

Primavera Árabe: vigilância e controle na sociedade da informação

Branco Di Fátima*

As novas tecnologias de informação e comunicação (TICs) engendraram possibilidades infinitas de organização, mobilização, disseminação e partilha de dados nos movimentos sociais organizados ou de livre manifestação cidadã na sociedade da informação. A Internet inaugurou um novo cenário para debates ao dar visibilidade a dilemas políticos, culturais, ecológicos, étnicos e econômicos de caráter local, regionalizados ou de nicho, além de possibilitar que os mesmos possam ser acompanhados, em tempo real, por uma parcela significativa da população mundial com acesso a informações mediadas por computadores.

Manifestações de insatisfação social que marcaram o ano de 2011 como *Occupy Wall Street*, nos Estados Unidos, *Indignados*, na Espanha, os protestos de estudantes no Chile, o motim de jovens na Inglaterra e o Movimento 15 de Outubro – organizado pelas redes sociais e que suscitou mobilizações em mais de mil cidades de 85 países na referida data – apresentam características típicas dos movimentos sociais contemporâ-

neos. A utilização de redes de diálogos e troca de informações contínuas cria sinergia para que essas manifestações não sejam atos isolados, mas trabalhos conjuntos que encontram apoio mútuo pela utilização da Internet.

Mesmo levando em conta a variedade de setores que precisaríamos citar para classificar as reivindicações dos movimentos sociais do século XXI, que vão facilmente de temáticas ambientais à luta pelos direitos humanos, da busca de condições dignas de vida na zona rural à proteção dos animais, o que vivenciamos na sua maioria é uma insatisfação com o modelo de democracia representativa vigente.

Os altos índices de desemprego, o empobrecimento da classe trabalhadora, as engrenagens do capitalismo, o aparelho consumista criado pelo mercado de lucros e o modelo financeiro neoliberal são motivos propagados para justificar os protestos e os atos de desobediência civil no Ocidente. Ricos cada vez mais ricos e pobres cada vez mais pobres, se refere o slogan *We Are 99 Percent*, do *Occupy Movement*, em referência a alta concentração de renda de 1% da população mais rica do planeta e o empobrecimento dos outros 99%.

*Mestrando em Comunicação, Cultura e Tecnologias da Informação pelo Instituto Universitário de Lisboa (ISCTE-IUL). Pós-graduado em Produção e Crítica Cultural pelo Instituto de Educação Continuada (IEC). Graduado em jornalismo pela Pontifícia Universidade Católica de Minas Gerais (PUC/MG).

Além das similaridades já listadas, a utilização da Internet em diferentes níveis e escalas de comprometimento como mecanismo de propagação de vídeos, fotografias, textos, manifestos, cartilhas, mobilização, compartilhamento de dados, organização de passeatas é um elemento presente em todas essas ebulições sociais. Segundo Fuchs (2011), na sociedade contemporânea “a acessibilidade não é apenas o acesso a um espaço físico, mas também o acesso aos espaços informativos”. Se por um lado as manifestações sustentam a utopia de profundas transformações nas estruturas vigentes, por outro são marcadas pela utilização intensa das TICs como ferramenta para aglutinar, mobilizar, criar fluxos de ideias, diálogos, debate político e informar os insatisfeitos sobre a agenda dos próximos atos.

O êxito da ação desta diversidade de movimentos sociais com que nos deparamos hoje, depende, obrigatoriamente, da capacidade de confluência e de articulação da sua ação, que poderá ser desenvolvida numa teia de relações diversas, bilaterais, multilaterais, conforme as condições concretas. Dessa articulação, emanará a capacidade de reconstruir e adquirir novos poderes. O caminho é, por um lado, o trabalho no terreno e, por outro, a transposição da mensagem para os *media*, no sentido de se atingirem consensos sociais sem os quais não há mobilização. (Silva, 2003, p. 41)

Os movimentos sociais contemporâneos transcendem a organização sindical, a lide-

ranças centralizadas, a personalização ideológica, os partidos políticos, setores da Igreja, a núcleos físicos de debates como no século XVIII na Europa e nas décadas de 1960, 70 e 80 na América Latina. No final do ano de 2010 e em 2011, no Norte da África e Oriente Médio, milhões de pessoas ganharam as ruas, de maneira espontânea e sem o auxílio de máquinas partidárias, para protestar contra regimes ditatoriais que governavam ou ainda governam países nas duas regiões. O objetivo das mobilizações, de forma claramente especificada, era derrubar governos que ignoram os mais elementares preceitos de participação cívica, democracia, respeito aos direitos humanos, liberdade de expressão, política e de imprensa e construir melhores condições de vida para a população.

A Primavera Árabe – assim como ficaram conhecidas no Ocidente as manifestações – suscita debates sobre o papel desempenhado pelas TICs e pela Internet para o êxito alcançado em alguns dos países. Especificamente, as atenções são voltadas com mais frequência para os casos da Tunísia, com a queda do general Ben Ali (14 de janeiro de 2011); do Egito, com o fim do governo de Hosni Mubarak (11 de fevereiro 2011) e da Líbia, com o linchamento público do ditador Muammar Kadafi (20 de outubro de 2011).

Frases difundidas em cartazes e grafites nos muros das cidades de Alexandria, Túnis, Trípoli e Cairo expressavam o agradecimento da população às plataformas de interação social na Internet como o Facebook, o YouTube e o Twitter. Escritas em árabe, inglês e francês, as sentenças narrativas, que ganharam destaque nas páginas dos principais jornais do mundo e chamaram a atenção dos canais de televisão e emissoras de rá-

dio, diziam: “merci Facebook”, “thank you, Twitter” etc. Entrevistas concedidas por líderes políticos, religiosos e ativistas das regiões após a queda dos ditadores sempre suscitaram a importância das redes sociais para o fim dos anos de opressão.

Analistas internacionais chegaram a dizer, precipitadamente, que a Primavera Árabe era uma revolução das redes sociais, ou, ainda, nas redes sociais, dado a importância das plataformas para os acontecimentos decorridos. O que se observou nos dias subsequentes ao fim dos governos ditatoriais foi uma supervalorização do papel da Internet no desenrolar dos fatos propriamente ditos. Como se as manifestações não pudessem existir sem o auxílio do Facebook ou que só foram realizadas por causa do Twitter. Obviamente, nenhuma das considerações se revelaria correta se não levarmos em conta o contexto econômico, social e político em que tais disputas de poder foram travadas. O próprio criador do Facebook, Mark Zuckerberg, diminuiu a importância da rede social para os levantes populares. “Seria extremamente arrogante para qualquer empresa de tecnologia reivindicar papel significativo” nas revoltas, disse ele durante encontro entre representantes de empresas de tecnologia e os líderes dos países do G8 em Paris.

Neste artigo trabalhamos com a ideia de que a Primavera Árabe foi e ainda é uma revolução de povos insatisfeitos com modelos de governo instaurados e que se utilizaram das redes sociais como ferramentas de organização e mobilização de protestos que culminaram na ocupação pacífica, na maioria dos casos, de ruas, praças, bairros e espaços públicos das maiores cidades e pequenas vilas do Norte da África e Oriente Médio.

Na medida do possível, procuramos não colocar sob o mesmo foco analítico os diferentes países envolvidos pela aura da Primavera Árabe sem antes dar-lhes atenção individualizada. O que pode parecer uma realidade similar aos olhos ocidentalizados, na verdade, revela ser emaranhados de contextos particulares e distintos entre si. O que deu certo em um determinado país, simplesmente, pode ser sinônimo de fracasso em outro, devido aos fatores geográficos, tribais, éticos, religiosos, sociais, políticos, educacionais, econômicos etc. Como alertou o próprio ditador Muammar Kadafi, pouco antes da sua derrocada: “A Líbia não é a Tunísia e nem o Egito. Será uma guerra civil. Haverá banho de sangue nas ruas”.

Não deixamos de levar em conta o importante papel que a Internet teve nas manifestações como ferramenta poderosíssima de ativismo online e que transcendeu os limites das telas dos computadores para as ruas. Procuramos, sobretudo, é ver a sua utilização dentro de um contexto histórico mais complexo e alargado. Compreender o papel das tecnologias de comunicação e informação nos levantes do Norte da África e Oriente Médio é, sobretudo, compreender as mesmas como parte fundamental de uma engrenagem de insatisfação popular que eclodiu em forma de protestos pacíficos nas ruas e não como o motor propulsor da Primavera Árabe, assim como ressalta Allagui e Kuebler (2011).

Negligenciando a complexidade dessas transformações, a mídia convencional atribuiu a derrubada de Ben Ali e Mubarak às mídias sociais (...) enquanto profundos problemas de corrupção na maio-

ria dos estados árabes foram deixados de lado. Tunisianos e egípcios decidiram colocar fim aos anos de corrupção e humilhação. Tendo usado o Facebook, telefones celulares, YouTube ou apenas o boca a boca para isso. (Allagui e Kuebler, 2011, p. 1, tradução minha)

Todavia, quais seriam os limites de segurança e de proteção da privacidade na Internet para a utilização das novas tecnologias de comunicação pelos movimentos sociais contemporâneos? A mesma população que encontrou nas plataformas de interação na web e nas mensagens de telefones móveis (SMS) mecanismos de organização, mobilização e fluxo de informações para os protestos da Primavera Árabe também foi surpreendida com violentos contra-ataques dos governos totalitários pelo mesmo canal. A rede foi amplamente utilizada como mecanismo de controle e vigilância de cidadãos. Denúncias feitas por organizações internacionais revelaram a existência de processos de vigilância sistemática, de massa e personalizada aos opositores políticos dos regimes no Norte da África e Oriente Médio. Com a ajuda de softwares e equipamentos desenvolvidos por empresas multinacionais e transnacionais do Ocidente, ativistas da Primavera Árabe tiveram suas ações rastreadas e terminaram presos e assassinados.

Não muito distante das análises realizadas por Fuchs (2011) sobre o controle de informações privadas pelas redes sociais e que seriam vendidas a empresas para a criação de propagandas dirigidas, direcionadas e para aumentar a disseminação das ideologias capitalistas, mas não tão longe ao ponto de pensar que os mecanismos de vigilân-

cia poderiam estar desassociados do aparato econômico. O debate também recai, sobretudo, em uma nova lógica de controle no ciberespaço, concatenadas com as teorias de vigiar para punir de Foucault (1975). “A vigilância torna-se operador econômico decisivo, na medida em que é ao mesmo tempo peça interna no aparelho de produção e engrenagem específica no poder disciplinar”.

O olhar recai sobre os mecanismos de controle utilizados pelos governos árabes para tentar deter as ondas de protestos civis no ciberespaço e que ganharam as ruas. Analisamos neste artigo a Primavera Árabe tendo como recorte o papel que a própria Internet desempenhou como instrumento de vigilância, controle e como promotora do fim do anonimato digital na sociedade da informação. Se por um lado a rede foi aclamada como redentora para povos sufocados pelo peso da opressão, por outro ela se transformou em um sofisticado mecanismo de coerção social a serviço das ditaduras árabes. Segundo Fuchs (2011), conteúdos criados pelos próprios usuários e disponibilizados nas redes sociais podem ser utilizados como isca para futuras identificações de desertores.

A web 2.0 pode ser usada como uma forma de vigilância, exerce poder e dominação, fazendo uso de qualidades específicas da Internet atuais, tais como o conteúdo gerado pelos próprios usuário ou os permanentes fluxos de comunicação dinâmicos. (Fuchs, 2011, p. 134, tradução minha)

Informações divulgadas pela organização inglesa *The Bureau of Investigative Journalism*, em reportagem do jornalista Pratap

Chatterjee, no dia 23 de outubro de 2011, revelam que softwares e equipamentos desenvolvidos pela companhia *Blue Coat Systems Inc.*, do Vale do Silício, na Califórnia (EUA), foram usados para monitorar o tráfego de dados da Internet na Síria. O artigo relata que “a mesma tecnologia pode ser usada para monitorar usuários e bloquear o acesso ao Facebook e ao Skype”, plataformas que se mostraram essenciais na organização e mobilização de protestos na Primavera Árabe.

Programas de computador e equipamentos desenvolvidos pela *Blue Coat Systems Inc.*, como o *Packet Shaper*, prometem “controlar o tráfego de conteúdo na web”, o “impacto de redes sociais como o Facebook” e “bloquear categorias inteiras de conteúdo” na Internet. Já o software *ProxySG 9000* pode “fornecer controle completo sobre todo o tráfego na web, autenticação e localização de usuários, filtragem, inspeção e gerenciamento de banda”. Todas as informações citadas neste parágrafo foram colhidas do site¹ da própria companhia, que descreve minuciosamente seus produtos.

No decorrer das denúncias contra a *Blue Coat*, o porta-voz da empresa, Steve Schick, afirmou para o *The Bureau of Investigative Journalism* não haver “evidências de que as tecnologias desenvolvidas pela sua companhia foram usadas na Síria”. A concordância com as acusações contrariaria as leis de exportação dos Estados Unidos, que desde 2004 prevê embargo ao país. No entanto, no dia 29 de outubro de 2011, o vice-presidente da empresa, Steve Daheb, voltou atrás e admitiu ao *The Wall Street Journal* que “pelo

¹Site da Blue Coat Systems Inc. www.bluecoat.com.

menos 13 de seus dispositivos vem sendo utilizados pelo governo sírio para reprimir e silenciar atividades online”.

De acordo com Steve Daheb, foram vendidos 14 *ProxySG 9000* para o Ministério das Comunicações do Irã, no final de 2010, por cerca de 700 mil dólares. Os equipamentos fizeram a rota a partir de uma filial da *Blue Coat* na Holanda para os Emirados Árabes Unidos. Neste percurso, pelo menos 13 equipamentos podem ter sido desviados para uso do governo de al-Assad, que de acordo com a Organização das Nações Unidas (ONU) já deixou um rastro de mais de nove mil mortos nos últimos meses na Síria. O *ProxySG 9000* promete “controle flexível sobre o conteúdo na web, de usuários e aplicações”.

O grupo de ciberativistas e hackers suecos, *Telecomix*², ajudou a confirmar e quantificar as suspeitas de vigilância na web pelo governo de Bashar al-Assad. A organização teve acesso aos dados do sistema de segurança da Internet da Síria. Segundo as informações divulgadas pelo *The Bureau of Investigative Journalism*, pelo menos 6% do tráfego de rede em um universo de 750 milhões de acessos foram filtrados e 26.700 tentativas de acesso a sites ligados a opositores do regime foram bloqueados ou monitorados no período de 22 de julho e 6 de agosto de 2011.

Outra variante contabilizada pelo *Telecomix* mostra que das 2.500 tentativas de conexão à página do Facebook dedicada à revolução na Síria³, pelo menos 1.575 foram bloqueadas e as outras 925 monitoradas. In-

²Site do grupo Telecomix. www.telecomix.org.

³Página do Facebook da revolução da Síria. www.facebook.com/syrian.revolution.

formações de usuários teriam sido rastreadas e armazenadas para consultas futuras pelos órgãos de repressão do ditador Bashar al-Assad. As mesmas denúncias de vigilância de cidadãos com auxílio das novas tecnologias de comunicação podem ser encontradas em análise feita por Barreto (2011) sobre as revoltas populares no Irã, país que supostamente teria comprado os 14 *ProxySG 9000* fabricados pela *Blue Coat Systems Inc.* O autor ressalta, no entanto, que utilizar os meios de comunicação como ferramenta de dominação e para manutenção de poder não é uma novidade inventada com a Internet.

Se num primeiro olhar se vê o sucesso do uso da Internet nas revoltas, por outro, sabe-se também que a onda verde que invadiu o Twitter e o Facebook durante a luta do povo iraniano contra o governo autoritário se virou contra eles, a partir do momento em que a revolta falhou e estas mesmas mídias servem hoje como banco de dados para a busca e apreensão de pessoas por esse regime. Mas isto também não é uma novidade histórica e nem a primeira vez que regimes autoritários se apoderam dos meios de comunicação para manter seu poder. (Barreto, 2011, p. 164)

O que fica evidenciado com as denúncias feitas pela *The Bureau of Investigative Journalism* e pelo *Telecomix* é a nítida associação entre empresas privadas – desenvolvedoras de tecnologias de vigilância com objetivos claros de produção da mais-valia – e governos ditatoriais em crise de legitimidade

frente a povos sufocados pela repressão. O caso Síria, analisado até aqui, revela um contexto em que empresas privadas vendem equipamentos de rastreamento e controle da Internet para ditaduras que não medem esforços para prolongar-se no poder, mesmo que para tanto tenham que criar rígidos “sistemas disciplinares” para silenciar milhares de vozes dissidentes com tortura e extermínio. Ou seja, “vigiar para punir” e, ainda, que “na essência de todos os sistemas disciplinares funciona um pequeno mecanismo penal” (Foucault, 1975).

O fim do anonimato digital na sociedade da informação segue, para Fuchs (2011), uma lógica capitalista que protege os interesses de conglomerados empresariais e o sigilo dos favorecidos nas grandes transações financeiras. Os *offshores* nos paraísos fiscais como as Ilhas Virgens Britânicas, a Suíça, o Panamá e as Ilhas Cayman escondem – com o auxílio das leis das referidas localidades e falhas no sistema legislativo – a identidade de políticos corruptos, empresários ligados ao narcotráfico, donos de empresas que recebem investimentos provenientes da lavagem de dinheiro e evasão de divisas. A lógica do anonimato na sociedade da informação protege a propriedade privada ao mesmo tempo em que viola os direitos de expressão, participação, de livre associação pacífica, de greve etc.

A privacidade no capitalismo pode ser caracterizada como um valor que é antagônico e, de um lado, manteve como um valor universal para proteger a propriedade privada, mas é ao mesmo tempo, permanentemente prejudicada pela vigilância das empresas na vida

dos seres humanos para fins de lucro e pela vigilância política administrativa para fins de defesa e aplicação da lei. (Fuchs, 2011, p. 144, tradução minha)

Os movimentos sociais contemporâneos, que tendem a utilizar o potencial das redes sociais como ferramenta de mobilização e organização, estão sujeitados a enfrentar violentas repressões por parte de estados autoritários com a ajuda dos mesmos canais na Internet. Aprender a driblar a recolha de informações ligadas à coerção e centralização de poder é um dos próximos dilemas impostos para a sobrevivência dos movimentos de hoje. A organização das manifestações no Egito, com o auxílio de ferramentas no ciberespaço e que levaram à queda do ditador Hosni Mubarak, no dia 11 de fevereiro de 2011, podem ensinar os primeiros passos contra a vigilância sistemática sobre as massas e a identificação de indivíduo na multidão.

De acordo com informações da *The Bureau of Investigative Journalism*, publicadas em reportagem do jornalista Pratap Chatterjee, os ativistas pró-democracia teriam encontrado em março de 2010, nos arquivos dos órgãos de inteligência de Mubarak, documentos que comprovam que os cidadãos egípcios estavam sendo vigiados antes e durante os levantes da Primavera Árabe. Foram recolhidos pelos manifestantes cópias de contratos, no valor de 287 mil libras, da compra do software *FinFisher*, fabricado pela empresa britânica *Gamma Group International*.

Os documentos apresentados por ativistas e citados neste artigo não tiveram a força necessária para identificar as verdadeiras re-

lações entre a *Gamma Group International* e a ditadura de Hosni Mubarak. Apesar das referências gráficas da empresa nos documentos, do destinatário indicado ser o *State Security Investigation Department*, no Cairo, e outras características típicas de documentos oficiais em inglês e árabe, falou-se até da falsificação dos papéis. Verdade ou não, a dúvida paira sobre a grande imprensa que trouxe a história para a superfície dos debates.

A *Gamma Group International* descreve o *FinFisher* em seu site⁴ como uma ferramenta que dará às “agências governamentais capacidade de infectar remotamente sistemas alvos” (minha tradução). Ou seja, a tecnologia é capaz de fazer o “controle remoto e soluções de infecção para aceder aos sistemas alvo, proporcionando acesso total às informações armazenadas, com a possibilidade de assumir o controle das funções a ponto de capturar comunicações e dados criptografados.” O *FinFisher* é descrito como uma ferramenta de espionagem do ciberespaço e que pode ajudar a localizar pessoas que utilizam telefones móveis e a Internet a partir da instalação de um vírus no aparelho do vigiado por meio de uma mensagem. Para Foucault (1975), os “meios de coerção fazem aqueles a quem eles são aplicados visíveis”.

O êxito dos manifestantes egípcios pode se atribuído, entre outros fatores, justamente à capacidade de encontrar mecanismos para driblar a vigilância promovida pelo governo de Hosni Mubarak. A ditadura chegou ao extremo de “desligar” a Internet no país por cinco dias (26-01 a 02-02-2011) com o

⁴Site da empresa britânica *Gamma Group International* www.gammagroup.com.

auxílio da *Vodafone Group*, uma das maiores companhias de telecomunicações que atuam no Egito. As informações que comprovam a associação entre empresas privadas e os governos árabes foram confirmadas pelo próprio executivo-chefe da *Vodafone Group*, Vittorio Colao, em Davos, na Suíça. Ele disse ter recebido ordens para que o serviço fosse “cortado” assim como a disponibilidade de enviar mensagens de texto (SMS) e de voz. “Não está a funcionar, será restabelecido (o serviço) quando formos autorizados”, disse. A empresa de telefonia também é acusada de omissão e apoio nos casos em que seus serviços foram utilizados para enviar mensagens pró-Mubarak ao povo do Egito.

Para burlar o corte de cinco dias imposto à Internet, os egípcios começaram a se conectar à rede via Europa, Estados Unidos e com a ajuda de grupos de *hackers* espalhados pelo globo, como o *Telecomix*. No dia 31 de janeiro, o motor de buscas Google lançou um serviço que convertia recados de voz em mensagens para o Twitter. A alternativa foi rapidamente adotada pelos manifestantes. Ainda no início das manifestações, a estratégia para confundir os órgãos de vigilância da Internet e a polícia era divulgar, no Facebook, um lugar qualquer onde os protestos populares aconteceriam e, depois, divulgar o lugar certo de boca em boca nos bairros, cafés e cortiços do Cairo e de Alexandria.

Em reportagem do *The New York Times*, o jornalista e correspondente no Egito, David D. Kirkpatrick, revela algumas das estratégias e o perfil adotado pelas pessoas por trás das manifestações on-line. “Eles introduziram profissionalismo – plantando falsos rumores, encenando, antes de desenhar seus

planos de batalha. Em seguida, traçaram a estratégia (...)”.

As linhas de argumentação apresentadas neste artigo ajudam a pensar a Internet, simultaneamente, como uma ferramenta de caráter dual para os movimentos sociais contemporâneos. De um lado a rede pode se transformar em um poderosíssimo instrumento de organização e mobilização de massas, compartilhamento de dados e difusão acelerada de informações ao redor do globo a favor da democracia. Do outro, um mecanismo sofisticado de vigilância, controle, rastreamento e punição de cidadãos a serviço de governos interessados em se prolongar no poder e capaz de ir até os últimos limites da violação para alcançar seus objetivos.

O fim do anonimato digital na sociedade da informação pode estar intimamente relacionado com a necessidade de invenção de um novo conceito para panóptico no século XXI. A capacidade de vigiar os cidadãos no ciberespaço, seja a partir de redes sociais para a criação de propagandas direcionadas ou com a ajuda de software como o *FinFisher*, *Packet Shaper* e *ProxySG 9000* para aperfeiçoar mecanismos de repressão do Estado, é uma realidade latente. Assim como salienta Foucault (1975, p.166), “quem está submetido a um campo de visibilidade, e sabe disso, retoma por sua conta as limitações do poder”.

Proteger a identidade de líderes, ativistas e grupos políticos comprometidos com transformações sociais profundas é indispensável frente ao risco eminente de represálias por parte de estruturas totalitárias. Por outro viés, essas identidades e estratégias de trabalho podem e são reveladas com a ajuda de aparatos desenvolvidos por empresas privadas e cooptados por governos ditatoriais,

como nos casos de Síria e Egito, analisados brevemente neste artigo. O que fica é a nítida associação do capitalismo corporativo e as máquinas de repressão do Estado.

Encontramos na Primavera Árabe o levante de povos sufocados por décadas, mas também a associação entre empresas privadas – interessadas na construção de mais-valia – e governos ditatoriais interessados em quebrar o sigilo dos seus cidadãos. Se a privacidade interessa às multinacionais para a obtenção de lucro muitas vezes por caminhos ilícitos, ela também é fundamental para garantir a integridade física e psicológica de membros dos movimentos sociais. Mediar esse conflito dual não é tarefa fácil. Fuchs (2011, p. 143) aponta um caminho para essa reflexão. “A questão não é, portanto, como a privacidade pode ser mais bem protegida, mas os casos em que a privacidade deve ser protegida e os casos que ela não deve ser”.

Referências Bibliográficas

- Allagui, Ilhem e Kuebler, Johanne (2011), *The Arab Spring and the Role of ICTs*, in *International Journal of Communication*. Disponível em: <http://ijoc.org/ojs/index.php/ijoc/article/viewFile/1392/616>. Acessado em 16-12-2011.
- Barreto, Fernando (2011), *Mídias Sociais e Mobilização social*, in *Para entender as mídias sociais*. Brasil, pp. 162-165. Disponível em: blog.colunaextra.com.br/2011/05/leitura-obrigatoria-para-entender-as.html. Acessado em 18-12-2011.
- Chatterjee, Pratap (2011), *US technology used to censor the Internet in Syria claim experts*, in *The Bureau of Investigative Journalism*. Disponível em: <http://migre.me/75GUk>. Acessado em 10-12-2011.
- Chatterjee, Pratap (2011), *Mundo Big Brother*, in *portal Pública*. Disponível em <http://apublica.org/2011/12/mundo-big-brother/>. Acessado em 10-12-2011.
- Devries, Jennifer, Malas, Nour e Sonne, Paul (2011), *U.S. Firm Acknowledges Syria Uses Its Gear to Block Web*, in *The Wall Street Journal*. Disponível em: <http://online.wsj.com/article/SB10001424052970203687504577001911398596328.html?mod=e2tw>. Acessado em 15-12-2011.
- Foucault, Michel (1975), *Vigiar e Punir*. Rio de Janeiro: Vozes, p. 262.
- Fuchs, Christian (2011), *An alternative view of privacy on Facebook*, in *Information 2*. Disponível em: www.mdpi.com/2078-2489/2/1/140/pdf, pp. 140-165. Acessado em 15-11-2011.
- Fuchs, Christian (2011), *New Media, Web 2.0 and Surveillance*, in *Sociology Compass 5/2*. Disponível em: <http://fuchs.uti.at/wp-content/uploads/Web20Surveillance.pdf>, pp. 134-147. Acessado em 11-12-2011.
- Horwitz, Sari (2011), *Syria using American software to censor Internet, experts say*, in *Washington Post*. Disponível em:

<http://migre.me/75GXP>. Acesso em 10-12-2011.

Kirkpatrick, David D. (09-02-2011), *Wired and Shrewd, Young Egyptians Guide Revolt*, in *The New York Times*. www.nytimes.com/2011/02/10/world/middleeast/10youth.html?ref=daviddkirkpatrick. Acesso em:18-12-2011.

Leyden, John (2011), *UK firm denies supplying spyware to Mubarak's secret police*, in *The Register*. Disponível em www.theregister.co.uk/2011/09/21/egypt_cyber_spy_controversy. Acesso em 11-12-2011.

Lyon, David (2004), *Globalizing Surveillance – Comparative and Sociological Perspectives*. Disponível em: http://club.fom.ru/books/Lyon04_2.pdf. Acesso em 10-12-2011.

Silva, Manuel Carvalho da (2003), *Os trabalhadores e os movimentos sociais de hoje*, in *Novas formas de mobilização popular*. Lisboa, Portugal: Campo das Letras, pp. 39-44.