Breves reflexões sobre Poder e Ciberespaço[1]

Brief Thoughts on Power and Cyberspace

LINO SANTOS[2]
ARMANDO MARQUES GUEDES[3]

Resumo: Num Estado de Direito, a luta política entre os vários grupos, que defendem ou atacam interesses de classe, económicos, profissionais, geracionais, de género, ou outros, embora regulada, é uma constante. Governos, empresas e cidadãos, individulamente ou em grupo, lutam pelos seus objectivos estabelecendo relações de poder. Os media sempre tiveram um papel instrumental neste contexto e o novo media do séc. XXI – o ciberespaço – não é excepção. As características estruturais e funcionais deste instrumento criaram novas condições para a mobilização e participação políticas, reavivando a crença na acção libertadora da técnica. Por outro lado, nenhuma outra tecnologia promoveu tanta concentração de poder nas grandes empresas da indústria digital, ou criou semelhantes condições para a vigilância activa dos cidadãos por parte dos Estados. Este artigo reune algumas reflexões sobre a importância do ciberespaço como dimensão de poder.

Palavras chave: *Ciberespaço, Media, Ciberutopia, Poder*

Abstract: The political struggle among groups defending or attacking class, economic, professional, generational, gender or any other interests, although regulated, is a constant. Governments, businesses and citizens, individually or as a group, fight for their porpuses by establishing relations of power between them, the media had always played an instrumental role with this regard and the new media of the 21st century – the cyberspace – is no exception. The structural and

---

[1] Entregue: 2.3.2015; aprovado: 30.5.2015.

[2] Doutorando em Direito e Segurança da Faculdade de Direito da Universidade Nova de Lisboa.

[3] Professor Associado com Agregação da Faculdade de Direito da Universidade Nova de Lisboa.

functional features of this new media fosters the conditions for the mobilisation and political action, bringing to life the strong belief on the liberating role of the technique. On the other hand, no other technology has promoted so much concentration of power in large companies, namely the digital industry, or created similar conditions for State surveillance of their citizens. This article gives us some reflections on the meaning of cyberspace as a dimension of power.

Key words: *Cyberspace, Media, Cyberutopia, Power*

Introdução

Em Junho de 2012 a internet contava com cerca de dois mil e quatrocentos milhões de utilizadores em todo o mundo,[4] dos quais 90% eram seus utilizadores, numa base diária, para comunicação nas redes sociais.[5] Usada inicialmente como meio seguro, rápido e económico de transmissão de informação, em poucos anos esta rede passou a suportar um mercado de serviços e aplicações de todo o tipo, tornando-se ainda num importante meio, tanto para a comunicação de massas, como para a comunicação interpessoal.

É neste contexto que ganha força o termo ciberespaço, um daqueles conceitos de que se dispõe sem grande procupação de exactidão e relativamente ao qual poucos dos que o usam saberia definir o sentido, senão de forma vaga. Na realidade, mesmo entre os especialistas, não existe um consenso em relação à sua abrangência. Tal como noutros termos afins como sejam cibernauta, ciberguerra ou ciberarma, o prefixo "ciber-" apela ao imaginário do virtual e transporta o receptor para o contexto das tecnologias da informação e da comunicação (TIC). Diferentes sectores da sociedade usam o termo ciberespaço para se referirem a coisas tão distintas como a rede planetária de computadores, a posibilidade de realizar actividades através da Internet, ou o

[4] Ver *Internet World Stats*, disponível em http://www.internetworldstats.com/stats.htm, consultado em Maio de 2014.

[5] Ver *Global Internet User Survey – 2012 Key Findings*, disponível em https://www.internetsociety.org/sites/default/files/GUIS-2012-Infographic.pdf, consultado em Maio de 2014.

armazenamento de informação na *cloud*, pelo que, numa perspectiva abrangente, podemos definir ciberespaço como o conjunto "[d]as diferentes vivências do espaço associado às tecnologias e à computação" (Strate, 1999, p. 383).

Não obstante a sua existência virtual, este meio configura um espaço de visibilidade e presença, onde indivíduos, grupos e Estados interagem, comunicam, simbolizam, lutam e exercem o poder. Se entendermos por poder, acompanhando o conceito das "três faces" de Lukes (1974), como a capacidade de vergar a vontade do outro pela argumentação, a capacidade de definir a agenda, ou seja, pré-definir o que é ou não discutido, e a capacidade de induzir vontades através das ideias e crenças, podemos questionar em que medida, e em que sentido, é que o ciberespaço permite reconfigurar as relações de poder entre os indivíduos, entre os indivíduos e o Estado, e mesmo entre Estados. Qual a sua capacidade para alterar os sempre precários equilibrios existentes?

Genericamente falando, o ciberespaço é um novo meio – ou um conjunto de novos meios – que configura um novo contexto nas relações institucionais, grupais ou individuais, com o potencial e a capacidade para alterar os equilibrios existentes. No âmbito das relações internacionais, e tendo em conta as suas características estruturais e funcionais, o ciberespaço representa uma oportunidade para alguns Estados reduzirem assimetrias relativamente a outros, para favorecer o surgimento de novos actores não Estatais ou, ainda, para reforçar o poder de actores não Estatais existentes, junto dos primeiros. Se, para actores Estatais, este espaço virtual representa um complexo campo de acção, onde confluem relações económicas, securitárias e de direitos humanos, onde a topologia transnacional dificulta o seu controlo e a acção, para os restantes significa um espaço de liberdade e a esperança na "difusão" das relações de poder estabelecidas.

O ciberespaço tem-se revelado uma espécie de "canivete suíço" da acção colectiva. As suas ferramentas, ainda que tragam novos temas para a agenda política, são principalmente catalizadoras da mobilização para a acção politica e amplificadoras do discurso politico – uma espécie de megafone planetário (Martins & Garcia, 2013). Por outro lado também os estados tiram proveito destas ferramentas. As fragili-

dades existentes nas TIC[6] e o baixo custo associado à sua exploração – pelo menos quando comparado com o investimento envolvido nos sectores tradicionais de armamento – permite a pequenos Estados, e mesmo a actores não Estatais, aspirar a reduzir assimetrias com as principais potências mundiais e a ver melhoradas as suas relações de poder na cena internacional. Paradoxalmente, os países mais industrializados e militarmente mais capazes são também os mais dependentes das TIC e, por conseguinte, os mais expostos a consequências de ciberataques. Esta dicotomia tem promovido uma corrida ao ciberarmamento de grande escala e o estabelecimento de relações difusas entre Estados e o cibercrime organizado – este bem mais experiente neste território.[7]

Como refere Joseph Nye, "o ciberespaço não irá substituir o espaço físico geográfico e não acabará com a soberania dos Estados, mas a difusão de poder no ciberespaço coexistirá e complicará, em grande medida, o que significa exercício de poder nestes domínios" (2010, p. 3).

Este artigo aborda a intercepção entre os conceitos de poder e de ciberespaço e, dentro desta, analisa a importância e o impacto das redes como dimensão de poder no século XXI. Numa primeira parte abordaremos o mito do ciberespaço como utopia libertadora e a importância das redes como instrumento de mobilização para a acção colectiva; numa segunda parte exploraremos o fim da privacidade e a concentração de poder nas grandes empresas de tecnologia digital; finalmente, numa terceira parte, será abordada a luta pelo controlo

---

[6] Todos os dias são descobertas e tornadas públicas dezenas de vulnerabilidades que, quando exploradas, permitem ao atacante afectar a disponibilidade, confidencialidade e integridade do(s) sistema(s) atacado(s). Um estudo bem conhecido da IBM estima que exista pelo menos um erro por cada mil linhas de código num programa de computador. Para ter uma ideia de dimensão do problema, um sistema operativo como o Windows tem mais de 50 milhões de linhas de código. Muitos erros ainda por descobrir.

[7] Alexander Klimburg defende que as fronteiras entre diferentes tipos de ciberconflitualidade, tais como o cibercrime organizado, o ciberterrorismo ou a ciberguerra são muito estreitas: "para a prespectiva de um ciber guerreiro, o cibercrime pode fornecer as bases técnicas (as ferramentas de software e o suporte logístico), o ciberterrorismo a base social (as redes de indivíduos e a motivação) com as quais executar ataques a redes de computadores de grupos ou nações inimigas" (2001, p.41).

do ciberespaço. O artigo termina com um conjunto de tópicos para futura exploração.

Ciberutopismo

Numa das suas últimas campanhas publicitárias, a empresa de telecomunicações portuguesa Optimus (agora fundida com outra empresa do mesmo ramo, a Zon, na NOS) apresentou uma série de anúncios tendo como pano de fundo uma curiosa aldeia, aparentemente remota e rústica, onde se juntavam as tribos urbanas mais díspares para cantar o famoso refrão dos Beatles, "All together now". A ironia da mensagem repousa na referência implícita ao conceito de "aldeia global" de Marshall McLuhan, que na década de 1960 profetizou a reunificação da humanidade numa comunidade à escala global graças ao advento da electrónica, constituindo a aldeia do anúncio uma metáfora para o mundo contemporâneo, a nova aldeia, unificado graças às tecnologias da informação e da comunicação. Pode dizer-se então que o anúncio retrata, numa versão da cultura popular, a visão do conhecido teórico canadiano, segundo a qual estariamos na presença de nada menos que um novo Pentecostes, no qual as novas tecnologias, em especial o computador e a electricidade, substituiriam eficazmente o Espírito Santo – "o computador, em suma, promete, através da tecnologia, o advento duma condição pentecostal de compreensão e união universais" (McLuhan, 2008, p. 94).

Este entendimento da Internet como meio de reunificação universal não é surpreendente quando visto em perspectiva. Tendo em conta a história do Ocidente, pode mesmo dizer-se que ao surgimento e disseminação de cada novo *media* corresponde uma onda de esperança nas potencialidades do mesmo para transcender as barreiras comunicacionais entre os povos. De algum modo, cada *media* reaviva o sonho de reunião da *oikumene*, que habita de forma latente o imaginário da civilização judaico-cristã. Armand Mattelart (2000) na sua *História da Utopia Planetária* elenca exemplos históricos em que esta esperança, ao mesmo tempo ecuménica e libertadora, se baseou no desenvolvimento de novas tecnologias de *media*, desde a imprensa escrita ao telégrafo,

da navegação aérea à rádiofonia e ao cinema. Cada um destes *media* gerou ondas de entusiasmo, sendo entendidos nas suas épocas como veículos de transmissão de ideias e liberdades públicas, e até como instrumentos da paz universal.

Os computadores e a Internet não foram excepção, e a crença na sua acção libertadora pode ser observada em vários grupos com várias formas. Provavelmente os primeiros a incorporar estes valores foram os *hackers*.[8] Num manifesto atribuído a *The Mentor* pode ler-se: "(...) E então aconteceu... uma porta abriu-se para o mundo... correndo depressa pela linha telefonica como heroína pelas veias de um viciado, um pulso electrónico é enviado, um refúgio para a incompetência do dia-a-dia, encontramos um quadro."[9] Marginalizado na vida real, o aluno narrador deste manifesto encontra uma válvula de escape e uma sensação de liberdade nesse mundo digital, bem como uma satisfação individual de conseguir aceder ao proibido e ultrapassar as barreiras de protecção edificadas pelas entidades mais poderosas do mundo e com isso motivar a admiração dos pares. A subcultura *hacker* permite explicar como uma acção virtual pode ser considerada gratificante, na medida em que os *hackers* experimentam sensações de controlo e poder nem sempre encontrados no mundo real e difíceis de compreender, como tal, por indivíduos externos a esta subcultura.

Na década de 1980 o jornalista Steven Levy elencou um conjunto de valores que veio a ser designado como ética *hacker*, onde se incluem o acesso livre e gratuito a tudo aquilo que pode ensinar algo sobre a forma como o mundo funciona; a desconfiança na autoridade e a crença na descentralização; a não discriminação e a igualdade de oportunidades; e a crença de que os computadores podem criar arte e beleza, bem com alterar a vida para melhor (Levy, 1984). Se as duas últimas afirmações revelam um predomínio da crença nas possibili-

---

[8] A origem do termo *hacker* tem origem ainda na década de 1950 com o advento dos primeiros computadores. O jargão técnico *hack* dizia respeito, nessa altura, a uma solução não óbvia e de certa forma elegante para um problema complexo e num contexto de escassos recursos computacionais (Taylor et al., 2006).

[9] Excerto traduzido do texto *The conscience of a hacker*, também conhecido por *Manifesto hacker*, escrito por *the mentor* em Janeiro de 1986, disponível em http://www.phrack.org/archives/7/P07-03, consultado em Fevereiro de 2014.

dades emancipatórias da tecnologia no seio da comunidade *hacker*, as restantes são respostas muito pragmáticas a problemas colocados pelo contexto em que se desenvolveram as ciências da computação, nomeadamente a escassez de meios computacionais e a consequente racionalização no acesso a estes, bem como a necessidade de partilhar os programas de computador (entendidos, não o esqueçamos, como criações artísticas) entre *hackers*. De salientar, igualmente, a ideia de desconfiança em relação à autoridade e ao poder instituído que, no contexto, se referia à burocracia exigida para o tão desejado acesso aos recursos de computação, mas que evoluiu no sentido de uma forte simpatia pelos ideais anarquistas (Denning, 1996).

Esta ideia de que o acesso aos recursos computacionais de hardware e de software deve ser livre, tal como o acesso a todo o tipo de conteúdos digitais, está na génese do movimento que defende o software livre[10] – que criou produtos de sucesso como o sistema operativo *Linux*, o cliente web *Firefox* ou as ferramentas de escritório *Open Office* – tendo sido incorporada também pelos grupos apologistas da *commons-based peer production*,[11] cuja maior realização terá sido a *Wikipedia*. Numa versão institucionalizada, a mesma ideia está na base dos vários partidos "Pirata" criados na Europa do norte ou em influentes movimentos, tais como o *Electronic Frontier Foundation,*[12] que pretende defender os direitos dos consumidores digitais, e a *Internet Society,*[13] que preconiza o desenvolvimento da "sociedade da informação". Todos estes grupos mimetizam a estrutura e a "ordem espontânea" que o ciberespaço lhes confere e em todos grassa a crença segundo a qual "o povo, armado de uma poderosa tecnologia, triunfaria sobre os mais brutais inimigos" (Morozov, 2012, p. 7).

---

[10] Ver *Free Software Foundation* em http://www.fsf.org/, consultado em Maio de 2014. Um estudo revela que 79% dos membros da comunidade de software livre (free software) e 33% dos membros da comunidade software livre comungam dos valores preconizados pelos *hackers* (Escher, 2004).

[11] Benkler e Nissenbaum referem-se à *commons-based peer production* como "um esforço colectivo de indivíduos que contribuem para um objectivo comum de forma mais ou menos informal e pouco estruturada" (Benkler & Nissenbaum, 2006, p.395).

[12] Ver https://www.eff.org/about, consultado em Maio de 2014.

[13] Ver http://www.internetsociety.org/who-we-are/mission, consultado em Maio de 2014.

Participação e acção colectiva

Utopias aparte, é inegável que o ciberespaço tem uma presença assídua no dia-a-dia de uma grande parte da sociedade e configura um meio comunicacional privilegiado. Não será assim exagerado afirmar que, tal como quando surgiram os jornais, a rádio e a televisão, também o aparecimento deste novo *media* veio alargar a chamada arena pública, idealizada por Hannah Arendt como o espaço onde os vários actores competem pelo protagonismo e pelo controlo. De facto as características estruturais e funcionais do ciberespaço, das quais destacamos aqui a arquitectura fim-a-fim – por oposição ao modelo de *broadcast* da imprensa tradicional, da rádio e da televisão –, ou a pressuposta anonimidade na utilização – ilustrada na célebre frase "on the internet nobody knows you're a dog" –, facilitam as várias dimensões da acção política colectiva.

Se atentarmos ao modelo preconizado por Charles Tilly, a arquitectura do ciberespaço afecta, de forma significativa, os cinco vectores que caracterizam a mobilização para a acção colectiva.[14] Por um lado, cataliza a associação em torno de interesses comuns. As *tags* em blogues, as *hashtags* no *twitter* e os metadados furtivamente colocados nas páginas *web* são parte integrante da funcionalidade destas ferramentas, e têm por objectivo precisamente orientar (ou mesmo afunilar, num processo de radicalização) o utilizador para os conteúdos da sua preferência, formando comunidades virtuais em torno de interesses comuns. Por outro, permite a participação anónima ou com recurso a múltiplas identidades digitais em redes de interesses tão diversas

[14] Tilly defende que a mobilização para a acção colectiva pode ser caracterizada através de cinco características comuns: (1) o *interesse* – como unidade de medida entre as vantagens e as desvantagens partilhadas por um grupo em relação às interacções com outro grupo; (2) A *organização* – como estrutura unificadora dos indivíduos e identidade de um grupo que prossege um mesmo interesse; (3) a *mobilização* – que se refere ao conjunto dos recursos disponíveis e sob o controlo de um grupo ou do comando de um grupo; (4) a *oportunidade* – que representa a relação entre o interesse e o *staus quo* das relações de poder entre um grupo e outros grupos ou instituções; e, finalmente, a *acção colectiva*, propriamente dita – como acção conjunto de um grupo na prossecução dos seus interesses (1978, p. 75).

como a paixão por um *hobby* particular, uma qualquer causa politica ou outra actividade mais obscura ou mesmo ilícita.

Estas comunidades, que reúnem simpatizantes espalhados pelos quatro cantos do planeta, operam em estruturas mais ou menos complexa e de forma mais ou menos organizada – por oposição às tradicionais estruturas hierárquicas (Denning, 2001). A estrutura destas redes pode variar desde a simples configuração em estrela, muito centrada na figura do fazedor de opinião, que espelha perfeitamente o palco onde "pessoas comuns se mostram como pseudo-celebridades" (Boyd, 2008, p. 113), até complexos grafos, de geometria variável, representando relações muiti-dimensionais, tais como os interesses individuais, as suas profissões ou as suas relações de afinidade, que proporcionam alianças tácticas entre grupos existentes ou a rápida cooptação e associação de indivíduos em torno de uma nova causa. No que se refere ao controlo, como é sugerido por Armando Marques Guedes (2010), diferentes ferramentas adaptam-se a diferentes fins. Os blogues e as redes sociais tradicionais – se é que as podemos designar desta forma – adaptam-se à acção estratégica e ao discurso político, enquanto as mesmas redes sociais, o *twitter* ou os SMS servem um propósito mais táctico e operacional dentro da própria acção colectiva. Todas estas ferramentas permitem o exercício de comando dentro da estrutura, onde o número de seguidores ou amigos representa o capital social do líder ou do tema.

Lembremo-nos, por exemplo, das reacções de protesto contra as propostas legislativas norte-americanas que pretendiam conter a pirataria informática ou a venda de produtos contrafeitos na Internet,[15] ou as

[15] O *Stop Online Piracy Act* (SOPA) visava dotar as forças de segurança norte americanas de instrumentos para combater a violação de direitos de autor e a contrafacção na Internet. Os mecanismos previstos no diploma inlcuiam, a pedido de um tribunal, o bloqueio de domínios Internet ou a imposição aos motores de busca para ocultarem resultados. Esta proposta de lei foi bastante criticada, quer por associações de consumidores por ser uma forte limitação dos seus direitos de livre expressão, quer pela indústria de conteúdos on-line norte-america por representar uma forte distorção concorrencial relativamente a empresas estrangeiras. Em ambos os casos seria uma contradição com o princípio da neutralidade da Internet. O PROTECT IP Act (*Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act*), ou PIPA tinha como objectivo dotar os titulares de direitos de autor e

violentas reações por parte de hacktivistas quando alguns Estados europeus tentaram aprovar nos seus parlamentos legislação semelhante.[16]

Estes exemplos são particularmente interessantes pois retratam o exercício de poder dentro e pelo ciberespaço, ou seja uma dimensão instrumental e uma dimensão estrutural. Tendo presente as concepções de Nye sobre *soft power* e de *hard power* aplicadas a este contexto (2010, pp. 5-8), representam manifestações da primeira, as acções pacíficas por parte de comunidades virtuais[17] como a *Wikipedia* que desligou temporariamente os seus serviços, ou a tomada de posição de grandes corporações como a *google*, cujo logótipo principal foi, durante o protesto, tapado por uma "barra de censura"; e exemplos da segunda, os ataques de negação de serviço (DDoS) a sítios governamentais na web da Polónia e da Eslovénia, realizados por hacktivistas.[18]

Estes grupos de indivíduos apresentam as mais diversas motivações, incuindo temas que são caros a uma esquerda pós-moderna, tais como os movimentos anti-globalização, os movimentos anti-guerra e a luta contra as grandes empresas multinacionais, bom como causas próximas de grupos de anarquistas como, por exemplo, o acesso livre à informação ou o repúdio a todo e qualquer tipo de autoridade. Na sua génese, estes grupos seguiam um modelo de movimento social não violento – ou desobediência civil electrónica – e transportavam as tácticas do activismo convencional *off-line* para o ciberespaço, numa tentativa de chamar a atenção da opinião pública e da classe política,

---

o governo norte-americano de mecanismos para bloquear o acessso a sítios web fora do território nacional.

[16] O *Anti-Counterfeiting Trade Agreement* (ACTA) é um tratado comercial internacional que visa combater o aumento da circulação global de bens falsificados e de pirataria de obras protegidas por direitos autorais. Também aqui os criticos contestam a redução dos direitos e liberdades na Internet introduzidos por este acordo.

[17] Ver "Anonymous Goes After World Governments in Wake of Anti-SOPA Protests", *Wired*, 25 de Janeiro de 2012, disponível em http://www.wired.com/2012/01/anonymous-internationalist/, "A Political Coming of Age for the Tech Industry", *New York Times*, 18 de Janeiro de 2012, consultados em Maio de 2014.

[18] Ver "Anonymous kicks off anti-SOPA DDoS rampage", *Computerworld*, disponível em http://www.computerworld.com.au/article/412926/anonymous_kicks_off_anti-sopa_ddos_rampage_--_updated/, "Anonymous shuts down Polish PM's web site", *The News*, disponível em http://www.thenews.pl/1/9/Artykul/83910,Anonymous-shuts-down-Polish-PMs-web-site, consultados em Maio de 2014.

para a sua causa (Samuel, 2004, p. 24). A natureza destas acções era muitas vezes performativa, tirando partido da cobertura mediática que a excentricidade e a espectacularidade dos seus métodos proporcionam. No entanto, o crescimento em tamanho e no número destes grupos, bem como o enfraquecimento das suas estrututas organizativas e índices de afinidade, tem resultado na radicalização e no aumento da violência das suas acções. Veja-se como exemplo, as várias dissidências do corpo principal do grupo *Anonymous* e a criação de grupos que ultrapassaram a linha performativa para o domínio do crime informático – que nada têm em comum com o activismo –, como os *Lulzsec*. Este facto reflete uma nova dinâmica social de violência e um movimento de deslocação do *soft* para o *hard power.*

As mega.dot.com

Numa prespectiva pós-estruturalista, Foucault defende que o poder não reside nas estruturas da sociedade – não é propriedade nem reside em ninguém—, mas antes no discurso. Neste sentido, quem quer que controle o discurso detém também o poder, ou seja, é capaz de impôr a sua vontade. Esta ideia interessa-nos, no sentido em que parte importante do pensamento utópico sobre o ciberespaço se desenvolve em torno da ideia de que este seria um espaço não regulado, onde todos teriam idênticas condições de uso da palavra e da imagem. Novos *media*, como o *facebook*, o *twitter* ou o *youtube*, seriam como outros tantos palcos onde qualquer indivíduo teria, quer a oportunidade, quer os meios, quer a audiência, para tornar pública qualquer notícia, crítica ou pensamento. Desta liberdade de discurso decorreria uma nova distribuição de poder – na medida em que o discurso dominante determina o centro do poder, qualquer um poderia ocupar esse centro, estando para tal apenas dependente do reconhecimento dos pares.

Analisando o funcionamento de motores de busca, de plataformas de partilha de informação e de redes sociais, surge porém a interrogação sobre se os novos *media* terão porventura o suposto efeito democratizador, assegurando a pluralidade necessária para funcionarem como agentes de mudança nas relações de poder, ou se, pelo contrário,

controlam o discurso, assumindo eles próprios o poder. Como referem Hermínio Martins e José Luís Garcia, "a regra da neutralidade da rede diz que esta estaria acessível a todos, sem discriminação de conteúdos, com excepções que se teriam de justificar caso a caso. No entanto, os filtros sucedem-se, em regimes democráticos, mas sobretudo em regimes autoritários" (2013, p. 289). No caso de regimes autoritários, como o chinês, a colocação de filtros que impedem certas pesquisas e o acesso e partilha de temas considerados contra-revolucionários, deixa poucas dúvidas quanto à vontade de controlo político, através da manipulação da opinião pública. Porém, também nos regimes democráticos se levantam questões. É importante lembrar que a mediação tecnológica dos processos de troca de informação no ciberespaço recorre a empresas comerciais, que têm como objectivo gerar lucro. Nas palavras de Ronald Deibert e Rafal Rohozinski, "a vida diária das pessoas é mediada não apenas através do Estado *per se,* mas dispersada nas núvens de comunicações electrónicas digitais detidas e operadas por entidades privadas" (2010, p. 11). E o valor bolsista de empresas como a *Google*, a *Amazon* ou o *Facebook*, depende da sua capacidade de recolher e concentrar informação, decorrente da passagem dos seus utilizadores pela rede, ou seja, depende da sua capacidade de seguir o rasto digital dos seus utilizadores. Porque um dos poucos modelos de negócio comprovadamente rentáveis no ciberespaço é a publicidade, o valor comercial destas empresas reside precisamente na informação que são capazes de recolher, e não nos produtos que vendem, até porque algumas delas não vendem produtos aos utilizadores, mas apenas informação sobre os seus utilizadores a terceiros.

Assim, o poder das empresas da indústria digital e dos *internet enablers* cresce exponencialmente com o número de utilizadores e com a quantidade de informação que é recolhida sobre estes. Quanto a esta informação, compreende desde dados pessoais (nome, morada, idade, educação, situação profissional e financeira, relacionamentos familiares, amorosos e de amizade) até interesses, gostos, *hobbys*, tendências políticas, religiosas e sexuais, passando pelos padrões de consumo de todo o tipo de bens e serviços. Curiosamente, esse poder é colocado nas mãos das empresas pelos próprios cibernautas. Ou seja, se de algum modo vivemos monitorizados por um "big brother", este

não foi, como na visão de Orwell, criado por um Estado totalitário, tendo antes sido contruído por todos os utilizadores da rede, que cedem informação sobre si próprios para usufruir das múltiplas vantagens do digital (Bauman & Lyon 2013). A imediaticidade das interações dentro das redes sociais e de outros serviços, associada a uma crescente capacidade de processamento e a uma "memória" sem limites dos serviços no ciberespaço, coloca estas empresas numa posição priveligiada de poder – como a de um psicólogo relativamente ao seu paciente. A relação entre o conhecimento acumulado sobre o indivíduo e a informação de contexto em tempo real – localização geográfica, sites visitados, palavras usadas – permite à empresa direccionar o indíviduo para produtos adaptados aos seus gostos e interesses, e mesmo ao seu estado de espírito. Esta capacidade pode ser usada para os mais diversos fins, desde os mais prosaicos – vender produtos e serviços – até aos mais sofisticados, como a realização de experiências de engenharia social ou psicológicas, a mediação da acção política ou, no limite, o "controlo remoto" do indivíduo.[19]

O papel central que no ciberespaço assumem corporações que, como se disse, retiram os seus proveitos da publicidade, tem ainda consequências no acesso aos conteúdos que são produzidos. Se por um lado existe liberdade de produzir e difundir conteúdos (de texto, som e imagem), isto não significa o retrocesso das chamadas "indústrias da cultura", para usar a terminologia dos autores da Escola de Frankfurt. Na verdade, observa-se uma ocupação destes espaços comunicacionais pelos tradicionais produtores de conteúdos, que difundem versões aparentemente distentas do mesmo discurso dominante. Suportado no sucesso de plataformas como a wikipedia ou do fenómeno de criação de software livre, Yochai Benkler (2002) avançou com a ideia de que esta comunidade em rede viria a substituir, como fontes de informação, as

[19] Ver o recente caso de um estudo académico do comportamento humano, publicado pela *New Scientist,* realizado sobre o facebook num conjunto de cerca de setecentos mil utilizadores desta plataforma, e que consistiu na avaliação das alterações no estado de espírito provocadas pela manipulação dos conteúdos apresentados. Ver "Facebook Manipulated 689,003 Users' Emotions For Science", *Forbes*, disponível em http://www.forbes.com/sites/kashmirhill/2014/06/28/facebook-manipulated-689003--users-emotions-for-science/, consultado em Junho de 2014.

empresas de produção de conteúdos. No entanto verificamos que, apesar do sucesso da produção em grupo, as principais megaplataformas são hoje dominadas por produtores profissionais que criaram os seus canais de difusão para legiões de seguidores. Citando Morozov, "as tecnologias que, supostamente, viriam conferir poder aos indivíduos, acabaram por reforçar o domínio das grandes corporações, enquanto as tecnologias que, supostamente, viriam estimular a participação democrática, produziram uma população de espectadores passivos" (Morozov, 2012, p. 276).

Por outro lado, os governos já perceberam que para um melhor controlo do ciberespaço – o seu e o dos outros na acepção de Martin Libiki – as *mega dot.com* podem desempenhar um papel fundamental, seja na topologia dos fluxos de informação, seja no desenho das proprias funcionalidades do serviço. É geopoliticamente relevante, para dar apenas um exemplo, a localização física do motor de busca planetário google. Este problema adensa-se quando passamos a falar de armazenamento de informação. Por exemplo na disputa entre a google e o governo da República Popular da China, em 2010, a última via a primeira como uma componente do poder norte-americano (Klimburg, 2011, p. 52).

The one domain to rule them all

A frase que serve de título a esta secção surge num trabalho recente de Martin Libicki (2012, p. 332), no qual defende que o ciberespaço é instrumental para a guerra nos vários domínios da acção militar clássicos (ar, mar, terra e espaço), mas não possui as características para ser elevado a domínio independente com uma doutrina própria na condução da guerra. O objectivo do autor foi o de relevar a transversalidade do ciberespaço relativamente aos restantes domínios "da natureza". No entanto, a alusão à fantasia de Tolkien e a referência ao poder do "anel" como instrumento de controlo de todas as criaturas da "Terra Média" – que encerra em si uma metáfora do poder (destrutivo) da técnica e da industrialização do início do século XX –, permite dar um outro sentido ao jogo de palavras de Libicki: o ciberespaço como domínio para o exercício de poder do Estado sobre os

seus cidadãos, empresas e adversários (e aliados). Recorrendo novamente a Arendt, o ciberespaço deixa de ser um espaço de presença e de visibilidade, e passa a ser um espaço de violência (Below, 2014, p. 108) – um espaço onde se destrói poder pela negação das condições para a discussão pública, que se quer "livre do uso da força e da coerção, dentro de um 'estádio' adequado para a expressão da pluralidade humana e igualdade cívica" (Villa, 1998, p. 148). Esta destruição de poder materializa-se nas várias formas de ocupação e controlo do ciberespaço pelos Estados.

Se, por um lado, este novo *media* transforma a acção política e dá poder a outros actores, por outro vem criar um conjunto de oportunidades – como nenhuma outra tecnologia o fez – para o controlo e a vigilância da sociedade. Talvez o caso mais evidente deste controlo seja o aparato tecnológico designado de *Great Firewall of China*,[20] uma infra-estrutura técnica, alegadamente capaz de monitorizar e de bloquear selectivamente comunicações e conteúdos dentro do ciberespaço chinês e entre este e o resto do mundo, numa espécie de "lápis azul" virtual e em tempo real. Contando que este exercício de censura não tem lugar num Estado de Direito, esta configuração tecnológia apresenta algumas vantagens, já que permite mapear conceitos tradicionais, por vezes de difícil aplicação neste contexto, tais como fronteira ou jurisdição. A criação de fronteiras digitais – ou "vestfaliarização" do ciberespaço – é desejado tanto por Estados totalitários, como por operadores de mercado e classes profissionais, que vêm exigindo aos Estados uma melhor eficiência na aplicação da lei e na protecção dos seus direitos. Como refere Evgeny Morozov, "[n]ão são só os militares que que estão preocupados com o controlo da *web*. As associações de pais querem que seja mais fácil restrear actividades pedófilas e proteger os seus filhos. Hollywood, a indústria musical e a editoras querem melhores formas de rastrear e eliminar a partilha não autorizada de conteúdos protegidos por direitos autorais. Os bancos querem melhores controlos de identidade para minimizar a fraude" (2012, p. 222).

[20] Numa tradução literal "grande corta-fogo da china", a designação alude, ao mesmo tempo, à ancestral fortificação militar chinesa que teve como objectivo proteger o território de invasões vindas do norte, e ao nome dado aos equipamentos de protecção de perímetro para redes locais ou empresariais – a *firewall*.

A rede não é neutra. As topologias global da internet e, agora, de cada uma das suas aplicações, encerram vantagens para os Estados que vão desde a vigilância passiva à espionagem. O facto de os Estados Unidos terem sido os primeiros a converter a rede académica global em internet comercial planetária, bem como a alojar a maior parte das *mega.dot.com* permite-lhes ser o centro geodésico do ciberespaço.[21] Este estatuto assegura que uma grande parte das comunicações mundiais fluem por território norte-americano, independentemente da origem ou do destino, e que a maior parte dos contéudos e metadados de utilização – dados de passagem – se encontram guardados em servidores de empresas norte-americanas. Este facto facilitou o desenvolvimento de programas de espionagem de grande intensidade, tais como o *echelon* ou o recentemente revelado *XKeyscore*, destinados a recolher e tratar grandes volumes de informação.[22]

Mas não é preciso ser-se o "centro da rede", basta parecer. Os Estados sem esse estatuto têm ao seu dispôr um conjunto de técnicas que lhes permite explorar o ciberespaço para acções de espionagem. Este conjunto de técnicas, genericamente designado como *Advanced Persistent Threat* (APT), permite a construção de várias camadas de redes virtuais de alvos seleccionados (*botnets*), dos quais é extraída informação de forma furtiva. São vários os exemplos conhecidos deste tipo de redes, atribuídos alegada e maioritariamente à Federação Russa e à República Popular da China.[23] Considerando, no entanto, que uma

---

[21] Ver J. Markoff, "Internet Traffic Begins to Bypass the U.S." *New York Times*, Agosto de 2008, disponível em http://www.nytimes.com/2008/08/30/business/30pipes.html, consultado em Maio de 2014.

[22] Sobre ambos estes casos ver "The US surveillance programms and their impact on EU citizens' fundamental rights", disponível em http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/briefingnote_/briefingnote_en.pdf, consultado em Maio de 2014. Ver igualmente o relatório Gerhard Schmid, "sobre a existência de um sistema global de intercepção de comunicações privadas e económicas (sistema de intercepção "ECHELON")" ao Parlamento Europeu, 2001, disponível em http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//PT, consultado em Janeiro de 2007.

[23] Ver Deibert, R. and R. Rohozinski (2009). *Tracking Ghostnet: Investigating a Cyber Espionage Network*. Technical report, University of Toronto. Disponível em http://www.f-secure.com/weblog/archives/ghostnet.pdf, consultado em Setembro de 2010; Kaspersky Labs (2013). *Kaspersky Lab Identifies 'MiniDuke', a New Malicious*

vez conhecida a *botnet*, qualquer actor – Estatal o outro – pode reaproveitar e desenvolver o seu código para outros fins, a vantagem deste tipo de operações é essencialmente táctica, com a agravante de poder voltar-se contra o criador. Por outro lado, estas ciberarmas encerram uma dualidade funcional: servem tanto para exploração e espionagem, como para realizar ataques disrruptivos e destrutivos.

Estranha-se, assim, que os Estados Unidos tenham, muito cedo, adoptado como estratégia para a superioridade no ciberespaço, a velha doutrina da dissuasão pela ameaça do uso da força que tanto sucesso teve durante a Guerra-Fria. Mathew Waxman sugere que "a estratégia norte-americana pode envolver um modelo clássico de dissuasão e de defesa militar, no qual [...] podem considerar o uso de ciberataques inovadores, geralmente fora do limite [da lei] excepto na legítima defesa, e podem considerar respostas militares a alguns tipos de ciberataques sofridos" (2011, p. 432). Esta doutrina foi construída durante a década de 1990 do século passado, por vários académicos e *think tanks* como forma de melhor proteger melhor o ciberespaço e as infra-estruturas críticas nacionais de ataques disruptivos e, por outro lado, como oportunidade de explorá-lo para projecção dos seus interesses (Denning, 1999; Libicki, 2007; Clarke & Knake, 2011). Ao mesmo tempo os coronéis Qiao Liang e Wang Xiangsui do Exército de Libertação do Povo Chinês, o livro "Unrestricted Warfare" (1999), defendem que a forma de equiparar o poder bélico norte-americano só é possível com uma abordagem de guerra assimétrica por todos os meios, nomeadamente por meios electrónicos. Estas duas visões têm levado vários Estados à afectação de significativos recursos ao desenvolvimento de capacidades defensivas e ofensivas, no que se pode designar como uma crescente militarização do ciberespaço (O'Connell,

---

Program Designed for Spying on Multiple Government Entities and Institutions Across the World. Technical report, Kaspersky Labs. Disponível em http://www.kaspersky.com/about/news/virus/2013/Kaspersky_Lab_Identifies_MiniDuke_a_New_Malicious_Program_Designed_for_Spying_on_Multiple_Government_Entities_and_Institutions_Across_the_World, consultado em Maio de 2014; Mandiant (2013). *APT1 Exposing One of China's Cyber Espionage Units*. Technical report. Disponível em http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf, consultado em Maio de 2014.

2012). Como resultado, acredita-se que, nos últimos anos, países como a China, os Estados Unidos, a Alemanha, a Itália e o Reino Unido, mas também a Coreia do Norte e ou o Irão,[24] tenham criado unidades de *hackers* dentro das suas estruturas de defesa militar (Roscini, 2010), bem como relações perigosas como o mundo do crime informático para suporte destas capacidades ofensivas. Neste contexto é importante questionar se essa militarização resultou num ciberespaço mais livre e mais seguro ou, se pelo contrário, e como observa O'Connell, "a Internet é agora bem menos segura do que era antes da existência de um Cibercomando [norte-americano] ou de um Centro de Excelência de Ciberdefesa da NATO" (2012, p. 209).

Exemplos de controlo e de violência como estes destroem um dos principais mitos dos ciberutópicos – o princípio da neutralidade da rede –, dando razão a Morozov, quando diz que "[m]uitas vezes o desenho das tecnologias simplesmente esconde as ideologias e as agendas políticas dos seus criadores" (2012, p. 222).

Conclusões

Os adventos do computador e da internet geraram, em vários grupos da sociedade, ondas de entusiasmo sobre as capacidades deste novo *media* – o ciberespaço – como veículo de transmissão de ideias e liberdade públicas, e até como instrumento da paz universal. Neste contexto nasceram movimentos, mais ou menos organizados, que defendem ideais de acesso livre a recursos computacionais e a conteúdos digitais, alguns deles institucionalizados em partidos políticos, revelando as potencialidades do ciberespaço como instrumento de mobilização e acção política. Esta potencialidade parte do pressuposto de que a rede é neutra – é um espaço livre de interferência, onde os cidadãos expressam os seus argumentos de forma igual.

[24] Os Estados Unidos e o Reino Unido foram primeiros em inlcuir, nas respectivas estratégias de cibersegurança, a componente ofensiva e a exploração do ciberespaço como meios de obtenção de vantagem competitiva.

O princípio da neutralidade da rede, defendido também por agentes políticos como factor de desenvolvimento, é um elemento chave na distribuição de poder pelos vários actores. Será que a defesa do princípio da neutralidade da rede é sutentável ou este é compatível com os perigos que vivemos? Este princípio beneficia os Estados mais desenvolvidos e a actual concentração de poder nas *mega.dot.com,* dificultando a aplicação de príncipios de um Estado de Direito, como o da segurança dos seus cidadãos. O balanço entre este benefício e a crescente dificuldade em proteger as próprias infra-estruturas, deverá justificar uma tendência de "vestfaliarização" do ciberespaço: "Num futuro próximo, os Estados delinearão um acordo formal para por cobro ao actual ingovernável e caótico ciberespaço" do qual resultará um novo mapa com fronteiras e limites. Definidas as fronteiras, serão erigidos muros e criadas leis internas para assegurar o governo da rede e reestabelecer a ordem natural das coisas (Demchak & Dombrowski, 2011, p. 57).

Em suma, sendo claro que o poder absoluto dos indivíduos cresceu, não é líquido afirmar o mesmo relativamente ao seu poder relativo. O ciberespaço e as novas tecnologias trouxeram poder a todos os agentes: indivíduos, empresas e Estados.

BIBLIOGRAFIA

Bauman, Z. & Lyon, D. (2013). Liquid Surveilance. Cambridge, UK: Polity Press.

Below, K. C. (2014). The utility of timeless thoughts: Hannah arendt's conceptions of power and violence in the age of cyberization. In J.-F. Kremer & B. Müller (Eds.), *Cyberspace and International Relations* (pp. 95-114). Springer.

Benkler, Y. (2002). Coase's penguin, or, linux and "the nature of the firm". *Yale Law Journal*, (pp. 369-446).

Benkler, Y. & Nissenbaum, H. (2006). Commons-based peer production and virtue*. *Journal of Political Philosophy*, 14(4), 394-419.

Boyd, D. (2008). Can social network sites enable political action? In A. Fine, M. Sifra, A. Rasiej, & J. Levy (Eds.), *rebooting america* (pp. 112-116). Creative Commons.

Clarke, R. A. & Knake, R. K. (2011). *Cyber war*. HarperCollins.

Deibert, R. & Rohozinski, R. (2010). Beyond denial: introducing next- generation information access controls. In R. Deibert, J. Palfrey, R. Rohozinski, & J. Zitrain (Eds.), *Access controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (pp. 3-14). MIT Press.

Demchak, C. C. & Dombrowski, P. (2011). Rise of a cybered westphalian age. *Strategic Studies*, 5(1), 32-61.

Denning, D. (2001). Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy In Arquilla, J. & Ronfeldt, D. (Eds.), *Networks and netwars: The future of terror, crime, and militancy* (pp. 239-288). Santa Monica, CA: RAND Corporation. Disponível em http://www.rand.org/pubs/monograph_reports/MR1382/MR1382.ch8.pdf, consultado em Maio de 2007.

Denning, D. E. (1996). Concerning hackers who break into computer systems. *High noon on the electronic frontier: Conceptual issues in cyberspace*, (pp. 137-164).

Denning, D. E. R. (1999). *Information warfare and security*. Addison-Wesley.

Escher, T. (2004). Political Motives of Developpers for Collaboration in GNU/Linux. PhD thesis, Universidade de Leicester. Disponível em http://opensource.mit.edu/papers/escher.pdf, consultado em 12 de Fevereiro de 2007.

Klimburg, A. (2011). Mobilising cyber power. Survival, 53(1), 41-60.

Levy, S. (1984). *Hackers: Heroes of the computer revolution*. Doubleday.

Liang, Q. & Xiangsui, W. (1999). *Unrestricted Warfare*. Pequim: PLA Literature and Arts Publishing House.

Libicki, M. C. (2007). *Conquest in cyberspace: National Security and Information Warfare*. Cambridge University Press.

Libicki, M. C. (2012). Cyberspace is not a warfighting domain. *I/S: A Journal of Law and Policy for the Information Society*, 8(2), 321-336.

Lukes, S. (1974). *Power: A radical view*. London: Macmillan.

Marques Guedes, A. (2010). The new geopolitical coordinates of cyberspace. *Revista Militar*, (2503/2504), 823-847.

Martins, H. & Garcia, J. L. (2013). WEB. In J. L. Cardoso, P. Magalhães, & J. Machado Pais (Eds.), *Portugal Social de A a Z*. Lisboa: Expresso.

Mattelart, A. (2000). *História da Utopia Planetária*. Bizâncio.

McLuhan, M. (2008). *Compreender os Meios de Comunicação. Estensões do Homem*. Lisboa: Relógio d'Água.

Morozov, E. (2012). *The net delusion: The dark side of Internet freedom*. PublicAffairs.

Nye Jr, J. S. (2010). *Cyber power*. Technical report, Belfer Center for Science and International Affairs, Harvard Kennedy School.

O'Connell, M. E. (2012). Cyber security without cyber war. *Journal of Conflict and Security Law*, 17(2), 187-209.

Roscini, M. (2010). World wide warfare-'jus ad bellum' and the use of cyber force. *Max Planck Yearbook of United Nations Law*, 14, 85-130.

Samuel, A. (2004). *Hacktivism and the Future of Political Participation*. PhD thesis, Oxford University. Disponível em http://www.alexandrasamuel.com/dissertation/pdfs/Samuel-Hacktivism- entire.pdf, consultado em Setembro de 2008.

Strate, L. (1999). The varieties of cyberspace: Problems in definition and delimitation. *Western Journal of Communication*, 63(3), 382-412.

Taylor, R. W., Fritsch, E. J., Holt, T. J., & Liederbach, J. (2006). *Digital crime and digital terrorism*. Pearson/Prentice Hall.

Tilly, C. (1978). *From mobilization to revolution*. Nova Iorque: McGraw-Hill.

Villa, D. R. (1998). The philosopher versus the citizen: Arendt, strauss, and socrates. *Political theory*, 26(2), 147-172.

Waxman, M. C. (2011). Cyber-attacks and the use of force: Back to the future of article 2 (4). *Yale Journal of International Law*, 36, 421-459.