MEDIA, CIDADANIA, BIG DATA

FRANCISCO RUI CÁDIMA
FACULDADE DE CIÊNCIAS SOCIAIS E HUMANAS / UNIVERSIDADE NOVA DE LISBOA

"Depois de Snowden, ninguém está certo quanto ao que realmente acontece com esses dados e quanto às inúmeras maneiras pelas quais eles podem ser alvo de abusos"
Evgeny Morozov

Públicos e organizações no novo contexto digital: no quadro de uma cidadania activa, participativa, os primeiros procuram gerir e proteger (ou desproteger) os seus próprios dados, enquanto os segundos, num contexto de mercado, entendem-nos como matéria de tratamento algorítmico, transformando o cidadão em sujeito/target estatístico. As grandes organizações têm, inclusive, um comportamento dual: blindam os seus dados e procuram canibalizar os demais. Tratando-se das grandes plataformas digitais (Google, Facebook, etc.) e de entidades de segurança nacional (NSA), o nível de armazenamento de dados e o grau de captura e interacção entre ambas assume características secretistas algo dramáticas, perdendo aqui o cidadão qualquer controlo sobre a sua privacidade e a sua "pegada digital".

Tanto no primeiro como no segundo caso, estamos perante a anulação da prerrogativa de protecção de dados pessoais, primeiro com um efeito de mercado e consumo, depois com um efeito cívico e político. Mas em qualquer das situações, do que se trata genericamente é, por um lado, de uma progressiva elisão, de um apagamento do cidadão, e, por outro, de uma cada vez mais crítica presença de um "algorithmic turn" nas estratégias das organizações, tornando-as reféns do chamado Big Data e dos seus limites. O que, inevitavelmente, vem reforçar os alertas não só sobre a volubilidade e uma potencialmente crítica "despersonificação" do consumidor, como, finalmente, sobre a actual crise mais global da própria experiência democrática.

Tendo como um dos focos principais desta reflexão a questão da vigilância na era digital, começaríamos por constatar algo muito liminar: a Internet está, por assim dizer, dividida em duas grandes categorias de utilizadores – os que não querem

saber das questões da sua própria privacidade (e muito menos da dos outros), e os que consideram que essa é uma espécie de "pecado mortal" da rede, e que, por conseguinte, esta deve ser, de alguma forma, regulada nesse âmbito.

Naturalmente, esta é uma questão que tem vindo a ganhar uma certa notoriedade na era pós-Wikileaks. Mas ganhou uma outra dimensão com as "disclosures" de Edward Snowden – e tudo o que ficámos a saber sobre a NSA.

Na era pós-Snowden ficou a saber-se que existe na agência norte-americana NSA um programa com o acrónimo PRISM que tem como objectivo recolher de forma regular e massiva todo o tipo de informações privadas e metadados das grandes plataformas digitais do Facebook, da Google, Microsoft, Apple, Skype, etc...

Numa entrevista dada ao The Guardian – "I, spy: Edward Snowden in exile" [1], Snowden alertava para os "palheiros" de dados e para a frágil auditoria dos sistemas e dos seus analistas por parte da própria NSA e referia que o mais importante são os metadados (que é a informação sobre localização, contactos, pegada digital das pessoas, etc.). Curiosamente, Snowden parecia dar mais atenção às fragilidades que cada vez mais o campo do jornalismo enfrenta, do que à perda de privacidade por parte dos utilizadores e dos cidadãos em geral.

Ele próprio, aliás, afirma na entrevista que fazer hoje jornalismo "é incomensuravelmente mais difícil"… Pelo que está a apostar num projecto no quadro da liberdade de imprensa, criando uma ferramenta específica para os jornalistas poderem comunicar em segurança:

> *Os jornalistas têm de estar particularmente atentos a qualquer tipo de sinalização de rede; qualquer tipo de conexão; qualquer tipo de dispositivo de leitura de matrículas por onde passem quando se dirigem a um ponto de encontro; qualquer lugar onde usem o seu cartão de crédito; qualquer lugar onde levem o seu telemóvel; qualquer e-mail que troquem com uma fonte. – dizia Snowden.*

Para além disso, não deixa de ser bastante significativo, que nos primeiros contactos de Snowden com Greenwald (ainda Greenwald não conhecia a verdadeira identidade de quem o procurava), o ex-funcionário da NSA tenha feito um vídeo de 10 minutos com o título "PGP para jornalistas", isto é, um pequeno manual sobre

1 Entrevista dada aos jornalistas Alan Rusbridger and Ewen MacAskill e publicada no The Guardian a 19 de Julho de 2014, cf. http://www.theguardian.com/world/2014/jul/18/-sp-edward-snowden-interview-rusbridger-macaskill. Publicada no Expresso – Revista, a 2 de Agosto de 2014, sob o título "Levo uma vida bastante livre, não ando por aí disfarçado".

o *software* de encriptação Pretty Good Privacy, cujo objectivo era permitir que Greenwald pudesse não só aceder à informação que Snowden tinha para lhe enviar, como ainda que o jornalista pudesse utilizar *e-mail*, por exemplo, de forma segura.

Numa situação de escrutínio da coisa pública ou de denúncia de um acto grave cometido por uma administração pública ou por uma empresa, a protecção do *whistleblower* – o seu anonimato – é, portanto, fundamental, quer utilize uma plataforma específica para o efeito, quer ceda as suas informações aos *media*, ou a um jornalista, passando, neste último caso, a ser considerado uma "fonte" – o que, de um modo geral, lhe confere prerrogativas específicas…

Dada a cada vez maior falta de confiança nos sistemas de *media* tradicionais, a criação de plataformas intermédias entre fontes e meios de comunicação, que se pretendem substituir de certa maneira à própria esfera do jornalismo e dos seus constrangimentos, tem sido algo evidente, sobretudo a partir da criação da WikiLeaks, OpenLeaks, entre outras e agora da plataforma referida por Edward Snowden.

Quando chegamos a este nível mais avançado, isto é, quando estamos perante *disclosures* como as de Julian Assange ou de Edward Snowden, a questão que se coloca é se a violação de segurança de um determinado sistema público, militar ou de Estado – pode ou não – deve ou não – ser considerado uma espécie de "hacktivismo ético", ou, pelo contrário, ser considerado um crime contra a segurança do Estado…

A resposta tem, pelo menos, duas faces: a dos tribunais, que chegarão às suas conclusões, e a da opinião pública. Esta, sendo óbvio que se divide por múltiplas visões do problema, terá, de um modo geral, um alinhamento comum – o do reconhecimento da utilidade "pública" de uma *disclosure*, mesmo quando a própria opinião pública é a última a saber… Mas, de qualquer modo, a primeira a ter interesse em sabê-lo…

Veja-se um pouco mais em pormenor o caso Snowden, fundamentalmente a partir da perspectiva de Glenn Greenwald, no seu já citado livro *Snowden sem esconderijo*. Diz-nos Greenwald que há uma diferença crucial entre vigiar a Net respeitando o quadro constitucional e o princípio jurídico, e vigiar a pretexto da segurança do Estado e à revelia do seu próprio quadro normativo específico. No caso dos EUA, e concretamente em relação às práticas da Agência Nacional de Segurança – NSA, a questão está em saber se a vigilância do cidadão é ou não feita através de mandado judicial e qual, então, o verdadeiro valor da privacidade na era digital tendo em atenção a protecção que a própria Quarta Emenda constitucional assegura.

Isto é, a referida emenda proíbe não somente a busca e apreensão sem motivo razoável ou indício de culpabilidade, como obriga a que haja mandado judicial, sendo que se aplica sempre a regra de exclusão, ou seja, uma prova obtida mediante

violação à Quarta Emenda não é aceite pelo tribunal. No caso dos EUA há, no entanto, uma *nuance* não negligenciável: a existência, ainda que secreta também, de um tribunal específico no quadro do Foreign Intelligence Surveillance Act (FISA), que concede autorização para escutas e vigilância electrónica de comunicações de estrangeiros – e o Patriot Act de 2001 que alarga essa possibilidade aos próprios cidadãos nacionais (em todo o caso, relativamente a estes, supor-se-ia sempre com mandato judicial).

Com este pano de fundo, melhor se percebe a argumentação dos defensores dos *whistleblowers* (dos denunciantes), sobretudo quando os mesmos sistemas de "varrimento" de tráfego da Web e as mesmas práticas de vigilância emergiram e emergem de forma indiscriminada, na Líbia de Kadhafi, na China, em 2014, ou nos EUA de Obama… Quer dizer, neste início da era digital, em matéria de vigilância das comunicações, as administrações detêm hoje sistemas e *softwares* ultrassofisticados, muito idênticos nos diferentes casos, e tornaram-se todas, de alguma maneira, secretistas e policiais, desrespeitando a transparência e a prática da democracia.

Isso constitui de facto um problema para a actual ordem democrática. Como bem assinalou Evgeny Morozov[2] as revelações de Snowden apontam para uma ameaça emergente (ainda não reconhecida) ao espírito da democracia, que só irá agravar-se à medida que os meios de coleta, registo e análise de um cada vez maior volume de dados se tornam mais ubíquos.

Há então que encontrar um paradigma alternativo, uma espécie de "agenda de decrescimento", para este contexto, paralelo a um progressivo declínio de participação cívica no sistema político. Para Morozov, uma crença ingênua em serviços de big data reduz os espaços que antes estavam abertos à deliberação pública, e conclui:

> *O problema que enfrentamos não é o de falta de controle sobre dados individuais; é o fato de que, armados com tantos dados, os sistemas políticos modernos parecem acreditar que é possível dispensar os cidadãos – enquanto os cidadãos, desfrutando da cornucópia do 'conteúdo', não hesitam em abandonar o reino político.*

Face ao pouco escrutável poder dos Estados, dos grandes conglomerados e das

2 Evgeny Morozov, "Como sanar o deficit de democracia exposto por Snowden", Folha de S. Paulo, 20/01/2014. http://www1.folha.uol.com.br/colunas/evgenymorozov/2014/01/1398996-como-sanar-o-deficit-de-democracia-exposto-porsnowden.shtml.

corporações, das ligações das plataformas digitais com os sistemas de segurança nacionais, etc., têm emergido na esfera pública determinado tipo de acções individuais e colectivas que se têm vindo a designar por "hactivismo ético", havendo ainda movimentos mais radicais, começando pelos Anonymous, continuando pela *deep net* e chegando inclusive ao cibercrime.

É matéria jurídica complexa – e não há consenso, por assim dizer, sob a questão da diferenciação "ética" de algumas violações de sistemas ou mesmo ataques de negação de serviço (Distributed Denial of Service – DDoS) quando estes têm objectivos apenas informativos ou mesmo cívicos. Veja-se, sob este ponto de vista, o caso espanhol, onde é justamente isso que se passa em plena discussão de alteração legislativa.[3]

A atitude de Snowden foi muito marcada pela sua experiência como analista de sistemas de vigilância e pelo facto de sentir um "dever moral" de divulgar o que estava em causa relativamente à liberdade na Internet e à privacidade dos cidadãos em geral, sobretudo com a possibilidade de acesso integral às suas comunicações com base no controlo global da indústria das telecomunicações e da Internet. Diz Snowden:

> *As coisas que vi começaram a perturbar-me verdadeiramente. (…) Eu podia ver os drones a vigiarem, em tempo real, as pessoas que eles poderiam vir a matar. Podíamos vigiar aldeias inteiras e ver o que todas as pessoas faziam. Vi a NSA controlar as actividades de pessoas na Internet à medida que teclavam. Fiquei a saber quão invasivas as capacidades de vigilância dos EUA se tinham tornado.*[4]

Mas se o seu objectivo, aliás, como o próprio confirma, foi despoletar o debate no espaço público e alertar a opinião pública mundial para os limites e perigos dos sistemas de vigilância na era digital, então conseguiu-o plenamente. Estas são realmente questões na ordem do dia.

Através dos sistemas de Big Data e de *data mining*, reconfigurados, por exemplo, nos processos de *microtargeting* e de análise preditiva, emergem novos problemas. Nestes novos sistemas de agregação e cruzamento de dados, um dos temas mais

3 Mercè Molist, "¿Es delito el 'hacking ético'?", El Mundo, 16, 17 e 23 de Agosto de 2014. http://www.elmundo.es/tecnologia/2014/08/09/53e316a9268e3ea4038b456b.html; http://www.elmundo.es/tecnologia/2014/08/17/53eeef97268e3e31558b456c.html; http://www.elmundo.es/tecnologia/2014/08/23/53f740d5ca4741a6568b457e.html.

4 Greenwald, op. cit., p. 61.

preocupantes é justamente o da privacidade e a protecção de dados pessoais perante as lógicas complexas de análise inteligente de informação. Estes dispositivos analíticos de dados, que respondem, em primeiro lugar, a lógicas algorítmicas de gestão da informação, pretendem prioritariamente atender a uma necessidade de ordem comercial ou instrumental (por exemplo, política) e, nessa medida, estruturam todas as suas complexas operações com o objectivo de identificar tipos de relações, correlações ou padrões de uso nos dados que gerem, quer na sua própria plataforma, quer cedendo dados às bases relacionais que operacionalizam o tratamento inteligente da informação obtida quer do mundo virtual, quer do mundo real.

Nestas novas dinâmicas, o cidadão, o consumidor, ou o "prosumer", são, por assim dizer, cada vez mais, os últimos a saber da sua própria tomada de decisão, seja em que contexto for. Seja num acto de compra de um produto numa qualquer área da grande distribuição, seja num qualquer processo eleitoral no momento de deixar o seu voto na urna, seja como destinatário de correio de promoções de uma qualquer rede comercial de retalho...

O que é curioso é que mesmo havendo a consciência e o conhecimento de que as coisas se passam efectivamente assim, a resistência do cidadão perante a enorme quantidade de dispositivos facilitadores das dinâmicas de rastreamento é muito reduzida. Aparentemente, os utilizadores das redes sociais, perante a possibilidade da disponibilização "global" da sua informação, mesmo íntima, preferem antes expor-se do que preservar-se, havendo sinais de que essa é já uma espécie de "naturalização" do digital, primeiramente com os *digital natives* mas cada vez mais também com as gerações anteriores.

Ao invés, então, de se configurar uma tradicional resistência do cidadão perante as "netvigilâncias" – das declaradas às absolutamente indetectáveis –, sucede afinal uma banal exposição. Exposição, aliás, não somente confirmada –, e objectivo primeiro –, de todas essas grandes plataformas, mas, fundamentalmente, conceito estratégico operacional do sistema, porventura configurando-se desse modo como uma das vertentes da "ideologia da Internet", ou no mito de um mundo de absoluta eficiência digital, moldado pelo colete de forças de Sillicon Valley.

O tema do Big Data foi objecto de uma reflexão aprofundada por parte de Viktor Mayer-Schönberger e de Kenneth Cukier (Big Data: A Revolution That Will Transform How We Live, Work, and Think). Nesta sua obra de 2013, estes autores abordam os impactos dramáticos que o Big Data está já a ter sobre a economia, a política e a sociedade em geral. A análise crítica de vastas colecções de informação mudará

certamente a maneira como pensamos o mundo em geral, a cultura, a inovação, e sobretudo como nos adaptaremos a essa nova realidade dada por um novo patamar do conhecimento.

Há aqui, no entanto, um outro tópico nada negligenciável que é o das centrais de inteligência e de informação –, caso da NSA –, que aplicam análise preditiva e Big Data não somente a fim de anteciparem fenómenos de turbulência social, terrorismo, atentados, etc., mas também, sob esse primeiro objectivo, para controlar e registar praticamente todas as comunicações via redes digitais, sejam elas sobre IP, por satélite, ou móveis, tendo inclusivamente capacidade de recuperar dados, desde listas de contactos a comunicações escritas, localização dos utilizadores, etc. Hoje, nem mesmo o anonimato na rede dá qualquer garantia aos utilizadores.

Com a Predictive Analytics[5] percebe-se que os sistemas de Big Data são cada vez mais o magma que faz mover o mundo de superfície, seja na política, na finança, na saúde, na distribuição, ou noutro qualquer sector. A análise preditiva utiliza determinadas estratégias informacionais, como por exemplo o "persuasion modeling", que tem por objectivo produzir influência a partir de dados, complementando metodologias de *microtargeting*, o que sucede, por exemplo, na área política dos EUA de há alguns anos a esta parte.

Em 2012 a campanha de Obama utilizou essas estratégias para influenciar e monitorizar eleitores e inclusivamente fazer previsão por eleitor a partir de modelos que a partir dessas previsões direccionavam as estratégias de influência e persuasão por eleitor também. Mas encontramos usos idênticos quer nos sistemas de segurança, quer na medicina, quer na procura das melhores opções no diagnóstico, ou mesmo no tratamento, e ainda nas áreas da comercialização e retalho, onde esta análise procura potenciar e fidelizar clientes. A análise preditiva optimiza o seu método, fundamentalmente, através de modelos de conjunto. Como se se tratasse de inteligência colectiva a actuar em simultâneo, estes modelos preditivos quando agregados e estruturados a partir de modelos "big data" adquirem desempenhos e respostas absolutamente surpreendentes. Daí dizer-se que neste novo contexto não faltará muito para detectar o criminoso mesmo antes dele cometer o crime…

Boa parte da experiência do utilizador é reconvertida pelas grandes plataformas em informação comercial redistribuída pela economia virtual e simultaneamente pela real, como vimos, da grande distribuição aos sistemas de comunicação, financeiros,

5 Eric Siegel (2013) Predictive Analytics: The Power to Predict Who Will Click, Buy, Lie, or Die. New Jersey: Wiley.

de saúde, etc. O rasto deixado diariamente por milhares de milhões de Likes no Facebook produz um manancial de informação nada despiciendo, sobre cada um e todos os utilizadores.

Tem, necessariamente, um valor comercial, estimado, em termos do sistema publicitário, em cerca de 1200 dólares/ano por utilizador, isto quando essa informação relativa a cada perfil individual não chega a custar um cêntimo sempre que vendida em pacotes de dados.

Outra boa parte da experiência do utilizador é convertida em dados de performance, naquilo a que se chama o "quantified self", uma cartografia do eu de grande detalhe informativo sobre o parecer, o ser e o fazer, agora não já enquanto ferida narcísica de corpo elidido através de um qualquer processo de imagem de síntese, mas corpo tornado "gadget" a partir do momento em que são reconvertidas todas as suas dimensões em dados e perfis.

Essa informação, de início, começou por constar nos cartões de saúde associados, por exemplo, a seguros de vida, mas diversificou-se enormemente com os sistemas operativos móveis e as lojas de aplicações. Tudo é possível controlar através das mais inesperadas aplicações, do ritmo cardíaco aos quilómetros de marcha, da energia calórica da alimentação diária à coordenação da agenda, do tempo gasto a consultar os *e-mails* ou a usar o telemóvel, passando pela gestão agregada de várias dessas actividades, como é possível através do Google Now, ou ainda do comportamento online do utilizador e dos seus amigos no Facebook, através da aplicação "Personal Analytics" da Wolfram-Alpha, um motor de busca que responde às perguntas mais diversas sobre as redes de amigos, gera relatórios e faz análise de milhares de domínios sobre a rede e a vida "social" de cada utilizador do Facebook.

Daí que faça cada vez mais sentido a premonição do século passado – de que um dia – e esse dia é já hoje –, ninguém nos conhecerá melhor do que o "nosso" *software*.

Quer, portanto, no plano da sobreexposição pública das vivências e intimidades dos indivíduos nas redes sociais, nas suas redes de amigos, ou mesmo em redes de partilha mais alargada –, quer no plano do controlo do sujeito – e do próprio corpo –, através de aplicações e *gadgets* de todo o género, do que se trata, finalmente, é de uma clara monitorização (cedida graciosamente pelos utilizadores da rede às plataformas de dados) da vida privada de cada um.

A rede passa assim por ser um novo dispositivo *panopticon* de duplo sentido, que não somente vigia os outros a partir de um centro com vários nós ou núcleos,

mas também vigia o hipotético vigilante, registando cada uma das suas acções de vigilância, e cada link, cada like, cada desejo de link, dir-se-ia…

Quais então as consequências do Big Data, do "algorithmic turn" e da análise preditiva no contexto de consolidação e radicação do digital na sociedade contemporânea? Desde logo, consequências profundas no modo de organização, na economia, no conhecimento, na própria interacção, mas também no controlo, na exposição/localização (por exemplo com a aplicação Nearby Friends, do Facebook) e na vigilância dos cidadãos por sistemas altamente sofisticados, como tivemos a prova com as "disclosures" de Edward Snowden.

Os dados, hoje, são uma matéria-prima privilegiada na economia em geral, já considerada equivalente ao capital e ao trabalho. Os algoritmos são criados com competências bastante improváveis, como, por exemplo, produzir informação jornalística para os próprios media…

Para Mozorov, *a sobreinformação pode-nos aborrecer tanto quanto a penúria de informação* [6], e a verdade é que o estado permanente de recepção cataléptica é a norma entre os adictos das redes sociais, fortemente dominadas pelo "factoidismo", pelo acontecimento sem substância.

Do que se trata genericamente é, por um lado, de uma progressiva elisão, de um apagamento do cidadão, e, por outro, de uma cada vez mais crítica presença de um "algorithmic turn" nas estratégias dos Estados, militares e das grandes plataformas digitais, tornando-as reféns do chamado Big Data e dos seus limites. O que, inevitavelmente, vem reforçar os alertas não só sobre a volubilidade e uma potencialmente crítica "despersonificação" do cidadão, como, finalmente, sobre a actual crise mais global da própria experiência democrática.

Face ao "maelstrom", à torrente, ao turbilhão de informação, impõe-se um distanciamento, uma reflexão, uma estética, ou talvez mesmo uma ecologia que reconverta práticas, hábitos e modelos, reconfigurando a exposição e a adicção impulsiva em selecção, visão crítica e vigilância.

BIBLIOGRAFIA

Alan Rusbridger and Ewen MacAskill (2014), "I, spy: Edward Snowden in exile ".The Guardian, 19 July. http://www.theguardian.com/world/2014/jul/18/-sp-edward-snowden-interview-rusbridger-macaskill. Versão portuguesa no Expresso – Revista, 2 de Agosto de 2014, "Levo uma vida bastante livre, não ando por aí disfarçado".

6 Evgeny Morozov "Réapprendre l'ennui", Books, nº 53, Avril 2014, p.40.

Alexandre Martins (2014), "Tribunal europeu reconhece 'direito ao esquecimento' na Internet", Público online 13/05. http://www.publico.pt/mundo/noticia/tribunal-europeu-defende-direito-a-ser-esquecido-na-internet-1635712

Bianka Bosker (2013), "Google Aims To Patent Policy Violation Checker, Potentially Revolutionizing Email Snooping", Huffington Post, 5/7. http://www.huffingtonpost.com/2013/05/06/google-policy-violation-checker_n_3224363.html?utm_hp_ref=technology

Charles Duhigg (2012), "How Companies Learn Your Secrets", NYT, February 16. Acedido em 18.08.2014.http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=5&hp&.

Eric Siegel (2013). Predictive Analytics: The Power to Predict Who Will Click, Buy, Lie, or Die. New Jersey: Wiley.

Evgeny Morozov (2014). "Como sanar o deficit de democracia exposto por Snowden", *Folha de S. Paulo*, 20/01. http://www1.folha.uol.com.br/colunas/evgenymorozov/2014/01/1398996-como-sanar-o-deficit-de-democracia-exposto-porsnowden.shtml.

_____, (2014a). "Réapprendre l'ennui", Books, nº 53, Avril, p.40.

F. Rui Cádima (2013). "O Facebook, as redes sociais e o direito ao esquecimento". Media & Jornalismo. Lisboa: Mariposa Azual, V. 12, nº 22, pp. 177-209. http://www.cimj.org/images/stories/docs_cimj/mj22_cdima2.pdf

Glenn Greenwald (2014). Snowden sem esconderijo, Lisboa: Bertrand.

Mercè Molist (2014). "¿Es delito el 'hacking ético'?", El Mundo, 16, 17 e 23 de Agosto. http://www.elmundo.es/tecnologia/2014/08/09/53e316a9268e3ea4038b456b.html; http://www.elmundo.es/tecnologia/2014/08/17/53eeef97268e3e31558b456c.html; http://www.elmundo.es/tecnologia/2014/08/23/53f740d5ca4741a6568b457e.html.

Rosa Jiménez Cano (2014). "Secret, entre la libertad de expresión y el insulto". El País, 24 de Agosto. http://tecnologia.elpais.com/tecnologia/2014/08/24/actualidad/1408899415_877844.html

Sasha Issenberg (2012). The Victory Lab, The Secret Science of Winning Campaigns. New York: Crown Publishers.

Thomas Shulz (2014). "Profeta do 'admirável mundo novo'", Courrier Internacional, Lisboa, nº 221, Julho, pp.41-47. Publicado originalmente na Der Spiegel, sob o título "Larry und die Mondfahrer", 1 de Março de 2014.