociais *online* que foram identificados os transgressores. Foram criadas páginas nas redes sociais, como a "Vancouver Riot

Pics: Post Your Photos", no Facebook, a condenar os acontecimentos e a identificar imagens dos tumultuosos. Em duas semanas foram colocadas, na referida página do Facebook, cerca de 12.587 comentários com informações várias referentes aos tumultos (Schneider, Trottier, 2012). Esta informação é inteiramente organizada e disponibilizada nas redes sociais por pessoas não ligadas a entidades policiais, de segurança ou governamentais. A administração da citada página na rede social Facebook é inteiramente da responsabilidade da comunidade civil, no entanto a mesma é alvo de rigoroso escrutínio por parte de entidades policiais como o Vancouver Police Department.

Os tumultos de Vancouver de 2011 vieram demonstrar que a Vigilância Lateral e Participativa nas redes sociais é uma ferramenta de valor acrescido para as forças policiais e de segurança. No caso referenciado, o *crowdsourcing* de policiamento efetuado no Facebook, foi um exemplo bem-sucedido de cooperação entre uma sociedade civil mobilizada e digitalmente literata e as forças policiais (Schneider, Trottier, 2012).

Ainda referente aos tumultos de Vancouver de 2011, três relatórios oficiais concluíram que: (1) acontecimentos como o ocorrido são muitas vezes imprevisíveis, (2) as redes sociais são ferramentas importantes de comunicação entre a comunidade civil e as forças policiais e de segurança e (3) o papel das redes sociais na aplicação da lei deve e pode ser explorado (Schneider, Trottier, 2012).

Passando ao segundo caso, o atentado de Boston, a exemplo do que sucedeu com o primeiro caso reportado, teve a sua exposição pública inicial na rede social Facebook. A comunidade *online* 4chan condenou de imediato os atentados e assumiu a responsabilidade na identificação e divulgação dos suspeitos. A comunidade 4Chan, com as suas páginas de Facebook e Twitter, foi a primeira, ainda antes de qualquer outro canal de comunicação social, a identificar e divulgar imagens dos suspeitos dos atentados - Dzhokhar e Tamerlan Tsarnaev. Embora com contornos distintos, os dois casos são demonstrativos de inúmeras características comuns e distintivas de uma Vigilância Participativa, a saber: a exemplo do que se passou na situação anterior, a administração da página de Facebook do 4Chan é inteiramente da responsabilidade da comunidade 4Chan; os conteúdos disponibilizados referentes aos dois suspeitos foram de imediato alvo de escrutínio por parte da agência governamental Federal Bureau of Investigation (FBI) e divulgados pelos meios de comunicação do mundo inteiro. Também no caso dos atentados de Boston o *crowdsourcing* de policiamento e a cooperação, entre uma sociedade civil mobilizada e digitalmente literata e as forças policiais, foi bem-sucedido.

Em ambos os acontecimentos, é legítimo identificar os *smartphones* e os dispositivos móveis com ligação à Internet como as ferramentas responsáveis pela Vigilância Lateral e Participativa na Web 2.0. Face aos casos expostos podemos avançar com a hipótese de que a videovigilância está hoje fortemente presente com as câmaras de vigilância nas ruas e com os *smartphones* nos bolsos. Saliente-se, ainda, a quase imediata auto implicação dos intervenientes e das suas ações criminosas, através da documentação e exibição voluntária de fotografias e filmes nas redes sociais *online*.

Os episódios em causa são reveladores de uma propensão por parte da Sociedade em Rede e seus participantes ativos, nomeadamente da Web 2.0, em condenar publicamente determinadas ações que ameacem a ordem social, assumindo responsabilidades na identificação e divulgação de implicados em ações criminosas.

Conclusão

Vivemos na contemporaneidade um novo paradigma da vigilância em que a disseminação da mesma é resultado de uma congregação de interesses e motivações políticas e económicas. A atual conjuntura internacional e o instável panorama geopolítico mundial são propiciadores ao aumento da vigilância. Vale a pena, neste contexto referir o conceito de Pânico Moral, definido por Stanley Cohen como um sentimento intenso, expresso numa população sobre um qualquer assunto que pareça ameaçar a ordem social (Cohen, 1972). Este sentimento intenso, que (supostamente) ameaça a ordem social é essencialmente difundido pelos *media* e pela classe política, e é justificativo para a implementação sistemática de projetos de vigilância. A vigilância enquanto fenómeno complexo assume distintas aplicabilidades na sociedade contemporânea e como tal é hoje alvo de atenção privilegiada na investigação académica, nomeadamente na área das Ciências Sociais.

O novo paradigma da vigilância tem o seu expoente máximo de atuação na Sociedade em Rede, nomeadamente nas redes sociais *online* que envolvem a interação de biliões de pessoas à escala mundial. O surgimento da Web 2.0 na Internet originou uma multiplicidade de dinâmicas sociais, que encaram a fluidez na comunicação e a acessibilidade à informação como pontos-chave. O impacto da Web 2.0 na Sociedade em Rede é notório igualmente pela sua capacidade de tornar o individuo mutuamente consumidor e produtor de conteúdos (*prosumer*), apesar da desproporção que ainda existe entre uns e outros (os que só consomem continuam a ser a grande maioria, comparados com os chamados *prosumers*). Estas características, inerentes à Web 2.0, são atualmente alvo de enorme atenção por parte de entidades governamentais

e empresariais.

Com o surgimento da Web 2.0 surgem fenómenos de vigilância singulares como o referenciado neste artigo, o fenómeno da Vigilância Lateral. Este particular fenómeno de vigilância, que se carateriza pela monitorização dos pares, está hoje amplamente disseminado em ambiente 2.0. Da vigilância casual e realizada ao nível do utilizador comum, à vigilância concertada e massificada das entidades empresarias e governamentais.

A Vigilância Lateral na Web 2.0 é fundamentalmente uma vigilância participativa e interpessoal realizada nas redes sociais, com o objetivo de condenar (comentando, incitando à ação e à partilha de informação) situações que ameacem a ordem social, cooperando, por exemplo, na identificação de transgressores implicados e na disponibilização em rede das suas identidades.

Os exemplos referidos neste artigo, apesar de serem fenómenos recentes, são identificativos do potencial participativo e "vigilante" da Sociedade em Rede em que vivemos, onde os dispositivos móveis com ligação à Internet assumem um papel cada vez mais premente e onde a Web 2.0 prolifera.

No Reino Unido, país do mundo com o maior número de câmaras de vigilância na via pública, surgem projetos recentes e inovadores, introduzindo conceitos de *crowdsourcing* de videovigilância através da Internet, (por exemplo a Facewatch ou a CrimeStoppers UK) (Trottier, 2012a). Estes projetos presentes na Internet e alguns deles na Web 2.0 possuem inúmeras aplicações, que vão desde a monitorização de uma determinada zona, a partir de um computador pessoal; à recolha de informações de criminosos com entrega de recompensas; ou à identificação de crimes empresariais. Numa outra vertente, como referenciado anteriormente, um instável panorama geopolítico mundial, com repercussões diretas e notórias nas sociedades ocidentais é propiciador a uma vigilância lateral e participativa de policiamento na Web 2.0. Fenómenos recentes e mediáticos de natureza terrorista, como as execuções filmadas em direto, são perpetrados pelo denominado Estado Islâmico (EI). Em virtude de uma apropriação hábil das redes sociais, nomeadamente Twitter e Facebook, na vertente comunicacional e não só, são realizados recrutamentos de militantes, um pouco por todo o mundo, para as fileiras do EI.

Também aqui, na disseminação da propaganda terrorista de grupos como o EI, a Vigilância Lateral e Participativa na Web 2.0 é verificável. A comunidade Anonymous posiciona-se com as suas usuais comunicações em vídeo[10] e incita, através

[10] https://www.youtube.com/watch?v=BPE_sRhZp6M

de operações como a de código - #OpISIS, a cooperação na denúncia de utilizadores e contas de propaganda do EI, na plataforma Twitter. Recomenda procedimentos *online* para denúncia de ações propagandísticas terroristas.

A Vigilância Lateral e Participativa na Web 2.0, no que diz respeito ao policiamento, é um fenómeno que tem vindo a merecer a maior atenção por parte das forças de segurança pelas suas capacidades de atuação. Por um lado, vê-se surgir uma rede de cidadãos comprometidos e empenhados que compilam provas de envolvimentos em crimes e as disponibilizam nas redes sociais. Por outro lado, observamos a existência de um cada vez maior número de utilizadores de ferramentas de Web 2.0, que expõem cada vez mais a vida quotidiana e as interações sociais. A confluência destes fenómenos obriga a uma cada vez maior atenção e reflexão por parte das Ciências Sociais, no seu esforço de compreensão das sociedades contemporâneas.

Referências Bibliográficas

ALBRECHTSLUND, Anders (2008), *Online Social Networking as Participatory Surveillance*, First Monday 13(3).

ANDREJEVIC, Mark (2002), "The Work of Watching one Another: Lateral Surveillance, Risk and Governance", *Surveillance & Society – Peoples watching People* (ed. Wood) 2 (4): 479-497.

- (2007*), iSpy: Surveillance and Power in the Interactive Era (Culture America)*, University Press of Kansas.

CASTELLS, Manuel (2001), *The Internet Galaxy: Reflections on the Internet, Business, and Society*, Oxford University Press.

COHEN, Stanley (1972), *Folk Devils and Moral Panics*, MacGibbon and Kee, Ltd.

COTTRILL, Caitlin (2011), "Location Privacy: Who Protects?" *Urisa Journal*, pp. 49-59.

ESTÊVÃO, Tiago (2014), *A Vigilância nas Sociedades Contemporâneas – O Estudo de Caso do INDECT*, Tese de Mestrado em Comunicação, Cultura e Tecnologias da Informação, Lisboa, ISCTE-IUL.

- (2014a), "O Novo Paradigma da Vigilância na Sociedade Contemporânea – Who Watches the Watchers", *Observatório (OBS*)*, Vol.8, nº 2, [online]. Disponível em: http://obs.obercom.pt/index.php/obs/article/view/787.

FOUCAULT, Michel (1977), *Discipline and Punish, The Birth of the Prison*, Middlesex, England, Penguin Books, Ltd.

FROIS, Catarina (2011), *Vigilância e Poder*, Lisboa, Editora Mundos Sociais.

FUCHS, Christian (2011), *New Media, Web 2.0 and Surveillance*, Sociology Compass 5/2.

FUCHS, Christian; BOERSMA, Kees; ALBRECHTSLUND, Anders; SANDOVAL, Marisol (2011), *Internet and Surveillance: The Challenges of Web 2.0 and Social Media*, New York and London Routledge.

GIDDENS, Anthony (1985), *The Nation-State and Violence*, Cambridge, England, Polity Press.

GREENWALD, Gleen (2014), *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*, New York, USA, Metropolitan Books.

HARDING, Luke (2014), *The Snowden Files – The Inside Story of the World's Most Wanted Man*, New York, Vintage Books.

KOSKELA, Hille (2004), "Webcams, TV Shows and Mobile Phones: Empowering Exhibitionism", *Surve*illance & Society 2 (2/3), pp. 199-215.

LYON, David (1998), *The Surveillance Society – Monitoring Everyday Life*, Buckingham, England, Open University Press.

- (2003), "Surveillance Technology and Surveillance Society", *in* Thomas J. Misa; Phlip Brey and Andrew Feenberg (eds), *Modernity and Technology*,161-184, Cambridge: MIT Press.

LYON, David (2007), *Surveillance Studies – An Overview*, Cambridge, England, Polity Press.

MANN, Steve (2005), "Sousveillance and Cyberglogs, A 30-Year Empirical Voyage Through Ethical, Legal and Policy Issues", *Presence: Teleoperators and Virtual Environments* 14(6), pp. 625–646.

PAPACHARISSI, Zizi; GIBSON, Paige (2011), "Fifteen Minutes of Privacy: Privacy, Sociality, and Publicity on Social Network Sites", *Privacy Online: Theoretical Approaches and Research Perspectives on the Role of Privacy in the Social Web*.

SCHNEIDER, Christopher; TROTTIER, Daniel (2012), "The 2011 Vancouver Riot and the Role of Facebook in Crowd-Sourced Policing", *BC Studies*, nº 175, pp. 57-72.

TROTTIER, Daniel (2012), "Policing Social Media", *Canadian Sociological Association*, pp. 411-425.

- (2012a), "An Inventory and Evaluation of CCTV Internet Crowd-Sourcing", *Centre for Science, Society & Citizenship*.

- (2012b), "Interpersonal Surveillance on Social Media", *Canadian Journal of Communication*, Vol. 37 (2012), pp. 319-332.

TUROW, Joseph (2005), "Audience Construction and Culture Production: Marketing Surveillance in the Digital Age", *The ANNALS of the American Academy of Political and Social Science*, 597 (1), pp. 103-121.

- (2006), *Cracking the Consumer Code: Advertising, Anxiety and Surveillance", in* Kevin Hagerty and Richard V. Ericson (eds.), *The Digital Age. In the New Politics of Surveillance and Visibility*, pp. 279-307, Toronto: University of Toronto Press.

Rita Espanha (autora de correspondência). Professora Auxiliar no ISCTE-Instituto Universitário de Lisboa (ISCTE-IUL) (Lisboa, Portugal). Diretora do Mestrado em Comunicação Cultura e Tecnologias de Informação. Investigadora do Centro de Investigação e Estudos de Sociologia (CIES-IUL) (Lisboa, Portugal). Editora da revista internacional Observatório (OBS*). Endereço de correspondência: Centro de Investigação e Estudos de Sociologia (CIES-IUL) (ISCTE-IUL), Avenida das Forças Armadas 1649-026, Lisboa, Portugal. E-mail: rita.espanha@iscte.pt

Tiago Estêvão. Doutorando em Ciências da Comunicação, no Centro de Investigação e Estudos de Sociologia (CIES-IUL) (Lisboa, Portugal). Endereço de correspondência: Centro de Investigação e Estudos de Sociologia (CIES-IUL), Avenida das Forças Armadas 1649-026, Lisboa, Portugal. E-mail: tiagovaz.estevao@gmail.com

Artigo recebido em 25 de outubro de 2015. Publicação aprovada em 23 de setembro de 2016.