A Comunicação Vigiada: nota sobre a suspeição na Cibercultura

Paulo C. Cunha Filho *

As tecnologias digitais colocaram-nos perante uma nova geração de imagens que vem abalar a cultura de confianças que as imagens técnicas modernas tinham estabelecido. Em questão está não só o novo estatuto dos simulacros digitais, assim como também o velho estatuto das imagens analógicas. Duas culturas visuais que, ao coexistirem na atualidade, instalam um regime de crenças visuais misto e tendencialmente desorientado. Entre o "isto foi" fotográfico (Barthes) e o "isto pode não ter sido" digital, as imagens técnicas contemporâneas ressaltaram um estado de irritação há muito arredado das práticas visuais do Ocidente. Em que cremos crer do programa das imagens que hoje observamos?

digital - crença - irritação

Digital technologies have offered us a new generation of images that questions the culture of confidence that the modern technical images had once established. At stake is not just the digital *simulacra*'s new status but also the old analogical images' one. Two visual cultures whose coexistence installs a mixed visual beliefs' regime which shows tendency to disorientation. Between the photographical "this has been" (Barthes) and the digital "this may not have been" the contemporary technical images have stressed a state of irritation far-out from the recent visual practices in the Occident. In what do we believe to believe from the program of the images we observe nowadays?

digital - belief - irritation

* Professor do Programa de Pós-graduação em Comunicação da Universidade Federal de Pernambuco. (Paulo@ufpe.br)

Les technologies numériques nous ont placés devant une nouvelle gérération d'images qui vient bouleverser la culture de confiances établie par les images techniques modernes. Il ne s'agit pas seulement d'un nouveau statut des simulacres numériques mais aussi du vieux statut des images analogiques. Ce sont deux cultures visuelles que installent un regime de croyances visualles mixte et tendanciellement desoriente par sa coexistence à l'actualité. Entre lê "ça a été" photographique (Barthes) er lê "ça peut ne pás avoir été" numérique lês images techniques contemporaines ont relevées un état d'irritation distancié pour très long temps des pratiques visualles de l'Occidebt. En quoi croyons-nous croine du programme des images qu'on observe aujourd'hui?

numérique - croyance - irritation

Las tecnologías digitales nos han colocado delante de una nueva generación de imágenes que vienen a debilitar la cultura de confianza que las imágenes técnicas modernas han establecido. En cuestión está no solamente el nuevo estatuto de los simulacros digitales, sino también el viejo estatuto de las imagenes analógicas. Dos culturas visuales que al coexistir, en la actualidad, instalan un régimen de creencias visuales mixto y tendencialmente desorientado. Así, entre el "ésto fue" fotográfico (Barthes) y el "ésto puede no haber sido" digital, las imágenes técnicas contemporáneas resaltarán un estado de irritación desviado hace mucho tiempo de las práticas visuales de Occidente. ¿En qué creemos creer del programa de las imágenes que observamos hoy?

Digital - creencia - irritación

O aparato da justiça punitiva tem que ater-se,
agora, a esta nova realidade, realidade incorpórea.

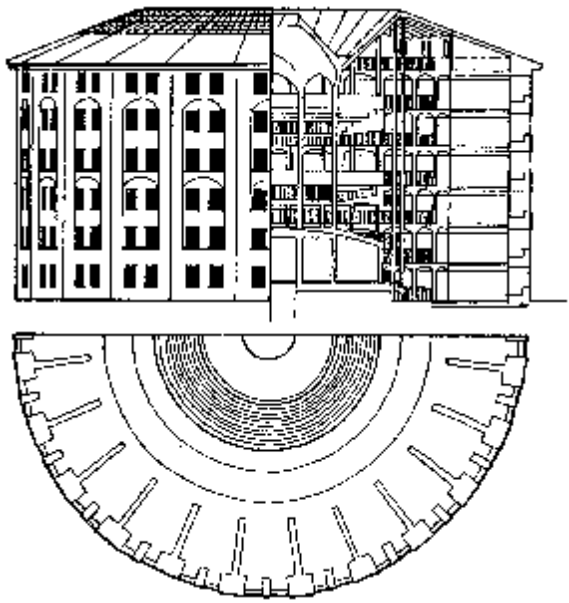
Michel Foucault

Ver sem ser visto é uma figura específica do poder. Seja o poder tomado como capacidade de agir, como faculdade moral ou legal de fazer ou como autoridade, esta figura – forma, símbolo ou alegoria – é historicamente determinada: o poder emana de um personagem que é *sagrado*[1] - e visível, sobretudo naquilo que tem de sagrado - antes mesmo de ser um chefe político ou militar. O poder é, na verdade, o selo de um árbitro soberano apenas parcialmente visível (e portanto inatingível), que mata sem poder ser morto[2]. O poder é visível – e exulta dessa visibilidade -, mas o poderoso é um homem invisível[3], inatacável nessa invisibilidade, visível apenas como imagem pública construída, donde decorre "a importância do ritual, do mito e do símbolo na política em todos os tempos" (Burke, 1994:210).

Voyeur absoluto, o poderoso engendra e é engendrado pelo panoptismo, na forma como foi analisado por Foucault[4] a partir do trabalho do utilitarista Jeremy Bentham[5], na aurora da classe média, quando a reforma das instituições sociais deveria se consolidar a partir de "idéias práticas", entre as quais brilhava, pela sua lógica e pela sua simplicidade, o *Panopticon* – o projeto de prisão na qual os detentos podiam ser permanentemente observados por guardas eternamente invisíveis. Esta era a diferença essencial assegurada no projeto panóptico: uns vêem, outros apenas são vistos; os que vêem nunca serão vistos, enquanto os observados nunca estarão aptos a ver.

Na sua criação, Bentham apontava para um poder implicado na valorização superior da razão sobre a tradição e a moral, assim como na crença de que as leis podiam ser descritas e aplicadas *cientificamente*[6]. Resultado de uma genealogia moral e legal representada por uma edificação complexa: o *Panopticon* é, antes de qualquer coisa, um projeto arquitetônico no qual estão associados uma torre central e um edifício circular dividido em células. Cada célula ocupa um trecho que vai do pátio interno à parede circular externa, permitindo assim a abertura de janelas internas e ex-

ternas. Os ocupantes das células são retroiluminados, isolados uns dos outros por paredes laterais e passíveis de serem vigiados coletivamente e individualmente por um observador que, na torre, permanece despercebido para eles. Bentham foi precioso: projetou inclusive cortinas e conexões entre as celas para evitar os efeitos de luz ou de ruído que poderiam trair a presença do observador. O *Panopticon* anuncia, na forma de uma edificação, o estabelecimento de um regime social assimétrico em que, de um lado, alguém vê sem ser visto e, de outro lado, alguém é visto sem ver o seu observador. Assimetria explícita do poder, como analisou mais tarde



Foucault (2002:166-167), uma vez que repousa na posse diferenciada do conhecimento:

O Panopticon de Jeremy Bentham

> Daí o efeito mais importante do Panóptico: induzir no detento um estado consciente e permanente de visibilidade que assegura o funcionamento automático do poder. Fazer com que a vigilância seja permanente em seus efeitos, mesmo se é descontínua em sua ação; que a perfeição do poder tenda a tornar inútil a atualidade de seu exercício; que esse aparelho arquitetural seja uma máquina de criar e sustentar uma relação de poder independente daquele que o exerce; enfim, que os detentos se encontrem presos numa situação de poder de que eles mesmos são os portadores. Para isso, é ao mesmo tempo excessivo e muito pouco que o prisioneiro seja observado sem cessar por um vigia: muito

> pouco, pois o essencial é que ele se saiba vigiado; excessivo, porque ele não tem necessidade de sê-lo efetivamente. Por isso Bentham colocou o princípio de que o poder devia ser visível e inverificável.

Na análise de Foucault (2002:166), o cidadão observado é continuamente o *objeto de uma informação*, jamais *sujeito da comunicação*. Assim, a nova visibilidade garantida pelo *Panopticon*, entre os séculos 18 e 19, foi projetada para assegurar que a vigilância pudesse ser ao mesmo tempo global e individualizada. Tratava-se da eclosão de um fato social total que prepondera no ocidente desde então e, justamente nessa perspectiva, cabe questionar se, além de preponderar, também se expandiria com a incorporação de ferramentas e procedimentos característicos da contemporaneidade, isto é, entre outras dimensões, verificar em que medida as tecnologias que hoje caracterizam a Cibercultura estariam ou não renovando o potencial de vigilância panóptico.

Antes de tudo – e para deixar claro o projeto deste ensaio logo de saída -, a Cibercultura é apreciada aqui como uma dimensão da cultura contemporânea "marcada pelas tecnologias digitais", maneira de "de escapar, seja de um determinismo técnico, seja de um determinismo social" (Lemos, 2003). De um modo mais explícito, a motivação desse questionamento poderia estar vinculada ao fato de que a hipermídia parece reconstituir, reciclar, reelaborar, de forma evidente, as dimensões do global e do individual que estão associadas à idéia do *Panopticon*. Por um lado, do ponto de vista do usuário, sabe-se que a hipermídia trabalha tanto no *modo sinótico* (ou seja, oferece a possibilidade de uma aproximação genérica ao conjunto de informações) quanto no *modo analítico* (isto é, permitindo o adensamento da informação a partir de pontos de ancoragem específicos). Do ponto de vista estrutural, as redes telemáticas estão baseadas na mesma bipolaridade: elas são conjuntos genéricos e globais de nós e conexões, mas, ao mesmo tempo, são agrupamentos setoriais e locais, cuja constituição define a existência da própria rede à qual se vinculam.

Haveria, talvez, pelo menos hipoteticamente, uma forma de interpretar o caráter rizomático da informação digital a partir da possibilidade que ele oferece de ser apenas parcialmente visto pelo usuário comum e globalmente vigiado - seja pelos agentes do poder institucional, seja por indivíduos que, independente do fato de estarem vinculados a estruturas de

segurança, exercem a vigilância digital. O que pode levar à questão, diretamente colocada: seria a Cibercultura uma reelaboração contemporânea do panoptismo clássico? Mesmo correndo o risco de parecer excessiva, a hipótese se sustenta porque, tanto do ponto de vista estrutural (digamos: tecnológico) quanto do ponto de vista do uso individual (digamos: comportamental), as Tecnologias da Informação e da Comunicação e as práticas que elas justificam, alimentando a Cibercultura, são potencialmente capazes de permitir a expansão do modelo de vigilância panóptica que nasce no século 18.

É o que mostrou recentemente, aliás, Thomas Y. Levy (2002), ao propor uma oportuna aproximação do trabalho de Bentham com a Cibercultura, procurando analisar o "estado da arte panóptica", num período em que as questões de segurança (e, paralelamente, o problema das liberdades civis) estão assumindo proporções inauditas. Para ele, o contemporâneo colocou em operação novas e poderosas tecnologias de vigilância da informação, um verdadeiro arsenal de "olhos" e "ouvidos" maquínicos que ampliou o foco da suspeição da esfera militar para a esfera doméstica na mesma velocidade com que os terminais foram implantados inicialmente nos centros de defesa e nas universidades, em seguida nos escritórios, nas residências e finalmente nos objetos portáteis e móveis do reino do *wireless*. Thomas Levy argumenta que essa dimensão produz novas articulações entre design e poder, entre imagem e opressão, entre representação e vigilância, a partir do contexto em que Bentham criou o *Panopticon* até a instalação do ciberespaço. Câmeras escondidas (ou nem tão escondidas assim, já que tantas vezes solicitam que cidadãos sorriam para elas), imagens captadas por satélite, invasões não autorizadas de bancos de dados e computadores pessoais, reconfiguram a dinâmica do ver (parcialmente) e do ser visto (completamente).

Mas a preocupação de Thomas Levy em *Ctrl [Space]: Rhetorics of Surveillance from Bentham to Big Brother* é, sobretudo, verificar de que maneira os artistas contemporâneos (como Dan Graham, Yoko Ono e Peter Weibel, entre muitos outros) estão lidando com o panoptismo na era digital e representando essa dimensão social na arquitetura, na vídeoarte, na fotografia e em outros campos da expressão artística. É possível argumentar, inclusive, que Thomas Levy procurou evitar um certo tratamento

paranóico da questão, contentando-se em interpretar as influências dessa realidade nas dinâmicas representativas da arte contemporânea. No entanto, o problema do modelo panóptico de poder em sua fase cibernética está muito aquém da sua recuperação pela arte: simplesmente porque, antes mesmo de ser sentida e representada pelos artistas, esse modelo de vigilância envolve funcionários de governo, pesquisadores, cientistas e pessoas comuns nas suas transações digitais. A face mais evidente desse modelo é provavelmente aquela que opõe agentes de segurança e aos que realizam os típicos "crimes virtuais" (terroristas, traficantes, neonazistas, pedófilos, *money-cleaners* e *hackers* que disseminam vírus na web)[7]. Ao verificar a existência dessa linha de tensão entre o crime ou a subversão virtuais (mais ou menos organizados, mais ou menos bem intencionados) e as forças de segurança (mais ou menos institucionalizadas, mais ou menos controladas pela sociedade civil), boa parte das ações de vigilância parecem ganhar uma forte justificação, qual seja: a Cibercultura não estaria – ou pelo menos não deveria estar - fora da lei; e os crimes que nela são cometidos deveriam ser descobertos e punidos. Impedir que traficantes, espiões, terroristas e chefes de quadrilha se comuniquem, conspirem, ajam e escondam-se usando a Internet parece ser um desafio justificado e praticado efetivamente pelos governos centrais desde 1996, pelo menos.

Nos últimos anos, percebe-se que as esferas de poder (sobretudo governamentais) cobram e recebem da sociedade a missão de combater os crimes praticados no âmbito da web, abrindo, em contrapartida, a possibilidade conseqüente de extrapolar essa tarefa e, a partir do uso crescente de Tecnologias da Informação e da Comunicação, ampliar o poder do Estado ou das corporações e reduzir os espaços de liberdade privada dos usuários. As agências estatais de informação passam a usufruir o direito de - ou mesmo sem direito algum, em certas circunstâncias - supervisionar as atividades de grupos e de indivíduos nas redes telemáticas que, por sua vez, tornam-se elementos de uma estrutura de monitoração, regulação e controle que lhes escapa[8]. Aparentemente, nada mais panóptico.

Competentes na criação de metáforas paranóicas, representantes de órgãos de segurança e de informação através do mundo advertem que, sem vigilância contínua e adequada (o que significa tecnologicamente

performática, capaz de estar sempre, pelo menos, um passo a frente do que é permitido no nível comercial), o contemporâneo haveria de ser vítima, em algum ponto de sua evolução, de uma hecatombe informacional de proporções bíblicas. Nos Estados Unidos foi inclusive criada a expressão *Electronic Pearl Harbor*[9] para definir o desastre que ocorreria com o desligamento completo ou parcial das redes telemáticas estratégicas. É nesse contexto que se define a vigilância estatal/corporativa na Cibercultura, espécie de totalitarismo *intensivo* e, no entanto, *invisível* do qual fala Giddens (1987) em *The Nation-State and Violence*[10]. Um contexto que viria corroborar com a hipótese da expansão do panoptismo clássico, exacerbado pelas próprias tecnologias da informação[11].

Seria a *nova vigilância* baseada em computadores e redes, com as características elencadas por Gary Marx (1991:131-133), entre as quais a transcendência dos limites habituais de tempo, distância, fronteira e escuridão e a capacidade de reprodução e transferência de informações:

> *They permit combining discrete types of information, whether it's voice, computer data, fax, electronic mail, video. They permit altering data. They involve remote access, which is crucial in terms of accountability questions. They may be done invisibly, leaving no footprints. They can be done without the subject's knowledge or consent. They are more intensive, they probe deeper. They reveal previously inaccessible information. They're also more extensive and they cover broader areas.*

Outra característica curiosa dessa nova vigilância – além das elencadas por Marx acima - é sua capacidade de atingir tanto indivíduos previamente identificados quanto grupos aleatórios de usuários[12]. Estamos aqui diante da instalação, na Cibercultura, da vigilância prévia, apriorística, "preventiva", cujo foco não é um criminoso de fato e sim de um possível crime que deve ser antecipado e combatido antes mesmo que venha a ocorrer. Algo próximo daquilo que aponta para o futuro o filme *Minority Report*[13], ou seja: a noção de "pré-crime" e as práticas preventivas de combate a desvios que ainda nem ocorreram.

O ponto importante é que tudo o que a ficção científica aponta para o futuro parece estar em plena operação no contemporâneo. Embora sejam extremamente sigilosos e por isso mesmo tratados como questão de segurança nacional, os sistemas de vigilância vinculados à Cibercultura já começam a ser razoavelmente bem conhecidos pelos inevitáveis vazamentos oriundos das próprias agências de informação. Por exemplo, um

desses sistemas é fruto do Acordo UKUSA[14] (da junção das siglas do Reino Unido e dos Estados Unidos). Suspeita-se – para não se dizer sabe-se - que esse acordo permita a supervisão de praticamente todo o tráfego de correios eletrônicos e de fax, automaticamente submetido à análise e à supervisão, independente das leis de proteção às liberdades individuais dos países envolvidos ou não no acordo. A base tecnológica (ou seja, no linguajar técnico em voga, o *framework*) de vigilância e intercepção do UKUSA chama-se *Echelon* (que, em francês, significa unidade militar: "esquadrão"), provavelmente implementada desde os anos 70 e tornada operacional pelo menos desde 1995 para interceptar e-mails não criptografados, fax e chamadas telefônicas realizadas através das redes telemáticas. Ao contrário dos sistemas de espionagem surgidos na Guerra Fria, o *Echelon* nasceu para atender objetivos não-militares, principalmente governamentais e empresariais. Segundo as informações hoje disponíveis, o sistema não visaria a interceptação de mensagens de usuários específicos, mas supervisionaria indiscriminadamente um grande número de transmissões a partir de elementos da mensagem que apontam para indícios previamente selecionados, como palavras-chave por exemplo. Trata-se, na verdade, de uma estrutura multiforme de vigilância (geográfica, institucional e tecnologicamente falando) capaz de acessar mensagens transmitidas por satélite, transmissões em microondas, por cabos, por fibras óticas e por rádio[15]. Em resumo, o *Echelon* é capaz de interceptar, gravar e analisar, nos seus servidores, milhões de mensagens a partir de indícios pré-estabelecidas (nomes, cifras, localidades, assuntos) que, uma vez detectadas, são cruzadas com uma lista de números de telefone e de endereços eletrônicos suspeitos.

O sistema anglo-americano teria um correspondente na Rússia, onde o Serviço Federal de Segurança (o FSB, sucessor da KGB) também teria estabelecido um procedimento de vigilância da Internet, em associação com a Agência Estatal de Comunicações (*Goskomsvyaz*) e cujos padrões de operação podem ser lidos na própria rede[16]. Do mesmo modo, a União Européia aparentemente criou um sistema de vigilância, em parceria com o FBI americano[17]. O resultado concreto disso foi o *Enfopol*, propondo uma colaboração ativa entre os parceiros, através de uma "interface virtual" e visando a "interceptação de telecomunicações relacionadas às novas

tecnologias"[18]. Em todos os casos, sejam os anglo-americanos, os russos ou os europeus, uma curiosa proximidade de propósitos e simetria de justificativas, como mostra Francisco Bernal, em *Big Brother Capabilities in an Online World: State surveillance in the Internet*, um dos mais completos trabalhos sobre sistemas militares, governamentais e corporativos de espionagem digital:

> *Police statements often refer to the danger of lagging behind while organized crime and terrorism are exploiting high technology and when national borders are opening up. But their own declared goals are not served better when simultaneously all privacy rights are taken away from individuals. Furthermore, the way in which all this is done suggests a mental regression into 'Big Brother' thinking. Politicians and civil servants are making top-down decisions, far removed from the public. A democratic debate has barely taken place so far.*

Todos os elementos levantados por Bernal apontam para a expansão da vocação de vigilância que orienta os impérios e as grandes corporações. Mas seriam suficientes para provar que o panoptismo clássico encontrou na Cibercultura o seu campo mais produtivo? De certa maneira, seria possível afirmar que estamos diante de uma mera incorporação, por parte dos aparelhos de controle e vigilância, das Tecnologias da Informação e da Comunicação. Nada de novo, portanto. Nada que permitisse interpretar, como já dissemos, o caráter rizomático da informação digital a partir da possibilidade que ele oferece de ser apenas parcialmente visto pelo usuário comum e globalmente vigiado, isto é, concluir que a Cibercultura seja uma reelaboração contemporânea do panoptismo clássico. Nesse sentido, Mark Winokur [2003] faz, em *The Ambiguous Panopticon: Foucault and the Codes of Cyberspace,* uma aproximação extremamente pertinente entre fatos como os elencados por Bernal e o trabalho de Michel Foucault. Ao contatar que o status da Internet enquanto *ferramenta global* (ou *ferramenta da globalização*) ainda é pouco claro, Winokur afirma que, no momento, a única idéia efetivamente plausível é a de que a Internet é a atualização material da indeterminação pós-estrutural que caracteriza a representação e a teoria cultural do contemporâneo. De modo que, para o autor, essa indefinição propõe uma reelaboração do próprio conceito de panoptismo [Winoukur, 2003]: *"This redefinition in turn allows us to ask questions about the nature of Internet representation. We may ask not only whether the Internet signifies*

panopticism, but whether it redefines 'construction' and 'signification' themselves".

Assim, Winokur acredita que, se o panoptismo tem sido usado como modelo para a observação da Cibercultura, é porque, de um lado, permite conceber as redes telemáticas como estruturas capazes de distribuir elementos de vigilância (coleta de informações, criptografia, espionagem) e, de outro lado, metaforizar um padrão societário baseado no autoritarismo de uma oligarquia que utiliza as novas tecnologias para promover a vigilância social. Nesse sentido, Winokur critica as abordagens de outros autores, como Lyon (1996), que fazem apenas uma discussão do panoptismo na Cibercultura *per se*, ou seja, procurando verificar como as agências de informação usam a Internet para coagir "externamente" os indivíduos, mas sem questionar como esse tipo de autoridade é "internalizada".

Como se sabe, a ampliação exponencial dos usos da Internet provocou a geração de novas utopias, entre elas a de que as redes digitais poderiam funcionar como espaços de uma reação subversiva aos modelos de controle, vigilância e punição do panoptismo. Da mesma forma, e por outro lado, o uso do modelo panóptico tem servido para levantar distopias radicais, baseadas na idéias de que as redes limitariam as relações sociais e, inclusive, a nossa capacidade de pensar fora da Internet. O uso genérico e diluído do modelo panóptico pode, de fato, como propõe Winokur, conduzir a um questionamento do padrão de vigilância na Cibercultura:

> *Is the Internet surveillant? Without question. But is the Internet surveillant after the manner of the panopticon? We cannot answer this question by means of sociological accounts that are simply interested in the government and corporate tendency to get to know us better through Internet spying. The panopticon does not use information just to know us; it also deploys information to create us, to constitute us as compliant workers and consumers. Essentially, if it is panoptic, the Internet must serve the same panoptic/enlightenment function of social control through a physical control of the body in space and a rhetorical control of the definition of subjectivity that other panoptic institutions do.*

É essa dúvida, afinal, que leva Winokur a repensar o panoptismo em Foucault, apontando para as seguintes peculiaridades: (a) a prisão panóptica de Bentham é utilizada por Foucault como uma metáfora do nascimento de um modelo social onde as instituições tornaram-se disciplinares; (b) as instituições tornam-se disciplinares porque elas representam um *corpo de conhecimento*; (c) o conhecimento disciplinar é sempre coercitivo, destilando modos particulares de comportamento e de crença; (d) o

discurso tem um papel fundamental na coerção social, já que o conhecimento disciplinar se articula a partir de uma linguagem própria, acessível apenas a poucos adeptos; (e) finalmente, a autoridade é internalizada por cada agente da vigilância, fazendo com que a sociedade panóptica empregue instituições para distribuir o poder através da sociedade.

A partir desses tópicos, que tentam sintetizar o conceito foucaultiano de panoptismo, Winokur dedica-se a verificar se, de fato, eles podem ser observados nas condições atuais de operação da Internet. A idéia de que a sociedade coercitiva surgida no período clássico funda-se num conjunto de ferramentas/objetos/máquinas – conjunto este associado a um padrão de vigilância internalizado pelos seus agentes -, oferece um quadro para que o autor observe de maneira muito particular um elemento específico da tecnologia digital: o monitor do computador. Diferente de todos os demais *écrans* anteriores utilizados pelo homem (o das sombras chinesas, o do cinema, o da televisão), "nos observa enquanto nós o observamos". Essa bidirecionalidade do monitor do computador seria para Winokur "genuinamente recíproca", de uma maneira que nem a televisão nem a tela do cinema poderiam alcançar[19]. É claro que a bidirecionalidade do monitor do computador ainda é extremamente restrita, limitando-se a patamares muito elementares da representação gráfica e a certos códigos de linguagem computacional que se tornam "visíveis" a partir de comandos do mouse do usuário. Boa parte dos processos de conexão, de transferência e de acesso continua opaca, principalmente ao usuário comum, notadamente aqueles que abrem o computador pessoal ao controle externo. A partir dessa visão do monitor como plataforma de observação bi-direcional, Winokur também retoma um tema ancestral dos estudos da Cibercultura ao considerar que, como instrumento de comunicação, a Internet quebra com o velho modelo monopolístico e vertical da comunicação de massa (um-todos) e permite aos conectados e instrumentalizados a possibilidade de criar páginas e interagir através de boletins eletrônicos, e-mails, *chat rooms* e jogos eletrônicos.

Assim, a condição característica do panoptismo, ou seja, a assimetria explícita do poder, baseada na posse diferenciada do conhecimento (alguém nos observa, não percebemos quem nos observa), estaria pelo menos parcialmente comprometida. Nessa perspectiva, o hipertexto transmite ao usuário uma impressão de escolha, a sensação de que a navegação

é uma "experimentação excitante de bricolagem" (Winokur), mesmo quando levamos em consideração que as oportunidades interativas do hipertexto são ainda muito limitadas, tecnicamente controladas e ideologicamente orientadas (os *hiperlinks* conduzem a trajetos baseados nos mesmos princípios verticais e monopolísticos da comunicação de massa).

Outra dimensão peculiar da Internet amplamente trabalhada pelos utópicos, a geração de avatares a partir dos quais é possível flexibilizar as representações identitárias, também parece insuficiente para livrar os usuários comuns da condição de observados. Ao incorporar personagens criados pela sua fantasia particular, cada internauta vive a ilusão de poder ser múltiplo, ser legião, ser quem quiser. Na maior parte das atividades sociais, isto é, naquelas que são institucionalmente controladas (trabalho e finanças, por exemplo), todos os registros e comportamentos estão limitados ao estritamente convencionado para aquém do ciberespaço. O usuário pode trocar de nome, de sexo, de cor, de aparência num *chat room* ou num *game*, mas não pode ousar fazê-lo numa transação bancária ou num currículo on-line, sob pena de ser reconduzido a um contexto caracterizado por parâmetros rígidos de controle e punição.

A visão idealizada da hipermídia, ou seja, da condição de emissão-recepção de conteúdos, de flexibilização relativa das identidades, entre outros aspectos circunstanciais, levam os críticos utópicos a classificar a Internet como o extremo oposto do Panopticon. No entanto, as representações hipermidiáticas são apenas um pouco mais permissivas do que as mídias tradicionais, acrescentando um número ainda extremamente limitado de possibilidades aos que já eram conhecidos com os usos do cinema, da televisão e do vídeo. Conseqüentemente, o *empowering* atribuído à comunicação digital poderia ser considerado o motor de uma visão parcial e inadequada, encobridora da dimensão de controle e vigilância que estaria camuflada sob a capa da ampliação de opções, da flexibilização comportamental, da deriva identitária. Essa sensação é que leva autores como Lessig [2000:5-6] a afirmar: *"[w]e have every reason to believe that cyberspace, left to itself, will not fulfill the promise of freedom. Left to itself, cyberspace will become a perfect tool of control"*.

Na dialética nem sempre clara da utopia-distopia[20] associada à Cibercultura, o essencial talvez seja entender que, muito mais do que um

problema de coleta de informações por parte de agências governamentais de espionagem, a vigilância na Internet aponta para a criação de um amplo e invisível sistema de controle comercial, com diversas corporações empregando softwares para conhecer os desejos dos usuários-consumidores. O desdobramento do panoptismo para o campo do consumo é definitivamente uma invenção típica da Cibercultura (seria possível dizer: uma ferramenta típica do capitalismo tardio), mesmo se é possível reconhecer que as empresas sempre fizeram espionagem comercial e que, na verdade, boa parte da espionagem militar ou governamental sempre teve o foco nas questões econômico-financeiras e nos conflitos delas oriundas.

Resta ainda uma condição particular e perceptível nas redes telemáticas: o fato de os usuários estarem iniciando uma corrida em direção à internalização do espírito de vigilância e controle. Não são poucos os exemplos dessa corrida pelo menos entre aquela categoria de usuários razoavelmente especializada nas linguagens computacionais e nas potencialidades que elas oferecem para interceptar informações distribuídas. Como diz ainda Winokur [2003]:

> *Does the Internet similarly institute an internal agency that ensures a vision of authority and society in which each person is her own and her neighbor's monitor? Certainly software exists that encourages the tendency toward self- and peer-surveillance, and among other blandishments, such software is advertised as security against corporate and governmental surveillance. Anti-virus software, spyware, anti-spyware, anti-pornography software, firewalls, Trojans, anti-Trojan programs, worms, data-erasure programs, and other forms of self-surveillance - software more or less readily available to all Internet citizens - can infiltrate other computers or monitor the penetrations into one's own computer; it is possible to locate the source of the attack, thus monitoring the activities and strategies of individuals and corporations.*

Na verdade, é possível imaginar que as Tecnologias da Informação e da Comunicação em geral – e a Internet em particular – podem ser empregadas a serviço de instituições disciplinares, mas pode parecer imprudente considerar esse conjunto de ferramentas e comportamentos como um tipo particular de aparelho disciplinar. Ademais, como Foucault defendia, as instituições tornam-se disciplinares ao assumir a dimensão de um *corpo de conhecimento* (segundo a equação *poder-saber*) e talvez seja excessivo atribuir às instituições da tecnocultura essa dimensão, por mais que elas destilem um tecnoleto peculiar que não deixa de ser socialmente excludente[21]. Como também parece ser um disparate absoluto – apesar de todas as

artimanhas já atestadas dos órgãos de segurança e das grandes corporações – imaginar que a Internet (por exemplo) opere segundo um conhecimento disciplinar propriamente coercitivo - mesmo se, pouco a pouco, seja possível verificar a consolidação de certos modos particulares de comportamento autoritário e de crença no jogo da vigilância entre alguns usuários.

Sobretudo, no caso das tecnologias do contemporâneo, há que se relativizar o papel discursivo, tão importante na concepção de Foucault para a definição do panoptismo, na coerção social: admitindo-se, como queria Foucault, que o conhecimento disciplinar se articula a partir de uma linguagem própria, acessível apenas a poucos adeptos, precisaríamos estudar com muito mais atenção de que forma o sistema discursivo da tecnocultura tende a se particularizar como elemento propriamente coercitivo – e não como gêneros precários, como os discursos em chatroons, emoticons, que são meros operadores de subculturas de baixo impacto enunciativo. Sem dúvida, deve-se considerar atentamente o papel das linguagens escritas e reescritas pelos programadores. Afinal, como afirma categoricamente Flusser (2002:27), "o poder passou do proprietário para o programados de sistemas". Há, evidentemente, algo de secreto e controlador na sintaxe dos programas, linguagens muitas vezes indecifráveis muitas vezes para outros programadores, e inclusive escritas por programas desenhados para escrever programas. A questão é: seriam estas linguagens efetivamente disciplinares e coercitivas?

Resta, ainda, a evidência de que os usuários das tecnologias contemporâneas da informação e da comunicação estão paulatinamente internalizando a autoridade, ou seja, colocando-se na condição de participante do jogo do observador-observado. Muitos usuários, de fato, incorporam o papel de agentes da vigilância, distribuindo poder através de certos estratos sociais e apontando para uma sociedade de controle muito mais sofisticada. Basta lembrar do papel extremamente controlador e autoritário de alguns "mestres" de RPG ou de certos gestores de listas de discussão. Seria essa uma razão para completar o quadro de "leis da Cibercultura" descrito por André Lemos (2003)? Como sabemos, para o autor, esse quadro legal é constituído pela "lei da reconfiguração" (reconfigurar práticas, modalidades midiáticas, espaços, sem a substituição de seus respectivos antecedentes), pela "lei da liberação do pólo da

emissão" (a emergência de vozes e discursos anteriormente reprimidos pela edição da informação pelos *mass media*) e pela "lei da conectividade generalizada" (é possível estar só sem estar isolado). Haveria, em alguma dimensão da Cibercultura, algo que pudesse ser chamado de "lei da vigilância"? É provável que, vinculado ao conjunto possível de negatividades das tecnologias, o contemporâneo aponta para um contrato curioso em que usuários alternam-se na posição de controladores e de controlados, um pós-panoptismo (Boyne, 2000) rompendo de vez com as velhas limitações entre o público e o privado, entre o pessoal e o grupal, entre o secreto e o exposto. Como, afinal, entender aspectos tão diversos como a riqueza dos diários "íntimos" publicizados na rede ou a porosidade essencial e contraditória dos *firewalls*? Nessa perspectiva, é possível recuperar a avaliação reativa de Jean Baudrillard (2002:56):

> Por trás de cada tela de televisão e de computador, em cada operação técnica à qual é confrontado diariamente, o indivíduo é analisado de volta, função por função, testado, experimentado, fragmentado, assediado, limitado a responder – doravante sujeito fractal, consagrado à disseminação nas redes, ao preço da mortificação do olhar, do corpo, do mundo real.

Contrato social reinventado no qual o jogo do visível e do invisível, do controle e do descontrole é redimensionado para além do bem e do mal.

Notas

1 *Sagrado* tenta aqui dar conta da condição que James George Frazer (1854-1941) atribuía aos reis, isto é, a de pertencer a uma ordem de coisas separada, reservada, inviolável; esse pertencimento inviolável seria uma qualidade de potência, uma condição incondicionada, ou seja, que não está submetida a nenhuma outra condição [Lalande, 1996:974 e 1038]. Parece evidente que essa condição longe de restringir-se às figuras reais, desdobra-se e regenera-se nas ditaduras e nas democracias presidencialistas ou parlamentaristas modernas.

2 No *Leviathan*, Thomas Hobbes argumenta que a monarquia absolutista é uma forma ideal de governo para livrar os homens do seu próprio egoísmo e as nações da maldade popular. "As paixões que fazem os homens tender para a paz são o medo da morte, o desejo daquelas coisas que são necessárias para uma vida confortável, e a esperança de consegui-las através do trabalho" (Hobbes, 1988:77). Mesmo admitindo que o rei podia ter conselheiros (a quem deveria "escutar", mas não necessariamente "ouvir"), Hobbes acreditava que o poder só podia ser consistente se a decisão final sempre coubesse ao soberano.

3 No conhecido conto de terror psicológico, de 1889, intitulado *O Homem Invisível (The Invisible Man)*, H.G. Wells (1866–1946) cria uma das mais interessantes distopias literárias que conhecemos, ao contar como um jovem cientista passa a viver

a insuportável angústia criada pelo seu próprio experimento: usando a si próprio como cobaia, o cientista descobre a chave da invisibilidade e é incapaz de reverter essa condição, permitindo a Wells discorrer sobre os efeitos caóticos da invisibilidade.

4 FOUCAULT, 2002, sobretudo o Capítulo III

5 O trabalho de Bentham mais conhecido sobre a questão da punição e da vigilância é o texto de 1789, chamado *Introduction to the Principles of Morals and Legislation*.

6 Não apenas as leis podiam ser baseadas em critérios "científicos" como elas ganhariam eficiência se os legisladores pudessem entender que a natureza humana é motivada pelos princípios do prazer e da dor. Na *Introduction to the Principles of Morals and Legislation*,Bentham defende*: "Nature has placed mankind under the governance of two sovereign masters, pain and pleasure. It is for them alone to point out what we ought to do, as well as to determine what we shall do. On the one hand the standard of right and wrong, on the other the chain of causes and effects, are fastened to their throne. They govern us in all we do, in all we say, in all we think: every effort we can make to throw off our subjection, will serve but to demonstrate and confirm it".*

7 Tim May, fundador do grupo *Cypherpunks* criou a expressão "quarto cavaleiros do infocalipse" para definir terroristas, traficantes, pedófilos e os que fazem lavagem de dinheiro na Internet. Ao usar o termo, ele queria chamar a atenção para uma tática recorrente do governo americano que consiste em exagerar as possíveis ameaças desses criminosos virtuais para ampliar o controle e a vigilância sobre os usuários comuns da Internet: *"The State will of course try to slow or halt the apread of this technology, citing national security concerns, use of the technology by drug dealers and tax evaders, and fears of societal desintegration. Many of these concerns will be valid; cripto anarchy will allow national secrets to be traded freely and will allow illicit and stolen materials to be trated. An anonymous computerized market will even make possible abhorrent markets for assassinations ans extortion. Various criminal and foreing elements will be active users of CryptoNet. But this will not halt the spread of crypto anarchy"(*May, 1996:238). Essa teoria de May parece ser confirmada quando observamos as declarações do Departamento de Crimes Computacionais da Justiça americana. Por exemplo, o paper apresentado por Scott Charney (1999) no seminário *The Global Internet*, onde ele diz que "não haveria vigilância se todo mundo respeitasse a lei, mas eles não estão respeitando. A maioria das pessoas respeita a lei e devem ser deixadas em paz. Mas para aqueles que não são corretos, ou que são perigosos para a comunidade, as forças da lei precisam das ferramentas para investigá-los com rigor".

8 Burnham (1983), já na década de 80, advertia para o que ele chama de *autonomous technology* (tecnologia autônoma), ou seja, o aumento do controle direto sobre as pessoas a partir do desenvolvimento da informática.

9 Conferir em Smith (1998). É curioso observar como esse tipo de expressão catastrófica se aproxima do jargão utilizado por alguns críticos da Sociedade da Informação, notadamente os franceses Paul Virilio e Jean Baudrillard.

10 Giddens define o totalitarismo como um sistema extremamente focado num tipo de vigilância que não é apenas um reflexo do capitalismo, mas uma geração de poder intrínseca.

11 Lyon (1996) não mede as palavras para falar de *"a prison-like society, where invisible observers track our digital footprints"*.

12 Yaman Akdeniz, membro do CyberLaw Research Unit of Leeds University, e Caspar Bowden, da Foundation for Information Policy Research, procuraram diferenciar o que chamam de *vigilância de massa* e *vigilância pessoal* (BOWDEN & AKDENIZ, 1999). O foco da *vigilância de massa* seriam grupos de interesse particulares eleitos

pelas organizações de controle. Já a *vigilância pessoal* seria focada num indivíduo previamente identificado. Esses autores também definem uma outra técnica de vigilância, denominada *Computer Profiling*, que usa estudos estatísticos, lógica indutiva e estruturas comportamentais para estabelecer uma lista de indivíduos suspeitos.

13 O filme foi dirigido por Steven Spielberg, lançado em 2002, e tem um sintomático slogan: *"You can't hide; get ready to run"*. O lançamento do filme foi acompanhado da elaboração de um hoje famoso website (www.minorityreport.com), com direito a um link para uma curiosa associação (*Citizens for a Murder Free America*, ou seja, como ele se apresenta, um *precrime website*). É lá que encontra-se a definição de pré-crime: *"Precrime is a groundbreaking homicide prevention system developed by a team of techlonogists and crime specialists under the authority of the United States government. Unlike conventional law enforcement methods, Precrime never fails. This is because Precrime uses a revolutionary new technology called previsualization that allows police detectives to witness, verify, and halt murders before thay occur".*

14 Uma das primeiras referências ao Acordo UKUSA é de 1972, muito antes portanto da implantação da Internet comercial, quando um ex-analista de inteligência da *National Security Agency* (NSA) concedeu uma entrevista à revista *Ramparts* (ver referência na bibliografia) sob o pseudônimo de "Winslow Peck" e afirmou que o acordo envolvia, além do Reino Unido e dos Estados Unidos, o Canadá, a Austrália e a Nova Zelândia. Alemanha e Dinamarca colaboram com o sistema num nível secundário. O texto está disponível online em: http://jya.com/nsa-elint.htm.

15 O pesquisador inglês Duncan Campbell tem publicado uma série de artigos sobre o Echelon, a partir de 1988. Nestes textos, Campbell garante que as agencies de informação americanas, com apoio das grandes potências ocidentais, são capazes de monitorar praticamente todas as comunicações civis.

16 Conferir em http://www.libertarium.ru/eng/sorm/sormdocengl.html.

17 O FBI promoveu em 1993 o *"International Law Enforcement Telecommunications Seminar"* (ILETS). Entre as agências de segurança que participaram desse seminário fechado estavam, além dos Estados Unidos, do Canadá, do Reino Unido e da Austrália, representantes da Espanha, da Alemanha, da França, da Holanda, da Suécia, da Dinamarca e da Noruega.

18 Conferir em http://www.heise.de/tp/english.

19 Winokur também lembra que, assim como a televisão, a Internet sintetiza "todos os espaços num só espaço", isto é, o espaço do monitor do usuário, embora tenha sido incapaz de transformar, como o cinema e a televisão, "todos os espectadores num só espectador" (mesmo se parece estabelecer audiências monolíticas e inconscientes).

20 Para muitos autores, longe de se abrir para as utopias, a comunicação digital criou as condições para a realização maxima da distopia analisada por Foucault. Como afirma, com todas as letras, Mitchell (1995): *"[S]ince electronic data collection and digital collation techniques are so much more powerful than any that could be deployed in the past, they provide the means to create the ultimate Foucauldian dystopia".* Vale salientar aqui, como recomenda o pesquisador Eduardo Duarte, que as hipóteses apocalípticas, já muito ironizadas e desgastadas no âmbito da Cibercultura, são tão legítimas quanto as integradas. Ou seja: na medida em que os cenários catastróficos forem estabelecidos a partir de fatos, de dados, de testes, deveriam ter valor científico e serem tratados enquanto tal.

21 Não é possível esquecer, no entanto, como demonstra Foucault, que as tecnociências da era moderna (a partir do século XVIII) se fundam a partir de num tecnoleto particular que, em certa perspectiva, estabelecem o agenciamento maquínico de um discurso que representa um novo poder disciplinar. Nesse sentido, as tecnologias da Informação e da Comunicação poderiam, portanto, ser consideradas formas mais sofistica-

das e radicais do mesmo movimento disciplinar nas quais vingaram as tecnociências, pois elas estariam vinculadas a um aparelho disciplinar a serviço de um *agenciamento*, uma seja, uma força capaz de articular um fenômeno ou um processo, que implica no estabelecimento de territórios e, ao mesmo tempo, na desterritorialização, um sistema instável, com imensa mobilidade (Deleuze, 1988).

Bibliografia

BAUDRILLARD, Jean. *A troca Impossível*. Rio de Janeiro: Nova Fronteira, 2002.

BENTHAM, Jeremy. *The Works of Jeremy Bentham*, (ed. John Bowring), London, 1838-1843; Reedição New York, 1962.

BERNAL, Francisco J.. "Big Brother is Online". In: *CyberSociology.com*, números 6 e 7. London, 1999.

BERNAL, Francisco J.. "Big Brother Capabilities in an Online World: State surveillance in the Internet", 2003. Disponível on-line in http://www.bernal.co.uk/

BOYNE, Roy. "Post-Panopticism". In: *Economy and Society* 29, número 2, maio de 2000.

BOWDEN, Casper e AKDENIZ, Yaman. "Cryptography and Democracy: Dilemmas of Freedom," in Liberty eds., *Liberating Cyberspace:* Civil Liberties, Human Rights, and the Internet. London: Pluto Press. pp. 81-125. Disponível on-line in http://www.cyber-rigths.org/reports/yacb.pdf, 1999.

BURKE, Peter. *A Fabricação do Rei:* a construção da imagem pública de Luís XIV. Rio de Janeiro: Jorge Zahar Editor, 1994.

BURNHAM, David. *The Rise of Computer State*. New York: Vintage Books, 1983.

CAMBPELL, Duncan. "They've got it taped". *New Statesman*, London. 12 August, pp. 10-12 e capa, 1988.

CAMPBELL, Duncan e CONNOR, Steve. *On the Record:* Surveillance, Computers and Privacy. London: Michael Joseph, 1986.

DELEUZE, Gilles. *Foucault*. São Paulo: Brasiliense, 1988.

FLUSSER, Vilém. *Filosofia da Caixa Preta:* ensaios para uma futura filosofia da fotografia. Rio de Janeiro: Relume Dumará, 2002.

FOUCAULT, Michel. *Vigiar e Punir:* nascimento da prisão. Petrópolis: Vozes, 1987.

GIDDENS, Anthony. *The Nation-State and Violence.* Volume Two of a Contemporary Critique of Historical Materialism. Cambridge: Polity Press, 1987.

HARAWAY, Donna. "Manifesto for Cyborgs: Science, Technology, and Socialist Feminism in the 1980's". In: *Socialist Review* 80, 1985.

HOBBES, Thomas. *Leviatã ou Matéria, Forma e Poder de um Estado Eclesiástico e civil.* São Paulo: Nova Cultural, 1988.

LALANDE, André. *Vocabulário Técnico e Crítico da Filosofia*. São Paulo: Martins Fontes, 1996.

LANDOW, George P. (ed.). *Hyper/Text/Theory*, Baltimore: The Johns Hopkins University Press, 1994.

LANDOW, George P.. *Hypertext 2.0:* The Convergence of Contemporary Critical Theory and Technolog. Baltimore: The Johns Hopkins University Press, 1992.

LEMOS, André. "Cibercultura. Alguns pontos para entender a nossa época". In: LEMOS, André e CUNHA, Paulo (orgs.) *Olhares sobre a Cibercultura*. Porto Alegre: Sulina, 2003.

LESSING, Lawrence. *Code and Other Laws of Cyberspace.* New York: Basic Books.

LEVY, Thomas Y. *Ctrl [Space]:* Rhetorics of Surveillance from Bentham to Big Brother. Cambridge: MIT Press, 2002.

LYON, David. *The Electronic Eye.* The Raising of Surveillance Society. Cambridge: Polity Press, 1996.

LYON, David e ZUREIK, Elia (eds.). *Computers, Surveillance, and Privacy.* Minnesota: University of Minnesota Press, 1996.

MAY, Timothy C.. "A Crypto-Anarchist Manifesto". In: LUDLOW, Peter. *High Noon on the Eletronic Frontier*. Cambridge: MIT Press, 1996.

MARX, Gary T.. *Undercover. Police Surveillance in America*. Berkeley: University of California Press, 1988.

MARX, Gary T.. "Computer-Based Surveillance of Individuals" in WARREN, Jim et al. [ed.] *The First Conference on Computers, Freedom and Privacy,* 1991. IEEE Computer Society Press. Los Alamitos, USA. Disponível on-line in http://www.cpsr.org/conferences/cfp91/nycum.html

MITCHELL, William J. *City of Bits:* Space, Place, and the Infobahn. Cambridge: MIT Press, 1995.

RAMPARTS, Vol. 11. No. 2, August 1972, pp. 35-50. Disponível on-line in http://www.jya.com/nsa-elint.htm

SMITH, George. "An Electronic Pearl Harbor? Not Likely". In: FINNERAN, Kevin (ed.) *Issues in Sciences and Technology*, Autumn 1998, Richardson: The University of Texas at Dallas Publisher, 1998.

SUNDARAM, Ravi. "Beyond the Nationalist Panopticon: The Experience of Cyberpublics in India". In: CALDWELL, John T. (ed.) *Electronic Media and Technoculture.* New Jersey: Rutgers University Press, 1985.

WELLS, H. G. [1889]. *The Invisible Man*. Texto completo disponível on-line in http://www.bartleby.com/1003/

WINOKUR, Mark. *The Ambiguous Panopticon:* Foucault and the Codes of Cyberspace. 2003. Disponível on-line in: http://www.ctheory.net/text_file.asp?pick=371