



O (des)controlo da Internet: *bad bots*, *astroturfing* e *flogging*

F. Rui CÁDIMA¹

Resumo

A Internet atravessa atualmente uma fase complexa e difícil de definir dadas as características algo movediças e instáveis da sua evolução. Pode, por exemplo, identificar-se uma luta de contrários, entre uma tendência que procura preservar a essência “aberta” da rede, a sua plena transparência e acessibilidade e uma outra tendência que defende uma rede fortemente encriptada, que salvguarde em primeiro lugar o anonimato do utilizador. Provavelmente nenhuma delas se afirmará de forma exclusiva, pelo que as “disfunções” aqui verificadas neste texto – os bad bots, o astroturfing e o flogging – serão estratégias com as quais teremos doravante de conviver, cada vez mais, enquanto utilizadores da rede.

Palavras-chave:

Internet; *astroturfing*; *flogging*; regulação.

205

The (un)controlled Internet: bad bots, astroturfing and flogging

Abstract

The Internet is currently undergoing a complex and difficult phase given the volatile and unstable characteristics in its development. It is possible, for instance, to identify a struggle between the trend that seeks to preserve the "open" nature of the Internet, its full transparency and accessibility, and another trend that advocates a strongly encrypted network, safeguarding primarily the user's anonymity. Probably none of them will win on an exclusive basis, reason why the "dysfunctions" reported in this text - the bad bots, the astroturfing and flogging - will be strategies with which we increasingly have to live from now on as users of the network.

Keywords:

Internet; *astroturfing*; *flogging*; regulation

¹Professor Catedrático do Departamento de Ciências da Comunicação da Faculdade de Ciências Sociais e Humanas. Universidade Nova de Lisboa.



El (des)control de Internet: bad bots, astroturfing y flogging

Resumen

Internet se encuentra actualmente en una fase compleja y difícil dadas las características cambiantes e inestables de su evolución. Se puede, por ejemplo, identificar una lucha entre una tendencia que busca preservar la naturaleza "abierta" de la red, su plena transparencia y su accesibilidad contra una otra tendencia que aboga por una red fuertemente cifrada, que garantiza en primer lugar el anonimato del usuario. Probablemente ninguna de ellas se consolidará en exclusiva, por lo que las "disfunciones" que se observan en este texto - los *robots malos*, el *astroturfing* y el *flogging* - serán estrategias con las que tenemos de aquí en fuera que convivir, cada vez más, como usuarios de la red.

Palabras clave:

Internet; *astroturfing*; *flogging*; regulación.

“O **astroturfing** e as suas vozes **astroturfs** criam no espaço público disfunções suscetíveis de interferir no exercício da comunicação democrática e da democracia.”

Sophie Boulay

Introdução

Em termos de *media* e, conseqüentemente, em termos de opinião pública em geral, parece não haver grande preocupação com os *bad bots* e as suas maquinações automáticas e anónimas na Internet. Muitos cibernautas desconhecem mesmo esta realidade e as suas mais profundas implicações. E isto apesar do tráfego gerado por *robots* ser idêntico a todo o restante tráfego da Internet gerado por humanos.

De acordo com o 2015 Bot Traffic Report, da Incapsula (ZEFMAN, 2015), pela primeira vez, justamente nesse ano, o tráfego web dos utilizadores foi superior ao dos *robots*: 51,5 por cento de todo o tráfego *online* foi efetivamente de humanos, face aos 48,5 por cento de *robots*, sendo que neste caso há que distinguir entre os *bad bots* (29 por cento) e os *good bots* (19,5 por cento). Digamos que os *bad bots* são os intrusos maliciosos que começam no *spam* e no *scrawler* e deixam um rastro de *sites hackeados*, de *phishing*, de negação de serviço (DDoS), etc. Repare-se que cerca de 90 por cento de todos os eventos de segurança na rede são resultado da atividade de *bad bots*. Este é, portanto, um problema de grande impacto e melindre, com algumas conseqüências dramáticas nomeadamente no plano da liberdade de expressão e deve, por conseguinte, suscitar a máxima atenção da cidadania.

Ao contrário destes, os *good bots* são as “abelhas operárias” da Internet que contribuem decisivamente para o seu controlo e para o seu crescimento. São criados e

geridos por empresas legítimas e conhecidas no mercado, que usam *bots* para facilitar a gestão de tarefas automatizadas, recolha e rastreamento de dados, *tracking* aberto e não malicioso.

Astroturfing

Entre uns e outros há um território híbrido, onde as dinâmicas de automatismos na rede, naturalmente também baseadas em *bots*, se cruzam com estratégias de criação de perfis e contas falsas em diferentes plataformas digitais, com objetivos maliciosos, de propaganda, etc. E esta é uma outra área a levantar preocupação na rede e já com um histórico significativo ao longo dos últimos anos, sobretudo em matéria de *astroturfing*.

Veja-se, por exemplo, este caso: “Concorrente da Uber acusada de fazer 400 mil pedidos de transporte falsos” (COSTA, 2016). De acordo com a notícia, a Ola, concorrente direta da Uber no mercado indiano, era acusada de ter criado, com números de telefone falsos, 90 mil contas através das quais fizeram à Uber cerca de 400 mil pedidos falsos de transporte. Os pedidos de transporte teriam sido cancelados em cima da hora, mas a Uber alegava prejuízos avultados e pretendia uma indemnização em 6,6 milhões de euros. Afinal, nada que a própria Uber não tenha feito no passado, neste caso, em relação à Lyft, sua concorrente direta em São Francisco...

Este exemplo, aqui circunscrito ao mercado de transportes urbanos, pode ser encontrado, com implicações bem mais complexas, em áreas tão sensíveis como a política e o fenómeno eleitoral, no retalho em geral, na grande distribuição, na participação cívica em países com problemas de direitos humanos, etc. Na mesma altura em que surgia o problema com a Uber na Índia, no Cambodja havia notícia de *astroturfing* na política local (PURTILL, 2016). Hun Sen, um dos mais antigos líderes do mundo no poder, é agora o protagonista, sendo que o Cambodja está identificado como sendo um país com claros problemas de direitos humanos. A questão foi assinalada pelo jornal Phnom Penh Post, reportando um aumento suspeito nos fãs internacionais de Hun Sen, cujo número quase duplicou em fevereiro de 2016. De acordo com dados do *site* de análise Socialbakers.com, o volume de novos fãs do primeiro-ministro vinha, estranhamente, da Índia e das Filipinas. Sam Rainsy, opositor de Hun Sen, no exílio, referiu tratar-se claramente de uma situação de criação de falsos perfis no Facebook para artificialmente aumentar o número de seguidores e de *likes*. Ao que Hun Sen responderia: “I am just happy that I, Hun Sen, have been recognized by



Indian people and people in other countries as the Prime Minister of Cambodia”...

É óbvio que as grandes plataformas digitais são o intermediário por excelência para estas estratégias agressivas, eticamente condenáveis e/ou ilegais, consoante os diferentes países tenham ou não legislação adequada na área do *marketing* e da publicidade. Mas, por vezes, são as próprias plataformas que assumem o risco... Em 2016 o Facebook (DOCTOROW, 2016) envolveu-se numa campanha de *astroturfing* que teria atingido os 1,4 milhões de comentários contra o projeto de Net Neutrality do TRAI (regulador telco indiano), num contexto completamente desadequado ao solicitado pelo operador da Índia. Tratando-se de um documento então em consulta pública, que pretendia obter pareceres abalizados nomeadamente de *stakeholders* e de especialistas, o Facebook acabou dessa forma por se ver envolvido numa campanha eticamente condenável e desajustada ao contexto, também politicamente incorreta, contra a Net Neutrality na Índia (quando se dizia a favor dela nos EUA), tendo sido acusado inclusive de “web based colonialism” (LAFRANCE, 2016) na sua forma de gerir um processo que lhe era desfavorável. E isto porque a ser aprovada a resolução – como o foi –, o seu projeto Free Basics seria penalizado. Desde logo porque estava a cobrar de forma diferenciada por dados em função do conteúdo ou da aplicação acedidos pelo utilizador, sendo que o acesso ao Facebook era, naturalmente, grátis. Ora, este é precisamente o objetivo fundamental de qualquer política de *net neutrality*, isto é, pugnar por uma Internet aberta e não pela diferenciação de preços consoante os serviços acedidos pelos utilizadores.

A verdade é que essas estratégias de ocultação da identidade com fins eticamente condenáveis ou mesmo com enquadramento criminal têm surgido regularmente, inclusive na área do jornalismo e na academia, sendo certo que muito provavelmente os casos conhecidos são apenas alguns dos poucos que chegam efetivamente a ser conhecidos publicamente, como reportava a associação canadiana de defesa do consumidor no seu estudo sobre o tema intitulado *Bloggers or Floggers? Undercover advertising exposed* (2012, p. 15):

Em abril de 2006, o Los Angeles Times retirou do seu blogue o vencedor do Prêmio Pulitzer, Michael A. Hiltzik, porque ele estava discutindo com os leitores sob um nome falso. A mesma situação ocorreu com o escritor Lee Siegel da revista New Republic, que blogou sob o nome “sprezzatura”, e com John Lott, que entre 2000 e 2003 blogou sob o nome “Mary Rosh”. O historiador Orlando Figes





também foi apanhado em atividade semelhante.² (BLOGGERS..., 2012, p. 15, tradução nossa).

Astroturfing é então uma estratégia desenvolvida agora, sobretudo, *online*, por indivíduos ou grupos de pressão organizados, em regra utilizando falsas identidades e/ou falsos endereços de IP, com o objetivo, por exemplo, de manipular informação, atacar ou humilhar um concorrente, ou de criar a impressão de grande apoio para uma política, um indivíduo ou um produto, uma marca, etc., onde esse apoio obviamente não existe.

A discussão sobre o *astroturfing* na área política teve um momento alto, há poucos anos, devido às notícias que surgiram nos *media* em torno das estratégias de manipulação da opinião pública na Rússia de Putin. Adam Bienkov (2012), na altura, reportava o assunto no Guardian:

Afirmar de que um grupo pró-Kremlin financiou uma vasta rede de ativistas on-line para criar a ilusão de um apoio generalizado a Vladimir Putin pode parecer um conto bizarro relative a um Estado autoritário. No entanto, o uso dos chamados grupos “astroturf” é generalizado em todas as nações e estilos de vida, da China à Grã-Bretanha, das resenhas de livros às pesquisas on-line, e dos grandes negócios à política local (BIENKOV, 2012, tradução nossa).

No caso da Rússia, a questão prendia-se, portanto, com a contestação às eleições de 2011, tema abordado também por Evgeny Morozov (2012) na imprensa mundial. Este russo, exilado nos EUA, denunciou o facto desta prática anónima ter sido dominada por *bots* que geriam dezenas de milhares de contas falsas no Twitter com o objetivo de confundir e manipular o debate público em torno da transparência eleitoral e da falta de democraticidade do regime. Sabia-se, na altura, que uma alegada organização pró-Kremlin, a Nashi, muito bem financiada, dirigia uma complexa estratégia propagandística *online* em defesa do regime. Outras organizações presentes na *net* desenvolviam também acções propagandísticas no mesmo sentido, como é o caso do grupo I Really Do Like Putin. O The Guardian (ELDER, 2012) referia então que dados obtidos por *hackers* russos do grupo Anonymous revelavam que teriam sido gastas centenas de milhares de libras pelo Nashi em redes que envolviam *bloggers*, jornalistas afetos ao regime e outras estratégias de contra-informação *online*, como o

² O caso de Orlando Figes, considerado pelo Guardian um dos historiadores britânicos de referência, adquire uma dimensão especial. Veja-se a este propósito o artigo de Richard Lea e Matthew Taylor, “Historian Orlando Figes admits posting Amazon reviews that trashed rivals”, *The Guardian* online, Friday 23 April 2010. <http://www.theguardian.com/books/2010/apr/23/historian-orlando-figes-amazon-reviews-rivals>. Acedido em 28 de março de 2016.



ataque massivo às caixas de comentários das notícias publicadas pela imprensa não afeta ao regime, ou a presença nos fóruns *online*, nos *chats*, manipulação de *ratings* e *viewcounts* no You Tube, DDoS – ataques de negação de serviço a *websites* da oposição, etc., de forma a ajudar a criar uma imagem lisonjeira de Putin, combater a oposição e denegrir os rivais políticos.

Flogging

O *flogging* diferencia-se do *astroturfing*, dado que se enquadra sobretudo no âmbito da blogosfera ou na utilização abusiva de *websites* do género, com formas menos claras ou subliminares de promoção ou publicidade, onde seria suposto haver autenticidade e transparência. Noutros casos, trata-se de blogues criados especificamente por empresas, com objetivos comerciais, sem que haja uma identificação da sua origem. Uma coisa é certa e segura: o utilizador não deve à partida, não pode aceitar como bom todo e qualquer conteúdo que lhe surja *online*. Esta é a regra número um... A regra número dois é não esquecer que a maior parte dos casos de *flogging* identificados nos estudos sobre a matéria é criada por empresas de relações públicas e agências de publicidade, claro que a pedido de grandes corporações.

No conhecido manual de *marketing* de Michael R. Solomon (2009), publicado em 2009, há uma referência ao *flogging*. Solomon reconhece que os blogues despertavam a atenção de múltiplas grandes companhias e empresas, no sentido de otimizarem estratégias de marketing por meio de técnicas como o “word of mouth”, sendo que havia já algumas situações reportadas com utilização eticamente condenável da blogosfera. Solomon dá o exemplo da Microsoft, que, em 2007, começou por promover os seus novos *laptops* com *software* Vista, ainda antes do lançamento público, junto de alguns *bloggers* da área de tecnologia, o que teria então sido visto como uma prática menos própria. Contudo, na sua perspectiva, “o mais famigerado delito de *blogging*” (SOLOMON, 2009, p. 405) teria sido alegadamente cometido pela Wal-Mart in 2006, quando contratou uma empresa de *marketing* e relações públicas para criar e gerir blogues favoráveis à companhia, reforçando a notoriedade da marca.

O *flogging* era então visto como uma prática associada à crescente popularidade dos *bloggers*, que, por isso mesmo, eram procurados por empresas, sobretudo as mais diretamente relacionadas com as temáticas dos blogues em questão, havendo assim lugar a remuneração pelas referências e/ou promoção de produtos e/ou marcas que iam



surgindo nesses mesmos blogues. Mas se neste caso se poderia dizer que estávamos perante uma prática de publicidade discutível, embora eventualmente legítima, noutras situações, sobretudo quando o que está em causa é a criação de falsos blogues, tal já não será assim, nem tão pouco aceitável. Os blogues falsos (por vezes surgem também como *flogs* ou *flogging*) procuram, em regra, por detrás da ocultação de fonte ou identidade, corporativa ou pessoal, criar conteúdo que pode consistir em comentários ou auto-promoção e legitimar-se como meio aparentemente independente para assim poder credibilizar o seu enunciado, seja ele dirigido à notoriedade de uma marca, à promoção de um produto ou à defesa de um político... E tem por norma, como objetivo, tornar-se viral, ou pelo menos ambiciona sê-lo, mas desde logo procura gerar partilhas, comentários, *likes*, etc., em torno desse mesmo tópico.

Não há dúvida, de qualquer modo, de que essas estratégias colidem diretamente com normas profissionais estabelecidas, nomeadamente com o código de ética da Public Relations Society of America, por exemplo, ou as orientações do Chartered Institute of Public Relations (UK), que não reconhece o *flogging* ou o *astroturfing* como práticas aceitáveis na sua área profissional. O já citado estudo realizado no Canadá pela associação de defesa dos consumidores Option Consommateurs – *Bloggers or Floggers? Undercover advertising exposed* (2012, p. iii) chegava à mesma conclusão:

Um certo número de práticas de negócios questionáveis são frequentes nos *social media*. Entre estas estão o *flogging* (criação de blogs falsos) ou o *astroturfing* (usando um pseudônimo e uma identidade falsa para interagir com os consumidores). Cada vez mais, as empresas estão recorrendo a essas práticas como ferramentas de marketing e publicidade. Passam por cidadãos particulares, e ao fazê-lo, enganam os consumidores. Esta é a principal razão por que tais práticas são condenadas por especialistas em marketing e relações públicas (BLOGGERS, 2012, p. iii, tradução nossa).

Basicamente, o estudo aponta nas suas principais conclusões para o facto de os fenómenos de *flogging* e de *astroturfing* estarem bastante generalizados, sendo utilizados mesmo pelas grandes empresas; não ser conhecida nenhuma ferramenta para detetar essas práticas, pelo que a única forma de identificar situações do género era por meio de investigação aprofundada. No caso dos EUA e do Reino Unido, havia já regulamentação dessas práticas na altura do lançamento do estudo, sendo que no Canadá apenas havia uma única lei aplicável, no caso, a respeito da publicidade falsa ou enganosa. Também não havia jurisprudência no Canadá relacionada com *flogging* ou *astroturfing*, nem a possibilidade de processo formal de queixa nessa matéria, ou





mesmo que a instituição pudesse acolher tais reclamações. A questão é que estamos ainda a ver apenas a ponta do iceberg... Toda a atenção não será pois demais para conhecer, monitorizar e regulamentar esse fenómeno.

Até porque o *flogging* pode, inclusive, emergir por vias bastante ínvias e em áreas demasiado sensíveis, como é o caso da saúde e do *marketing* farmacêutico, ou mesmo da saúde mental, da doença em estado terminal, por exemplo. No primeiro caso, que é um pouco ambivalente – sendo difícil perceber, por exemplo, se a narrativa é real, publicitária ou ficcional, ou se os registos de utilizadores são reais ou não –, existe, nomeadamente, o estudo de Manon Niquette (2010) que incide sobre o tema do *marketing* nas redes sociais, na área da saúde, aplicado ao problema do défice de atenção com ou sem hiperatividade, em particular sobre o carácter publicitário das mensagens criadas por uma empresa farmacêutica para comunidades *online*.

Nas conclusões do estudo, que incidiu apenas sobre páginas no Facebook, que a autora refere como sendo uma *TDAH Maman*, com mais de 9 mil membros à altura do estudo, e uma outra página de um grupo de interesse não comercial, designada como “*TDAH*” (refira-se que a autora não analisa em função da sua autenticidade, mas em função apenas do texto enunciado, aplicando a análise linguística do discurso), são identificados procedimentos que caracterizam a especificidade, mas também o enviesamento dessas páginas de *marketing* farmacêutico em relação ao produto e aos protagonistas envolvidos. Isto é, refere-se, por exemplo, que há claramente uma sobrevalorização do papel das mães envolvidas, dando também uma imagem do comportamento da criança que é à partida bem acolhida pelas mães, e estruturando finalmente o conteúdo da informação a favor da toma do medicamento, relevando ainda de forma favorável a opinião de professores e de médicos prescritores para reforçar a mensagem aquisitiva.

Num outro plano, que já se enquadra na esfera da saúde mental, encontramos casos onde a referência é, por exemplo, a síndrome de Münchhausen. Esta síndrome é, no fundo, um transtorno do foro psiquiátrico, uma desordem comportamental em que o paciente, geralmente em contexto hospitalar, simula, de forma deliberada e compulsiva, ter sintomas graves, dores, doenças, fundamentalmente para atrair a simpatia das equipas médicas e de enfermagem, obter cuidados, sentir-se o centro das atenções, e de alguma forma exercitar as capacidades predatórias do grande manipulador que, em princípio, será.





O caso mais conhecido de síndrome de Münchhausen na Internet foi o da *blogger* australiana Belle Gibson (MONTAGUE, 2015), que começou por fingir estar a viver ela própria um caso trágico de cancro. A história simulada de Gibson teve uma amplitude tremenda, ao ponto de ter enganado centenas de milhares de pessoas. Muitos dos seus seguidores no Instagram (cerca de 200 mil) compraram inclusive a *app* que ela criou propositadamente para o efeito (awarded Best App of 2013) e vários outros ainda seguiam-na no seu *website*. A própria Apple e grandes editores foram também enganados nesse processo:

Gibson lançou a aplicação The Whole Pantry em 2013, cheia de dicas de vida saudável e receitas. Ela prometeu um terço das receitas dos 300.000 download (\$ 3,79 por download) para a caridade. A revista Elle referiu-se a Gibson como “A mulher mais inspiradora que você conheceu neste ano”, a Cosmopolitan concedeu-lhe o prêmio *Fun, Fearless Female* e a Penguin publicou seu livro de receitas. A Apple pré-instalou o seu aplicativo no Apple Watch e levou-a ao seu lançamento em Silicon Valley (MONTAGUE, 2015, tradução nossa).

Tanto a *app* The Whole Pantry como o livro publicado pela Penguin foram verdadeiros *best-sellers*. Belle Gibson confessaria mais tarde, na edição de maio de 2015 da revista The Australian Women's Weekly que tudo não passou de uma ficção... Desde que, em maio de 2013, Gibson iniciou esta grande mistificação nas redes sociais, decorreram dois anos até que finalmente se percebeu toda a enganadora montagem *online* por uma jovem que aparentemente mal sabia o que era um cancro... Mas, sem quaisquer acusações criminais para Gibson, quase diríamos, tal como Montague, no The Guardian: “A aula de mestre de Belle Gibson terminou, mas outras se lhe seguirão”... O facto é que, à data, não estava completamente terminada: entrando na Google Play Store, ainda era possível, um ano depois da denúncia do caso pela própria, adquirir a *app* The Whole Pantry, para Android³, pela quantia de 2,05 Euros.

Conclusão

As práticas de *flogging* e de *astrourfing* estão hoje de tal modo disseminadas na Internet que se torna claramente difícil a sua regulação e monitorização ou mesmo somente a sua simples identificação. Trata-se de uma espécie de *dark web* da parte visível do iceberg, que pretende sobretudo criar efeitos perversos e impactos imediatos

³ https://play.google.com/store/apps/details?id=com.thewholepantry&hl=pt_BR. Acedido em 26 de março de 2016. No caso da Apple já não era possível obter a mesma *app*: “The Whole Pantry vanishes from App Store, Apple Watch app showcase”. Roger Fingas, appleinsider, March 18, 2015. <http://appleinsider.com/articles/15/03/18/the-whole-pantry-vanishes-from-app-store-apple-watch-app-showcase>. Acedido em 26 de Março de 2016.





na opinião pública, ambiciona a viralidade nas diferentes plataformas web em que se apresenta, entra nos motores de busca, inunda-nos as caixas de comentários, e, no entanto, é fundamentalmente automática, anónima e manipuladora. Daí a sua importância e a atenção que nos deve merecer. Quer nos países de contencioso com os direitos humanos, quer mesmo na Europa e nos Estados Unidos, onde, pelo que vimos, colocam-se também situações extremamente complexas e dramáticas, algumas delas com impactos profundos na saúde pública, no consumo e no bem-estar geral dos cidadãos. Mas outras, igualmente preocupantes, colocam-se também no campo da economia e da política, e no plano dos direitos cívicos e da liberdade de imprensa e de expressão.

Sharyl Attkisson, jornalista de investigação norte-americana, defendeu que, com o grande desenvolvimento das redes sociais e da Internet, há uma nova indústria de Relações Públicas no centro da política norte-americana, sendo que “métodos sub-reptícios de *astroturfing* são agora mais importantes para os grupos de interesses do que o *lobbying* tradicional do Congresso” (ATTKISSON, 2016). Que fazer, então, face a esta nova realidade, face às múltiplas centrais anónimas de contra-informação, *marketing* e propaganda, tecnologicamente avançadas, que atuam na rede e procuram censurar, manipular e converter o sistema de *media* e a opinião pública à sua própria agenda? Que fazer, face a uma estratégia de comunicação prejudicial, eticamente condenável, e com impactos claros, por exemplo, na *agenda-building* e na *agenda-setting* (BOULAY, 2012), enfim, nas diferentes agendas do espaço público, no consumidor, na opinião pública e no ciberespaço?

A nossa maior preocupação vai exatamente para o sistema de *media*, o velho quarto poder, muito acossado neste início de século pela revolução digital e pelas crises financeira e económica, a que se somam agora grupos de interesses poderosos que constroem a sua mensagem com base na opacidade, suportados em *big data* e na nova “física da cultura”, a qual está, finalmente, a substituir os velhos *gatekeepers* do jornalismo por fontes disseminadas e disfarçadas na rede e por automatismos *online*. O que significa que os alertas estão hoje a soar mais alto que nunca, mas poucos serão os que lhes estão a dar a atenção devida.

Referências

ATTKISSON, Sharyl Attkisson. Top 10 astroturfers. sharylattkisson.com, 22 mar. 2016. Disponível em: <<https://sharylattkisson.com/top-10-astroturfers/>>. Acesso em: 28



mar. 2016.

BIENKOV, Adam. Astroturfing: what is it and why does it matter? **The Guardian**, 8 fev. 2012. Disponível em: <<http://www.theguardian.com/commentisfree/2012/feb/08/what-is-astroturfing>>. Acesso em: 24 mar. 2016.

BLOGGERS or floggers? Undercover advertising exposed. Research Report. **Option Consommateurs**. Disponível em: <http://www.option-consommateurs.org/documents/principal/en/File/oc_ic01_blogueurs_ou_annonceurs_rapport_eng_2012.pdf>. Acesso em: 18 jun. 2014.

BOULAY, Sophie. Usurpation de l'identité citoyenne dans l'espace public: Astroturfing et communication politique. Thèse de doctorat en communication (policopié). Université du Québec à Montréal, fév. 2012.

COSTA, Alexandre. Concorrente da Uber acusada de fazer 400 mil pedidos de transporte falsos. **Expresso online**, 24 mar. 2016. Disponível em: <<http://expresso.sapo.pt/internacional/2016-03-24-Concorrente-da-Uber-acusada-de-fazer-400-mil-pedidos-de-transporte-falsos>>. Acesso em: 24 mar. 2016.

DOCTOROW, Cory. India's telcoms regulator says it will ignore Facebook's astroturf army. **Boingboing.net**, 2 jan. 2016. Disponível em: <<http://boingboing.net/2016/01/02/indias-telcoms-regulator-say.html>>. Acesso em: 28 mar. 2016.

ELDER, Miriam. Hacked emails allege Russian youth group Nashi paying bloggers. **The Guardian online**, 7 fev. 2012. Disponível em: <<http://www.theguardian.com/world/2012/feb/07/hacked-emails-nashi-putin-bloggers>>. Acesso em: 28 mar. 2016.

FINGAS, Roger. The Whole Pantry vanishes from App Store, Apple Watch app showcase. **appleinsider**, 18 mar. 2015. Disponível em: <<http://appleinsider.com/articles/15/03/18/the-whole-pantry-vanishes-from-app-store-apple-watch-app-showcase>>. Acesso em: 26 mar. 2016.

LAFRANCE, Adrienne. Facebook and the New Colonialism. **The Atlantic online**, 11 fev. 2016. Disponível em: <<http://www.theatlantic.com/technology/archive/2016/02/facebook-and-the-new-colonialism/462393/>>. Acesso em: 26 mar. 2016.

LEA, Richard; TAYLOR, Matthew. Historian Orlando Figes admits posting Amazon reviews that trashed rivals. **The Guardian online**, 23 abr. 2010. Disponível em: <<http://www.theguardian.com/books/2010/apr/23/historian-orlando-figes-amazon-reviews-rivals>>. Acesso em: 28 mar. 2016.

MONTAGUE, Jules. Münchhausen by internet: the sickness bloggers who fake it online. **The Guardian online**, 29 abr. 2015. Disponível em: <<http://www.theguardian.com/society/2015/apr/29/jules-gibson-munchausen-by-internet-sickness-bloggers-fake-it-whole-pantry>>. Acesso em: 26 mar. 2016.

MOROZOV, Evgeny. Na vida digital, cada vez mais intermediários. **Folha de S. Paulo**, 29 out. 2012. Disponível em: <<http://www1.folha.uol.com.br/colunas/evgenymorozov/1175587-na-vida-digital-cada-vez-mais-intermediarios.shtml>>. Acesso em: 4 jan. 2013.

NIQUETTE, Manon. Marketing pharmaceutique et médias sociaux: Analyse critique du discours d'une page FacebookMD sur le TDA/H. **Revue Internationale sur le Médicament**, vol. 3, 2010, p. 53-116. Disponível em: <<http://www.aiicm-iiapc.com/files/sites/18/2015/06/RIM3-2-Niquette51-116.pdf>>. Acesso em: 26 de mar. 2016.

PURTILL, Corine. Cambodia's prime minister is accused of buying Facebook likes to boost engagement numbers. **Quartz**, 24 mar. 2016. Disponível em: <<http://qz.com/647285/cambodias-prime-minister-is-accused-of-buying-facebook-likes-to-boost-engagement-numbers/>>. Acesso em: 25 mar. 2016.

SOLOMON, Michael R. et altri. **Marketing**: real people, real decisions. Londres: Financial Times/ Prentice Hall, 2009.

ZEFMAN, Igal. 2015 Bot Traffic Report: Humans Take Back the Web, Bad Bots Not Giving Any Ground. **Imperva Incapsula**, 9 dez. 2015. Disponível em: <<https://www.incapsula.com/blog/bot-traffic-report-2015.html>>. Acesso em: 25 mar. 2016.