revista Fronteiras – estudos midiáticos
VIII(2): 152-159, maio/agosto 2006

Dispositivos de vigilância no ciberespaço: duplos digitais e identidades simuladas

Fernanda Bruno[1]

O artigo trata dos dispositivos de vigilância hoje inscritos no ciberespaço e suas implicações para a produção de identidades e subjetividades. Pretende-se mostrar como o monitoramento de ações e comunicações no ciberespaço é convertido em informações que irão compor bancos de dados e perfis computacionais que buscam antecipar preferências, tendências, escolhas, traços psíquicos ou comportamentais de indivíduos ou grupos Para tanto, analisa-se a lógica de composição de bancos de dados e de perfis computacionais, visando apreender aí os traços gerais da produção de duplos digitais e da simulação de identidades.

Palavras-chave: vigilância, ciberespaço, identidade.

Surveillance technologies in cyberspace: data doubles and simulated identities. This article deals with the surveillance technologies in cyberspace and their implications on the production of identities and subjectivities. It aims to show how the monitoring of actions and communication in cyberspace is converted into information that creates data bases and computer profiles designed to anticipate preferences, trends, choices and psychic or behavioral features of individuals or groups. Hence, it analyzes the logic of computerized profiles and data bases, aiming at understanding the production of data doubles and the simulation of identities.

Key words: surveillance, cyberspace, identity.

Cet article analyse les dispositifs de surveillance dans le cyberspace et leur rôle dans la production des identités et des subjectivités. Il vise à montrer comment la surveillance des actions et des communications dans le cyberespace est transformée en informations qui sont constituées en bases de données et en profils. Ceux-ci procèdent par l'anticipation des préférences, des tendances, des choix et des traits psychiques ou comportementaux des individus ou des groupes. Pour comprendre ce phénomène on analyse la logique des profils et des bases de données, visant à appréhender la production des doubles digitaux et la simulation des identités.

Mots-clés: surveillance, cyberspace, identité.

[1] Doutora em Comunicação e Cultura pela Universidade Federal do Rio de Janeiro. Professora do Programa de Pós-Graduação em Comunicação da UFRJ. Coordenadora da Linha Tecnologias da Comunicação e Estéticas do PPGCOM/UFRJ. Coordenadora do CiberIdea: Núcleo de Pesquisa em Tecnologias da Comunicação, Cultura e Subjetividade/UFRJ. E-mail: fgbruno@matrix.com.br

De: yyyyyyy@gmail.com
Para: xxxxxxx@gmail.com
Data: 03/06/2005
Assunto: Re: sonho

Ah bom, agora entendi o sonho...
Mudando de assunto, vc já viu esses links aí do lado direito?? Nunca tinha visto, fiquei surpreso; eles lêem o conteúdo das mensagens?

De: xxxxxxxx@gmail.com
Para: yyyyyyy@gmail.com
Data: 03/06/2005
Assunto: Re: sonho

Sim, já tinha visto, mas felizmente nem sempre eles acertam ;-)) e segundo o "Termo de Privacidade do GMAIL", "nenhum humano lê as suas mensagens ... o Gmail veicula anúncios relevantes usando um processo completamente automatizado".

A conversa acima se passa no *Gmail*, serviço gratuito de webmail disponibilizado pelo *Google* (www.gmail.com). Os *links* mencionados nestas mensagens são anúncios direcionados, baseados no conteúdo do e-mail exibido. Se, por exemplo, você usa o termo "viagem" em um e-mail, aparece no canto direito de sua tela uma série de *links* como: "Quer viajar de graça?", "Zeus Táxi Aéreo", "STB Viagem Internacional". Se usa "olhos", os *links* podem ser "Oftalmo Care", "Eye Care Hospital de Olhos", "Excelência Oftalmológica". O que primeiro inquieta nesses anúncios é o fato de eles serem direcionados segundo o conteúdo das mensagens enviadas/recebidas. A primeira pergunta é se tais conteúdos são lidos pelos técnicos do *Gmail*, o qual responde, como vimos, que ninguém os lê, isto é, nenhum humano, mas sim programas informáticos automatizados. Vejamos com mais detalhes o que diz o *Gmail*:

> *Após efetuar login em sua conta Gmail, o Google exibirá anúncios direcionados e outras informações relevantes baseadas no conteúdo do e-mail exibido. Em um processo completamente automatizado, computadores processam o texto em uma mensagem e relacionam-no a anúncios ou informações relacionadas no amplo banco de dados do Google. Nenhuma pessoa lê sua correspondência para direcionar anúncios ou outras informações sem seu consentimento. Os anunciantes recebem um registro do número total de impressões e cliques para cada anúncio. Nenhuma informação pessoal de quem visualizou o anúncio é recebida [...] Contudo, quando você estiver no site do anunciante, ele pode coletar informações pessoais sobre você* (http://mail.google.com/mail).

Passada a impressão de que suas mensagens estão sendo lidas sem o seu conhecimento e consentimento, uma olhada mais demorada nos anúncios exibidos logo revela a fragilidade da precisão na "oferta" de "anúncios relevantes e *links* de seu interesse". Ainda que seja esta a intenção, há falhas evidentes. Além do número limitado de anunciantes, o programa de direcionamento de conteúdo não é capaz de contextualização semântica, não é capaz, por exemplo, de saber se a "viagem" em questão é uma viagem de férias, uma viagem imaginária, um desvario do pensamento; ou se os "olhos" escritos na mensagem são biológicos, sensoriais, metafóricos. Além disso, em algumas ocasiões os anúncios e *links* são tão díspares que é impossível saber que princípio de classificação os mobiliza e/ou que palavras-chave lhes serviram de base. É possível, por exemplo, que se direcione para um mesmo conjunto de mensagens o seguinte grupo de anúncios e links: "Mensagem do Graal", "Livro de Fotos do Brasil", "Aluguel de Roupas", "Quer um celular novo?" e "Ramos e soluções web". Neste caso, é impossível saber o que reúne temas tão díspares num mesmo grupo, classe ou categoria.

Mas o que precisamente nos interessa neste exemplo que abre nosso artigo? Ele introduz o tema que se pretende explorar: os novos dispositivos de vigilância inscritos no ciberespaço e suas implicações para a produção de identidades e subjetividades. Pretende-se mostrar como o monitoramento de ações e comunicações no ciberespaço é convertido em informações que irão compor bancos de dados e perfis computacionais que buscam antecipar preferências, tendências, escolhas, traços psíquicos ou comportamentais de indivíduos ou grupos. No exemplo mencionado, já encontramos algumas das principais características dessa nova forma de vigilância. Em primeiro lugar, trata-se de uma vigilância que não mais isola e imobiliza indivíduos em espaços de confinamento, mas que se aproxima ou mesmo se confunde com o fluxo cotidiano de trocas informacionais e comunicacionais. Uma vigilância que se exerce menos com o olhar do que com sistemas de coleta, registro e classificação da informação; menos sobre corpos do que sobre dados e rastros deixados no ciberespaço; menos com o fim de corrigir e reformar do que com o fim de projetar tendências, preferências, interesses. No nosso exemplo, as mensagens cotidianas enviadas pelos usuários do *Gmail* são monitoradas por programas que irão coletar, processar e classificar conteúdos das mensagens em bancos de dados e constituir perfis que projetem informações sobre possíveis interesses desses usuários, aos quais os anúncios e *links* visam

atender. Nota-se que a comunicação entre indivíduos é quase que automaticamente convertida em informação a seu respeito. Além do *Gmail* e outros serviços do *Google*, há muitos outros exemplos de constituição de um novo dispositivo de vigilância e controle cuja morada é o ciberespaço. Vejamos mais de perto quais são as peças deste dispositivo que qualificamos de novo.

O dispositivo: informação, banco de dados, perfis

Se tomarmos como referência as análises de Foucault sobre os dispositivos de vigilância na Modernidade, identificamos dois elementos centrais: o olhar (as táticas do ver e do ser visto) e as técnicas de coleta, registro e classificação da informação sobre os indivíduos. Tais dispositivos instauram um regime de visibilidade que é inseparável da própria constituição da subjetividade e do indivíduo moderno. As instituições disciplinares funcionam como verdadeiros observatórios da multiplicidade humana e inauguram um mecanismo de vigilância que individualiza pelo olhar, colocando cada indivíduo sob o foco de uma visibilidade que atravessa e ao mesmo tempo produz seu corpo e sua alma (Foucault, 1983a).

Além do olhar, a informação é o segundo elemento-chave dos dispositivos de vigilância. O alcance e os efeitos da observação disciplinar não poderiam contar apenas com o olhar, eles requeriam também todo um "sistema de registro intenso e de acumulação documentária" (Foucault, 1983a, p. 168) ... com seus métodos de identificação, de assimilação ou de descrição. Na escola, no exército, na fábrica, nos hospitais, nas prisões, os sujeitos são, ao mesmo tempo, olhados e objetivados através de exames que irão constituir registros dos seus dados individuais (suas competências, evoluções, falhas, sintomas, características físicas e psíquicas, biografia etc.) e organizar campos comparativos que permitam classificar, formar categorias, estabelecer médias, fixar normas (Foucault, 1983a, p. 169). Foucault reconhece neste "aparelho de escrita, nestas pequenas técnicas de anotação, registro, de constituição de processos, de colocação de colunas um dos agentes fundamentais da liberação epistemológica das ciências do indivíduo" (Foucault, 1983a, p. 169). Vemos que a Modernidade faz o indivíduo comum entrar não apenas num campo de visibilidade, mas também num campo de informações, notações e descrições, até então privilégio dos heróis e do poderio. Ao figurar nestes campos, o indivíduo se constitui, ao mesmo tempo, como "um objeto para o conhecimento e uma tomada para o poder" (Foucault, 1983a, p. 170).

Ao voltarmos a atenção para os dispositivos de vigilância contemporâneos, particularmente para a vigilância digital, vemos uma enorme ampliação das capacidades de coleta, registro e processamento de informações sobre indivíduos. Diversos autores vêem aí uma espécie de superpanóptico, que não mais se restringe aos espaços fechados das instituições, mas se estende tanto sobre dimensões alargadas do espaço físico quanto sobre o ciberespaço, ampliando enormemente o número de indivíduos sujeitos à vigilância (Lyon, 2003; Poster, 1995; Bogard, 1996, Norris e Armstrong, 1999; Marx, 2002). No entanto, se compararmos tais sistemas informacionais com os sistemas disciplinares e panópticos, notaremos algumas transformações nas técnicas e procedimentos adotados, nos jogos de poder e de saber, nos efeitos sobre a subjetividade e a identidade. Este artigo prioriza a análise destas transformações que integram os atuais dispositivos de vigilância. Se a modernidade inventou o seu "aparelho de escrita", próprio das engrenagens da disciplina, aparelho essencial para a constituição do indivíduo moderno e de sua identidade, qual é o aparelho ou dispositivo constituído pelas novas tecnologias de informação e de comunicação? Qual é a sua gramática e quais são seus efeitos sobre os indivíduos e suas identidades?

Em linhas gerais, o dispositivo de vigilância digital tem três elementos centrais: a informação, os bancos de dados e os perfis computacionais (*profiles*). A informação é o elemento-base, a ponto de a vigilância atual ser freqüentemente designada na língua inglesa como *dataveillance* (Clarke, 1994). A convergência da informática com as telecomunicações criou uma situação em que o campo de comportamentos, ações e comunicações dos indivíduos muitas vezes coincide com os próprios sistemas de coleta, registro e distribuição de informação. As mesmas tecnologias que ampliam as possibilidades de emissão, acesso e distribuição da informação tornam-se instrumentos de vigilância e controle; as mesmas tecnologias que possibilitaram o anonimato nas trocas sociais e comunicacionais mostram-se eficientes instrumentos de identificação. A vigilância se confunde hoje com a própria paisagem do ciberespaço.

Nota-se neste processo a diminuição relativa da importância da visão e do olhar. A economia do poder na vigilância digital parece prescindir da presença visível do observador e do observado. Na maioria das vezes, a vigilância se dá sobre informações e não sobre pessoas. Os dados não são, em si mesmos, nem muito reveladores nem facilmente acessíveis aos sentidos nus, pois, além de serem extremamente

numerosos, são fragmentados e não compõem um indivíduo a ser apreendido pelo olhar; estes indivíduos só emergem num segundo momento graças às técnicas de composição de perfis computacionais. Este processo é especialmente claro na convergência do uso de câmeras de vigilância com os bancos de dados e as técnicas de composição de perfis. O uso exclusivo de câmeras de vigilância mostrou-se pouco eficaz para os propósitos policiais e de segurança na medida em que o imenso volume de imagens geradas é praticamente impossível de ser processado de modo a produzir identificações precisas e informação individualizada (Norris, 2003). Além disso, embora a câmera possa atuar como um dispositivo preventivo (inibindo a ocorrência de crimes e infrações), ela não tem alcance preditivo e antecipatório, como querem as atuais políticas de segurança. O futuro das câmeras ou do olhar é, neste caso, a digitalização. "Com os sistemas de detecção de vídeo digitais, a própria imagem de vídeo se torna a fonte de informação" (Norris, 2003, p. 268-269). Associadas a bancos de dados e a procedimentos de composição de perfis, as imagens geradas pelas câmeras conjugarão uma ampliação do alcance do olhar com uma expansão da capacidade de coletar e produzir informação individualizada.

> *Doravante, todos os que passarem sob este olhar vigilante digitalizado poderão ser classificados como infrator/não-infrator, suspeito/insuspeito, procurado/não procurado etc. A classificação não mais reside no conhecimento face a face; ela está inscrita no banco de dados* (Norris, 2003, p. 270).

Ou seja, não basta ver e documentar, é preciso classificar e produzir conhecimento, de modo a aumentar o poder social da informação coletada. Aí entram os bancos de dados, seus algoritmos e os perfis computacionais. É central na vigilância contemporânea a composição e o cruzamento de bancos de dados *on-line* e *off-line* de diversos tipos (comportamental, biométrico, genético, geodemográfico etc.) e com propósitos diferentes. Supõe-se que o acesso a tais fontes de informação sobre indivíduos e populações seja o melhor método de checar e monitorar comportamentos, influenciar pessoas e populações, antecipar e prevenir riscos (Lyon, 2003). Esta máquina de coletar e processar informação é também uma máquina epistemológica, que deve converter tais informações em conhecimento sobre os indivíduos e/ou grupos.

Se compararmos o dispositivo disciplinar com o dispositivo atual, perceberemos que no primeiro a informação é extraída de uma observação presencial e a partir de procedimentos hermenêuticos que procuram desvelar, para além do comportamento e dos aspectos visíveis, uma interioridade, uma personalidade ou um psiquismo que se encontravam insinuados na superfície dos discursos e atos. Deste modo, o indivíduo era, ao mesmo tempo, conhecido na sua "singularidade" e incluído numa categoria geral condizente com a sua estrutura psíquica, comportamental, sintomatológica, patológica etc. Na vigilância digital, o ritual do exame e seus procedimentos hermenêuticos são substituídos pelos perfis computacionais e seus procedimentos algorítmicos e estatísticos. Muitas vezes, o indivíduo não se oferece à observação nem como uma "presença" nem como uma totalidade ou unidade a ser interrogada, examinada, conhecida. Uma ação ou comunicação sua gera uma informação que, muitas vezes, corresponde a uma parcela ou fragmento de sua existência – consumidor, profissional, paciente etc. – e que irá figurar em bancos de dados ordenados segundo certas categorias gerais. Isto é, neste caso a informação é, ao mesmo tempo, pessoal, individualizada (posto que são ações e comunicações individuais que as geram) e relativamente desvinculada do próprio indivíduo, seja porque ela pode constar nos sistemas de registro e coleta segundo uma classificação impessoal e não identificada a indivíduos particulares (gênero, raça, faixa etária, classe social etc.), seja porque ela pode interessar apenas na sua parcialidade, sem relação necessária com outras dimensões da identidade ou existência dos indivíduos (como certos *spams* publicitários, direcionados para grupos específicos que são eleitos por possuírem uma característica comum, como a profissão), seja porque a informação geralmente antecede o indivíduo (enquanto presença e totalidade/unidade) nos sistemas de coleta e registro.

Cabe perguntar se esse processo de "observação" sem olho, rosto ou nome sobre dados inicialmente impessoais merece ainda o nome de vigilância e se ele pode ter algum efeito sobre a subjetividade e a identidade. Para responder a esta questão, é preciso compreender melhor a lógica dos bancos de dados e dos perfis computacionais.

Os bancos de dados não concernem, primeiramente, a indivíduos ou pessoas particulares, mas a grupos e populações organizados segundo categorias financeiras, biológicas, comportamentais, profissionais, educacionais, atuariais, raciais, geográficas, legais etc. Eles se situam inicialmente num nível infra-individual. No entanto, não têm apenas a função de arquivo, mas uma função conjugada de registro, classificação, predição e intervenção. Com o uso de algoritmos e programas de composição de perfis, os bancos de dados pretendem conter tanto o saber quanto o controle sobre o passado, o presente e o futuro dos indivíduos. Mas a sua lógica é menos a da exatidão no registro da informação do que a da agilidade e eficiência na sua recuperação e utilização (Poster, 1995), que é sobretudo preditiva. O

cruzamento de dados organizados em categorias amplas irá projetar, simular e antecipar perfis que correspondam a indivíduos e corpos "reais" a serem pessoalmente monitorados, cuidados, tratados, informados, acessados por ofertas de consumo, incluídos ou excluídos em listas de mensagens publicitárias, marketing direto, campanhas de prevenção de algum tipo de risco etc.

Há inúmeras empresas de pesquisa na Internet, como a *Redsheriff*, *DoubleClick* e *Bluestreak*, por exemplo, que rastreiam os movimentos dos internautas que visitam os sites a elas filiados e produzem um registro de suas atividades *on-line*: que sites visitam, que arquivos baixam, que tipo informação buscam. Tais empresas constroem, assim, valiosos bancos de dados sobre os usuários, suas preferências e interesses atuais e potenciais. É importante notar que o próprio ato de classificação dos indivíduos nestes segmentos já tem um potencial estimativo a partir do qual serão compostos perfis de indivíduos. "Este procedimento, conhecido como *computer profiling,* segue uma lógica mais indutiva 'para determinar indicadores de características e/ou padrões comportamentais que são relacionados à ocorrência de certo comportamento'" (Bennett, 1996, p. 241). A partir da análise desses dados e da correlação entre múltiplas variáveis, compõem-se perfis do consumidor "típico" de música eletrônica, do portador de doenças cardiovasculares, do traficante, do bom administrador etc. Tais dispositivos operam como máquinas inferenciais de diferenças (Gandy, 1996), e os perfis aí gerados muitas vezes promovem a passagem do infra-individual para o individual.

O saber aí constituído não concerne apenas à identidade atual dos indivíduos, mas também ao seu valor econômico potencial, suas preferências potenciais de consumo, suas tendências e inclinações comportamentais, suas capacidades profissionais, aos riscos a que estão sujeitos, às doenças que podem vir a desenvolver. Vale ainda notar que o principal objetivo em jogo não é tanto produzir um saber sobre um indivíduo especificamente identificável, mas usar um conjunto de informações pessoais para agir sobre outros indivíduos, que permanecem desconhecidos até se transformarem em perfis que despertem algum tipo de interesse médico, comercial, legal, financeiro, governamental etc. Esse saber é, ao mesmo tempo, controle, pois antecipa o que cada um é, o que pode fazer e o que pode "escolher".

Um conhecido exemplo comercial de composição de perfis é a *amazon.com*, livraria virtual, onde o ato de consumo ou busca em seu *site* deixa rastros que são convertidos em informação e estratégias de marketing. A livraria disponibiliza agentes "facilitadores" de busca e compra que geram ainda mais conhecimento sobre as preferências, tendências e inclinações de seus consumidores. Um dos objetivos centrais desses agentes é antecipar para o consumidor desejos e preferências na forma de oferta de produtos que ele sequer havia pensado ou sabia que existiam. Trata-se de uma "oferta" que pretende ser superindividualizada, mas essa individualização almejada pelo perfil é menos da ordem da verdade ou da representação do que da ordem da simulação, da performatividade e da proação[2]. Isto é, o perfil é menos um retrato fiel que representa, neste caso, a verdade dos desejos inerentes ao consumidor do que uma simulação deste desejo, que, ao se anunciar, tem uma efetividade performativa e proativa, fazendo passar à realidade o que era apenas uma possibilidade, uma potencialidade.

Um outro exemplo relativamente familiar é a produção de perfis no campo da saúde, mais especificamente da epidemiologia dos fatores de risco. A partir da análise e cruzamento de dados como faixa etária, gênero, dados genéticos e hábitos de vida, são estabelecidas correlações entre a presença de certas características e a probabilidade de ocorrência de certas doenças. Deste modo, são produzidos perfis de portadores de doenças crônico-degenerativas, por exemplo, que não indicam a presença destas enfermidades no corpo atual de um indivíduo, mas antecipam uma virtualidade e, neste mesmo movimento, a tornam efetiva, na medida em que o indivíduo passa a se portar como um doente virtual, mudando a sua dieta alimentar, seus hábitos de vida, realizando exames médicos etc. Também aqui o perfil é mais performativo que verdadeiro, mais proativo que representativo.

Para a vigilância inscrita nos bancos de dados e perfis, a previsão e a antecipação de tendências são mais importantes que a detecção de uma presença qualquer. Enquanto o panóptico encarnava um modelo ótico e espacial de visão total, a vigilância digital põe em obra uma visibilidade que é sobretudo informacional e temporal, onde não basta tudo ver, mas principalmente prever, a ponto de preceder o evento. Ou melhor, tudo ver no âmbito do espaço e dos corpos atuais e presentes só faz sentido, só é operacional se essa visão for capaz de projetar cenários, tendências, preferências. E mais, essa antevisão produz efeitos não tanto pela sua acuidade na previsão do futuro, mas sim pelo próprio processo de antecipação, que acaba por intervir nas escolhas, comportamentos e ações presentes, tornando efetivo o que se antecipou. Tais antevisões não são, portanto, nem

[2] A noção de personalização proativa ganha força no marketing (Dholakia e Zwick, 2001).

verdadeiras nem falsas, mas efetivas, performativas. Na língua inglesa o próprio termo "*profile*" (perfil) expressa essa temporalidade da vigilância digital – um "pro-file" é um pré-registro, uma pré-ordenação. Percebe-se que nessa vigilância se constituem "objetos", ou melhor, "sujeitos" de uma visão futura, e é precisamente este processo que nos interessa na análise dos efeitos sobre a produção das identidades e subjetividades contemporâneas.

Duplos digitais, identidades simuladas

As implicações da vigilância digital nas subjetividades e identidades contemporâneas permanecem indefinidas e em grande parte desconhecidas. Apontaremos aqui algumas hipóteses ainda provisórias tendo em vista situações em que essa vigilância discreta, tão maquínica quanto humana, pode ser direta ou indiretamente matéria de experiência dos indivíduos e do modo como eles se concebem, cuidam de si mesmos e efetuam suas escolhas em certos domínios de suas vidas. Ressaltaremos o caráter preditivo, antecipatório e performativo da vigilância digital.

As identidades projetadas em bancos de dados na forma de perfis computacionais são espécies de duplos digitais ou simulações de identidades cuja efetividade não depende de vínculos profundos com os indivíduos a que correspondem, nem de um espelhamento fiel de uma personalidade ou caráter subjacentes. Ou seja, elas não *são* identidades "dadas', mas *se tornam* "reais" ou "efetivas" na sua função antecipatória mesma, quando os indivíduos se identificam ou se reconhecem de algum modo no perfil antecipado, acionando desde então algum tipo de comportamento, cuidado ou escolha. Quando, por exemplo, aceito uma oferta personalizada de produto que eu nem mesmo sabia existir ou que não havia desejado previamente, torno efetivo o perfil ou identidade que me foi antecipado e, ao mesmo tempo, reforço-o para futuras previsões tanto a meu respeito quanto a respeito de outros indivíduos que habitam bancos de dados similares. Os bancos de dados e seus perfis operam, pois, como máquinas performativas (Poster, 1995) com uma função quase "oracular", dado que não representam uma realidade prévia ou subjacente, nem prevêem um futuro certo e necessário, mas efetuam uma 'realidade' ou "identidade" na medida mesma em que a prevêem, a projetam ou a antecipam.

Nota-se que essa nova maquinaria identitária dispensa pouca atenção à interioridade dos sujeitos que ela visa, ressaltando o processo de exteriorização das subjetividades contemporâneas. É da exterioridade das ações, comportamentos e transações eletrônicas que se extrai ou se projeta a subjetividade, com uma identidade que não estava plenamente presente. Claro que o indivíduo, a subjetividade, a identidade são sempre, em alguma medida, efeitos do processo de vigilância, de modo que eles nunca estão inteiramente dados, mas são em grande parte constituídos, transformados por esse processo. Contudo, se mais uma vez o comparamos com a vigilância disciplinar, notamos que aí a presença física do louco, do criminoso, do perverso, do doente é desde o início requerida. E o que faz deles esses seres marginais é o peso de uma história familiar, a força insistente de desejos inconscientes, uma intrincada e obscura causalidade psicológica, que vêm determinar, do seu interior em sombra, uma série de ações e comportamentos exteriores e visíveis. Eis por que a vigilância moderna deve ver e agir *através*, *sob* a superfície dos corpos e comportamentos de modo a incidir sobre a interioridade, a alma dos indivíduos. Na atualidade, trata-se sobretudo de ver *adiante*, de *prever* e predizer, a partir dos cruzamentos e análises de dados, indivíduos e seus atos potenciais; seja para contê-los (como no caso de crimes, doenças, em que tende a predominar uma vigilância preventiva), seja para incitá-los (como no caso do consumo, da publicidade e do marketing).

A vigilância moderna instaurava uma série de rituais de observação e exame que deviam tornar as superfícies transparentes e revelar, sob os disfarces da aparência, a verdade recolhida na profundidade dos corpos e almas. Diferentemente, a vigilância digital não está tão interessada na verdade e na profundidade, mas na performance, nos fluxos de informação e comunicação. A visibilidade aí construída não corresponde ao desvelamento de uma profundidade essencial, mas à antevisão e construção de superfícies ou cenários que orientem e intervenham no campo de ações, escolhas, cuidados dos indivíduos.

Transformações recentes nas estratégias de marketing fornecem um bom exemplo dessa passagem da vigilância disciplinar para a digital. Num interessante artigo sobre mobilidade e pesquisa de marketing, Arvidsson (2004) mostra como as pesquisas sobre motivação e consumo até as décadas de 1960/70 supunham que as verdadeiras fontes de decisão residiam escondidas na profundidade do inconsciente do consumidor. Progressivamente, a identidade do consumidor passa a ser pesquisada, definida e vigiada na sua mobilidade no espaço físico e midiático.

> *By means of in-depth interviews, motivation researchers thus tried to reveal such hidden or unconscious*

> *real motives behind consumer decisions, and transform them into new market niches and advertising arguments […] Previously it had been thought that consumers bought and desired certain kinds of goods because their identity (or "personality", to use the term in vogue at the time) was in a particular way. Now it became possible to think consumer identity as an effect of purchase patterns* (Arvidsson, 2004, p. 8).

Uma avaliação possível de todo esse processo consiste em caracterizá-lo como um dos efeitos ou signos da fragmentação das identidades, da perda de referências estáveis e da morte do sujeito unificado. Este é um diagnóstico possível e mesmo correto, mas amplo o suficiente para conter tantas coisas que acaba diluindo aquilo mesmo que pretende explicar. Além dessa avaliação, que não deve ser desconsiderada, a compreensão do estatuto destes duplos digitais e destas identidades simuladas deve levar em conta ao menos duas características da cultura contemporânea: em primeiro lugar, a familiaridade, promovida pelas tecnologias de comunicação, com imagens, eventos, ambientes e existências que tornam indecidíveis os limites entre realidade e ficção, modelo e realidade, imagem e referente, observador e observado. Apenas numa sociedade já familiarizada com tais ambigüidades, os perfis extraídos de bancos de dados podem ter alguma efetividade. Assim como a imagem digital é uma imagem-código à diferença da imagem-representação, pois não há real que subsista por trás da imagem e sim o real como imagem, o perfil é uma identidade-código. "Rather than the profiling resembling the cases, increasingly the cases start to resemble the profiles" (Bogard, 1996, p. 27).

A segunda característica de nossa cultura que auxilia na compreensão do que estamos tratando reside na relação entre o poder e a temporalidade. Numa fórmula ao mesmo tempo elegante e aguda, Foucault define o poder como uma "ação sobre a ação possível" (Foucault, 1983b). Essa definição é particularmente pertinente ao modo como o poder se exerce hoje e, em especial, à vigilância digital, na medida em que ela pretende agir sobre a ação possível de indivíduos ou grupos, em vez de querer reformá-los, como na vigilância disciplinar. Hoje não se quer curar ou reformar o criminoso, o doente físico ou mental, mas sim impedir o crime, prevenir a doença ou minimizar seus riscos. Os atuais dispositivos de vigilância são máquinas de produzir futuro, de simular cenários, desejos, preferências, inclinações. E esse futuro artefatual, essas "biografias futuras" (Bogard, 1996) não são previsões de um porvir certo e necessário, mas simulações que orientam, conduzem todo um campo de ações, cuidados e escolhas possíveis. Um dos perigos facilmente identificáveis nesse processo é o sufocamento do possível e a condenação do presente. Um caso exemplar deste perigo se deu com uma menina de 16 anos residente nos EUA, folha de imigrantes muçulmanos, que foi convidada a se retirar deste país porque foi enquadrada num perfil de "menina-bomba potencial", elaborado pelo FBI fundamentalmente a partir do monitoramento de suas navegações na Internet, onde costumava frequentar o *chat* de um clérigo islâmico em Londres que vem sendo acusado de encorajar bombas suicidas[3]. Neste caso, é evidente que as tendências e inclinações projetadas no perfil acabaram por condenar o presente ao futuro simulado, sufocando inúmeras outras possibilidades certamente presentes na identidade de uma adolescente. O referido país, segundo seu discurso oficial, não poderia correr o risco de o perfil ser verdadeiro, mesmo sabendo que ele podia ser falso; em todos os casos, ressaltamos, ele foi efetivo.

É preciso, contudo, chamar a atenção para o fato de que tais constrangimentos e perigos próprios desta forma de poder não refletem um regime totalitário, opressor ou conspiratório. A composição de bancos de dados e perfis não está apenas a serviço de mecanismos e circuitos de exclusão, mas está presente também e principalmente nos circuitos de inclusão – consumo, saúde, trabalho, educação, entretenimento. Embora em alguns casos-limite eles possam ser extremamente impositivos, é importante perceber que em diversos campos eles atuam como "tecnologias da liberdade" (Rose, 2000), próprias para governar à distância, através e não a despeito de escolhas autônomas, indivíduos e entidades relativamente independentes. Numa atitude relativamente similar ao caso mencionado, mulheres extirpam preventivamente seios e úteros quando se enquadram num perfil de portadoras virtuais de câncer. Os indivíduos são aí chamados à prudência e responsabilidade por seu destino, a calcular seu futuro e prover sua segurança, ao incitamento contínuo ao consumo, à melhora de si, ao constante monitoramento da saúde e interminável gestão de riscos. Bem sabemos o quanto senhas e programas computacionais, cartões de crédito, carteiras de trânsito, cartões de seguro-saúde etc. permitem o acesso a diversos privilégios, constituindo uma vigilância e um controle inscritos nos próprios circuitos de inclusão.

Além disso, toda essa proliferação dos dispositivos de visibilidade e vigilância em nossa cultura está repleta de ambigüidades, onde os desejos do ver e do ser visto, do

[3] *New York Times*, 17/06/2005.

voyeurismo e do exibicionismo se misturam. Na linha dos já conhecidos *reality-shows*, uma iniciativa recente em Londres radicaliza essa mistura: cerca de 20 mil moradores poderão assistir, através de um canal comunitário, a imagens de 11 câmeras de CCTV dispostas na sua vizinhança; há estimativas de que a audiência seria maior que a de programas televisivos. Um outro exemplo que mistura exibição e vigilância é o *Orkut*, um software de constituição de "redes sociais" ligado ao *website* de buscas *Google* (www.orkut.com). A rede reúne pessoas que se apresentam na forma de perfis (constituídos de fotos, gostos e preferências pessoais, listas de amigos etc.) e participam de comunidades de diversos tipos. Além de formar comunidades na Internet, o *Orkut* visa ser um grande "laboratório" de pesquisa sobre comportamentos, preferências e personalidades, bem como sobre o seu papel na formação de redes sociais. Deste modo, é um grande banco de dados vivo e dinâmico que permite constituir outros bancos de dados mais específicos e perfis de indivíduos ou grupos a partir das trocas sociais e do que as pessoas declaram acerca de si mesmas (em seus *profiles*) ou acerca dos outros.

Num artigo sobre o *Club Nexus*, uma comunidade *on-line* da Universidade de Stanford que deu origem à rede social que leva o nome de seu criador, Orkut Buyukkokten expõe seus objetivos:

> *The data presents an opportunity to study, among other things, the online community's structure, social interactions and how factors such as personality and interests influence one's choice of friends. In this paper we take the first step of analyzing the community as a social network, and compare profiles supplied by the users to characterize connections* (Adamic *et al*., 2003, p. 1).

No lugar da perspectiva da hipervigilância panóptica e totalitária, o controle é melhor compreendido como operando através de acessos condicionais a circuitos de consumo e civilidade, bem aí onde se obtêm os "benefícios da liberdade".

Referências

ADAMIC, L.; BUYOKKOKTEN, O. e ADAR, E. 2003. A social network caught in the web. *First Monday*, **8**(6). Acessado em 07/11/2004, disponível em http://www.firstmonday.org/issues/issue8_6/adamic/index.html.

ARVIDSSON, A. 2004. On the "Pre-History of the panoptic sort": mobility in market research. *Surveillance and Society*, **1**(4):1-9.

BENNET, C.J. 1996. The public surveillance of personal data: a cross-national analysis. *In*: D. LYON (org.), *Surveillance as social sorting: Privacy, risk and digital discrimination*. London, Routledge, p. 37-49.

BOGARD, W. 1996. *The simulation of surveillance: Hypercontrol in telematic societies*. Cambridge, Cambridge University Press, 217 p.

CLARKE, R. 1994. The digital persona and its application to data surveillance. *Information Society*, **10**(2):23-45.

DHOLAKIA, N. e ZWICK, D. 2001. Privacy and consumer agency in the information age: Between prying profilers and preening webcams. *JRConsumers.com*, 1:1-17.

FOUCAULT, M. 1983a. *Vigiar e punir*. Petrópolis, Vozes, 272 p.

FOUCAULT, M. 1983b. O sujeito e o poder. *In:* P. RABINOW e H. DREYFUS, *Foucault: uma trajetória filosófica: para além do estruturalismo e da hermenêutica*. Rio de janeiro, Forense Universitária, p. 131-149.

GANDY, O. 1993. *The panoptic sort: A political economy of personal information*. Boulder, Westview Press, 289 p.

GANDY, O. 1996. Coming to terms with the Panoptic Sort. *In*: D. LYON (org.), *Surveillance as social sorting: Privacy, risk and digital discrimination*. London, Routledge, p. 132-155.

LYON, D. (org.). 2003. *Surveillance as social sorting: Privacy, risk and digital discrimination*. London, Routledge, 284 p.

MARX, G.T. 2002. What's new about the "new surveillance"? Classifying for change and continuity. *Surveillance & Society*, **1**(1):9-29.

NORRIS, C. e ARMSTRONG, G. 1999. *The maximum surveillance society: The rise of CCTV*. Oxford, Berg, 312 p.

NORRIS, C. 2003. From personal to digital: CCTV, the panopticon, and the technological mediation of suspicion and social control. *In*: D. LYON (org.), *Surveillance as social sorting: Privacy, risk and digital discrimination*. London, Routledge, p. 67-81.

POSTER, M. 1995. *The second media age*. Cambridge, Polity Press, 186 p.

ROSE, N. 2000. Government and control. *British Journal of Criminology*, **40**:36-48.

Submetido em: 19/07/2006
Aceito em: 05/09/2006