Sérgio Amadeu da Silveira
É sociólogo e doutor em Ciência Política pela Universidade de São Paulo. É professor da pós-graduação da Faculdade de Comunicação Cásper Líbero.

Redes cibernéticas e tecnologias do anonimato

Cybernetics networks and anonymity technologies

Redes cibernéticas y tecnologías del anonimato

RESUMO
O texto trata do anonimato na sociedade do controle. Depois de problematizar a natureza das tecnologias cibernéticas, a relação entre arquitetura da rede e as possibilidades da comunicação anônima, resgata o debate entre o liberalismo e o utilitarismo, a partir de uma investigação genealógica dos fundamentos discursivos que buscam legitimar ou deslegitimar o anonimato na esfera pública interconectada. A pesquisa culmina na análise do papel da comunicação anônima em relação ao controle e à vigilância em redes cibernéticas. Por fim, observa como os valores da privacidade e do não-controle dos fluxos informacionais competem com os novos ideais forjados pelo mercado das tecnologias amigáveis e confortáveis, um dos fundamentos da sociedade de controle.
Palavras-chave
Anonimato; sociedade de controle; comunicação anônima.

ABSTRACT
The present paper approaches anonymity within control society. Starting by questioning the nature of cyber technologies and the relation between the net's architecture and the possibility of an anonymous communication, the text recovers the debate between liberalism and utilitarianism. It departs from a genealogical investigation of discursive foundations which aim at legitimating or delegitimizing anonymity in the interconnected public sphere. The research culminates with an analysis of the role of anonymous communication and its relation to control and vigilance in cyber networks. Finally, it observes how the values of privacy and non-control of informational flows compete with new ideals forged by friendly and comfortable market technologies, one of the basics of control society.
Keywords
Anonymity ; Control society ; Anonymous communication.

RESUMEN
El texto es sobre el anonimato en la sociedad de control. Después del problema de la naturaleza de las tecnologías cibernéticas, la relación entre arquitectura de red y las posibilidades de comunicación anónima, rescata el debate entre el liberalismo y el utilitarismo, a partir de una investigación genealógica de los fundamentos discursivos que buscan legitimar o deslegitimar el anonimato en la esfera pública interconectada. La cumbre de la investigación está en el análisis del papel de la comunicación anónima con relación al control y a la vigilancia en redes cibernéticas. Por fin, se observa como los valores de la privacidad y del no control de los flujos informacionales compiten con los nuevos ideales fabricados por el mercado de las tecnologías amistosas y confortables, un de los fundamentos de la sociedad de control.
Palabras clave
Anonimato; Sociedad de control; Comunicación anónima.

Data de submissão: 6/2009
Data de publicação: 8/2009

1. Contexto

A expansão da Internet e a elevação de sua importância para o conjunto de atividades sociais, culturais e econômicas trouxeram a questão do anonimato para o rol de preocupações relevantes no cenário comunicacional (AGRE; ROTENBERG, 1997; DYSON, 1998). Depois de apontar as implicações sócio-tecnológicas dos fluxos informacionais não-identificados nominalmente, o objetivo principal deste levantamento é o de apontar as diferenças e semelhanças no debate e nas antinomias sobre o anonimato na modernidade em relação ao existente no campo da cibercultura.

O anonimato aqui é entendido como condição ou qualidade da comunicação não-identificada, ou seja, da interação entre vários interagentes que não possuem identidade explícita ou que a ocultam. Como anonímia, ausência de nome ou assinatura, também será considerada a multi-interação (PRIMO, 2008), mútuas e reativas, entre humanos e máquinas dotadas de programas informacionais, onde a anonimidade se manifesta perceptível ou de modo sub-reptício.

Deve ser destacado ainda que a idéia de anonimato remete-nos a uma série de relações sociais que dizem respeito à identidade, à subjetividade, ao controle, à segurança e aos direitos civis. Exem-

plificando, é possível destacar que a arquitetura da Internet e seus principais protocolos de conexão, ao assegurarem a comunicação distribuída sem a necessidade de identificação, dificulta o controle, e, ao assegurar a navegação de quem oculta um nome, também garante a navegação daqueles que construíram múltiplas identidades. Para problematizar essas relações a Internet é analisada como portadora de tecnologias do anonimato.

2. Tecnologias de controle e rotas de fuga

A Internet é uma rede cibernética. Trata-se de uma rede distribuída, não apenas descentralizada (UGARTE, 2008), que se baseia em um sistema de localização de nomes de domínios extremamente hierarquizado, o *Domain Name System*. Além disso, todas a horizontalidade e flexibilidade de suas camadas lógicas se realizam sobre uma infra-estrutura dependente de um número diminuto de operadoras de Telecom.

Essas e outras contradições levaram Pierre Mounier a afirmar que

> A Internet como 'espaço público', como 'bem comum' do qual ninguém pode legitimamente querer se apoderar. Esse conceito do ciberespaço parece hoje natural, evidente. Mas ele é apenas uma das visões possíveis da comunicação dos computadores em rede. É mesmo provável que não represente mais do que uma etapa transitória, a que vivemos atualmente, na história do desenvolvimento da Internet." (MOUNIER, 2006, p. 71)

Em uma outra direção, David de Ugarte defende que nas redes distribuídas não existem filtros

exclusivos, nem dependência de um único nó para que um internauta se comunique. As mensagens podem ser roteadas por diferentes caminhos, ou seja, os fluxos de informação podem seguir diversos percursos na rede. Para sustentar essa visão, Ugarte recorre à definição de Alexander Bard e Jan Söderqvist segundo a qual uma rede distribuída é aquela em que "todo ator individual decide sobre si mesmo, mas carece de capacidade e da oportunidade para decidir sobre qualquer dos demais atores" (UGARTE, 2008, p. 35).

Essa afirmação é um ponto crucial para o debate sobre o lugar e a legitimidade da comunicação anônima. Antes mesmo de observarmos as tecnologias de controle ou de escape que habitam na Internet, é preciso compreender o significado de uma rede cibernética. Depois é necessário tentar definir se a estrutura da Internet é mais propícia ao controle ou ao não-controle dos interagentes e buscar compreender se a arquitetura de rede protege ou dificulta as tecnologias do anonimato.

Cibernética é um termo que tem origem na palavra grega *kubernétikê,* podendo ser traduzido pelas expresssões "arte de pilotar", "arte de governar". Foi introduzido na língua inglesa, em 1948, pelo cientista Norbert Wiener. A cibernética é uma ciência da organização que enfatiza a dinâmica da natureza e dos modelos da organização e auto-organização dos sistemas. Busca comparar os mecanismos de controle automático e de regulação entre os fluxos de informação, sem os quais os sistemas aceleram seus níveis entrópicos até se desorganizarem por completo.

O termo cibernética tem a ver com processos de controle e de comunicação de animais, homens e

máquinas, ou seja, de como a informação é processada e controlada em sistemas vivos ou artificiais (WIENER, 1998). Aqui é preciso destacar que uma rede cibernética construída artificialmente é uma rede de controle e não somente de comunicação. As tecnologias digitais são baseadas em códigos que delimitam o nosso comportamento (LESSIG, 1999) e são articuladas em redes que dependem de protocolos de comunicação e de controle (GALLOWAY, 2004). Nesse sentido, a comunicação anônima dos interagentes é o atenuante ou o antídoto ao controle totalizante engendrado pelo diagrama que regula e opera em toda a organização da rede.

Duas questões surgem dessa afirmação: existem organizadores da Internet? Porque os protocolos da rede são de comunicação e, ao mesmo tempo, de controle?

A Internet foi construída a partir da Arpanet, uma rede formada no contexto da Guerra Fria e com objetivos militares e acadêmicos. Surpreendentemente, sua evolução foi fortemente influenciada pela cultura hacker que, por sua vez, carregava valores da contracultura norte-americana da década de 1960. Não existia uma instituição proprietária da rede, fosse uma corporação ou uma universidade, pois a partir da década de 1970 ela era vista como um experimento coletivo. Pesquisadores acadêmicos, engenheiros e comunidades de usuários foram reconfigurando o funcionamento da rede. Os grupos de trabalho voluntários que formulavam RFCs[1], documentos aprovados consensualmente para a definição das regras e soluções técnicas para a rede, foram o instrumento principal de organização de seu

[1] Request for Coments.

desenvolvimento. Assim, podemos responder à primeira questão afirmando que os protocolos são os principais organizadores da comunicação mediada por computador.

O tipo de comunicação existente na Internet é realizado de acordo com uma arquitetura de rede que pode ser entendida como a descrição dos formatos de dados e dos procedimentos usados para a comunicação entre seus nós ou pontos. Ela pode ser decomposta em dois elementos importantes: os protocolos, que trazem os padrões, regras e procedimentos de comunicação, e a topologia da rede (NETWORK, 2008). Protocolos podem ser definidos como um conjunto de regras e convenções para a comunicação entre os dispositivos dessa rede. Um protocolo inclui formatação de regras que especificam como os dados são transformados em mensagens. Também pode incluir convenções de como formatar mensagens de aviso ou realizar a compressão de dados de modo confiável para apoiar uma rede de comunicação de alto desempenho (MITCHEL, 2008).

A topologia da rede pode ser pensada como um mapa. Trata-se do "arranjo físico e lógico dos elementos de uma rede. Duas redes têm a mesma topologia se a sua configuração de conexão, de ligação entre seus pontos, for a mesma, embora possam diferir em suas interligações físicas, distâncias entre nós, taxas de transmissão ou tipos de sinal" (TELECOMMUNICATIONS, 2008). A topologia física é a configuração física ou diz respeito aos caminhos da interligação dos cabos, roteadores, *switches,* concentradores, enfim, componentes físicos de uma rede. A topologia lógica de uma rede é a configuração esquemática que reflete o funcionamento da

rede e como será a ligação entre os usuários dessa rede. A topologia física pode ter um desenho diferente da topologia lógica.

Agora é preciso responder a questão se a estrutura da Internet é mais propícia ao controle ou ao não-controle dos interagentes. Esta questão se relaciona diretamente com o a dúvida sobre a arquitetura de rede, a saber, se ela protege ou dificulta as tecnologias do anonimato.

Para responder essas indagações é possível seguir o caminho de Galloway que sugere que a Internet *"is that protocol is based on a contradiction between two opposing machines: One machine radically distributes control into autonomous locales, the other machine focuses control into rigidly hierarchies"* (GALLOWAY, 2004, p. 8). Tal tensão dialética criaria um clima acolhedor para o controle protocolar. Sem dúvida, os protocolos controlam a comunicação dos interagentes em rede. Todavia, os protocolos fundamentais da rede, principalmente o conjunto TCP/IP, asseguram a comunicação anônima. Ninguém pode se comunicar na Internet sem um IP, nem mesmo é possível abrir uma página da web sem um endereço IP. Mas, não existe nenhuma necessidade de vincular uma identidade civil a um número de IP para que a comunicação se estabeleça.

A privacidade, entendida como a habilidade de se controlar o acesso aos seus dados pessoais está cada vez mais dependente do anonimato. Privacidade também deve ser considerada como a capacidade de evitar a identificação de sua navegação na rede, ou seja, de vinculação da identidade civil aos registros da navegação de um determinado IP. Se a atual arquitetura lógica da rede é organizada de

modo a garantir que toda a navegação deixe rastros digitais, simultaneamente os principais protocolos da Internet garantem a comunicação sem o necessário vinculo entre um IP de origem do fluxo de dados e uma identidade.

Por esses motivos, existem projetos de Lei em vários parlamentos que visam obrigar os provedores de acesso à Internet a proibirem o uso das redes sem identificação positiva dos cidadãos, uma vez que o padrão da comunicação na rede assegura o anonimato. Sem a possibilidade da navegação anônima, diante de uma infra-estrutura privada operada por corporações oligopolistas de telecomunicações, as possibilidades de controle e vigilância dos passos dos interagentes no ciberespaço serão as mesmas que observamos atualmente na China.

Uma das principais tecnologias do anonimato, desenvolvida por hackers, diante da pressão pelo controle vigilantista, é uma aplicação chamada Tor. Trata-se de um software que impede a chamada análise de tráfico, uma forma de vigilância que ameaça a liberdade e a privacidade na rede. Com a análise de tráfego dos pacotes de informação que são trocados pela rede é possível descobrir toda a rota de origem de uma informação, além de permitir uma série de estatísticas que assegurem a identificação de padrões. O Tor distribui a comunicação através de uma rede de voluntários transmissores ao redor do mundo (TOR, 2009), impedindo o monitoramento da conexão, dos sites acessados e evitando que se descubra a localização física dos interagentes.

Trabalhando no envio de pacotes de uma mesma mensagem por várias rotas na rede, impedindo que se encontre um único IP de origem e de destino,

o Tor protege até mesmo empresas contra análises que busquem identificar se elas possuem funcionários que trabalham até tarde, se eles utilizam sites de busca de emprego, se estão se comunicando com escritórios de advocacia ou instituições governamentais, se usam mecanismos de busca e quais buscas são realizadas, entre outras análises. Além disso, "grupos como Indymedia recomendam Tor para salvaguardar a privacidade e segurança online dos seus membros. Grupos activistas como Electronic Frontier Foundation (EFF) apoiam o desenvolvimento de Tor como um mecanismo para manter as liberdades civis online" (Ibidem). O Tor pode ser entendido como uma rede tecno-social de proteção do anonimato e da privacidade, contra formas de intrusão.

3. O debate moderno sobre a legitimidade do anonimato

A modernidade forjou um sujeito histórico portador de direitos e de uma identidade individual. Trouxe também a comunicação de massas e novos ideais do que seria o legítimo e o ilegítimo em uma interação social. Como bem apontou Zygmunt Bauman, a modernidade tinha um especial horror à indefinição, à incerteza e à ausência de controle. Nesse contexto, o anonimato foi considerado um fator de incerteza em um mundo que clamava por identidades precisas e centradas. Assim, para avançarmos na compreensão da aversão moderna à comunicação anônima é importante observar os embates entre liberais e utilitaristas a respeito da privacidade. Neles emergem as contradições do mundo cartesiano sobre o anonimato.

O utilitarismo tem em Jeremy Bentham (1748 - 1832) o seu maior expoente. Para ele, a busca da felicidade é o maior ideal e finalidade humana. Isaiah Berlin escreveu que "Bentham e [James] Mil acreditavam na educação e legislação como caminho para a felicidade. Mas se uma via mais curta fosse descoberta... poderiam muito bem ter aceito esta alternativa como melhor do que as que advogavam, porque mais eficaz e talvez menos custosa" (BERLIN, 2000, p. XIII) Assim, o pensamento utilitarista permitia avaliar, e até mesmo calcular, o modo mais eficiente de busca do bem estar social:

> O credo que aceita a utilidade ou o princípio da maior felicidade como fundação moral sustenta que as ações são corretas na medida em que tendem a promover a felicidade e erradas conforme tendem a produzir o contrário da felicidade. Por felicidade se entende prazer e ausência de dor; por infelicidade, dor e a privação do prazer. (MILL, 2000, p. 187)

Bentham buscava soluções sociais que fossem efetivas na promoção da felicidade para o maior número possível de cidadãos. Defendeu a supressão de qualquer incerteza quanto às identidades pessoais, uma vez que isso obscurecia a classificação e o correspondente cálculo geral necessário a estruturar o bem-estar social. Para ele, era necessário o reconhecimento total dos indivíduos, bem como era preciso uma polícia geral das identidades:

> É preciso aumentar, [Bentham] sublinha com insistência, os meios de reconhecer e encontrar os indivíduos: 'Na capital do Japão, a cada um é obrigado a

> usar seu próprio nome sobre a roupa' (PPL, p. 557). 'Nas universidades inglesas, os alunos usam uma roupa particular. Nas *charity schools*, cada qual tem não somente um uniforme, mas uma placa numerada. Não falemos dos soldados. É o mesmo que se pode querer, que os pobres usem uniforme' (PM, p. 389). (MILLER, 2008, p. 108).

Benjamin Constant (1767-1830), liberal francês de origem suíça, foi pioneiro ao refletir sobre a importância de valores como a privacidade e o anonimato. Combateu a visão utilitarista e defendeu que o anonimato, como integrante da privacidade, era imprescindível à liberdade dos modernos, bem como, era fundamental à distinção entre as esferas pública e privada. Na crítica às teses de Bentham, Constant considerava o direito como um princípio e a utilidade apenas como um resultado, um efeito.

> O pretexto de prevenção do crime tem as maiores e mais incalculáveis consequências. A criminalidade potencial é inseparável da liberdade de todos, das vidas de todas as classes, do crescimento de todas as faculdades humanas. Os que detém a autoridade, alegando interminavelmente o receio de que um crime possa ser cometido, podem tecer uma vasta teia que envolva todos os inocentes (CONSTANT, 2007, p. 146).

Paul De Heart considera que o debate moderno sobre a legitimidade do anonimato também estava vinculado ao embate do pensamento liberal contra a visão republicana. De Heart considera que o republicanismo rejeita a esfera privada e subordina a liberdade individual aos interesses do coletivo social.

Para o pesquisador, as raízes desse pensamento vêm do pensamento político grego-romano, inspirado naquilo que Constant chamou de concepção de liberdade dos antigos:

> Em Roma, os censores vigiam até no interior das famílias. As leis regulamentavam os costumes e, como tudo dependia dos costumes, não havia nada que as leis não regulamentassem. (...) Assim, entre os antigos, o indivíduo, quase sempre soberano nas questões públicas, é escravo em todos seus assuntos privados. (CONSTANT, 1985, p. 11)

A idéia de liberdade para os modernos, segundo Constant, incorpora a esfera privada e os direitos dos indivíduos diante das maiorias. Para ele, não cabe ao Estado legislar sobre tudo, sobre comportamentos, crenças, inclinações e fantasias dos indivíduos. De Heart argumenta que o termo inglês *idiot* vem do grego *idiotes*, palavra que caracterizava a pessoa privada, alguém que não se engajava na vida pública da *pólis*. Para os Gregos, privacidade como valor era inexistente.

Em Atenas antiga existia um procedimento jurídico denominado *graphé paranomon*. Por ele, qualquer um poderia ser processado e julgado por proferir o que a maioria da *pólis* considerava "uma proposta ilegal". Assim, o orador político deveria assumir "os riscos de seu discurso" (FINLEY, 1988, p. 130). A liberdade de expressão exigia responsabilidade, ou seja, a necessária responsabilização daquele que fala. Tal fundamento sobreviveu aos tempos e foi retomado na comunicação moderna, na construção da chamada esfera pública.

4. Esfera pública interconectada e anonimato

As principais diferenças da esfera pública interconectada para uma esfera pública controlada pelos *mass media* são os baixos custos para se tornar um falante e sua arquitetura informacional distribuída, sem necessidade de autorizações e controles para e dela participar (BENKLER, 2006). A esfera pública interconectada é um espaço comunicacional em que os sujeitos privados discutem e realizam suas críticas públicas ao poder, tal como ocorria na esfera pública burguesa (HABERMAS, 1984), sendo bem mais acessível e diversificada do que a esfera controlada pelas corporações de comunicação.

Neste novo cenário de uma esfera pública constituída nas redes informacionais, o direito de blogar anonimamente é defendido pela *Electronic Frontier Foundation* (ELETRONIC, 2009). A entidade propõe que a livre expressão deve ser protegida de quaisquer tipos de pressão, política, religiosa, ideológica, profissional, corporativa, pública ou privada, por isso, a comunicação sem a necessária identificação do sujeito comunicante é considerada uma das condições do direito à opinião. Nesse mesmo sentido, Ian Clarke, criador e programador principal da rede Freenet, um típico hacker, no texto *The Philosophy behind Freenet* esclarece:

> But why is anonymity necessary?
> You cannot have freedom of speech without the option to remain anonymous. Most censorship is retrospective, it is generally much easier to curtail free speech by punishing those who exercise it afterward, rather than preventing them from doing it in the first place. The only way to prevent this is to

> remain anonymous. It is a common misconception that you cannot trust anonymous information. This is not necessarily true, using digital signatures people can create a secure anonymous pseudonym which, in time, people can learn to trust. Freenet incorporates a mechanism called "subspaces" to facilitate this (CLARK, 2009).

O argumento hacker sobre a verdade e a verificação dos conteúdos anônimos passa pelos mecanismos de reputação, de denúncia colaborativa e pelas redes de confiança, ou seja, os "instrumentos interativos de busca e enquete da comunicação distribuída tornam o anonimato reputável" (ANTOUN, 2008, p. 17). A prática de escrever textos públicos com pseudônimos, *nicknames*, perfis falsos, não é nova. Sem dúvida, um codinome pode construir uma forte reputação a partir dos seus argumentos.

Um grande exemplo da força dos argumentos acima da autoria, ocorreu em 1787, quando Alexander Hamilton convenceu James Madison e John Jay a tentar persuadir os votantes da convenção do Estado de Nova York a aprovar a nova Constituição dos Estados Unidos, elaborada na Filadélfia, naquele ano. Passaram a publicar no *Independent Journal*, uma série de artigos assinados pelo pseudônimo coletivo "Publius". Foram 85 textos que vieram a ser conhecidos como "Os artigos federalistas" que Thomas Jefferson chamaria de o melhor comentário jamais escrito sobre princípios de governo. O pseudônimo, mais do que proteger seus autores, permitia que os argumentos federalistas fossem analisados em si a despeito de quaisquer antipatias e simpatias por quem os escreveram.

Já a principal tese contra o anonimato na esfera pública parte das possíveis consequências negativas da ausência de responsabilidade pelo que é dito. Manifesta-se no que Habermas, em sua investigação sobre a pragmática universal pela busca das condições universais de compreensão mútua, denominou de pretensão de validade de um discurso como verdade (HABERMAS, 1996). Um efeito nefasto do argumento anônimo irresponsável e moralmente repreensível, inverídico, mas apresentado como verdadeiro e correto, é o de gerar uma rápida ação injusta, cujos efeitos não podem ser reparados.

Partindo de uma outra ordem de argumentos, Mark Poster rejeita a idéia de que a internet poderia ser a concretização da esfera pública indo além da crítica à comunicação anônima. Poster sustenta que a descorporificação na rede não pode substituir o encontro face-a-face. Nas redes, estaríamos vivendo uma desestabilização generalizada do sujeito. A multiplicação de representações e simulacros no ciberespaço nos leva a um estado de hiper-realidade, conforme descrito por Baudrillard, onde oposições binárias real/irreal, sujeito/objeto, público/privado, homem/máquina, tenderiam a implodir, e um mundo de simulacros emergiria podendo se tornar a única realidade para os participantes. Desse modo, o uso público da razão comunicativa estaria prejudicado no ciberespaço (POSTER, 1997).

5. Momento hobbesiano da cibercultura ou estruturação da sociedade do controle?

É preciso distinguir pelo menos três cenários do anonimato ou da comunicação sem identificação nominal dos sujeitos interagentes: 1) na navegação

pelo ciberespaço, com a possibilidade de impedir a vinculação do rastro digital a quem navega, e, a invisibilidade diante dos sistemas de georeferenciamento; 2) no debate público, enquanto modo legítimo do exercício da liberdade de expressão; 3) na conexão entre aparelhos e na interação entre humanos e máquinas de processamento.

Qualquer uma das legítimas necessidades de anonimato traz consigo dificuldades, pois acaba permitindo o seu uso para atividades ilícitas e ilegítimas. Esther Dyson, ex-presidente do Internet Corporation for Assigned Names and Numbers (ICANN)[2], problematizou tais dificuldades:

> No final, precisamos lidar com o lado sombrio do anonimato em vez de colocar todo ele fora da lei. É melhor para nós viver na atual situação de liberdade com riscos que estimula a liberdade com certas compensações. Qualquer tentativa de automatizar o processo de conceder o anonimato poderia torná-lo mais rastreável... e certamente chamaria atenção para seus usuários. Se o anonimato desenfreado se torna um problema, haverá tempo suficiente para lidar com ele. De fato, o perigo está mais provavelmente em outra direção — excesso de vigilância do governo e muito pouca privacidade (DYSON, 1998: 254).

Essas ambiguidades têm sido o fundamento para as tentativas da supressão da comunicação

[2] A ICANN é responsável pela coordenação global do sistema de identificadores exclusivos da Internet. Entre esses identificadores estão nomes de domínio (como .org, .museum e códigos de países, como .UK) e os endereços usados em vários protocolos da Internet.

anônima em redes digitais, e, constituem-se em uma das características mais marcantes da sociedade do controle (FOUCAULT, 1996; DELEUZE, 1992; LAZZARATO, 2006; GALLOWAY, 2004). No mesmo sentido, Fernanda Bruno escreveu que "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" (BRUNO, 2006: 154).

> Nas sociedades de controle, ao contrário, o essencial não é mais uma assinatura nem um número, mas uma cifra, a cifra é uma senha, ao passo que as sociedades disciplinares são reguladas por palavras de ordem (tanto do ponto de vista da integração quanto da resistência). A linguagem numérica do controle é feita de cifras, que marcam o acesso à informação, ou a rejeição. Não se está mais diante do par massa-indivíduo. Os indivíduos tornaram-se 'dividuais', divisíveis, e as massas tornaram-se amostras, dados, mercados ou 'bancos' (DELEUZE, 1992: 222)

O controle é avesso ao anônimo, ao incerto e ao nômade. Enquanto combates contra o anonimato são travados no terreno da definição dos códigos[3] e protocolos, como também no plano dos Estados, onde parlamentos ensaiam legislações de controle da rede, o Mercado prepara a agradável destruição da privacidade. O conforto, as facilidades, as tecno-

[3] A garantia do anonimato e da privacidade, em uma sociedade em que o software torna-se intermediário das comunicações, aponta para a *transparência* do código-fonte do software como um tema relevante.

logias amigáveis vão se tornando importantes constituintes da sociedade do controle. Acima da privacidade e do não-controle de nossos fluxos está o ideal do conforto, da velocidade de atualização do virtual, da extrema funcionalidade e amigabilidade. Esses termos vão assumindo a mesma importância social que o direitos ao íntimo, a autonomia e a não-intrusão em nossa comunicação cotidiana.

O exemplo mais completo desse cenário pode ser encontrado observando o usuário do Gmail. Uma vez tendo inserido sua senha e acessado seu correio, a Corporação Google, proprietária do serviço de e-mail, vincula imediatamente o IP ao interagente, além de enviar um *cookie*[4] para a máquina do usuário. Ele pode entrar diretamente no Orkut, no Blogger, no Google Docs e no seu perfil do YouTube, sem necessidade de identificação, uma vez que a Corporação Google cruzou todos os seus dados e sabe exatamente quem está navegando com aquele IP. Mais do que isso, todas as pesquisas que o interagente realizar no mecanismo de busca poderão ser registradas para análise de padrões de comportamento.

Recentemente, a corporação Google lançou um software que permite aos usuários de celulares e de outros dispositivos móveis saber a localização de seus amigos e familiares instantaneamente no Google Maps. O *release* da corporação, reproduzido pela imprensa mundial, dizia: "Você não somente controla exatamente quem pode ver sua localização, mas tam-

[4] Segundo a Wikipedia, *cookie* é "um grupo de dados trocados entre o navegador e o servidor de páginas, colocado num arquivo (ficheiro) de texto criado no computador do utilizador. A sua função principal é a de manter a persistência de sessões HTTP."

bém decide que locais eles podem ver". O *release* somente não realça que a corporação saberá exatamente onde cada usuário cadastrado estiver. O confortável e divertido sistema anula o anonimato, confirma o biopoder e permite perceber que as redes vão se tornando móveis e a mobilidade expande as dinâmicas pós-hobbesianas da sociedade de controle.

Referências

AGRE, P E.; ROTENBERG, M. **Technology and privacy: the new landcaspe**. Cambridge, Massachusets: The MIT Press, 1997.

ANTOUN, H. De uma teia à outra: a explosão do comum e o surgimento da vigilância participativa. In: **Web 2.0: participação e vigilância na era da comunicação distribuída** / Henrique Antoun (org.). Rio de Janeiro: Mauad Editora, 2008.

BAUMAN, Z. **Modernidade e ambivalência**. Rio de Janeiro: Jorge Zahar Ed., 1999.

BENKLER, Y. **The wealth of networks: how social production transforms markets and freedom**. New Haven and London: Yale University Press, 2006.

BENTHAM, J. **O panóptico**. Belo Horizonte: Autêntica Editora, 2008.

BERLIN, I. Introdução. In: **A liberdade; Utilitarismo** / John Stuart Mill. São Paulo: Martins Fontes, 2000.

BRUNO, F. **Dispositivos de vigilância no ciberespaço: duplos digitais e identidades simuladas**. Revista Fronteiras. Vol VIII, Nº 2, maio/agosto 2006.

CLARK, I. **The Philosophy behind Freenet**. Disponível em: <http://freenetproject.org/philosophy.html> . Acesso em: 10 fev. 2009.

CONSTANT, B. **Da liberdade dos antigos comparada à dos modernos**. Revista Filosofia Política, No. 2, pp. 9-25. Porto Alegre: L&PM Editores, 1985.

_____. **Princípios de política aplicáveis a todos os governos**. Rio de Janeiro: TOPBOOKS Editora, 2007.

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

_____. **Foucault**. São Paulo: Brasiliense, 2006.

DE HEART, P. Benjamin Constant's refutation of republican and utilitarian arguments against anonymity. In: **Digital anonymity and the law: tensions and dimensions**. Edited by C. Nicoll; J. E. J. Prins; M. J. M. van Dellen. Cambridge: Cambridge University Press, 2003. (Information Technology & Law Series)

DYSON, E. **Release 2.0**. Rio de Janeiro: Campus, 1998.

ELETRONIC Frontier Foundation. Bloggers have the right to stay anonymous. Disponível: <http://www.eff.org/issues/bloggers>. Acesso em: 10 fev. 2009.

FINLEY, M.I. **Democracia antiga e moderna**. Rio de Janeiro: Graal, 1988.

FOUCAULT, M. **Vigiar e punir**. Petrópolis,RJ: Editora Vozes,1996.

GALLOWAY, A. **Protocol: how control exists after decentralization**. Cambridge, Massachusetts: The MIT Press, 2004.

HABERMAS, J. **Mudança estrutural da esfera pública**. Rio de Janeiro: Tempo Brasileiro, 1984.

_____. **Racionalidade e Comunicação**. Lisboa, Portugal: Edições 70, 1996.

HALL, S. **A identidade cultural na pós-modernidade**. Rio de Janeiro: DP&A Editora, 2006.

LAZZARATO, M. (**As revoluções do capitalismo**. Rio de Janeiro: Civilização Brasileira, 2006.

LESSIG, L. **Code and oher laws of cyberspace**. New York: Basic Books, 1999.

MADISON, J; HAMILTON, A; JAY, J. **Os artigos federalistas**. Rio de Janeiro: Nova Fronteira, 1996.

MAFFESOLI, M. **Sobre o nomadismo**. Rio de Janeiro: Record, 2001.

MARX, G. T. **What's in a Name? Some Reflections on the Sociology of Anonymity**. Disponível: <http://web.mit.edu/gtmarx/www/anon.html>. Acesso em: 10 jan. 2009.

MILL, J. S. **A liberdade / Utilitarismo**. São Paulo: Martins Fontes, 2000.

MILLER, J. A máquina panóptica de Jeremy Bentham. In: **O Panóptico** / Jeremy Bentham. Belo Horizonte: Autêntica Editora, 2008.

MITCHELL, B. **protocol (network).** About.com**.** Disponível em: <http://compnetworking.about.com/od/networkprotocols/l/bldef_protocol.htm>. Acesso em: 12 nov. 2007.

MOUNIER, P. **Os donos da rede: as tramas políticas da internet**. São Paulo: Edições Loyola, 2006.

NETWORK Architecture. A description of data formats & procedures used for communication between nodes. Disponível: <http://www.connectworld.net/cgi-bin/iec/05GLSN.html>. Acesso em: 23 mar. 2008.

POSTER, M. Cyberdemocracy: Internet and the Public Sphere. In D. Porter (ed.), **Internet Culture**. New York: Routledge, 1997.

PRIMO, A. **Interação mediada por computador**. Porto Alegre: Edições Sulinas, 2008.

REUTERS. Google lança software de localização de usuários de celular. Disponível em: <http://www.abril.com.br/noticias/tecnologia/google-lanca-software-localizacao-usuarios-celular-258483.shtml>. Acesso em: 12 fev. 2009.

TELECOMMUNICATIONS: Glossary of Telecommunication Terms. Disponível em: <http://www.its.bldrdoc.gov/fs-1037/fs-1037c.htm> Acesso em: 20 fev. 2008.

TOR. Overview. Disponível em: <https://www.torproject.org/overview.html.pt>. Acesso em: 10 fev. 2009.

UGARTE, D. **O poder das redes**. Porto Alegre: EDIPUCRS, 2008.

WIENER, N. **Cibernética: o el control y comunicación en animales y máquinas**. Barcelona: Tusquets Editores, 1998.

Trabalho apresentado ao Grupo de Trabalho "Comunicação e Cibercultura", do XVIII Encontro da Compós, na PUC-MG, Belo Horizonte, MG, em junho de 2009.