



JOSÉ PEDRO TEIXEIRA FERNANDES

Da utopia da sociedade em rede à realidade da sociedade de risco

Análise Social, 207, XLVIII (2.º), 2013

ISSN ONLINE 2182-2999

EDIÇÃO E PROPRIEDADE

Instituto de Ciências Sociais da Universidade de Lisboa. Av. Professor Aníbal de Bettencourt, 9
1600-189 Lisboa Portugal — analise.social@ics.ul.pt



Análise Social, 207, XLVIII (2.º), 2013, 260-286

Da utopia da sociedade em rede à realidade da sociedade de risco. Neste artigo é passada em revista a emergência da sociedade em rede, com as suas raízes na internet, na invenção da *World Wide Web* e na revolução digital. É também revisitado o *ethos* da “cultura da internet” e a sua projeção na sociedade em rede. Em seguida, é fornecida uma macro visão da “galáxia internet”, um fenómeno desigual e em rápida expansão. Por último, são analisadas algumas tendências que sugerem a crescente transformação da sociedade em rede numa sociedade de risco. Entre a perda de neutralidade da *web* e o risco da ciber guerra, constata-se uma substituição do idealismo inicial por preocupações económicas e securitárias.

Palavras-chave: sociedade em rede; sociedade de risco; *web*; ciber guerra.

From the utopia of the network society to the reality of risk society. This article begins with a review of the emergence of network society, with its roots in the Internet, the invention of the World Wide Web, and the digital revolution. The ethos of “Internet culture” and its projection in the network society is also revisited. Then comes a macro view of the “Internet Galaxy”, an unequal and rapidly expanding phenomenon. Finally, it analyses some trends that suggest the growing transformation of the network society in a society of risk. In between the loss of the neutrality of the Web and the risk of cyber warfare, there is a growing replacement of the idealism of the pioneers by economic and security concerns.

Keywords: network society; risk society; web; cyber war.

José Pedro T. Fernandes » jptfernandes@gmail.com » Instituto Superior de Ciências Empresariais e do Turismo.

JOSÉ PEDRO TEIXEIRA FERNANDES

Da utopia da sociedade em rede à realidade da sociedade de risco

Um novo mundo está a tomar forma neste final de milénio. Tem origem mais ou menos no fim dos anos sessenta e meados da década de setenta na coincidência histórica de três processos independentes: revolução da tecnologia da informação; crise económica do capitalismo e do estatismo e a consequente reestruturação de ambos [...] A interação entre esses processos e as reações por eles desencadeadas fizeram surgir uma nova estrutura social dominante, a sociedade em rede; uma nova economia, a economia informacional/global; e uma nova cultura, a cultura da virtualidade real. Castells [1999, p. 411]

INTRODUÇÃO¹

Decorridos mais de vinte anos desde a invenção e divulgação pública da *World Wide Web*² por Timothy John Berners-Lee (Tim Berners-Lee), dispomos de um horizonte temporal alargado para olhar retrospectivamente os primeiros tempos da *web*. Este distanciamento cronológico permite confrontar as expectativas iniciais com a realidade em que esta se transformou. Assim, neste artigo, propomo-nos revisitar a sociedade em rede a partir da teorização iniciada por Manuel Castells e outros, há cerca de uma década e meia atrás. O principal objetivo é analisar o seu percurso ao longo dos primeiros vinte anos, e avaliar em que medida estará a originar uma sociedade de risco, no sentido que Ulrich Beck deu ao conceito. Na análise da evolução/transformação ocorrida, uma ênfase especial será dada aos ideais tecno-libertários iniciais e à posterior

1 O autor agradece as sugestões efetuadas pelos *referees* anónimos, que contribuíram para valorizar a versão final deste artigo.

2 A 6 de agosto de 1991 Tim Berners-Lee tornou a sua invenção da *World Wide Web* acessível à comunidade dos utilizadores da internet.

ascensão do uso económico-empresarial e das preocupações com a segurança na rede. Questões específicas a que também vamos procurar responder são: (i) saber em que medida tais tendências estão a pôr em causa a neutralidade da internet e a liberdade e democracia; (ii) saber se prenunciam uma sociedade de risco, onde a rede se está a transformar num espaço de conflito e de ciber-guerra.

A EMERGÊNCIA DA SOCIEDADE EM REDE: INTERNET, *WORLD WIDE WEB*³ E REVOLUÇÃO DIGITAL

É bem conhecido que a internet teve a sua origem na década de 60 do século XX, no contexto da competição da Guerra Fria, entre os EUA e a ex-União Soviética. Esta surgiu como resultado de uma colaboração entre os meios militares e universitários norte-americanos, quando foi criado um sistema de comunicação entre computadores. Em termos de precursores da atual internet – e da sua parte mais conhecida, a *World Wide Web* –, existem alguns marcos relevantes que importa relembrar. Numa lógica futurista para a época, Norbert Wiener introduziu no final da década de 40 desse século, o conceito de “cibernética”, um neologismo cunhado a partir da palavra grega *kybernetiké*.⁴ No sentido que Norbert Wiener lhe deu, tratava-se de agir pelo comando e controlo da totalidade do ciclo de informações. Outro precursor, agora sobretudo do *ethos* da sociedade em rede, o qual terá inspirado a própria criação da *World Wide Web*, foi Stewart Brand com o seu visionário *Whole Earth Catalog*.⁵ As suas ideias influenciaram também a conceção da revista “tecno-libertária” *Wired* (Turner, 2008).

Em termos tecnológicos, a primeira antecessora da internet foi a ARPA (NET),⁶ criada pela *Advanced Research Projects Agency* – uma agência associada

3 Seguimos de perto a informação factual sobre história da internet elaborada pela Internet Society (2010), *A Brief History of the Internet*, acessível em <http://www.isoc.org/internet/history/brief.shtml> [Acedido a 04-04-2012]. Não sendo uma história crítica do seu processo de criação e difusão, ainda assim é útil em termos factuais e cronológicos para uma exposição sucinta como a aquela que é aqui efetuada.

4 Originalmente significava a arte de comando e controlo de um piloto sobre o navio e a sua rota.

5 O *Whole Earth Catalog* criado por Stewart Brand foi um livro inovador para a época, sendo apresentado sob a forma de um compêndio multidisciplinar. Em 1971 foi galardoado com o *National Book Award* dos EUA.

6 A ARPA(NET) foi criada em plena Guerra Fria, num contexto em que nos EUA se temia um eventual ataque nuclear soviético. Receava-se, entre outras consequências, que este pudesse levar à desarticulação da cadeia comando por rutura das comunicações. No âmbito da Rand Corporation – um prestigiado *think tank* com sede na Califórnia e que usualmente colabora com o Pentágono –, surgiu a ideia de construir um sistema de comunicações militar →

ao Pentágono – e pelo *Massachusetts Institute of Technology* (MIT). Tratou-se de uma rede experimental⁷ que tinha por objetivo permitir que os computadores comunicassem entre si, independentemente do fabricante, sistema operativo, *hardware* ou distância geográfica. Um outro marco relevante data de 1969, quando ocorreu aquilo que normalmente é considerado o envio da primeira mensagem de correio eletrónico (*email*).⁸ O processo deu-se entre um computador da Universidade da Califórnia (UCLA) e um outro computador situado no Stanford Research Institute. Em 1973 surgiu um novo avanço importante quando Robert Kahn, da ARPA, e Vinton Cerf, da Universidade de Stanford, na Califórnia, elaboraram, num trabalho conjunto, a arquitetura básica da internet. No final da década de 70, com os protocolos TCP/IP⁹ em fase avançada de desenvolvimento, foi constituído o *Internet Control and Configuration Board* (ICCB), um comité informal destinado a coordenar o desenvolvimento desses protocolos e da arquitetura de comunicação. Em 1983, a ARPA(NET)¹⁰ – à qual esteve ligado outro pioneiro, Jonathan Bruce Postel (ou Jon Postel, como é mais conhecido) – deu origem à *Military Network* (MILNET), usada para fins militares, bem como à ARPA-INTERNET, criada para pesquisa e desenvolvimento. Em meados dos anos 80, a *National Science Foundation* (NSF) dos EUA, tendo por objetivo distribuir o acesso aos cinco centros de supercomputadores, utilizou os protocolos da ARPA(NET) a NSF ligando-os entre si para formar o *backbone*¹¹ NSF(NET). As redes regionais foram formadas no fim dos anos 80 para fornecer acesso a este *backbone*, ao qual as universidades e organizações de pesquisa ligaram também as suas redes. A designação internet foi então utilizada para se referir ao conjunto rede.

Nesta fase embrionária, as *internetworks* eram essencialmente suportadas por financiamentos públicos, o que implicava, também, regras estritas sobre o

capaz de sobreviver a um ataque nuclear. Embora não fosse o objetivo original por detrás da ARPA(NET), a principal precursora da atual internet, esta proposta da Rand Corporation terá, de alguma maneira, influenciado também a investigação que levou à criação dessa rede.

7 A ARPA(NET) só foi declarada completamente operacional em 1975, sendo constituída por uma rede de linhas alugadas ligadas por nós especiais de comutação, chamados *Internet Message Processor* (IMP). A sua administração era efectuada pela *Defense Information Systems Agency* dos EUA.

8 Uma curiosidade que mostra como era incipiente a tecnologia original e nos dá uma ideia dos enormes avanços entretanto ocorridos: o texto da mensagem enviada era apenas “*login*” mas o computador que recebeu a mensagem parou de funcionar na letra “o”...

9 Transmission Control Protocol/Internet Protocol.

10 A ARPA(NET) foi formalmente extinta em 1990.

11 O *backbone* (espinha dorsal) designa um esquema de ligações centrais de um sistema mais amplo e de elevado desempenho.

seu uso. As organizações que podiam utilizar a internet – tipicamente agências governamentais e universidades – tinham de o efetuar no âmbito dessas regras. Ou seja, a rede podia ser usada ligada a atividades de pesquisa científica e tecnológica, ou para atividades académicas e educativas. Todavia, não podia ser utilizada, por exemplo, para fins comerciais ou publicitários. Tudo isto sofreu profundas alterações quando, no início da década de 90, a internet foi retirada do controlo militar passando a sua gestão para a *National Science Foundation* (NSF) dos EUA. Com a tecnologia para a criação de redes informáticas abertas ao domínio público e com as telecomunicações em processo de liberalização, a NSF avançou com a privatização da internet.¹² Foi nessa altura – finais de 1990 –, que foi inventada a *World Wide Web*¹³ (designação que poderá ser traduzida como “rede de alcance global”), pelo engenheiro britânico Tim Berners-Lee e os seus colegas do *Centre Européenne pour la Recherche Nucléaire* (CERN) de Genebra. A este se deve a primeira comunicação bem-sucedida entre *Hyper Text Transfer Protocol* (HTTP)¹⁴ e um servidor, utilizando o protocolo TCP/IP. A partir daqui, o fornecimento de *internetworks* passou a ser, crescentemente, uma atividade empresarial, dominada por empresas privadas. Estas começaram a fornecer serviços de internet para uso empresarial ou privado.

A SOCIEDADE EM REDE E A ECONOMIA DIGITAL NOS SEUS PRIMÓRDIOS

Conforme já referimos, a internet surgiu de forma inicialmente restrita, resultando da colaboração entre universidades e centros de investigação, mais ou menos próximos dos meios militares norte-americanos. Todavia, apesar das restrições dessa fase pioneira, existia também uma faceta importante de abertura à colaboração a nível internacional. Isto permitiu a todos

12 Ainda no decurso dos anos 80, o Departamento de Defesa dos EUA tinha decidido comercializar a tecnologia internet, financiando a inclusão do TCP/IP nos protocolos dos computadores fabricados por empresas norte-americanas. Desta forma, no início da década de 90, a maior parte dos computadores nos EUA estava já em condições de poder funcionar em rede.

13 A *World Wide Web* (ou só *web*) assenta na utilização de hiperligações para navegar entre documentos (chamados “páginas *web*”) com recurso a um *software* o *browser* (navegador). Assim, uma página na *web* é basicamente um ficheiro de texto escrito em linguagem HTML. Permite descrever a formatação do documento e incluir elementos gráficos ou ligações para outros documentos. Outra componente fundamental é o protocolo HTTP que permite vincular documentos alojados por computadores distantes (chamados servidores *web*). Os documentos são assim identificados por um endereço único, o URL, permitindo localizar um recurso em qualquer servidor da rede internet.

14 Ver Tim Berners-Lee (1990), *World Wide Web: Proposal for a HyperText Project*, acessível em <http://www.w3.org/Proposal.html> [Acedido a 04-04-2012].

os que tivessem interesse, e, obviamente também, os conhecimentos técnicos necessários, uma possibilidade de participar no processo da sua construção e desenvolvimento. Esta lógica de trabalho “comunitário”, não lucrativo, característica da contracultura da década de 60 está, assim, inscrita no próprio *ethos* da internet e da sociedade em rede. Hoje, as suas projeções mais óbvias são o movimento para o *software* livre¹⁵ e os “partidos piratas”, os quais estão a emergir no espetro político.¹⁶ Mas, como foi visto, na altura, o despontar da internet/*web* e da sociedade em rede? Entre os teorizadores mais influentes dos primórdios encontramos o sociólogo Manuel Castells, com diversas publicações de perfil académico-científico. Por sua vez, numa perspetiva menos estritamente académica e com um enfoque mais empresarial, o nome provavelmente mais influente foi Don Tapscott. Vejamos como estes retratavam a emergência da internet/*web* e da sociedade em rede nas suas múltiplas facetas.

Para Manuel Castells, a internet/*web* e a sociedade em rede eram o resultado de uma “encruzilhada insólita entre a ciência, a investigação militar e a cultura libertária” (2004, p. 34). No seu *ethos* encontrava-se também inscrita a filiação na contracultura dos anos 60, mas inserida num contexto marcado por múltiplas influências heterogéneas. Na realidade, Manuel Castells (2004, p. 83) filiou a “cultura da internet” de forma bastante abrangente. Viu-a como tendo sido “construída sobre a crença tecnocrática no progresso humano através da tecnologia, praticada por comunidades de *hackers* que prosperam num ambiente de criatividade tecnológica livre e aberta, assente em redes virtuais, dedicadas a reinventar a sociedade”. Mas viu-a também como “materializada por empreendedores capitalistas” que impulsionavam uma “nova economia”¹⁷,

15 Ver, entre outros, a Free Software Foundation, acessível em <http://www.fsf.org/> e a Open Source Initiative, acessível em <http://www.opensource.org/> [Acedidos em 04-04-2012].

16 O mais recente caso de um “partido pirata” em ascensão ocorreu na Alemanha onde, até pela importância do país, poderá ser um exemplo para outros movimentos sociais e políticos de protesto. Ver William Boston (2012), “Pirates’ Deal a Blow on Germany’s Political Status Quo” in *Wall Street Journal* (10 de abril, p. A10), Acessível em <http://online.wsj.com/article/SB10001424052702304587704577333922727849932.html> [Acedido a 12-04-2012].

17 A este propósito, Robert Hassan (2008, p. 23), afirma que, *lato sensu*, a sociedade da informação (conceito mais ou menos próximo de sociedade em rede de Manuel Castells), é sucessora da sociedade industrial. A informação “circula sob a forma de ideias, conceitos e inovação” nos assuntos mais diversos – sendo “replicada como *bits* e *bytes* digitais através da computadorização –, estará a substituir o trabalho e a lógica relativamente estática da fábrica e maquinaria, como força organizadora central da sociedade”. Assim, “a moderna sociedade industrial, com uma dinâmica relativamente ordenada e organizada”, teria dado lugar a uma “sociedade da informação pós-moderna, em que a desorganização e a fragmentação serão as suas características salientes”.

a qual começava a ter um peso crescente nas atividades de produção e de criação de riqueza.

Partindo da referida definição, autonomizou quatro dimensões relevantes, cada uma das quais com a sua contribuição própria: (i) a dimensão da cultura tecnomeritocrática; (ii) a dimensão da cultura *hacker*¹⁸; (iii) a dimensão da cultura comunitária virtual; (iv) e a dimensão da cultura empreendedora. Em primeiro lugar, a cultura tecnomeritocrática, a qual está inscrita no ambiente que permitiu a invenção da internet. Este foi um ambiente académico-científico, de tipo elitista, orientado para a inovação tecnológica, largamente estimulado pela própria comunidade científica, sobretudo pelo seu impacto prestigiante dentro desta e na sociedade em geral. Em segundo lugar, a dimensão da cultura *hacker* – no sentido inicial do conceito. Embora a lógica do *hacker*, dos primeiros tempos da revolução digital, tivesse também por objetivo a inovação tecnológica, assentava num ideal que não era exatamente o da técnico-meritocracia. A lógica típica da cultura *hacker* era poder usar livremente os conhecimentos produzidos por outros, e, de forma também livre, ou seja, sem intuítos comerciais, tornar os novos conhecimentos acessíveis a outros na rede. A cultura *hacker* está, assim, igualmente, no cerne do referido movimento para o *software* livre. Por outro lado, os *hackers* originais da revolução informática poderiam ser qualificados como imbuídos de uma visão “libertária”, ou até “anárquica”, pois não dependiam de nenhuma instituição educativa, empresarial ou outra. Este tipo de *hacker*, pelo seu lado visionário, e pelo seu papel determinante na fase de criação da internet, aproximou-se do “génio criativo”, no sentido que esta designação adquire no mundo das artes. Em terceiro lugar, a dimensão comunitária virtual, a qual está diretamente relacionada com o uso dado à tecnologia. Integram-se nesta cultura comunitária virtual os que tendem a utilizar a internet sobretudo para o desenvolvimento de contactos ou relações sociais. Tipicamente são indivíduos com conhecimentos técnicos limitados, tendo apenas competências na ótica do utilizador, de maior ou menor dimensão. Todavia, mostram grande apetência pela utilização da *World Wide Web* desde a sua “explosão” em meados dos anos 90. Esta dimensão

18 O termo *hacker* tem, pelo menos, dois significados diferentes: (i) o de especialista, quase visionário, com grandes conhecimentos em computadores, tecnologia digital e/ou programação. Neste sentido, o uso do termo *hacker* – que é o efetuado por Manuel Castells quando se refere à “cultura *hacker*” –, tem conotações positivas e predominou nos primeiros tempos da revolução eletrónica e informática até aos anos 80. Mas há um outro sentido, que é o uso mais corrente atual, com uma conotação bastante negativa: (ii) o de alguém mais ou menos dotado para a informática que usa o seu conhecimento especializado em computadores, programação e/ou tecnologia digital para ações abusivas e/ou ilegais de acesso a outros computadores e redes, bem como para praticar atos maliciosos que podem produzir danos de maior ou menor dimensão.

transformou a internet num novo “instrumento para a organização social, a ação coletiva e a construção de sentido” (Castells, 2004, p. 76). Uma quarta e última dimensão surge ligada à cultura empreendedora e está estreitamente direcionada para um uso económico, e com fins lucrativos, da tecnologia. A cultura empreendedora alicerça-se na inovação empresarial e no apoio financeiro a projetos de risco elevado, sendo movida por uma perspectiva de lucros muito significativos resultantes da aposta em *start-ups* de base tecnológica, ligados à economia digital em fase de afirmação.

Em relação à teorização de Don Tapscott (1997), conforme já referimos, foi efetuada sobretudo numa perspectiva empresarial, sendo mais livre de preocupações estritamente académico-científicas.¹⁹ Mais do que nos fenómenos gerais da sociedade em rede – como encontramos na teorização de Castells –, Tapscott centrou-se na emergência da nova economia ou economia digital (ou *e-economia*), uma designação popularizada pelo próprio nas suas publicações e palestras. Para este, a emergente economia digital, teorizada em contraponto com a “velha economia”, surgia com um conjunto de múltiplas características²⁰ distintas: (i) CONHECIMENTO – o qual se tornou uma componente fundamental dos produtos/serviços; (ii) DIGITALIZAÇÃO – passou a dominar nas transações comerciais e financeiras e na comunicação humana; (iii) VIRTUALIZAÇÃO – levando a uma prevalência do virtual sobre o físico e com implicações para a natureza da atividade económica; (iv) MOLECULARIZAÇÃO – substituição da produção em massa por produção “à medida”; (v) INTEGRAÇÃO/TRABALHO EM REDE – surgimento de uma economia com múltiplas e profundas interconexões dos indivíduos e organizações; (vi) DESINTERMEDIÇÃO – eliminação de intermediários nas atividades económicas, como agentes, corretores, grossistas ou até retalhistas; (vii) CONVERGÊNCIA – dos setores económicos-chave no uso de sistemas informação, na comunicação e conteúdos; (viii) INOVAÇÃO – a criatividade e a imaginação inovadora empresarial tornam-se decisivas para a competitividade empresarial; (ix) PRODCONSUMO – desvanecimento da distância que separa consumidores e produtores podendo os próprios consumidores associar-se ao processo produtivo – transformando-se em *prosumers* –, por exemplo quando a sua informação e/ou ideias passam a ser incorporadas em produtos/serviços; (x) IMEDIATICIDADE – surgimento de uma economia em tempo real, onde são efetuadas transações comerciais e financeiras com meios

19 O que se explica pelo próprio perfil do autor e objetivos das suas publicações. Estas não são tanto para um público estritamente académico mas antes pretendem chegar ao universo mais vasto de todos os envolvidos nas atividades económico-empresariais.

20 Na apresentação dessas características seguimos de perto a síntese feita no artigo de Dias e Correia (1999, pp. 104-107).

eletrônicos; (xi) GLOBALIZAÇÃO – afirmação de uma economia cada vez mais interligada a nível mundial, nas suas múltiplas dimensões, que faz perder relevância ao Estado-nação como unidade político-económica; e (xii) CLIVAGENS – enormes contrastes sociais tendem a surgir com empregos altamente remunerados para jovens recém-formados, contrastando com despedimentos em massa de trabalhadores mais velhos, inadaptados à economia digital. Tendência para o aumento do fosso que separa os que têm dos que não têm, quer em termos de riqueza, quer no acesso aos novos instrumentos da sociedade em rede.

Quanto a Castells, embora não tenha teorizado especificamente para os aspetos empresariais da sociedade em rede, como fez Tapscott, também não ignorou essa faceta. A existência de práticas empresariais inovadoras, organizadas em torno das redes, foi igualmente objeto do seu interesse e análise. O mesmo se pode dizer quanto à capacidade de gerar conhecimento permitida pelo acesso à informação aberta *online*, combinada com as ideias inovadoras. Na sua ótica, estes foram os principais alicerces sobre os quais se começou a erigir a nova economia (Castells, 2004, p. 100). Para Castells, essas tendências não eram exclusivas das empresas relacionadas com a internet, ou do setor tecnológico. Tratava-se, antes, de tendências generalizadas que estavam a ocorrer de forma transversal a toda a economia. Tal como Tapscott, considerou também que o facto de a rede tornar possível obter um *feedback* dos consumidores, em tempo praticamente real, tinha significativas consequências nas formas de produção e de gestão.²¹ Fora da chamada economia real, um traço característico importante assinalado por Castells foi a volatilidade dos mercados financeiros. Estes tendiam a ser crescentemente dominados por “turbulências de informação” (Castells, 2004, p. 112) e a tornar-se mais instáveis e imprevisíveis na medida que se afastaram das tradicionais formas prudenciais de avaliação do mundo dos negócios – uma análise bastante presciente, sobretudo se pensarmos na forma como surgiu a crise financeira de 2007/2008 nos EUA. Na economia e sociedade em rede, o risco, a incerteza e a mudança tornavam-se, assim, numa característica dominante dos mercados financeiros. Esta tendência também foi alimentada pela multiplicidade de informações *online*, muitas delas difíceis de confirmar, tornando-se quase impossível destrinçar, pelo menos em tempo útil, a informação fidedigna dos rumores ou manipulações. Obviamente que tudo isto trouxe dificuldades acrescidas na tomada de decisão pelos investidores, gerando, não invulgarmente, reações instantâneas, por vezes irracionais, de alguma forma impulsionadas pela avalanche (des)informativa da sociedade em rede.

21 Aquilo a que Alvin Toffler, no seu livro originalmente publicado em 1980, sob o título *The Third Wave (A Terceira Vaga)* – e, mais tarde, Don Tapscott, chamaram *prosumers*.

Por sua vez, fora do terreno económico e dos mercados financeiros, surgiram lógicas de sociabilidade novas, através das comunidades virtuais. As pessoas passaram crescentemente a organizar-se em torno dos seus valores, afinidades, projetos e interesses específicos, usando as novas possibilidades tecnológicas conferidas pela revolução digital (internet, telemóveis, correio eletrónico, etc.). Com a sociedade em rede verificou-se uma transição do predomínio das tradicionais relações primárias – família, lugar de residência, emprego –, para um novo sistema de relações sociais de base mais individualista (Castells, 2004, p. 158). Naturalmente que aqui poderíamos também incluir a tendência para a expansão do teletrabalho²² (por vezes designado como “trabalho na era digital”), especialmente notória no setor dos serviços – por exemplo através do *outsourcing* de *call-centers*, de empresas telefónicas, bancárias, etc. Outra tendência, agora no cruzamento do social e do político, foi a do surgimento de movimentos sociais ativos na internet – grupos feministas, ecologistas, religiosos, pacifistas, entre outros. A rede converteu-se, assim, num espaço para ativismo em prol de “causas”, ou, então, num espaço privilegiado para manifestar descontentamento, em termos sociais e políticos ou para mobilizar pessoas para ações no mundo real. Castells viu nessa tendência uma forma de aumentar a liberdade e de *empowerment* (“empoderamento”) do cidadão. Nesta ótica, a internet trazia uma mais-valia para a democratização, permitindo, tendencialmente, igualar “as condições nas quais distintos atores e instituições podem agir” (Castells, 2004, p. 197).

UMA “REDE GALÁXICA” ONDE O “PINGUIM CONFRONTA O LEVIATÃ”²³

Um dos pioneiros da internet, Joseph Carl Robnett Licklider (ou apenas J. C. R. Licklider), referia-se, em 1962, à formação de uma “rede galáctica”. Provavelmente influenciado por essa designação, Castells (2004) deu a um dos seus livros subsequentes sobre a sociedade em rede o título de *A Galáxia Internet: Reflexões sobre Internet, Negócios e Sociedade*. Tratou-se, pela própria formação do autor, de uma obra de perfil sociológico que procurou analisar a internet para além dos aspetos tecnológicos, interpretando o(s) seu(s) uso(s)

22 Por definição será o trabalho à distância realizado fora do espaço físico da empresa ou organização à qual o trabalhador está ligado. O uso das redes, a videoconferência, a utilização partilhada de documentos em tempo real, ou a redistribuição de chamadas telefónicas, são alguns dos exemplos mais óbvios de teletrabalho propiciados pela revolução informática e digital em curso.

23 Adaptação do título do livro de Yochai Benkler (2011).

como um fenómeno social e humano. Mas, tendo como critério de referência o número de utilizadores da rede, qual é hoje a verdadeira dimensão da “galáxia internet”? Para responder a esta questão vamos recorrer às estatísticas disponibilizadas pela *Internet World Stats*. Embora não se trate de informação neutra, pois é recolhida e tratada essencialmente para fins comerciais²⁴ – e se possam discutir também os critérios usados para esse efeito –, as suas estatísticas não deixam fornecer uma imagem aproximada da atual dimensão da “galáxia Internet”. Começando por dar uma visão panorâmica, uma das coisas que chama à atenção é a forma como o número de utilizadores da internet cresceu, de maneira avassaladora, ao longo da primeira década do século XXI. Atualmente esse número supera já os 2,2 biliões de utilizadores ativos em todo o mundo, encontrando-se o valor mais significativo (1 016 biliões), na Ásia²⁵ – que é também o continente mais vasto, heterogéneo e populoso do planeta. Esta predominância da Ásia, no seu conjunto, não significa que, em termos relativos, a taxa de penetração da internet na população total desse continente seja elevada comparativamente a outras regiões mundiais. Na realidade, quando olhamos para as taxas de penetração da internet, verificamos que a Ásia – apesar de todo o seu potencial para se tornar o “centro do mundo” ao longo do século XXI –, ainda tem um longo caminho a percorrer. Obviamente que esta visão macro do continente asiático aglutina realidades completamente heterogéneas, em termos económicos, sociais e de acesso à rede. Basta pensarmos no que é, por exemplo, a realidade do Japão, da Coreia do Sul ou de Singapura, face à da Mongólia, à do Afeganistão ou do Butão. De qualquer maneira, importa reter que a taxa atual de penetração da internet (percentagem de utilizadores da internet na população total), é de 26,2%, enquanto nas áreas do mundo de desenvolvimento mais antigo, como a Europa e a América do Norte, a sua taxa de penetração é muito superior: 61,3% na Europa continental e 78,6% na América do Norte. Pela sua própria dimensão populacional, verifica-se um peso dos asiáticos no uso da rede superior aos das populações de qualquer um dos outros continentes. De facto, em finais de 2011, 44,8% dos utilizadores da internet tinham origem na Ásia, enquanto 22,1 % tinham origem na Europa continental e 12,0% na América do Norte. Nas restantes áreas do mundo verificam-se valores menores, que denotam baixas taxas médias de penetração

24 Segundo a apresentação feita no próprio *website* da *Internet World Stats* é uma fonte útil para “international online market research, the latest Internet statistics, world Internet penetration data, world population statistics, telecommunications information reports, and Facebook Stats by country”. Acessível em <http://www.internetworldstats.com/> [Acedido em 12-04-2012].

25 Ver *Internet World Stats*, acessível em <http://www.internetworldstats.com/stats.htm> [Acedido em 12-04-2012].

da internet no conjunto da população – a exceção é a Oceânia/Austrália, que origina 1,1 % dos utilizadores mundiais, com escassas dezenas de milhões de pessoas. O peso dos utilizadores oriundos da América Latina no global é de 10,4%, de África ronda os 6,2%, e do Médio Oriente os 3,4%.²⁶

Embora estes dados mostrem que a “galáxia internet” é uma realidade notoriamente desigual, onde os graus de acesso à rede são muito variáveis dentro das regiões do mundo e os países considerados – o que levanta, desde logo, o problema dos excluídos da sociedade em rede –, é inegável constatar-se a existência de um processo que pode ser considerado de globalização. Mais de 2,2 biliões de seres humanos, um pouco por todo o planeta, estão ligados em rede e potencialmente em contacto – ou seja, cerca de 30% da população mundial, tendo em conta que a população mundial se cifra atualmente nos 7 0006 biliões de habitantes.²⁷ Para além disso, a tendência expectável é a de que o número de utilizadores aumente significativamente nas próximas décadas, quer em termos absolutos, quer em termos relativos, intensificando este processo de globalização.

Um outro dado interessante está relacionado com a questão das línguas. De facto, para existir uma sociedade em rede globalizada é condição *sine qua non*, mas não suficiente, a difusão de uma tecnologia que permita o contacto e a interação. É também necessário que exista(am) uma ou mais línguas que seja(m) um instrumento transversal de comunicação. Por outras palavras, é necessária uma “língua franca” global, a par de línguas francas regionais, tal como ocorreu, em termos históricos, com o latim no Ocidente medieval europeu. Claro que isto também pode ter um preço a pagar. Esse preço é a progressiva exclusão e irrelevância a que tendem a ser condenadas as línguas que não podem atingir esse estatuto, seja pelo número de falantes nativos ser reduzido, ou por outras razões de tipo geográfico, económico ou cultural. À primeira vista, a internet é uma babel de línguas, e é um também um espaço de liberdade bastante propício à revitalização ou recriação de línguas que não tinham o seu estatuto oficial reconhecido pelos governos, ou estavam tendencialmente “mortas”. Uma das aplicações mais emblemáticas da *World Wide Web* e dos ideais comunitários da rede – a enciclopédia livre Wikipédia, onde coexistem o melhor e o pior em termos de conhecimento humano –, transmite-nos nitidamente essa ideia, ao anunciar ter edições em 276 línguas.²⁸ A questão é

26 Ver Internet World Stats, acessível em <http://www.internetworldstats.com/stats.htm> [Acedido em 12-04-2012].

27 Ver us Census Bureau, acessível em <http://www.census.gov/main/www/popclock.html> [Acedido em 12/04/2012].

28 Número das edições da Wikipédia em diferentes línguas à data de 8 de fevereiro de 2010.

que essa enorme diversidade linguística é, em grande parte, “folclórica”. Para a esmagadora maioria dos utilizadores da rede é irrelevante, quer do ponto de vista do interesse ou curiosidade cultural, quer, sobretudo, do ponto de vista mais pragmático de meio de comunicação. Como já era expectável encontra-se uma primazia do inglês (536,6 milhões de utilizadores nessa língua) – os mais críticos dirão mesmo que a expansão da internet e da globalização favoreceram o “imperialismo cultural” da língua inglesa.

Mas será o modelo de enciclopédia aberta da Wikipédia – com a sua babel de línguas e onde todos podem colaborar –, um sinal de substituição da racionalidade económica capitalista, baseada nos interesses próprios (egoísmo) do indivíduo, por formas mais altruístas e colaborativas? Será este modelo uma alternativa viável à lógica capitalista extremada, de prossecução dos interesses próprios, que está na origem da crise financeira de 2007-2008, iniciada nos EUA, mas com repercussões mundiais? Estará a expansão da “rede galáctica” a abrir caminho a um novo tipo de economia e sociedade menos hierárquica, mais democrática e colaborativa e onde o indivíduo tem maior liberdade? No campo económico-empresarial, Don Tapscott e Anthony Williams (2006, p. 18) sustentam que entrámos numa nova fase – aquilo a que chamam o modelo “Wikinomics” –, na qual “as pessoas participam na economia de uma forma como nunca ocorreu antes”. Inovadoras formas de “colaboração em massa” estão a mudar a maneira como os bens e serviços são inventados, produzidos, comercializados e distribuídos globalmente”. Numa abordagem mais abrangente – no cruzamento de uma reflexão filosófico-político-jurídico-empresarial –, Yochai Benkler, professor da Universidade de Harvard, e um dos diretores do *Berkman Center for Internet and Society* dá respostas afirmativas a essas questões. Na sua mais recente publicação, com o curioso título *The Penguin and the Leviathan (O Pinguim e o Leviatã)*, Benkler (2011), autor e ativista dos ideais tecno-libertários da internet, veio reforçar as suas teses anteriores, divulgadas em 2006 em *The Wealth of Networks*.²⁹ Neste livro, cujo título sugere já a intenção de interagir com o trabalho clássico de Adam Smith, *Riqueza das Nações* de 1776, Benkler defendia as virtudes dos novos modelos de produção colaborativa de “bens não-proprietários”, enquanto no *The Penguin and the*

Ver Wikipédia, http://pt.wikipedia.org/wiki/Wikipedia:Wikip%C3%A9dia_em_outras_l%C3%ADnguas [Acedido em 12/04/2012].

29 Em coerência com os ideais tecno-libertários do próprio autor, bem como das suas teses sobre os bens não-proprietários, este disponibiliza uma versão digital livro *The Wealth of Networks: How Social Production Transforms Markets and Freedom* em http://www.benkler.org/Benkler_Wealth_Of_Networks.pdf. Está também o capítulo 1, na tradução em língua portuguesa, acessível livremente na Wikipédia em http://cyber.law.harvard.edu/wealth_of_networks/A_Riqueza_das_Redes_-_Capítulo_1 [Acedidos em 12-04-2012].

Leviathan, pretendeu por em confronto o que considera ser o antigo “modelo do Leviatã” – uma referência à clássica obra de Thomas Hobbes de 1651³⁰ –, com o novo “modelo do Pinguim” – o símbolo do GNU (General Public License)³¹/Linux³², o sistema operativo de código aberto de maior sucesso na sociedade em rede e economia digital. Desta forma, Benkler procurou rejeitar a ligação entre racionalidade e egoísmo, fortemente enraizada na economia e ciência política. Segundo este, novas formas colaborativas estão crescentemente a afirmar-se, e não só em enciclopédias digitais como a Wikipédia, mas também no universo económico-empresarial – neste aspeto, a sua visão aproxima-se, em parte, do modelo “Wikinomics” de Tapscott. Benkler aponta vários exemplos, entre os quais o da fábrica da *Toyota* na Califórnia e da *Southwest Airlines*. Para este, o facto de tais empresas terem adotado modelos de gestão e processos de produção cooperativos, bem sucedidos, seriam evidências empíricas confirmativas das suas teses. Todavia, a tendência colaborativa é apenas uma entre outras, frequentemente contraditórias, que se detetam na sociedade em rede. A questão é mais complexa e multifaceta do que Benkler, Tapscott e outros entusiastas tecno-libertários pretendem admitir, como veremos em seguida.

SOCIEDADE EM REDE, SOCIEDADE DE RISCO

No âmbito da reflexão sociológica sobre o atual período da humanidade, Ulrich Beck, tal como Anthony Giddens, rotulam o período contemporâneo de “modernização reflexiva”, ou como “segunda modernidade”. A atual fase é vista com um período em que os princípios da modernidade foram levados ao extremo e se radicalizaram. Assim, a primeira modernidade teria sido caracterizada pela confiança no progresso e pela crença na possibilidade de controlo do desenvolvimento científico-tecnológico e da natureza. Por sua vez, a

30 O título da obra de Thomas Hobbes, *Leviathan or The Matter, Forme and Power of a Common Wealth Ecclesiasticall and Civil* (1651), evoca um monstro mitológico dotado de uma força sobrehumana – o Leviatã. Esta foi a metáfora usada para justificar a necessidade do poder do Estado. Hobbes via no chamado “estado de natureza” não só uma situação de máxima liberdade dos indivíduos, como também uma situação de máxima insegurança. O “estado de natureza” era caracterizado pelo conflito, pela anarquia, e pela “guerra de todos contra todos” (*bellum omnium contra omnes*).

31 É a designação da licença para *software* livre concebida por Richard Stallman em 1989, no âmbito do projeto GNU da *Free Software Foundation*.

32 O “Tux” é a mascote oficial do sistema operativo GNU/Linux. Ver *The History of Tux the Linux*, Penguin, Acessível em http://www.sjbaker.org/wiki/index.php?title=The_History_of_Tux_the_Linux_Penguin [Acedido em 04-12-2012].

“modernidade reflexiva” será a fase contemporânea. Nela, o desenvolvimento da ciência e da tecnologia já não permitem prever integralmente os riscos que contribuíram para criar, nem realizar um controlo efetivo dos mesmos. Importa notar que na abordagem original de Beck, o arquétipo do “risco” identificavam-se com questões ecológicas e a sua relação com a tecnologia. A falta de ênfase na sociedade em rede – notória quando comparada com trabalhos como o de Castells – resulta, desde logo, do facto de o conceito de “sociedade de risco” ser anterior à expansão da internet para fora dos meios académico e militar e ao surgimento da sociedade em rede. Recordar-se que o conceito de “sociedade de risco” foi pela primeira vez proposto em 1986³³, em língua alemã, ainda no contexto da político-ideológico da Guerra Fria. Ganhou posteriormente uma ampla difusão, a partir de 1992, com a sua tradução e publicação em língua inglesa, agora já num contexto de pós-Guerra Fria e de globalização em marcha. Mais recentemente, num outro trabalho originalmente publicado em finais dos anos 90, Beck (2002) fazia notar que “à medida que se desvanece o mundo bipolar, passamos de um mundo de inimigos a um mundo de perigos e de riscos”. Sobre o significado de risco, Ulrich Beck clarifica-o da seguinte forma:

Risco é o enfoque moderno da previsão e controlo das consequências futuras da ação humana, das diversas consequências não desejadas da modernidade radicalizada. É uma tentativa (institucionalizada) de colonizar o futuro, um mapa cognitivo. Toda a sociedade, obviamente, experimentou perigos. Todavia, o regime do risco é uma função de ordem nova: não é nacional, mas global. Está intimamente relacionado com o processo administrativo e de decisão. Anteriormente, essas decisões eram tomadas com normas fixas de calculabilidade, ligando meios e fins, causas e efeitos. A “sociedade de risco global” invalidou precisamente essas normas [Beck, 2002, p. 5].

Segundo este autor, tudo isto se tornou muito evidente nas companhias de seguros privadas, provavelmente o “melhor símbolo do cálculo e da segurança alternativa, as quais não cobrem os desastres nucleares, nem as mudanças climáticas e as suas consequências, nem o colapso das economias asiáticas, nem os riscos de baixa probabilidade e graves consequências de diversos tipos de tecnologia futura. De facto, os seguros privados não cobrem a maiorias das tecnologias controversas, como a engenharia genética. Sobre os aspetos novos que esta noção implica acrescenta ainda o seguinte: “o conceito de risco e de sociedade de risco combina o que em tempos se excluía mutuamente:

33 Coincidindo a publicação deste livro com o desastre nuclear de Chernobyl na Ucrânia (na altura integrada na ex-União Soviética), o que provavelmente contribuiu para a sua rápida popularidade.

sociedade e natureza, ciências sociais e ciências da matéria, construção discursiva do risco e materialidade das ameaças” (Beck, 2002, p. 5).

A referida ideia de risco e de sociedade de risco de Beck pode ser aplicada à sociedade em rede, na medida em que esta assenta numa criação tecnológica da modernidade reflexiva. O progresso tecnológico que permitiu a sociedade em rede – com todos os imensos benefícios que daí resultaram –, trouxe consigo uma nova área de risco para as sociedades humanas, consequência paradoxal (inevitável?) do seu sucesso. Para além das possibilidades de extorsão financeira, de vendas fraudulentas, de pornografia infantil, etc. – que cabem no âmbito das infrações legais e/ou criminalidade –, surgiram também possibilidades adicionais de difusão de ideologias políticas radicais e violentas e, aspeto de risco inteiramente novo, uma possibilidade de os conflitos internacionais decorrerem no ciberespaço, em paralelo, ou não, com uma guerra física (cinética). Paradoxalmente, esta nova possibilidade que, num cenário extremo, poderá ser imensamente destrutiva, só se tornou possível pelos avanços tecnológicos da sociedade em rede. Indubitavelmente, estamos perante mais um risco da atual modernidade reflexiva.

A PERDA DE NEUTRALIDADE³⁴ DA REDE E O “LADO NEGRO DA LIBERDADE NA INTERNET”

A internet e a *World Wide Web* estão hoje sujeitas a grandes incógnitas sobre a sua evolução futura. Continuarão a ser espaços de liberdade ligados globalmente, como em grande parte têm sido? Serão definitivamente dominadas por interesses económicos e comerciais? Os Estados afirmarão um crescente controlo sobre a rede e a informação que nela circula? Assistiremos à afirmação de fronteiras no ciberespaço e à “territorialização” nacional do mesmo por razões políticas e de segurança? Estas incógnitas estão hoje bem exemplificadas na encruzilhada com que se confronta a *World Wide Web*, duas décadas depois da sua criação. Num artigo publicado na revista *Wired* com o título provocatório “The web is dead. Long live the internet”, Chris Anderson e Michael Wolff

34 A neutralidade da rede, ou neutralidade da internet, significa que, por princípio, todas as informações que circulam na rede devem ser tratadas da mesma forma, sem interferências ou discriminações dos fornecedores de acesso à internet. Situações típicas de falta de neutralidade ocorrem quando, por razões comerciais, o acesso é deliberadamente limitado ou eliminado por bloqueio (restrição do acesso a determinados serviços ou *sites*) ou pelo estrangulamento (retardamento de certos tipos de tráfego afetando a velocidade e qualidade do acesso) favorecendo determinados *sites* em relação a outros. Note-se que estamos a excetuar desta questão os bloqueios ou restrições de acesso que resultam do cumprimento da legislação criminal pelos fornecedores de acesso à internet (por exemplo, por crimes de pirataria, pornografia infantil, etc.).

(2010) sustentam que o uso da *World Wide Web* já entrou numa fase de declínio. Para estes, o processo irá ainda acentuar-se mais nos próximos anos por um conjunto de razões tecnológicas e ligadas a interesses económicos e comerciais. Todavia, Anderson e Wolff não vêm esta tendência como problemática. Para estes autores, a *web* não é o culminar da revolução digital, mas apenas uma fase datada e em vias de ser ultrapassada:

[...] You've spent the day on the Internet – but not on the Web. And you are not alone. This is not a trivial distinction. Over the past few years, one of the most important shifts in the digital world has been the move from the wide-open Web to semiclosed platforms that use the Internet for transport but not the browser for display. It's driven primarily by the rise of the iPhone model of mobile computing, and it's a world Google can't crawl, one where HTML doesn't rule. And it's the world that consumers are increasingly choosing [Anderson e Wolf, 2010].

Ao que tudo indica, como reação ao artigo da *Wired*, o principal criador da *web*, Tim Berners-Lee (2010), num texto publicado na revista *Scientific American*, sob o título “Long live the web: A call for continued open standards and neutrality”, critica a tendência de fragmentação e de criação de plataformas semifechadas. Um alvo particular das suas críticas foram as redes sociais como o *LinkedIn* ou o *Facebook*, que representam “uma ameaça para a universalidade da rede”. Para Tim Berners-Lee (2010), está a surgir um crescente risco de perda de liberdade na rede. Essa liberdade tem permitido aos utilizadores acederem aos *websites* que desejam sem ficarem presos em “ilhas fragmentadas”. Alguns dos casos de maior sucesso dos últimos anos – como o já referido *Facebook* ou o *iTunes* da Apple –, ameaçam os próprios princípios fundadores da *web*. Este argumenta que estratégias como a utilizada pela *Apple*, com o *iTunes*, não só deixam a informação visível aos utilizadores restrita ao próprio *site*, como levam à formação de “ilhas fragmentadas” de informação. Desta forma, foram criadas barreiras à partilha de informação com o resto da *web*, pelo que a rede tende a “partir-se em pedaços” com prejuízo para o utilizador. Este deixa de poder beneficiar de um “espaço único e universal de informação”:

Several threats to the Web's universality have arisen recently. Cable television companies that sell Internet connectivity are considering whether to limit their Internet users to downloading only the company's mix of entertainment. Social-networking sites present a different kind of problem. Facebook, LinkedIn, Friendster and others typically provide value by capturing information as you enter it [...] Each site is a silo, walled off from the others. Yes, your site's pages are on the Web, but your data are not. You can access a Web page about a list of people you have created in one site, but you cannot send that list,

or items from it, to another site. The isolation occurs because each piece of information does not have a URI [Universal Resource Identifier]. Connections among data exist only within a site. So the more you enter, the more you become locked in. Your social-networking site becomes a central platform – a closed silo of content, and one that does not give you full control over your information in it. The more this kind of architecture gains widespread use, the more the Web becomes fragmented, and the less we enjoy a single, universal information space [Berners-Lee, 2010].

Mas as ameaças que pairam sobre a universalidade e neutralidade da rede não se ficam por aqui. Outro alvo de críticas do fundador da *web* são as empresas fornecedoras de acesso *wireless* à rede. Este denuncia a tendência discriminatória que se verifica em alguns fornecedores desse serviço, de baixar, deliberadamente, a velocidade de acesso a certos *websites*, em detrimento de outros (normalmente aqueles com os quais não foram feitos acordos). Naturalmente que tudo isto acaba por prejudicar os utilizadores e por limitar a sua liberdade de navegação na rede. Atente-se neste excerto do referido artigo:

Net neutrality maintains that if I have paid for an Internet connection at a certain quality, say, 300 Mbps, and you have paid for that quality, then our communications should take place at that quality. Protecting this concept would prevent a big ISP from sending you video from a media company it may own at 300 mbps but sending video from a competing media company at a slower rate. That amounts to commercial discrimination. Other complications could arise. What if your ISP made it easier for you to connect to a particular online shoe store and harder to reach others? That would be powerful control. What if the ISP made it difficult for you to go to Web sites about certain political parties, or religions, or sites about evolution? [Berners-Lee, 2010]

A propósito desta última questão, a da liberdade e privacidade na rede, Tim Berners-Lee mostrou ainda uma outra preocupação. Segundo este autor, há uma tendência dos governos, a qual não ocorre apenas nos Estados autoritários, de vigiar os hábitos dos seus cidadãos *online*. Tais mecanismos de controlo e vigilância dos Estados poderão ser considerado uma violação dos direitos inerentes ao ser humano na era da sociedade em rede – daí este falar na necessidade premente de defesa dos novos “direitos humanos eletrónicos”.

Num outro plano, mas incidindo também sobre a questão da liberdade e direitos humanos, uma denúncia cáustica do otimismo libertário da internet/*web* – nomeadamente quanto à convicção desta ser um meio “imparrável” de empoderamento do indivíduo e de difusão da democracia –, foi efetuada recentemente por Evgeny Morozov (2011). No seu livro *The Net Delusion. The Dark Side of Internet Freedom*, este académico e ativista dos

direitos humanos traçou um retrato bastante pessimista sobre o impacto da internet na difusão da liberdade e democracia a nível mundial. Nele mostrou, por exemplo, grande ceticismo quanto ao papel que o *Twitter* e outras redes sociais terão tido nos protestos no Irão em 2009, na altura da reeleição, vista como fraudulenta, de Mahmoud Ahmadinejad. Na sua opinião, esse impacto foi largamente sobrestimado pelos *media* e políticos ocidentais (um contra-argumento poderia ser, eventualmente, o do papel desempenhado pelas redes sociais no desencadear da chamada “Primavera Árabe”, durante o ano de 2011. Todavia, embora a questão não seja abordada no livro, dado ser anterior à eclosão destas revoltas populares, Morozov rejeitou também o seu papel determinante³⁵). Segundo este (Morozov, 2011, p. ix), não é por acaso que há uma crescente difusão de expressões como “recessão da liberdade”, saídas “do uso restrito dos *think-tank* para utilização corrente na linguagem pública”. Muitos decisores políticos começaram também a admitir que o “Consenso de Washington – esse conjunto de políticas dúbias, o qual, no passado, prometeu um paraíso neoliberal com grandes descontos –, foi substituído pelo Consenso de Pequim”. Este novo consenso, vangloria-se agora de “uma rápida-e-suja prosperidade sem ter de se maçar com essas incómodas instituições da democracia”. Como se chegou a esta situação que ainda há duas décadas atrás poucos achariam provável ocorrer? Para Morozov, a explicação passa, em primeira linha, pelo facto de o Ocidente ter vivido sobre os louros do final da Guerra-Fria. A partir daí, adotou uma abordagem laxista subestimando, largamente, a capacidade de os regimes autoritários se adaptarem ao mundo globalizado e à nova realidade da sociedade em rede. Estes, hoje, são de uma variedade e sofisticação muito diferente do passado. “Combinam autoritarismo com hedonismo e criaram um ambiente amigável ao consumo” e favorável aos negócios (Morozov, 2011, p. ix). Depois, há paradoxalmente os efeitos negativos da internet/web e da sociedade em rede, ou seja, um “lado negro” tipicamente subavaliado. Muitos decisores políticos entusiasmaram-se com o que este designou, de forma irónica, por “doutrina Google” – a “convicção entusiástica do poder libertador da tecnologia acompanhada pela vontade irresistível de alistar as *start-ups* de Silicon Valley na luta global pela liberdade” (Morozov, 2011, p. xiii). Morozov criticou essa convicção como um ciberutopismo, uma “crença ingénua na natureza emancipatória da comunicação *online*” (Morozov, 2011, p. xiii). Para este, tais convicções ciberutópicas deram origem a um “internetocentrismo” –

35 Ver Evgeny Morozov, “Facebook and Twitter are just places revolutionaries go” in *The Guardian* (07-03-2011), acessível em <http://www.guardian.co.uk/commentisfree/2011/mar/07/facebook-twitter-revolutionaries-cyber-utopians> [Acedido em 12-04-2012].

o qual constitui, nas suas palavras cáusticas, uma “droga altamente desorientadora”: leva a “ignorar o contexto e aprisiona os decisores políticos na crença de que têm um aliado útil e poderoso do seu lado” (Morozov, 2011, p. xvi).

ENTRE A “TRANSPARÊNCIA” NA POLÍTICA E A CIBERGUERRA: O CASO WIKILEAKS

Uma das facetas em que se prolongou a visão tecno-libertária para a atualidade foi a de que a internet poderia contribuir para criar uma nova era de “transparência” na política. Parece, pelo menos, ter sido essa a convicção/missão de Julian Assange, o carismático fundador do *site* *WikiLeaks*. Esta encontra-se plasmada no seu *slogan* “*help WikiLeaks keep the governments open*”. Mas o mundo dos *hackers* imbuídos da visão tecno-libertária foi só “uma parte do solo onde Julian Assange e o *WikiLeaks* cresceram” (Leigh e Harding, 2011, p. 56). A outra parte foram “os radicais anticapitalistas, a comunidade dos ativistas do ambiente, dos direitos humanos e dos revolucionários políticos designados, nos anos sessenta, como contracultura” (Leigh e Harding, 2011, p. 56). Tal como o nome sugere, o *WikiLeaks* começou por ser concebido como um projeto *wiki*, quer dizer, baseado na ideia de *site* editado pelos utilizadores – neste caso seriam uma espécie de “cidadãos jornalistas”. Mas Julian Assange e os seus colegas rapidamente se aperceberam de que o conteúdo dos materiais colocados – e a necessidade de remover a informação perigosa ou incriminadora –, tornavam esse modelo inviável (Leigh e Harding, p. 52). Em seu lugar, e para garantir a confidencialidade e a não identificação (anonimato) das fontes por meio de sistemas de vigilância na rede, foi usado um *software* que resultou do projeto TOR (“*The Onion Router*”) – ironicamente com origem militar.³⁶

Face ao perfil dos fundadores e objetivos do *Wikileaks*, não é surpreendente que as revelações de ficheiros diplomáticos tenham afetado sobretudo os EUA, como principal potência hegemónica, em termos político-económico-militares. Para uma parte significativa da opinião pública mundial, a revelação dos bastidores da sua diplomacia, dominado por manobras obscuras e entendimentos oportunistas, apenas terá vindo reforçar a convicção da perfídia³⁷ da política externa norte-americana – vista como largamente amoral, apesar do

36 Tratou-se de um projeto originalmente desenvolvido em 1995 nos meios militares, pelo *us Naval Research Laboratory* – o laboratório de pesquisa da marinha norte-americana –, o qual acabou por ser objeto de apropriação por diversos *hackers*.

37 Alguns veem mesmo aí argumentos adicionais para sustentar teorias da conspiração sobre a atuação dos EUA em acontecimentos marcantes da história do século xx e início do século xxi (o ataque japonês a Pearl Harbour, o assassinato de John F. Kennedy, o 11 de setembro, etc.).

discurso oficial em torno de princípios, valores e questões como a democracia e os direitos humanos. No entanto, passado o furor inicial sobre as revelações pelos *media* dos ficheiros *Wikileaks*, provavelmente o impacto mais duradouro do caso será ao nível das questões de segurança da rede e da confidencialidade da informação “sensível”, diplomática e não diplomática. A forma relativamente simples como se admite que as informações reveladas pelo *WikiLeaks* poderão ter sido obtidas, levanta muitas interrogações.³⁸ Embora a origem não seja oficialmente conhecida, as centenas de milhares de telegramas diplomáticos revelados em finais de 2010, poderão ter sido obtidos/subtraídos de forma similar à que terá sido efetuada pelo jovem militar Bradley Manning – detido sob acusação de ter sido responsável pelas revelações anteriores de documentos feitas pelo *Wikileaks* relativos às guerras do Afeganistão e do Iraque.

Importa aqui analisar a reação ocorrida na rede face às tentativas de impedir a divulgação dos telegramas diplomáticos, nomeadamente pelo governo dos EUA. Estas envolveram quer pressões políticas, quer ciberataques ao *site* do *WikiLeaks* de modo a tentar torná-lo inoperacional, quer ainda a pressões sobre as empresas onde o alojamento estava efetuado e sobre as empresas que lhe permitiam efetuar transações financeiras, ou seja, receber donativos para o seu funcionamento. Em retaliação, um grupo conhecido como *Anonymous*, que agregará, informalmente, cerca de um milhar de *hackers* “ativistas”, lançou um conjunto de ataques coordenados de negação distribuída de serviço (DDOS) aos *sites* das empresas *Mastercard*, *Visa* e *Paypal*. O motivo invocado foi essas empresas terem deixado de fornecer os seus serviços ao *WikiLeaks* – cedendo, assim, à pressão do governo dos EUA –, e impedindo-o de receber donativos de suporte ao seu funcionamento. Esses ciberataques, conhecidos como *Operation Payback*, deixaram temporariamente os respetivos *sites* inacessíveis ou extremamente lentos nas suas operações. Alvo de ataques similares foi também a *Amazon.com*, a qual passou a recusar o alojamento nos seus servidores ao *WikiLeaks*, devido a idênticas pressões governamentais.

Poderão tais ciberataques ser considerados atos de ciberguerra, como frequentemente foram retratados nos *media*? Em rigor conceptual não podem. Embora o aprofundamento desta questão ultrapasse o âmbito deste artigo, impõem-se algumas considerações sucintas. O termo “ciberguerra” só recentemente é objeto de um uso generalizado, todavia este data dos primórdios da

38 Assim, pelo menos nos tempos mais próximos, este “vazamento de informações” na praça pública irá dificultar muito o trabalho dos diplomatas norte-americanos no terreno. Face a esta quebra de confiança na capacidade de sigilo diplomático da principal potência mundial, a recolha de informações confidenciais tornou-se certamente mais difícil. Este é um “dano colateral” bastante difícil de reparar.

sociedade em rede. Surgiu originalmente em 1993, nos meios militares e de segurança ligados à Rand Corporation, por John Arquilla e David Ronfeldt (2002 e 2003 [1993]). Nessa altura, apesar do interesse suscitado, foi essencialmente visto como especulativo e futurista. Todavia, nos últimos anos, com a internet e a *web* a entrarem numa fase de maturidade, a percepção mudou. Provavelmente isso resultou, em grande parte, dos conflitos da Estónia (2007) e da Geórgia (2008) com a Rússia terem tido um campo de batalha paralelo na rede. Mais recentemente, em finais de 2010, o caso do vírus Stuxnet que afetou o programa nuclear iraniano, deu ainda mais plausibilidade a um cenário de ciberguerra. Entre os múltiplos livros e artigos recentemente produzidos sobre este assunto destaca-se o relatório elaborado para a OCDE³⁹ no âmbito do projeto “choques globais no futuro” intitulado “Reduzindo o risco sistémico da cibersegurança” (Sommer e Brown, 2011). Os seus autores procuraram avaliar o risco no mundo atual e no devir que é descortinável. Como estes explicam, no âmbito do pensamento sobre segurança e estratégia⁴⁰, o termo ciberguerra designa frequente “uma guerra conduzida substancialmente no ciberespaço ou no domínio virtual” (Sommer e Brown, 2011, p. 13). Esta conceção tem normalmente subjacente a ideia de que “as ciber guerras tendem a ser muito similares às guerras convencionais” (*idem*, 2011, p. 13) pelo que idênticas doutrinas de retaliação ou dissuasão poderão ser aplicadas. Em termos de legalidade internacional, Sommer e Brown sustentam que ciberguerra deverá se definida, tanto quanto possível, nos termos utilizados para uma guerra convencional ou “cinética”. Desde logo, será fundamental ter em conta as disposições atualmente contidas nos tratados internacionais.⁴¹ Para se decidir se um ato pode ser qualificado como (ciber)guerra, deverá submeter-se ao teste de verificar se é equivalente a um ataque convencional de guerra no seu objetivo, intensidade e duração.⁴²

39 Organização para a Cooperação e o Desenvolvimento Económico.

40 Um definição na perspetiva de segurança e estratégia de ciberguerra é dada pelo *Institute for Advanced Study of Information Warfare* dos EUA. Este instituto define-a como “o uso ofensivo e defensivo da informação e dos sistemas de informação para negar, explorar, corromper, ou destruir a informação de um adversário, processos baseados na informação, sistemas de informação e redes baseadas em computadores, enquanto se protegem as próprias. Tais ações são projetadas para atingir vantagens sobre adversários militares” (cit. in Sinks, 2008, p. 5).

41 Nomeadamente as convenções de Haia de 1899 e 1907, a Carta das Nações Unidas de 1945, a Convenção das Nações Unidas de 1948 sobre o genocídio e a Convenção das Nações Unidas de 1980 sobre armas convencionais excessivamente lesivas (ou cujos efeitos são indiscriminados) – ou seja, o normativo que integra o direito dos conflitos armados/direito internacional humanitário.

42 Para Sommer e Brown (2011, p. 13) há ainda “uma distinção a fazer entre atos que procuram atingir alvos militares e atos destinados a alvos civis”. Estes fazem notar que a “Carta →

Voltando ao caso dos cibertiques desencadeados em apoio ao *WikiLeaks*, o que se verifica é que estes se inserem na tendência para o uso livre do termo “ciberguerra” pelos *media*. Estes tendem a usar a palavra sempre que ocorre um ataque mais espetacular na rede envolvendo tipicamente *hackers*. No caso *WikiLeaks*, o que podemos constatar é que os cibertiques à *Mastercard*, *Visa*, *Paypal* e *Amazon.com* tiveram uma motivação que podemos considerar política e de protesto. Uma discussão sobre essa motivação política é efetuada por David Barnard-Wills (2011). Similar posição é sustentada por Yochai Benkler (2012), num recente artigo na *Foreign Affairs*, em reação a declarações do chefe do cibercomando dos EUA, o general Keith Alexander. Este apresentava o *Anonymous* – e o seu sub-produto, o *LulzSec* –, como ameaças à segurança nacional dos EUA, sugerindo que, num espaço de um ou dois anos, poderiam ter a capacidade de, através de um cibertaque, provocar uma corte, ainda que limitado, de energia elétrica. Para Benkler (2012), ver tais grupos “primeiramente como uma ameaça à cibersegurança” é uma “abordagem errada”. Segundo Benkler, estamos, sobretudo, perante algo mais parecido com os grupos/movimentos de protesto e a contracultura da década de 60. Assim, o que *Anonymous* e o *LulzSec* essencialmente têm feito, através de cibertiques, é contestar aquilo que “percepcionam como um abuso de poder dos governos e das empresas e promover a transparência na política e nos negócios”.

Para além dos argumentos de Barnard-Wills e de Benkler, sobre o carácter de protesto social e político dos cibertiques, importa notar que nenhuma das entidades envolvidas foi um ator estadual, sendo este, em princípio, um requisito necessário para a qualificação legal como ato de guerra. Não há, também, tanto quanto se sabe, provas ou indícios de atuação com a conivência, ativa ou passiva, de atores estaduais. Tudo isto reforça a ideia da desadequação da qualificação como ciberguerra⁴³, excetuado, claro, no sentido metafórico do termo. É necessário ainda ter em conta que os cibertiques em causa – recorrendo, sobretudo, à técnica de negação distribuída de serviço –, não utilizaram uma tecnologia particularmente sofisticada, nem provocaram danos, em termos materiais e físicos, comparáveis aos de uma guerra cinética. Tudo isto sugere, conforme já referimos, que estamos num plano mais comparável a uma manifestação política de protesto. Algo similar, por exemplo, a uma manifestação de rua contra empresas financeiras, numa situação em que alguns ativistas

→ das Nações Unidas requer uma justificação para a adoção de contra-medidas por aqueles que afirmam ter sido atacados. No essencial, a vítima deve ser capaz de produzir provas fidedignas sobre quem a atacou (algo nem sempre fácil no ciber mundo) e sobre os efeitos dos ataques.

43 Note-se que, por si só, o facto de não estarmos perante atores estaduais não significa de forma decisiva que estes possam ser mobilizados e atuar sob “procuração” de um Estado.

procuram impedir que estas abram as suas portas e os seus empregados trabalhem normalmente.

Por último, o facto do caso *WikiLeaks* não ter consubstanciado uma ciber guerra não afasta, naturalmente, a possibilidade da sua ocorrência. Uma rápida pesquisa sobre a literatura de segurança e estratégico-militar mostra até como a percepção dominante é a de que o risco tem vindo a aumentar. O caso mais recente dessa tendência é a NATO onde, no novo documento estratégico da organização, foi dado um especial destaque às ameaças à segurança na rede e aos ciberataques.⁴⁴ Independentemente da avaliação que se possa fazer desta tendência, é um facto que a revolução tecnológica e digital em curso está, indubitavelmente, a transformar a economia, a sociedade, e a maneira de fazer a guerra. Tanto quanto é possível avaliar hoje, a tendência é para que o chamado “ciberespaço” – entendido como a rede global de infraestruturas de tecnologias de informação interligadas entre si, especialmente as redes de telecomunicações e os sistemas de processamento dos computadores –, abra uma nova dimensão dos conflitos internacionais (Fernandes, 2012). Apesar das dificuldades em antecipar as consequências de uma ciber guerra, é de recear que estas possam ser bem negativas para o funcionamento das atuais sociedades complexas, cada vez mais dependentes das redes informáticas e de comunicação.

CONCLUSÕES

O progresso científico-tecnológico que permitiu a sociedade em rede trouxe consigo uma nova área de risco para as sociedades humanas, consequência paradoxal, e talvez inevitável, do seu próprio sucesso. A ideia de sociedade de risco de Beck capta bem essa realidade na atual sociedade em rede. Assim, é inequívoco estarmos perante mais um risco da modernidade reflexiva, o qual acresce ao catálogo de outros já bem conhecidos e diagnosticados, como o risco ecológico. Olhando retrospectivamente, é fácil constatar que nos criadores da internet e nos teorizadores dos primeiros tempos da sociedade em rede, o otimismo era a nota dominante, como se verifica na teorização dos anos 90 de Castells. Todavia, a utopia da sociedade em rede tornou-se uma realidade,

44 Nesse documento afirma-se que “os ciberataques estão a tornar-se cada vez mais frequentes, mais organizados e mais dispendiosos nos danos que infligem às administrações governamentais, empresas, economias e, potencialmente, também, às redes de transporte e abastecimento e outras infraestruturas; estes podem chegar a um limite que ameaça a prosperidade nacional e a prosperidade, segurança e estabilidade euro-atlântica. Ver NATO, *Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation (Adopted by Heads of State and Government in Lisbon, 2010)*, acessível em <http://www.nato.int> [Acedido a 04-04-2012].

mas não exatamente como os ideais tecno-libertários julgavam ser possível. Em parte isto ocorreu porque o mundo económico-empresarial se apropriou desta, submetendo-a às regras do mercado e da produção capitalista, ou seja, subvertendo o ideal comunitário de partilha e de colaboração numa base não lucrativa. Em parte ocorreu também porque a internet e a *web* se tornaram um espaço que mimetiza a complexidade da natureza humana.

Na atual sociedade em rede constata-se tendências contraditórias que tornam difícil discernir a sua evolução futura. Estas contradições estão bem refletidas na atual abordagem teórica. Por um lado, existe a tendência colaborativa em massa da “*wikinomics*”, dos bens “não-proprietários” e do modelo do “Pinguim” (Benkler, 2011), da nova era de “transparência” na política (Assange/WikiLeaks). Este aspeto é enfatizado por todos aqueles que continuam a discernir um futuro transformado pelos ideais tecno-libertários. Por outro lado, os riscos que afetam a sociedade em rede estão a ser objeto de crescente preocupação, nomeadamente quanto à possibilidade de perda de neutralidade da internet/*web* e da criação de “ilhas fragmentadas” (Berners-Lee, 1990 e 2010). O ciberutopismo e o “internetocentrismo” dos *media* e políticos ocidentais é corresponsabilizado pelo estado deplorável da liberdade e da democracia no mundo, ao subestimar a capacidade de os regimes autoritários se adaptarem à sociedade em rede (Morozov, 2011). Num outro plano, está ainda a crescente preocupação com a possibilidade de uma ciberguerra (Sommer e Brown, 2011; Clark e Knake, 2010), um risco que tem vindo a aumentar, pela crescente dependência da economia e da sociedade das redes informáticas e de telecomunicações. Independentemente dos benefícios, e de qual seja o futuro da sociedade em rede, tornou-se claro que esta já não se encontra na idade da inocência. Agora é também uma nova área de risco para as sociedades humanas.

BIBLIOGRAFIA

- ANDERSON, C., WOLFF, M. (2010), "The web is dead. Long live the internet". *Wired*, setembro, disponível em http://www.wired.com/magazine/2010/08/ff_webrip/all/1 [Acedido a 04-04-2012].
- ARQUILLA, J., RONFELDT, D. (2002), *Networks and Netwars: The Future of Terror, Crime, and Militancy*, Santa Monica, CA, Rand Corp.
- ARQUILLA, J., RONFELDT, D. (2003 [1993]), "Cyberwar is coming!". *Comparative Strategy*, 12 (2), pp. 141-165.
- BARNARD-WILLS, D. (2011), "'This is not a cyberwar, it's a...?': Wikileaks, anonymous and the politics of hegemony". *International Journal of Cyber Warfare and Terrorism*, 1 (1), pp. 13-23.
- BECK, U. (1992), *Risk Society: Towards a New Modernity*, Londres, Sage Publications.
- BECK, U. (2002), *La Sociedad del Riesgo Global*, trad. esp., Madrid, Siglo XXI.
- BENKLER, Y. (2006), *The Wealth of Networks: How Social Production Transforms Markets and Freedom*, New Haven, Yale University Press.
- BENKLER, Y. (2011), *The Penguin and the Leviathan: The Triumph of Cooperation Over Self-Interest*, Nova Iorque, Crown Business.
- BENKLER, Y. (2012), "Hacks of valor. Why anonymous is not a threat to national security". *Foreign Affairs*, disponível em <http://www.foreignaffairs.com/articles/137382/yochai-benkler/hacks-of-valor> [Acedido a 12-04-2012].
- BERNERS-LEE, T. (1990), *World Wide Web: Proposal for a HyperText Project*, disponível em <http://www.w3.org/Proposal.html> [Acedido a 04-04-2012].
- BERNERS-LEE, T. (2010), "Long live the web: A call for continued open standards and neutrality". *Scientific American*, disponível em <http://www.scientificamerican.com/article.cfm?id=long-live-the-web> [Acedido a 04-04-2012].
- CASTELLS, M. (1999), *A Era da Informação: Economia, Sociedade e Cultura*, vol. III, São Paulo, Paz e Terra.
- CASTELLS, M. (2002), *A Sociedade em Rede*, vol. I, Lisboa, Fundação Calouste Gulbenkian.
- CASTELLS, M. (2004), *A Galáxia Internet: Reflexões sobre Internet, Negócios e Sociedade*, Lisboa, Fundação Calouste Gulbenkian.
- CASTELLS, M. (2007), "Communication, power and counter-power in the network society". *International Journal of Communication*, 1, pp. 238-266.
- CASTELLS, M. (2009), *Communication and Power*, Oxford, Oxford University Press.
- CASTELLS, M., CARDOSO, G. [ed.] (2005), *The Network Society: From Knowledge to Policy*, Washington, Center for Transatlantic Relations-Johns Hopkins University.
- CLARK, R. A., KNAKE, R. K. (2010), *Cyber War. The Next Threat to National Security*, Nova Iorque, Harper Collins.
- DIAS, J. S., CORREIA, V. (1999), "Economia mundial - 'sociedades em rede', 'economia digital' ou 'nova economia?'". *Informação Internacional. Análise Económica e Política*, 2, pp. 97-122. Disponível em <http://www.dpp.pt/pt/pesquisa/Paginas/DetailArticle.aspx?contentId=3126> [Acedido a 12-04-2012].
- DOMSCHEIT-BERG, D. (2011), *Inside WikiLeaks. My Time With Julian Assange at the World's Most Dangerous Website*, trad. ing., Nova Iorque, Crown Publishing.
- FERNANDES, J.P.T. (2012), "A ciberguerra como nova dimensão dos conflitos internacionais". *R:I*, 33 (março), pp. 53-69.

- HASSAN, R. (2008), *The Information Society: Cyber Dreams and Digital Nightmares*, Cambridge, Polity Press.
- INTERNET SOCIETY (2010), *A Brief History of the Internet*. Disponível em <http://www.isoc.org/internet/history/brief.shtml> [Acedido a 12-04-2012].
- INTERNET WORLD STATS (2011), *Usage and Population Statistics*. Disponível em <http://www.internetworldstats.com/> [Acedido a 12-04-2012].
- LEIGH, D., HARDING, L. (2011), *WikiLeaks: Inside Julian Assange's War on Secrecy*, Londres, Guardian Books.
- LIBICKI, M. (2009), *Cyberdeterrence and Cyberwar*, Santa Monica, CA, Rand Corp.
- MOROZOV, E. (2011), *The Net Delusion. The Dark Side of Internet Freedom*, Nova Iorque, Public Affairs.
- SCHILLER, B. (2011), "Cybersecurity: politics, interests, choices". *OpenDemocracy*, disponível em <http://www.opendemocracy.net/ben-schiller/cybersecurity-politics-interests-choices> [Acedido a 12-04-2012].
- SINKS, M. A. (2008), *Cyber Warfare and International Law*. Research Report Submitted to the Faculty in Partial Fulfillment of the Graduation Requirements, Air Command and Staff College/Air University, Maxwell, AL.
- SOMMER, P., BROWN, I. (2011), *Reducing Systemic Cybersecurity Risk* (project on "Future Global Shocks"), Paris, OECD/IFP-International Future Program Department, disponível em <http://www.oecd.org/dataoecd/3/42/46894657.pdf> [Acedido a 12-04-2012].
- TAPSCOTT, D. (1997), *The Digital Economy: Promise and Peril In The Age of Networked Intelligence*, Nova Iorque, McGraw-Hill.
- TAPSCOTT, D., WILLIAMS, A. D. (2006), *Wikinomics. Como a Colaboração em Massa pode Mudar o seu Negócio*, trad. port., Rio de Janeiro, Nova Fronteira.
- TURNER, F. (2008), *From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism*, Chicago, Chicago University Press.

Recebido a 29-08-2011. Aceite para publicação a 31-07-2012.

FERNANDES, J. P. (2013), "Da utopia da sociedade em rede à realidade da sociedade de risco". *Análise Social*, 207, XLVIII (2.º), pp. 260-286.