Monitoramento, classificação e controle nos dispositivos de vigilância digital*

RESUMO
O ano de 2007 foi farto em notícias e protestos contra a vigilância de dados e a violação de privacidade por parte de diversos serviços na Internet. Os dispositivos de vigilância digital, usualmente pouco visíveis, começam a entrar na pauta das discussões sociais e políticas, mas o foco na questão da privacidade reduz o problema, o qual merece ser articulado a uma análise mais ampla dos processos de monitoramento, classificação e controle das informações sobre indivíduos. Este artigo efetua essa análise buscando apreender as transformações no estatuto do indivíduo e de sua identidade, assim como a emergência de modelos taxonômicos e de extração de padrões na vigilância digital, os quais atuam como instrumentos preditivo-performativos das condutas individuais.

PALAVRAS-CHAVE
vigilância digital
individualização
controle

ABSTRACT
The year 2007 was plentiful in news and protests against dataveillance and violation of privacy from various Internet services. The dataveillance devices, usually not visible, are becoming a subject of social and political discussions, but the focus on the issue of privacy reduces the problem, which must be articulated to a broader analysis of the processes of tracking, classification and control of information on individuals. This article makes that analysis seeking to understand the changes in the status of the individual and their identity as well as the emergence of taxonomic models and extraction of standards in digital surveillance, which acts as predictive and performative tools of the individual conduct.

KEY WORDS
dataveillance
individualization
control

Fernanda Bruno
Professora da Escola de Comunicação da UFRJ/RJ/BR
yfgbruno@matrix.com.br

Em novembro de 2007, o *Facebook*, uma das redes sociais mais populares dos EUA, tornou visível parte da vigilância digital inscrita em diversos ambientes na Internet. Essa vigilância, usualmente quase invisível, foi parcialmente revelada por um novo sistema de publicidade, o *Beacon Ads*. Segundo essa nova "publicidade social", os membros do *Facebook* podem ter a sua atividade nos sítios associados (The New York Times Co., Blockbuster, General Motors, Ebay etc.) monitorada e divulgada aos seus "amigos" na rede social, simulando uma propaganda "boca a boca". Se, por exemplo, um membro compra um filme num site associado ao *Facebook*, a sua rede de amigos pode receber uma notificação sobre a compra que fez, *links* para o produto, preços etc. O mecanismo publicitário permite, ainda, que empresas parceiras do *Facebook* tenham um perfil[1] similar aos dos demais membros e façam destes seus "amigos", ofertando produtos condizentes com seus perfis pessoais.

Em outros trabalhos (Bruno, 2006a; 2006b), mostrei como uma série de ambientes e serviços no ciberespaço, com finalidades diversas – sociabilidade (Orkut, Facebook), consumo (Amazon.com, E-bay), busca (Google Search Engine), entretenimento (YouTube, Second Life), informação (Google News, Google Zeitgeist) – continham, em seus próprios sistemas de funcionamento, meios de monitorar e classificar ações e comunicações dos indivíduos. Chamei estes mecanismos de dispositivo de vigilância digital e analisei os seus elementos centrais seguindo indícios mais ou menos seguros, dado que boa parte das ações deste dispositivo permanece pouco visível e conhecida. O *Beacon Ads*, entre outros casos, permitiu ver que as hipóteses propostas em trabalhos anteriores estavam bem trilhadas. Contudo, não é a aplicação publicitária da vigilância digital que me interessa, mas sim os seus mecanismos de monitoramento, classificação e controle dos indivíduos, que encontram no consumo e na publicidade apenas uma de suas muitas aplicações.

Na ocasião em que o *Beacon Ads* foi lançado, as notícias que circularam na grande mídia e na mídia independente tinham como preocupação central a privacidade dos usuários. Aliás, vale notar que o ano de 2007 foi farto em notícias e protestos contra a vigilância de dados e os seus atentados à privacidade. Essa vigilância discreta começa a entrar na pauta das discussões sociais e políticas, e o ano de 2007 foi significativo nesse sentido. No entanto, o foco na privacidade, embora legítimo, é limitado se não for acompanhado de uma problematização mais ampla dos processos característicos da vigilância digital. Vejamos por quê.

Dois argumentos, para ser breve: primeiro, é preciso

ter em mente que a noção de privacidade está em disputa. Ou seja, a definição tradicional, fundada nos princípios de proteção ao anonimato, à solidão e ao segredo, não é suficiente no contexto da vigilância digital (Gibbs et alli., 2005; Dholakia & Zwick, 2001). E mesmo a definição de informação individual do *Privacy Act*, já concebida nesse contexto, é insuficiente:

> Information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion. (The Privacy Act 1988, Sect 6).

A insuficiência, nesse caso, reside no princípio de identidade aparente ou passível de averiguação, pois muitas vezes pode-se prescindir dessa identificação. O próprio *Facebook* tornou anônimos seus bancos de dados antes de repassá-los às empresas associadas e não se pode dizer que com isso tenha respeitado a privacidade de seus membros. Em suma, é possível respeitar os princípios mencionados exercendo formas de monitoramento e uso de dados pessoais que colocam em risco o controle do indivíduo sobre as informações por ele geradas.

O segundo argumento: recolocar a questão da privacidade implica reforçar a sua dimensão coletiva, e não simplesmente privada e particular. Essa dimensão coletiva só pode ser problematizada se analisarmos os processos mais amplos de monitoramento, classificação e controle da informação individual, apreendendo o modo como os indivíduos e as identidades estão sendo produzidos, bem como as implicações ético-políticas em jogo. Este artigo pretende dar alguns passos nessa direção. Dando continuidade a textos anteriores, pretende-se aprofundar a análise dos processos indicados e mostrar como eles constituem um modelo taxonômico, epistêmico, identitário e preditivo, próprio às tecnologias de controle contemporâneas.

Definições e posições

Comecemos propondo a seguinte definição de vigilância digital: monitoramento sistemático, automatizado e à distância de ações e informações de indivíduos no ciberespaço, com o fim de conhecer e intervir nas suas condutas ou escolhas possíveis. Tal vigilância é aqui analisada segundo a noção de dispositivo, que conjuga três traços centrais: um conjunto de elementos heterogêneos, uma função estratégica, jogos e formações de poder e saber (Foucault, 1979). O dispositivo de vigilância digital tem entre seus principais elementos as tecnologias de monitoramento de ações, informações e comunicações dos indivíduos no ciberespaço, a montagem de bancos de dados e a elaboração de perfis computacionais (Bruno, 2006a). A compreensão destes elementos, das suas funções estratégicas e das relações de poder e saber que os atravessam depende de uma análise mais ampla dos seus processos constitutivos. Destaco quatro processos que, embora não se restrinjam à vigilância digital, se atualizam nela de forma singular: os mecanismos de coleta, monitoramento e arquivo de informação; os sistemas de classificação e conhecimento dos dados; os procedimentos de individualização e produção de identidades; as formas de controle sobre as ações e escolhas dos indivíduos.

Esses quatro processos são constitutivos dos sistemas de vigilância ao menos desde o século XVII. Supõe-se, assim, tanto a continuidade de alguns mecanismos modernos quanto a emergência de novas formas de vigilância e controle, ressaltando os contrastes entre a vigilância disciplinar e a digital. Esta última não é pensada segundo as metáforas sombrias do panoptismo e do Big Brother, em que se destacam a coerção e a dominação, mas segundo outras formas de governo da conduta humana, em que vigora uma ética de capitalização da liberdade e autonomia individuais (Rose, 1999)

.

Monitorar, coletar, arquivar

Nos últimos 40 anos, aproximadamente, vemos crescer vertiginosamente a capacidade de monitoramento e coleta de dados sobre indivíduos em diversos setores: trabalho, habitação, consumo, saúde, comunicações, deslocamentos, segurança, entretenimento, vida social, vida privada, etc. Essa bulimia de dados individuais é notável também na proliferação de tecnologias que já incluem em seu funcionamento mecanismos de monitoramento e coleta de dados individuais: cartões de crédito e de fidelidade, telefonia móvel, etiquetas RFID, cartões de transporte, sistemas de geolocalização por satélite, navegações e buscas on-line, participação em redes sociais, jogos ou ambientes colaborativos na Internet etc. Os sistemas de informação e comunicação da cibercultura se tornam tecnologias de vigilância potenciais. Lessig (1999), interrogado sobre o que há de novo na vigilância da era computacional, responde que é a facilidade de estocar e recuperar informações que derivam do monitoramento cotidiano das ações dos indivíduos.

A novidade não deve ocultar o longo histórico de coleta de dados sobre indivíduos e populações, elemento político importante de diversas tecnologias de governo. A história social dos números mostra que o termo "censor" (do qual deriva o nosso Censo estatal) data da antiguidade romana: o censor era tanto aquele que contava os homens para fins de taxação, obrigações militares e status político, quanto aquele que censurava e se encarregava do controle dos hábitos (Rose, 1999). A partir dos séculos XVII e XVIII, estreita-se a aliança das funções de vigilância e censura com as de cálculo e conhecimento. O termo "estatística" surge na Alemanha no século XVII significando "ciência dos Estados" e consistindo na coleta e tabulação sistemática de dados sobre cidadãos e fatos (Hacking, 1990), sendo posteriormente decisiva na máquina burocrática dos Estados modernos. Somos herdeiros dessa maquinaria, ainda

presente entre nós, mas ela é atravessada por novos processos e tecnologias que não apenas apontam a intensificação de mecanismos passados, como a emergência de modelos diferenciados de monitoramento e coleta dos dados.

Passemos a essas características diferenciais, iniciando pela pergunta sobre quem ou que instâncias são hoje capacitadas e/ou autorizadas a coletar dados individuais. A resposta poderia ser, no limite, qualquer um que tenha interesse e recursos técnicos para tanto, sendo estes cada vez mais acessíveis, automatizados e de baixo custo. Hoje é corriqueiro, por exemplo, tornar um simples sítio eletrônico um sistema de monitoramento dos seus visitantes e montar um razoável banco de dados sobre estes. Tanto o setor público quanto o privado podem hoje, respeitando regras mínimas de proteção à "privacidade", coletar, monitorar e estocar dados individuais. Não é necessário um saber específico, um posto de autoridade, uma autorização de centros de decisão. Até os anos 1970, aproximadamente, a coleta e estocagem de dados individuais pelo setor privado era pontual e eventual (Solove, 2004). A maior parte dos bancos e arquivos sobre indivíduos e populações era de domínio estrito e secreto dos Estados, constituindo um modelo centralizado, hierarquizado e exercido por figuras de autoridade científica ou administrativa. O cenário hoje é bastante distinto e vemos aumentar exponencialmente os bancos de dados tanto públicos quanto privados, bem como o cruzamento entre eles, constituindo uma *Personal Infomation Economy*, ramo bastante lucrativo de trocas informacionais (Lace, 2005). Além disso, essa massa de dados circula por uma rede descentralizada e com finalidades as mais distintas, da publicidade ao controle do crime, da promoção da saúde ao entretenimento.

Uma segunda característica diferencial consiste no tipo de dados coletados, ou seja, no que hoje se define como dado relevante e significativo. Podemos, grosseiramente, falar de dois conjuntos de dados: os relativamente estáveis, com pouca ou nenhuma variação ao longo do tempo, e os dados móveis ou circunstanciais. No primeiro estão, por exemplo, dados geodemográficos, biométricos, relativos a gênero etc. No segundo, constam dados comportamentais (comunicação, consumo, deslocamento, lazer), "transacionais" (uso de cartão de crédito e serviços, navegações em ambientes digitais), psicológicos (auto-declarações sobre personalidade, gosto), sociais (comunidades e amigos em ambientes digitais), entre outros.

É neste segundo conjunto que residem dados próprios à vigilância digital. Embora alguns não sejam novidade, muitos só se tornaram "coletáveis" de forma sistemática e ampla a partir da incorporação das novas tecnologias informacionais ao cotidiano. Estas permitiram uma coleta à distância e automatizada, capaz de capturar os dados em tempo real ou *in the wild*, sem as tradicionais mediações de entrevistadores e questionários. Além dessa facilitação, há um deslocamento do foco de interesse, que se volta menos para os atributos estáveis do que para os móveis e circunstanciais, cada vez mais particularizados. Esse deslocamento reflete um modo próprio de individualização em que tornam-se significativos e estratégicos os traços de superfície, provisórios e contingentes. Traços próprios às identidades modulares contemporâneas, distintos dos traços profundos e relativamente duráveis das identidades modernas.

Um último aspecto diferencial concerne à estocagem, cujo custo baixou enormemente nos últimos 30 anos, ampliando as capacidades de arquivo de toda sorte (Gandy, 2002). Detalhes de nossas vidas cotidianas e pessoais, antes perdidos no fundo de nossas memórias falhas, tornam-se hoje dados perenes e indefinidamente estocáveis. O termo *lifelog* surge para definir e questionar esse arquivamento minucioso da existência mediante tecnologias de computação pervasiva (Allen, 2007). Os tradicionais arquivos e próteses mnemônicas têm sempre limites de custo, espaço, duração e recuperação que abriam vacúolos de esquecimento em nossas memórias. Doravante, a potencial perenidade do arquivo o torna indefinidamente sujeito à interpretação e utilização futuras, o que tem efeitos nas formas de controle e predição da vigilância digital, conforme veremos. Na etimologia da palavra arquivo – *arkhê* – já estão os sentidos de começo e comando, como nota Derrida (2001). Dois princípios em um: o lugar em que as coisas começam e o ali onde os homens e os deuses comandam, onde se exerce a autoridade e a ordem social. Mas o sentido do arquivo também reside na classificação de seus conteúdos.

Classificar e conhecer

Qualquer conjunto de dados só ganha sentido se for analisado e classificado de modo a produzir conhecimento sobre a realidade ou os indivíduos a que se referem. No campo da vigilância, a história está repleta de vínculos entre o ato de inspecionar indivíduos e a produção de classificações e conhecimentos que permitam governar as suas condutas. Os procedimentos disciplinares criaram uma intensa acumulação de dados individuais que expressavam médias, fixavam normas e efetuavam, num mesmo gesto, a "liberação epistemológica das ciências do indivíduo" (Foucault, 1983). A estatística e o cálculo das probabilidades, por sua vez, buscavam apreender as leis do homem e fundar uma "física social" a partir das quais se criam, num só tempo, o ideal do "homem médio" e a era das massas (Ewald, 1996).

Os sistemas de classificação da vigilância digital inscrevem-se nessa linhagem, mas geram uma taxonomia própria com outras formas de individualização. Do mesmo modo, os grupos e populações não cabem confortavelmente nos termos modernos da massa. Os bancos de dados e perfis computacionais envolvem um sistema particular de classificação e conhecimento de indivíduos e grupos.

Os bancos de dados, em sua maioria, ordenam os

dados provenientes de indivíduos em categorias infra-individuais (Bruno, 2006a), podendo estas serem ou não atreladas a identificadores pessoais (como nome, endereço, número de CPF). Ressalto, retomando a questão da privacidade, que o caráter anônimo ou não do banco de dados pouco interfere nos seus efeitos sociais, taxonômicos e identitários. Vejamos.

As categorias infra-individuais podem ser criadas segundo um modelo "top-down", utilizando classes pré-estabelecidas – idade, gênero, profissão – ou segundo um modelo "bottom-up", gerando classes a partir da análise dos dados, como "freqüentadores do site Y que clicam nos links de tipo X"; "mulheres solteiras que usam pílula anticoncepcional e freqüentam sex shops". Essa categorização é submetida a um tratamento de segunda ordem, cujos métodos mais usuais são a mineração de dados (*data minig*) e a produção de perfis computacionais (*profiling*), os quais são complementares. A mineração de dados é uma técnica estatística aplicada que consiste num mecanismo automatizado de processamento de grandes volumes de dados cuja função central é a extração de padrões que gerem conhecimento. Não por acaso, este procedimento é chamado *Knowledge-Discovery in Databases* (Gandy, op.cit). Tais padrões são constituídos a partir de mecanismos de geração de regras, sendo mais comuns as de tipo associativo (similaridade, vizinhança, afinidade) entre pelo menos dois elementos, que depois diferenciam tipos de indivíduos ou grupos. Esses tipos correspondem a perfis computacionais gerados pelo mecanismo designado *profiling*. A geração de perfis segue uma lógica indutiva que visa "determinar indicadores de características e/ou padrões de comportamento que são relacionados à ocorrência de certos comportamentos" (Bennett, 1996).

Os padrões e regularidades daí extraídos permitem visualizar domínios com certa homogeneidade interna e fronteiras externas – de interesses, comportamentos, traços psicológicos – que de outro modo ficariam indefinidos ou fora do nosso campo de atenção. Assumem assim um formato mais dócil, calculável, legitimando e orientando intervenções diversas. Perfis de criminosos, consumidores, profissionais, doentes físicos ou mentais, tipos psicológicos ou comportamentais apresentam-se como padrões que ao mesmo tempo ordenam e objetivam a multiplicidade humana, legitimando formas de governá-la.

Mas que "ordem" humana e social está implicada nesse conhecimento gerado pela mineração de dados e perfis computacionais? Não se repetiria aí o tradicional meio de extrair normas e médias da diversidade social e humana, uma vez que se trata, mais uma vez, de determinar padrões e regularidades? Apostamos que não. A norma e a média são apenas um modo, moderno, de produzir padrão e de conceber a natureza e as leis humana e social. Os perfis são padrões que não representam nem a média nem a norma de um fator numa população – como o tamanho médio dos franceses de vinte e cinco anos (Quételet) ou o coeficiente médio de inteligência dos homens e mulheres (Binet). Não se trata, pois, de extrair uma regularidade (média) no seio de uma população e transformá-la num regulamento a ser seguido e avaliado (norma).

Diferentemente, os perfis encarnam múltiplas micro-regularidades no seio de inúmeras variáveis heterogêneas e, de modo algum, apresentam-se como regulamentos. A divisão norma/desvio não se aplica aos perfis, pois eles são padrões resultantes de combinatórias e regras associativas de tipo não valorativo entre muitas variáveis, podendo ser aplicáveis a potencialmente todas as qualidades e comportamentos humanos. O perfil não é nem uma medida nem um valor, mas um padrão de ocorrência de um certo fator (comportamento, interesse, patologia) num dado conjunto de variáveis. As médias e normas eram a referência comum das massas; os perfis são as micro-regularidades dos nichos, tribos, grupos.

Além disso, essas regularidades expressam tendências e potencialidades, em vez de refletirem uma natureza ou uma lei. Ainda que os perfis sejam padrões de similaridade interindividuais, eles não pretendem valer como leis do homem médio ou normal, mas como potencialidades dos mais variados tipos de indivíduos, dos mais gerais aos mais específicos. A taxonomia e o conhecimento não revelam aí um conjunto de características intrínsecas aos indivíduos, mas padrões de conduta e escolha na presença de fatores que constituem uma circunstância. Deste modo, a inadequação ao perfil não representa um desvio, mas uma contingência, uma particularidade a ser, não corrigida, mas incorporada ao próprio cálculo de determinação do perfil.

Teorias que utilizam o *profiling* para explicar a ocorrência de comportamentos criminosos, por exemplo, concebem o crime não mais como o resultado de uma patologia individual ou uma disfunção social, mas como um evento em que se articulam padrões motivacionais e "situações criminogênicas" (Garland, 2002). As teorias do criminoso ou da criminalidade cedem lugar à produção de perfis de ocorrência do evento criminal, o qual deve ser evitado por um controle das circunstâncias e oportunidades.

Todas essas diferenças entre os padrões presentes nos perfis computacionais e aqueles presentes nas noções modernas de média e norma ficarão mais claras se analisarmos a produção de identidades e individualizações em jogo.

Individualização e identidade

Os bancos de dados e sua taxonomia não são apenas máquinas epistêmicas, mas também máquinas identitárias. As identidades aí produzidas encontram nos perfis sua forma-padrão que implicam procedimentos específicos de individualização.

Como se viu, o perfil é um conjunto de traços que não concerne a um indivíduo particular, mas sim expressa

relações entre indivíduos, sendo mais interpessoal do que intrapessoal. O seu principal objetivo não é produzir um saber sobre um indivíduo identificável, mas usar um conjunto de informações pessoais para agir sobre similares. O perfil atua, ainda, como categorização da conduta visando a simulação de comportamentos futuros.

Tenho afirmado que os perfis são simulações de identidades (Bruno, 2006a), tanto no sentido de antecipação quanto no de modelização. Viu-se que os perfis são padrões estimativos que antecipam potencialidades - preferências potenciais de consumo, valor econômico potencial, tendências e inclinações comportamentais, capacidades profissionais, doenças virtuais. Um exemplo e uma visualização mais concreta da natureza dos perfis nos é dado por uma série de tabelas montadas a partir dos bancos de dados da rede social Club Nexus (Buyokkokten, 2003). Listo alguns elementos, uma breve amostra do modelo taxonômico em curso na cultura contemporânea, que deve ser semelhante ao da plataforma publicitária do Facebook.

Numa das tabelas que associava a forma como as pessoas usavam o seu tempo livre e os seus interesses acadêmicos, vemos padrões como: aqueles que passam o tempo livre estudando, tendem a se interessar por física, filosofia ou matemática; se preferem ver TV, demonstram interesse por relações internacionais; se passam a maior parte do tempo cumprindo compromissos, tendem a gostar de psicologia. Na tabela que associa traços de personalidade à escolha profissional, temos: aqueles que se declaram inteligentes, optam por física ou informática; os bem-sucedidos preferem informática, enquanto aqueles que se julgam atraentes, tendem a se interessar por relações internacionais ou ciência política. Numa grade mais ampla de nexos entre traços de personalidade e interesses diversos, encontramos: pessoas que se julgam atraentes costumam ler livros de negócios, assistir filmes eróticos, ouvir música "disco", fazer atividade física; os que se declaram pouco amáveis se interessam por livros de filosofia, escutam funk, vêem filmes eróticos ou independentes; os irresponsáveis gostam de filmes eróticos, GLS e independentes, costumam andar de skate e ouvir funk, jungle, reggae e trance; os socialmente adaptáveis gostam de livros de sociologia, praticam waterpolo e esqui, ouvem *house*, *rap* e *hip-hop*; os que se julgam bem sucedidos preferem os livros de negócios, jogam tênis, fazem atividades físicas para perder peso e gostam de fazer churrasco.

Vale notar que estes padrões não são baseados numa suposição de causalidade – ler livros de sociologia não leva ninguém a ouvir *house* ou *hip-hop* -, mas sim de correlação entre elementos. A determinação histórica, tão marcante da individualidade moderna, dá lugar à contingência das identidades contemporâneas. Noutros termos, o dossiê dá lugar ao perfil. Os aparatos disciplinares de vigilância constituíam dossiês com detalhes da trajetória de um indivíduo, suas falhas, evoluções, médias. Em nossas redes de vigilância digital, as trajetórias individuais interessam menos em sua unidade evolutiva do que em sua distribuição, fragmentação e combinatória. Isto é, interessam na medida em que possam gerar perfis, um agregado de características interpessoais que projetem tendências e padrões aplicáveis a comportamentos, personalidades, competências individuais. No dossiê, o indivíduo está presente *ab initio*; no perfil, o indivíduo e sua identidade surgem *a posteriori*.

As vigilâncias disciplinares criaram seus modelos de individualização descendente, em que aqueles sobre quem o poder se exercia eram os mais vigiados, examinados e registrados (Foucault, op. cit.). Crianças, loucos, histéricas, perversos e delinquentes preenchiam de detalhes a arquivística inglória dos dossiês e eram ainda mais individualizados que os medianos e normais. A vigilância digital desenha um outro eixo de individualização, que não apaga o anterior, mas se sobrepõe a ele. Podemos chamá-lo de individualização transversal ou combinatória, em que são mais vigiados, arquivados e classificados os indivíduos mais conectados às redes informacionais, e especialmente os que nelas são mais visíveis, participativos ou inseridos nos circuitos de consumo e civilidade. Estes serão mais classificados em bancos de dados e mais acessados por perfis de saúde, segurança, consumo, entretenimento etc. Surgem também, claro, novas formas de classificar criminosos, delinqüentes, doentes físicos ou mentais a partir de perfis, mas esses indicarão menos uma identidade a ser reformada, do que uma potencialidade a ser conjurada. Este ponto ficará mais claro adiante.

Mas os perfis são simulações também porque são modelizações da identidade. Como tais, não são representações fiéis ancoradas num referente, mas modelos que simulam uma realidade e encontram sua eficácia no efeito de real que produzem. Podemos falar aqui em efeitos de identidade, os quais não atendem a critérios de verdade e falsidade, mas sim de performatividade. O perfil é uma simulação pontual de identidades que ao se anunciar tem uma efetividade performativa e proativa, fazendo passar à realidade o que era apenas uma potencialidade. Aí reside uma última característica importante – a performatividade do perfil, que opera segundo um formato próximo ao oracular (Bruno, op. cit). Anuncia-se aqui a forma privilegiada de intervenção sobre as ações e escolhas indivíduos na vigilância digital.

Predição, Controle e Performance

Monitorar, arquivar, classificar, conhecer, individualizar, todos esses processos se conjugam a modos específicos de ação sobre os indivíduos, dentre os quais destacam-se os processos preditivos, constituindo uma série de "biografias futuras" (Bogard, 1996).

Que modalidade de futuro é aí produzida? Pode-se dizer que o perfil é uma espécie de oráculo na medida em que ele não implica uma acuidade na previsão de um futuro certo e necessário, mas a efetuação de uma reali-

dade antecipada. Tanto no perfil quanto no oráculo, trata-se menos de previsão do que da capacidade performativa da antecipação – o futuro antecipado torna-se efetivo ao ser enunciado.

Ao se montar, por exemplo, perfis de crianças hiperativas ou de jovens delinqüentes em áreas urbanas (Garland, op. cit), justificam-se campanhas de prevenção nos grupos de indivíduos que se "enquadram" neste perfil. Como se trata de uma virtualidade e não do diagnóstico de uma condição atual, o perfil só tem um efeito de verdade quando anuncia essa potencialidade, transformando tais crianças e jovens em doentes e delinqüentes que elas não eram antes da projeção do perfil. E se tais indivíduos e suas famílias acolhem esta projeção, efetiva-se mais fortemente o que se antecipou: eles passarão a se comportar, a se cuidar e orientar suas escolhas "como se" fossem, de fato, doentes ou delinquentes por antecipação, ainda que seja, paradoxalmente, para evitar a doença e a transgressão futuras. Se não acolhem, isso não significa que o perfil não tenha efeitos, pois uma série de acessos ou benefícios ligados à saúde, à educação ou ao trabalho podem ser dificultados ou negados a estes indivíduos.

O exemplo ajuda a compreender o tipo de intervenção que resulta dessas predições, que pretendem ser estratégicas em diversos setores. De um lado, essas simulações visam a redução de riscos nas políticas de investimentos, de publicidade, de saúde, de contenção do crime etc. De outro lado, elas visam agir sobre o campo de ações e escolhas possíveis dos indivíduos, ofertando a eles perfis que projetam cenários, produtos, riscos, interesses, tendências que devem incitar ou inibir comportamentos. Torna-se secundário reformar a alma, sendo a conduta e a ação os verdadeiros focos das tecnologias de controle e governo implicadas na vigilância digital. As identidades projetadas pelos perfis não visam tanto as consciências que sustentam a ação; elas dão um passo à frente e visam diretamente a própria ação. A "recompensa" e a "punição" que tais identidades trazem consigo é menos da ordem do ser, do que da ordem do acesso. Quanto maior a adequação ao perfil, maior é o acesso a circuitos de consumo e civilidade e mais perfis são gerados.

Não é de surpreender que um tal regime de predição e intervenção se constitua numa cultura em que o controle social se dá menos por coerção e prescrição de valores do que por simulação e incitação à realização e obtenção de resultados. Segundo Rose (op. cit), uma das principais características das tecnologias de controle atuais é sua pulverização em redes não hierarquizadas, em que a conduta dos cidadãos é continuamente modulada por uma lógica imanente ao conjunto de práticas sociais, "de acordo com princípios de otimização dos impulsos benignos e minimização dos malignos" (Idem, p. 325). O controle é exercido em regime de parceria pelos diversos agentes sociais, obedecendo a uma ética de compartilhamento de responsabilidades e riscos, de auto-controle e auto-gestão. Vale notar, ainda, que o caráter preditivo-performativo dos perfis conjuga-se a uma cultura da performance e nela atua tanto como tecnologia de capacitação das escolhas individuais quanto como tecnologia de controle.

A valorização da performance em nossa cultura tem uma trajetória longa e complexa, que ultrapassa os limites deste artigo. Resumiremos ao máximo esta trajetória, considerando o desenvolvimento, desde os anos 1960, de uma dinâmica de emancipação constituída tanto pelas reivindicações identitárias no plano político-social (mulheres, homossexuais), quanto pela incitação à iniciativa pessoal e à autonomia que, a partir dos anos 1980, estende o modelo de superação de si da competição esportiva e do empreendedorismo empresarial aos modos de vida individuais (Ehrenberg, 1999). Este duplo movimento põe em crise os modelos disciplinares de gestão de si, dando progressivamente lugar a um pluralismo normativo em que o indivíduo é cada vez mais proprietário de si mesmo. Emancipado das interdições que o impediam de escolher a própria vida, o indivíduo se vê atrelado ao imperativo oposto – o da autonomia, da iniciativa, da superação e escolha continuada. O empreendedorismo na vida privada e pública torna-se regra e a performance torna-se um modelo de estilo e sucesso das existências individuais.

Desde a década de 1990, com a difusão das mídias digitais e da Internet, a valorização da performance e da autonomia ganha novo fôlego com a possibilidade de os indivíduos passarem a produzir e distribuir informação e conteúdos diversos – música, literatura, vídeo, vida pessoal etc. Há bem pouco tempo, não mais que cinco anos, mais um impulso à iniciativa digital vem sendo anunciado como um novo modelo de produção de conteúdos em que participação e colaboração são centrais. Este impulso é em grande parte identificado com os ambientes da Web 2.0, cujas potencialidades são múltiplas e certamente não se reduzem a uma mera capitalização das performances individuais. As chamadas culturas livres e seu espírito colaborativo estão aí para mostrar que vias alternativas estão sendo traçadas, e esse é apenas um entre muitos exemplos. Mas no que tange ao tema aqui em questão, este impulso participativo pode ir de par com as tecnologias de vigilância e controle.

Rose (1999) observa que tais tecnologias operam através da instrumentalização de uma forma particular de liberdade. O autor sugere que as formas de poder e governo nas sociedades pós-industriais dependem cada vez mais da mobilização das capacidades pessoais e subjetivas dos indivíduos, entendidos como "livres para escolher" (Rose, op. cit). Conforme Lianos,

> O controle forma, assim, um dos componentes da liberdade pós-industrial. Ele se exprime nas regras de produção e utilização de sistemas, processos e objetos que são desejáveis como meios consagrados à construção autônoma da biografia individual e

da ação coletiva (2001, p.18).

As taxonomias e identidades produzidas pelos bancos de dados, a atuação dos perfis como tecnologias performativo-preditivas de controle e instrumentalização das escolhas individuais merecem ser incluídas nas reflexões sobre os efeitos da vigilância digital, atestando o quanto a violação à privacidade é apenas um dos aspectos que, embora relevante, é mais imediato e superficial. Sem problematizar essa dimensão pública e coletiva do dispositivo de vigilância contemporâneo, os jogos de saber, poder e controle aí implicados restarão confinados aos embates jurídicos e monetários de interesses privados ■FAMECOS

NOTAS

* Trabalho apresentado ao Grupo de Trabalho "Comunicação e Cibercultura", do XVII Encontro da Compós, na UNIP, São Paulo, SP, em junho de 2008.

1. Na sessão "Facebook pages", própria para os anunciantes**.**

REFERÊNCIAS

ADAMIC, L.; BUYOKKOKTEN, O. & ADAR, E. *A social network caught in the web.* First Monday, 8, 6, 2003.

ALLEN, A. *Dredging-up the Past: Lifelogging, Memory and Surveillance.* University of Pennsylvania Law School, 2007.

BENNET, C. J. The public surveillance of personal data: a cross-national analysis. In: LYON, D. (Org.). *Surveillance as social sorting*. Londres: Routledge, 37-49, 1996.

BOGARD, W. *The simulation of surveillance.* Cambridge University Press, 1996.

BRUNO, F. Dispositivos de vigilância no ciberespaço: duplos digitais e identidades simuladas. In: *Revista Fronteira*, São Leopoldo/RS, v. VIII, pp. 152-159, 2006a

_____. et alli. *O oráculo de Mountain View: o Google e sua cartografia do ciberespaço.* Ecompós, Brasília, v. 6, p. 1-21, 2006b.

DELEUZE, G. *Conversações*. São Paulo: 34, 1992.

DERRIDA, J. *Mal de arquivo.* Rio de Janeiro: Relume Dumará, 2001.

DHOLAKIA, N.; E ZWICK, D. Privacy and Consumer Agency in the Information Age. *JRConsumers.com*, 1, 1-17, 2001.

EHRENBERG, A. *Le culte de la performance.* Paris: Hachette, 1999.

EWALD, F. *Histoire de l'État Providence*. Paris : Grasset, 1996.

FOUCAULT, M. *Vigiar e Punir*. Petrópolis: Vozes, 1983.

GANDY, O. *Data mining and surveillance in the post-9.11 environment*. *IAMCR*, 2002.

GIBBS, M.; SHANKS, G.; LEDERMAN, R. Data Quality, Database Fragmentation and Information Privacy. *Surveillance & Society*, 3, 1, p. 45-58, 2005.

HACKING, I. *The taming of chance*. Cambridge University, 1990.

LACE, S. *The glass consumer*. Londres: Policy Press, 2005

LESSIG, L. *Code, and Other Laws of Cyberspace*. New York: Basic Books, 1999.

Lianos, M. *Le nouveau controle social*. Paris. L'Harmattan, 2001.

ROSE, N. *Powers of freedom*. Cambridge University, 1999.

SOLOVE, D. *The digital person*. New York: NYU Press, 2004.