61. Gellman, B.; Soltani, A. "NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say". *The Washington Post*. 30 de outubro de 2013. Acesse em: http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html/.
62. Levy, S. "How the NSA almost killed the internet". *Wired*. J)1 de julho de 2014. Acesse em: http://www.wired.com/2014/01/how-the-us-almost-killed-the-internet/all/.
63. Documentos do Centro para Democracia e Tecnologia norte-americano. Setembro de 2014: "Yahoo v. U.S. Prism documents", disponível em https://cdt.org/insight/yahoo-v-u-s-prism-documents
64. Veja, por exemplo, http://america.aljazeera.com/articles/multimedia/timeline-edward-snowden-revelations.html ou http://www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline
65. Gandy, O. *Coming the terms with chance: engaging rational discrimination and cumulative disadvantage*. London: Ashgate. 2012.
66. Turow, J. *The daily you: how the new advertising industry is defining your identity and your worth*. New Haven, CT: Yale University Press, 2012.
67. Andrejevic, M. *Infoglut: how too much information is changing the way we think and know*. London: Routledge, 2012. Veja também Andrejevic, M. *iSpy: surveillance and power in the interactive Era*. Lawrence: University of Kansas Press, 2007.
68. Marwick, A. *Status update: celebrity, publicity and branding in the social media age*. New Haven, CT: Yale University Press 2013.
69. Por exemplo, Raab, Charles e Benjamin Goold. Protecting information privacy. Equality and human rights Commission Research Report 69, 2011. Acesse em: http://www.equalityhumanrights.com/sites/default/files/documents/research/rr69.pdf
70. Amoore, L. "Security and the claim to privacy". *International Political Sociology*, vol.8 (1): 108-112. 2014.
71. Kitchin, R. *The data revolution: big data, open data, data infrastructures and their consequences*. London: Sage, 2014.
72. Morozov, E. "The real privacy problem". *MIT Technology Review*. Outubro, 2011. Acesse em: http://www.technologyreview.com/featuredstory/520426/the-real-privacy-problem
73. Clarke, R.; Morrell, M.; Stone, G.; Sunstein, C.; Swire, P. *The NSA Report: Liberty and Security in a Changing World*. Princeton, NJ and Oxford: Princeton University Press. 2014.
74. Zittrain, J. *The future of the internet*. New Haven, CT: Yale University Press, 2014.
75. A frase "(...) encontrar um equilíbrio entre privacidade e segurança" é rotineiramente entoada por governos e mídia, mas isso é na melhor das hipóteses, vazia, e, na pior, um disfarce para minar um e reforçar o outro.
76. Raab, C. "Privacy as a security value". *In*: *Jon Bing: En Hyllest / A Tribute*, Schartum, D. W.; Bygrave, L.; Bekken, A.G.B. (org) Oslo: Gyldendal, 2014. p. 39-58.
77. Lyon, D. *Surveillance after Snowden*. Cambridge: Polity, 2015.
78. Veja, por exemplo, a chamada do cientista político Charles D. Raab em 2013. Raab, C. "Studying surveillance: the contribution of political science?" *Political Insight*. October 29. 2013. Acesse em: http://www.psa.ac.uk/insight-plus/blog/studying-surveillance-contribution-political-science/.

RASTREAR, CLASSIFICAR, PERFORMAR*

Fernanda Bruno

No ano de 2010, o *Wall Street Journal* (WSJ) lançou une série de matérias e documentos revelando que inúmeros sites da internet utilizam quantidades expressivas de rastreadores das navegações e ações de seus visitantes. O *dictionary.com*, por exemplo, figura no topo da lista divulgada pelo *WSJ* (1), utilizando 234 tipos de rastreadores. A série, intitulada *What they know* (O que eles sabem) (2), mostra ainda como inúmeras corporações coletam e categorizam os rastros que deixamos na web, constituindo perfis de hábito, consumo, empregabilidade, longevidade, periculosidade etc. Em pesquisa realizada no mesmo ano no Brasil, identificamos a presença de 362 rastreadores de dados de usuários (cookies, flash cookies e web beacons) em apenas cinco sites da internet brasileira (Terra, UOL, Yahoo, Globo.com, YouTube) e de 295 rastreadores nas duas redes sociais mais populares no Brasil na ocasião (Orkut e Facebook). Cerca de 68% desses rastreadores atuam no campo do marketing online (3;4). Entretanto, ainda que habitualmente se enfatize o papel e os interesses do marketing neste contexto, é fundamental ressaltar que, além do marketing e da publicidade direcionada, o monitoramento de rastros pessoais na internet é de interesse comum a diferentes domínios: segurança, entretenimento, saúde, gestão do trabalho e recrutamento de pessoal, consultoria e propaganda política, desenvolvimento de produtos e serviços, vigilância e controle, inspeção policial e estatal etc.

Tecnicamente, o rastreamento e arquivamento das ações cotidianas na internet é possível graças à própria estrutura desta rede de comunicação distribuída e de seus navegadores, onde toda ação deixa um rastro potencialmente recuperável, constituindo um vasto, dinâmico e polifônico arquivo de nossas ações, escolhas, interesses, hábitos, opiniões etc. (3). Na série de matérias do WSJ, encontramos diversos exemplos de empresas cujo negócio consiste na coleta de rastros pessoais na internet e sua correlata categorização em bancos de dados e sistemas de *profiling*, visando orientar tanto escolhas de clientes de seguro de vida quanto ofertas de crédito e alvos de propaganda política, por exemplo.

A Acxiom Corp. (5), uma das maiores empresas de comércio e tratamento de dados da internet, monitora e categoriza diversas informações provenientes do comportamento online de milhões de americanos, cruzando-as com suas bases de dados offline. Tais dados, combinados a outros de natureza diversa, orientam, por exemplo, definições de bons e maus candidatos a seguros de vida. Os convencionais exames de sangue, considerados pouco amigáveis e explicitamente invasivos, dão lugar a análises preditivas que levam em conta

hábitos de vida, muitos deles sutilmente rastreáveis na internet, como "detalhes de compras online e por catálogo, assinaturas de revistas, atividades de lazer e informações de sites de redes sociais" (6).

A Deloitte Consulting (7), por sua vez, oferece serviços e tecnologias a seguros de vida, prometendo dimensionar o risco-saúde dos indivíduos e predizer suas expectativas de vida baseando-se em dossiês elaborados a partir de análise de dados coletados online e offline. No material promocional da empresa, conforme a matéria mencionada, consta uma suposta lista de dados coletados das figuras hipotéticas de Sarah e Beth, para as quais a empresa elabora perfis prospectivos de risco-saúde que categorizariam o bom e o mau cliente.

Este breve exemplo expõe não apenas uma categorização de bons e maus clientes de seguro de vida, mas um encadeamento de diversos sistemas de perfis que se apoiam – de risco financeiro, de estilo de vida saudável, de longevidade –, para os quais os dados comportamentais dos usuários da internet se tornam uma fonte valiosa para diversos fins.

O mesmo tipo de dados serve ao *profiling* de potenciais eleitores, permitindo orientar propaganda política para alvos supostamente certeiros. Consultores de partidos e candidatos políticos contratam empresas que monitoram os fluxos de atividades e rastros online, de modo a conhecer o que chamam de "linguagem corporal online" de republicanos e democratas nos EUA, por exemplo (8).

Se os traços de nossas atividades na rede permitem projetar perfis de longevidade, de saúde, de preferências políticas, por que eles não seriam utilizados para montar perfis de crédito e consumo? Há empresas que chegam a anunciar serem capazes de fazer previsões sobre o "valor de vida útil" de internautas com base em um simples clique em seu website (9).

Perfis de longevidade de consumo ou de preferências políticas operam como mecanismos de decisão e escolha de corporações sobre as qualidades potenciais de indivíduos, com efeitos expressivos sobre as oportunidades que lhes são ofertadas, bem como sobre o seu campo de ação possível, previamente limitado ao que está previsto nas bases de perfis. Uma lógica comum os atravessa e ela vale não apenas para os exemplos aqui mencionados, mas também para perfis de periculosidade e de empregabilidade, entre outros, dado que o monitoramento de atividades online para montagem de bancos de dados e sistemas de *profiling* são hoje práticas comuns tanto a instâncias de segurança (10) quanto aos procedimentos de seleção de pessoal por parte de empresas (11). A lógica que lhes é comum conjuga alguns princípios centrais, dos quais destaco brevemente os seguintes aspectos:

1. O RASTRO COMO EVIDÊNCIA A topologia dos rastros digitais na internet não é uniforme. Tais rastros são inscritos segundo camadas informacionais mais ou menos visíveis e mais ou menos vinculadas a indivíduos identificáveis. Além ou aquém das informações pessoais que divulgamos voluntariamente na web (postagens em blogs, dados de perfil e conversações nas redes sociais), toda ação efetuada na rede – navegação, busca, simples cliques em links, downloads, produção ou reprodução de conteúdo – deixa potencialmente um rastro, um vestígio, uma inscrição mais ou menos explícita, suscetível de ser capturada, recuperada, classificada. O rastro pessoal digital é, assim, o vestígio de uma ação efetuada por um indivíduo.

Os atuais dispositivos e redes de comunicação digital funcionam como um dispositivo de inscrição e memória : não apenas enviamos e recebemos mensagens, não apenas buscamos e produzimos informação, como também, ao fazer tudo isso, deixamos automaticamente, e não raro involuntariamente, rastros de nossa presença e de nossa ação (3). Tais rastros são monitorados e capturados, nutrindo bancos de dados complexos que tratam tais informações para extrair categorias supraindividuais ou interindividuais segundo parâmetros de afinidade e similaridade entre os elementos, permitindo traçar perfis – de consumo, de interesse, de comportamento, de competências etc. Como se viu nos exemplos apresentados, tais perfis irão atuar ou diferenciar indivíduos ou grupos com base num suposto saber que conteriam.

Uma das vias pela qual este tipo de saber busca legitimar-se (veremos outras vias no próximo tópico) consiste na pretensa objetividade própria à coleta, à análise e à categorização automatizadas desses rastros. Um dos argumentos de legitimação desta objetividade afirma que tais dados seriam coletados *in natura*, ou seja, diretamente das ações dos indivíduos no contexto mesmo de sua produção. Como se a coleta automatizada desses rastros em tempo real permitisse dispensar mediadores e mediações (e suas consequentes traduções), atribuindo ao rastro um estatuto de "evidência". A pretensão de objetividade também está atrelada ao caráter automatizado do tratamento desses rastros, que não seriam submetidos à interpretação humana, mas a procedimentos algorítmicos. Estes, por sua vez, revelam padrões que não são predefinidos (*top down*), mas que emergem no próprio cruzamento dos dados (*bottom-up*). Categorias que expressariam, portanto, um grau de objetividade mais agudo que quaisquer outras teorias, observações ou interpretações permitiriam.

Eis um argumento frágil e questionável, tanto do ponto de vista cognitivo quanto político: uma nova neutralidade e objetividade poderiam ser conquistadas graças a esse tipo de saber extraído de rastros digitais entendidos como evidências. É curioso perceber como a alegada "transparência" dos dados e do conhecimento que deles deriva não é posta em questão, em nenhum momento, pela notável opacidade do método e das ferramentas de rastreamento, arquivo e tratamento desses mesmos dados.

O valor econômico, estratégico e heurístico dos rastros digitais e do *profiling* reside, sobretudo, no tipo de conhecimento que eles permitem gerar. Qual é a especificidade deste saber, se considerarmos historicamente os diferentes modelos de conhecimento a partir de rastros, elaborados em diversos campos (semiologia, história, filologia, arqueologia, literatura, psicanálise, entre outros)? Primeiramente, o volume é determinante. Supõe-se, de modo geral, que o

fato mesmo de sua imensa quantidade esconde ou guarda estruturas e regras inscritas nas correlações sutis entre os dados. O termo *big data* propõe uma nova grandeza que procede tanto do aumento da capacidade de estocagem como da emergência de um novo tipo de saber que tais volumes de dados gerariam (12-14). Conforme um dos promotores dessa nova escala de saber:

> *Este é um mundo onde grandes quantidades de dados e matemática aplicada substituem qualquer outra ferramenta que poderia ser usada. Descarte toda a teoria do comportamento humano, da linguística à sociologia, esqueça a taxonomia, ontologia, e psicologia. Quem sabe por que as pessoas fazem o que fazem? O ponto é que eles fazem isso, e podemos acompanhar e medir com fidelidade sem precedentes. Com dados suficientes, os números falam por si. (*15).

O termo técnico empregado para designar o processo que permitiria fazer emergir o que estaria oculto é "mineração", proveniente do termo inglês *data-mining* (literalmente, mineração de dados). Ainda no plano técnico, dois procedimentos complementares são essenciais: mineração de dados *e profiling*. A mineração de dados consiste no tratamento algorítmico de grandes volumes de dados cuja função central é a extração de padrões que geram conhecimento específico a partir da correlação entre elementos segundo princípios de similaridade, vizinhança e afinidade, por exemplo. Não por acaso, este procedimento é chamado "*descoberta de conhecimento em bases de dados*" (16). O postulado dessas técnicas supõe que o tratamento automatizado seja capaz de revelar correlações imprevistas entre os dados.

O PERFIL FUNCIONA COMO UM MECANISMO DE TRIAGEM ALGORÍTMICA DO ACESSO A CIRCUITOS DE CONSUMO ...

2. "CORRELAÇÃO É SUFICIENTE" Tais correlações resultam numa longa e diversificada taxonomia dos usuários da web, revelando categorias engendradas pelas técnicas de *profiling*, complementar à mineração de dados.

O que tal conhecimento pode dizer sobre os indivíduos? De fato, ele diz menos sobre indivíduos pessoalmente identificáveis (ou seja, sobre "quem" são essas pessoas do ponto de vista de suas identidades civis) do que sobre suas ações, condutas, escolhas, as quais podem ser consequentemente suscitadas, orientadas, conjuradas. Se há uma individualidade vinculada a esse tipo de rastro e ao conhecimento que se pretende gerar a partir dele, ela é menos da ordem do passado que do futuro, menos da ordem da interioridade que da exterioridade, menos relativa a uma singularidade do que a regras de similaridade.

Vejamos cada um desses contrastes com mais detalhes (17). Ainda que os rastros digitais que compõem os perfis sejam vinculados a ações passadas, eles valem menos pela possibilidade de retraçar fatos ou identificar suas origens do que pela capacidade de projetar desejos, comportamentos e intenções futuras ou potenciais (18). Segundo definição proposta por Hildebrand (19):

> Neste sentido, o *profiling* é um modo indutivo de gerar conhecimento; as correlações representam uma probabilidade de que as coisas terão o mesmo resultado no futuro. O que elas não revelam é porque este deve ser o caso. Na verdade, criadores de perfil não estão muito interessados em causas ou razões, o seu interesse reside em uma previsão fiável, de modo a permitir a tomada de decisão adequada (19, p. 40).

Notemos que tais correlações presentes no perfil não exprimem um nexo causal nem explicativo entre os elementos. Em nenhum momento cabe explicar a relação entre ações, indivíduos e circunstâncias. Trata-se apenas de revelar correlações, estimar probabilidades de ocorrência e, se for o caso, intervir no curso das ações e condutas dos indivíduos. "A correlação é suficiente" é um dos princípios deste modelo de saber (20). E tal princípio é claro nos exemplos que acabamos de mencionar. Não se supõe que haja um vínculo causal ou explicativo entre "assistir pouco a televisão" e "ter uma expectativa de vida mais longa"; tampouco entre "amar fotografia" e "ser republicano", ou entre "adorar viajar" e "ser um bom cliente de crédito". A correlação ou a copresença de um número significativo de fatores numa população massiva é julgada suficiente para legitimar o perfil e suas categorizações, mesmo que haja, evidentemente, uma margem considerável de incerteza ou imprecisão em jogo.

O rastro digital de nossas ações, assim concebido, é tanto o vestígio de uma presença ou de uma ação passada quanto o índice de uma ação futura, mas este conhecimento não designa nem a trajetória singular de um indivíduo, nem o caminho que vai de sua ação a uma interioridade que a justificaria ou lhe daria sentido. Este conhecimento, pelo rastro digital, opera na superfície da ação e busca apreender não uma singularidade atrás do rastro mas modelos de similaridade, em vias de projetar condutas ou ações passíveis de intervenção.

3. PERFIL, PROATIVIDADE E PERFORMATIVIDADE O caráter proativo desse saber algorítmico dos rastros pessoais é notável e decisivo para os seus efeitos de poder e controle. A evidência supostamente revelada não tem a pretensão de ser uma "prova" e*x post facto* mas um vetor que permitiria agir antes do fato, ou antes da ação. A definição de poder como "ação sobre a ação possível" ganha uma atualidade particular, assim como a concepção de governo como a arte de conduzir condutas (21-22). Pois é precisamente a ação possível dos indivíduos que atrai a atenção e o interesse dos diversos ramos que se dedicam ao monitoramento dos rastros digitais e ao *profiling*. Trata-se aqui da ilusão de transformar o porvir num "futuro anterior", como aponta Didier Bigo (23). Um futuro de caráter imediato, pois atua no presente, e cuja efetividade pre-

tende-se proativa, pois trata-se menos de assegurar uma acuidade na previsão do que a performatividade da antecipação, que visa justamente tornar mais provável o que é antecipado.

A recompensa e a punição que tais individualidades trazem consigo é menos da ordem do ser do que da ordem do acesso. O perfil funciona como um mecanismo de triagem algorítmica do acesso a circuitos de consumo, bem-estar, civilidade etc. Os rastros heterogêneos coletados e minerados constituem gigantescos arquivos que operam como "memórias do futuro", a partir das quais se projetam perfis que pretendem agir antes do ato ou do fato.

Nesta gestão de possíveis e de rastreamento proativo, identidades algorítmicas são construídas através das técnicas de *profiling*. Mas é preciso ressaltar que o indivíduo surge como um alvo *a posteriori*, sendo antes um efeito do processo de monitoramento, ao invés de estar presente *ab initio*. Os perfis são menos o espelho de uma identidade do que uma projeção algorítmica de categorias que se pretendem ajustadas a indivíduos particulares, seja na forma de ofertas personalizadas de produtos e serviços potencialmente desejáveis, seja sob a forma de antecipação de comportamentos ou riscos a evitar.

O problema em jogo é perceptível: tal projeção de comportamentos e individualidades pode condenar o presente ao futuro antecipado. As implicações sobre as oportunidades informacionais, cognitivas, sociais e políticas dos indivíduos são diversas e ainda indefinidas. Tal categorização e gestão de possíveis pode funcionar, como vimos, como triagem ou filtro automatizado de acesso a espaços, informações, produtos, experiências, envolvendo por vezes mecanismos de discriminação automatizada (24).

CATEGORIAS EM DELÍRIO O estranhamento diante dessas categorizações vistas ao longo do texto traz a lembrança do conhecido texto de Jorge Luis Borges, no qual menciona uma enciclopédia chinesa intitulada *Empório celestial de conhecimentos benévolos*, cuja engenhosa classificação dos animais consistia em:

> a) pertencentes ao imperador, b) embalsamados, c) domesticados, d) leitões, e) sereias, f) fabulosos, g) cães em liberdade, h) incluídos na presente classificação, i) que se agitam como loucos, j) inumeráveis, k) desenhados com um pincel muito fino de pelo de camelo l) et cetera, m) que acabam de quebrar a bilha, n) que de longe parecem moscas (25, p. 170).

Tal classificação nos provoca o "riso que perturba todas as familiaridades do pensamento" (21, p.12), pois ela nos indica o nosso próprio limite, a nossa impossibilidade de pensá-la. A inquietação provocada por essa ordem impensável faz vir à tona a suspeita tácita de que os critérios com que ordenamos as coisas não lhes pertencem (26). Num mesmo golpe, nos força a pensar na multiplicidade de formas de ordenação possíveis (Cf. 21).

Os regimes de ordenação do mundo, sempre variáveis conforme sociedades e tempos, nos causam tão mais estranhamento quanto mais afastados de nossa idade e nossa geografia. Quanto mais longe do nosso presente e do nosso espaço, mais gritante se torna a sua contingência. Ainda assim, muitas vezes eles nos dizem algo, seja sobre o seu autor ou autores, seja sobre a cultura e a sociedade em que se constroem, seja sobre o momento histórico em que se constituem.

Um belo exemplo taxonômico, delicadamente feminino e de grande beleza poética, é o *Livro de cabeceira*, de Sei Shonagon (27), dama de honra da princesa japonesa Sadako, escrito no século XI. Este livro, de profunda sensibilidade, é todo composto de listas que não apenas enumeram coisas, mas as classificam e avaliam. Listas que acabam descrevendo menos as coisas mesmas e muito mais a percepção e a perspectiva de quem as ordena daquela maneira. As anotações de cabeceira de Sei Shonagon incluem, por exemplo, entre as "Coisas elegantes":

> Sobre um colete lilás, uma túnica branca; Filhotes de ganso; Numa tigela nova de metal, foi vertido xarope de cipó, com gelo socado; Um rosário de cristal de rocha; Neve depositada sobre as flores das glicínias e das ameixeiras; Um lindo bebê comendo morangos (27, p.23).

Entre as "Coisas que devem ser curtas", estão:

> O fio para coser algo de que se precisa logo em seguida; Um pedestal de abajur; Os cabelos de uma mulher de condição inferior. É bom que sejam cortados graciosamente curtos; O que diz uma moça (27, p.25).

Além destes, muitos outros itens recobrem suas listas: "Coisas de aspecto sujo"; "Coisas que dizem respeito a uma casa"; "Coisas que são distantes, embora próximas"; "Coisas consternantes"; "Coisas que só fazem passar"; "Coisas de bater o coração", entre outros.

Essas duas classificações estranhas e distantes de nós – a que nos apresenta Borges e a de Sei Shonagon – de algum modo nos ensinam a desconfiar de nossas próprias taxonomias e interrogá-las não tanto quanto à sua adequação às coisas que elas categorizam, mas sim quanto ao mundo e aos modos de vida que produzem. Os perfis e as taxonomias proativas profusamente construídas a partir do monitoramento de rastros pessoais digitais pretendem saber e decidir, muitas vezes a despeito dos sujeitos em questão, sobre o que eles podem e não podem desejar, conhecer, escolher. Sob a égide da multiplicação de ofertas personalizadas, é o próprio campo de experiência e de ação possível dos indivíduos que está em perigo.

Retornemos a Borges (28), no mesmo texto citado, em que nos lembra o que está em jogo, ao final: o imenso problema das palavras e das coisas, da ordem e da linguagem. Problema de que nos dá a "mais lúcida definição", em sua ilustre opinião, atribuída a Chesterton:

> O homem sabe que há na alma matizes mais desconcertantes, mais inumeráveis e mais anônimos que as cores de um bosque outonal. Crê,

no entanto, que esses matizes, em todas as suas fusões e conversões, podem ser representados com precisão por meio de um mecanismo arbitrário de grunhidos e chiados. Crê que mesmo de dentro de um corretor da Bolsa realmente saem ruídos que significam todos os mistérios da memória e todas as agonias do desejo. (28, p. 177).

Fernanda Bruno *é professora da Universidade Federal do Rio de Janeiro (UFRJ), pesquisadora do CNPq, coordenadora do MediaLab da UFRJ e membro da Rede Latino-Americana de Estudos em Vigilância, Tecnologia e Sociedade (Lavits).*

(*) Este artigo é uma versão em português do capítulo "Grilles de nos traces sur internet" publicado originalmente em francês no livro *Derrièrre les grilles: sortons du tout-évaluation*, Barbara Cassin (Org.), Editora Mille et une nuits, Paris, 2013. E*scrito em 2010, este artigo permanece pertinente e, ao mesmo tempo, mereceria ser atualizado. Nos cinco anos que afastam a escrita do texto e esta publicação, as técnicas e práticas de rastreamento e monitoramento online se ampliaram e se diversificaram, bem como o debate sobre o tema, especialmente impulsionado pelas revelações de Edward Snowden em 2013. Percebemos, assim, o quanto as tecnologias e as políticas em torno da apropriação de nossos dados online são marcadas por uma grande aceleração. Entretanto, os argumentos aqui propostos permanecem válidos para compreendermos as engrenagens envolvidas no rastreamento e classificação das nossas ações online, bem como as formas de controle que lhes são associadas. Neste sentido, o artigo segue contribuindo para questionarmos as políticas de dados em curso na web.*

NOTAS E REFERÊNCIAS

1. A lista divulgada pelo *Wall Street Journal* está disponível em http://blogs.wsj.com/wtk/
2. Cf. *Wall Street Journal*, "What they know", disponível em http://on.wsj.com/apQ9IN
3. Bruno, F.; Nascimento L. et alii. "Rastros humanos en internet: privacidad y seguimiento online em sítios web populares del Brasil". *Novática*, Madrid, año XXXVIII, n. 217, may/jun. 2012.
4. Sobre o relatório completo da pesquisa, Cf. Firmino, R.; Bruno, F. et alii. *Social impacts of the use and regulation of personal data in Latin America*. IDRC/Lavits, 2012. Disponível em: http://lavits.org/?p=193&lang=en
5. Acxiom Corp. (http://bit.ly/8Uz4BI). Na matéria mencionada, executivos da empresa afirmam que seu banco de dados contém informações sobre 500 milhões de consumidores ativos no mundo todo, com cerca de 1.500 dados por pessoa, sendo a maioria de adultos nos Estados Unidos. Seu lucro declarado no último ano fiscal foi de 77,26 milhões de dólares sobre um total de vendas de US$ 1,13 bilhão.
6. *Wall Street Journal*, 19 novembre 2010. http://on.wsj.com/crQVCW
7. Deloitte Consulting. www.deloitte.com/
8. Cf. http://www.lotame.com/
9. É o caso da empresa [x+1], reportado pelo *Wall Street Journal*. Cf. http://on.wsj.com/bUlR5G
10. Os arquivos da Agência de Segurança dos Estados Unidos, revelados por Edward Snowden, especialmente os documentos do programa PRISM, são uma demonstração clara das relações entre políticas de segurança de Estados e grandes corporações da internet, implicando o monitoramento de seus usuários em escala global. Greenwald, G. *No place to hide*. Brilliance Audio, 2014.
11. Diversos sites como fyiscreening; EmployeeScreenIQ; Abika prestam serviços de rastreamento de dados pessoais em redes sociais e afins, oferecendo a empresas dossiês detalhados dos rastros de indivíduos na web.
12. Bollier, D. *The promise and peril of big data*. Washington: The Aspen Institute, 2010.
13. Boyd, D.; Crawford, K. "Six provocations for big data". *In: A decade in internet time: Symposium on the dynamics of the internet and society*, 2011. Oxford: SSRN eLibrary. Disponível em: <http://dx.doi.org/10.2139/ssrn.1926431>. Acesso em: 05 Mar. 2013.
14. Manovich, L. "Trending: The promises and the challenges of big social data". *In:* Gold, *M. (Org.). Debates in the digital humanities*. Minneapolis: The University Of Minnesota Press, 2011.
15. Traduzido do original em inglês: "This is a world where massive amounts of data and applied mathematics replace every other tool that might be brought to bear. Out with every theory of human behavior, from linguistics to sociology. Forget taxonomy, ontology, and psychology. Who knows why people do what they do? The point is they do it, and we can track and measure it with unprecedented fidelity. With enough data, the numbers speak for themselves" Anderson, C. "The end of theory: The data deluge makes the scientific method obsolete". *Wired Magazine* 16.07, 23 June 2008.
16. Gandy, O. H. Data mining and surveillance in the post-9.11 environment. Political Economy Section, IAMCR. Barcelona, jul. 2002.
17. Estes contrastes inspiram-se, por contraste, em algumas características do modelo indiciário que o historiador Carlo Ginzburg (1989) atribui às ciências humanas e sociais modernas. Ginzburg, C. *Mitos, emblemas, sinais*. São Paulo: Companhia das Letras, 1989.
18. Vale notar, contudo, que o foco estratégico do *profiling* nas ações potenciais convive com outros procedimentos de rastreamento de dados na internet que visam retraçar origens de ações e identificar seus responsáveis.
19. Hildebrandt, M. and S. Gutwirth (eds). *Profiling the european citizen. Cross-disciplinary perspectives*. Dordrecht: Springer Science, 2008.
20. Anderson, Op. Cit., 2008.
21. Foucault, M. *As palavras e as coisas*. São Paulo: Martins Fontes, 1995.
22. Foucault, M. *Naissance de la biopolitique*. Paris: Gallimard/Seuil, 2004.
23. Bigo, D. "Security, surveillance and democracy". LISS Cost Conference, 2010.
24. Gangadharan, S. "Digital inclusion and data profiling". *First Monday*, Chicago, v. 17, n. 5, 2012.
25. Borges, J.L. "O idioma analítico de John Wilkins". In: *Obras completas*. Porto Alegre: Globo, 1999.
26. Vaz, P. *O inconsciente artificial*. São Paulo: Unimarco, 1997.
27. Sei Shônagon. *Notes de chevet*. Traduction par André Beaujard. Paris: Gallimard, 1997.
28. Borges, J.L., Op. Cit., 1999.