Surveillance in Latin America
"Vigilância, Segurança e Controle Social" . PUCPR . Curitiba . Brasil . 4-6 de março de 2009
ISSN 2175-9596

# VIGILÂNCIA NOS SITES DE REDE SOCIAL:
## apontamentos para o contexto latino-americano a partir do estudo do Facebook.com

*Surveillance on social networks websites: the Latin American case from the study of Facebook.com*

**Liliane da Costa Nascimento** [a]

[(a)] Universidade Federal do Rio de Janeiro, PPGCOM, ECO , Rio de Janeiro, RJ –Brasil, e-mail: cnasmp@yahoo.com.br.

**Resumo**

Em 2008, o site de rede social *Facebook.com* alcançou a marca de mais de 140 milhões de usuários ativos em todo o mundo e ultrapassou o *MySpace* em número de acessos diários de visitantes únicos. No contexto latino-americano, países como Chile, Colômbia, Venezuela, Argentina e México estão entre os quinze em todo o mundo que mais usam o serviço e somados, contabilizam mais de 13 milhões de usuários. A grande quantidade de informações reveladas espontaneamente pelos internautas nestes sites faz com que, por um lado, eles sejam associados ao nascimento de um novo *voyeurismo* social e novas práticas de exposição de si; por outro, eles colocam em jogo novas práxis de registro, acesso e tratamento de dados individuais, que podem ser usados para propostas de *social sorting*. O objetivo deste artigo é estudar os padrões de revelação de informações do público latino em comparação com o público norte-americano. Nossa metodologia de abordagem prevê a coleta e a análise de amostras significativas de perfis de redes latinas e norte-americanas, geográficas e universitárias, recolhidos no site entre os meses de dezembro de 2008 e fevereiro de 2009. Esperamos, assim, realizar apontamentos sobre as características da vigilância que ocorre nos sites de rede social, especialmente no *Facebook.com*.
Palavras Chave: Vigilância; Cibercultura; Redes sociais; Facebook.

## INTRODUÇÃO

Já se tornou lugar comum reafirmar a importância dos sites de rede social na reconfiguração da sociabilidade contemporânea. Cotidianamente, recorremos a estes dispositivos com objetivos diversos: ora a pura diversão de contemplarmos rostos desconhecidos, ora o

imperativo imediato de manter contato com amigos e conhecidos de uma maneira barata e conveniente, ora para obter de maneira silenciosa e fácil alguma informação sobre alguém. Nestes sites, o imperativo da exibição de si, fenômeno tão característico da sociedade contemporânea, é complementado por uma arquitetura de visibilidade planificada, que subsidia a emergência de um *voyeurismo* distribuído, no qual o olho público, em toda a sua pluralidade, se volta ao indivíduo ordinário: todos vêem todos, todos se exibem a todos, na espera ansiosa pelas novidades sociais que desta condição podem emergir. Como não é difícil perceber, esta generalização do ver e do ser visto pode ser associada à recente proliferação das tecnologias vigilantes, que têm equipado cidadãos comuns com aparatos que em um passado não muito distante, eram exclusividade de burocracias estatais organizadas. O termo vigilância, no entanto, apesar de gravitar pelo campo semântico das práticas ligadas ao olhar, denota um processo organizado através do qual populações são monitoradas e supervisionadas para propostas específicas (LYON; ZUREIK, 1996). Historicamente, ao longo dos anos, este fenômeno adquire lentamente novas associações. Inicialmente ele está atrelado à ação do estado e à evolução das forças capitalistas, acoplamentos que atuaram na direção de identificar os indivíduos, registrá-los, documentá-los, governá-los, conferi-los novos direitos ou extrair deles corpos produtivos e úteis. Hoje, diante das ameaças do crime e do terrorismo e da reconfiguração do papel do estado em uma economia globalizada, temos uma nova fase de expansão da vigilância, que pode ser situada mais precisamente a partir de do final do século XX (LYON, 2004). Muito têm se discutido sobre as especificidades e características deste processo, e este trabalho, igualmente, se propõe a equacionar contribuições sobre o tema, no contexto específico dos sites de rede social.

Com este objetivo, nos voltamos ao estudo do *Facebook*, site de rede social criado nos EUA em 2004 e que rapidamente se expandiu por todo o mundo, contando hoje com mais de 140 milhões de usuários ativos. No contexto latino, a despeito do site vir adquirido um número cada vez mais significativo de usuários, estudos sobre os padrões de uso desta parcela de público são raros ou inexistentes. Desta forma, circunscreveremos aqui quatro países latino-americanos: Argentina, Chile, Colômbia e México, que juntos, contam com mais de 11 milhões de usuários participantes. Visando subsidiar uma comparação com o público norte-americano, estudaremos também o Canadá. Após efetuarmos *download* de amostras significativas de perfis de dez redes, oito latino-americanas e duas canadenses, geográficas e de instituições de ensino superior, realizaremos apontamentos sobre o comportamento deste público, eleito como foco deste estudo. Assim, retomaremos questões sobre as hierarquias da vigilância e sobre como se articulam as dimensões social e de controle nas rotinas de uso

destes sites. Esperamos assim compreender como se dá a associação de fenômenos ligados ao manejo e ao uso de dados individuais subsidiados pelo site e a noção de vigilância.

## VIGILÂNCIA, CLASSIFICAÇÃO E PREDIÇÃO

A vigilância que ocorre no ciberespaço é marcada pelo monitoramento e registro dos rastros comunicativos deixados pelos internautas em seu uso cotidiano do meio para a classificação e posterior antecipação de comportamentos, preferências, tendências e interesses. Trata-se de uma lógica que responde, em grande medida, ao imperativo da personalização dos ambientes digitais e à promoção do consumo através da publicidade direcionada – em suma, ao recorrente imaginário da minimização dos riscos e da eficácia maximizada. Segundo Bruno, (2006, p. 154), "em linhas gerais, o dispositivo de vigilância digital tem três elementos centrais: a informação, os bancos de dados e os perfis computacionais". A coleta anônima de dados – que se dá em nível infra-individual – compõe bancos de dados, que permitirão o armazenamento e principalmente o tratamento da informação para a dedução de assertivas que permitam efetuar a classificação de indivíduos e/ou grupos. Trata-se de um processo estritamente informacional: nestes bancos, que abrigam dados em categorias específicas (de gênero, de faixa etária, profissionais, financeiras, biológicas, etc.), atuam algoritmos responsáveis pela composição de perfis, que serão usados, em um futuro próximo, para prever o comportamento humano, antecipando tendências, gostos, preferências, interesses. Assim, grosso modo, a vigilância que ocorre no ciberespaço começa com a conversão imediata das comunicações dos indivíduos em informações sobre algum aspecto particular de suas vidas. Esta informação é o ponto de partida para o processo de produção de um novo saber, que subsidia estratégias de gerenciamento social e amplia, em última instância, a eficácia do controle social através do aprimoramento do próprio sistema vigilante.

Vejamos em detalhes como se dá este processo de captura, formalização e classificação do comportamento humano. Em primeiro lugar, há uma comunicação unilateral dos indivíduos com os bancos de dados, que recebem e registram mensagens que eles sequer julgam estar enviando a estes repositórios (POSTER, 1990, p. 69). Trata-se, portanto, de uma resposta inconsciente, automatizada e não-direcional (POSTER, 1996, p. 187). Em geral, estas instâncias respondem a uma programação qualquer, que determina o armazenamento das informações solicitadas. Suas características principais são o alto nível de organização dos dados recebidos, que podem ser divididos, relacionados, agrupados, classificados e re-classificados segundo diferentes critérios; a acessibilidade instantânea e a capacidade de

registro praticamente infinito; e a facilidade de integração e/ou cruzamento de dados com os de outras bases, o que implica que diferentes tipos de informações sobre um determinado indivíduo podem ser relacionadas a partir de um simples processo de checagem de diferentes tipos de registro (profissionais, militares, de consumo, de saúde, educacionais, policiais, e assim por diante).

Desta forma, Poster (ibid., p. 186) situa o poder das bases de dados no fato de serem uma linguagem performativa, no sentido foucaultiano do discurso – não um conjunto de signos, mas uma prática que confere existência ao que enuncia. Os campos dos bancos de dados são aspectos do comportamento dos indivíduos, e sua representação através deste mecanismo fornece simulacros de cada um e de toda a população representada, para que informem, em um futuro próximo, processos de tomada de decisão que envolvem algum aspecto particular de suas existências. Assim, os bancos de dados não apenas formalizam, mas engendram identidades, e por isso, esta nova modalidade de poder reside justamente na reestruturação da natureza do indivíduo (ibid., p. 190). Uma nova forma de presença, múltipla e descentralizada, é inaugurada pela inserção nestes dispositivos de registro, originando, para cada um que ali é representado, identidades sociais adicionais adquiridas em um processo que implica a substituição da concepção moderna de sujeito – estável e coerente, marcada por uma subjetividade interiorizada – pela objetivação de aspectos particionados da existência, por uma abordagem caracterizada pela dispersão e pela heterogeneidade.

Cabe ressaltar que este processo é marcado por uma certa superficialidade diagnóstica: nele, os dados visados – coletados e tratados – são aqueles que registram aspectos mais evidentes e formalizáveis do comportamento humano, o que implica assumir que a vigilância contemporânea não endereça o indivíduo em sua toda a sua complexidade psicológica. Ao contrário, ela visa capturar o instante presente, os atos manifestos, as atitudes mais imediatas. Desta forma, estamos vivenciando uma mudança também no tipo de informação que é considerada significativa pelos aparatos vigilantes (BRUNO, 2006). Ao invés dos dados estáveis, referentes à categorias geodemográficas, biométricas, relativos a gênero, etc., que praticamente não se alteram com o curso do tempo, as informações visadas por esses dispositivos hoje são predominantes mutáveis, "comportamentais (comunicação, consumo, deslocamento, lazer), "transacionais" (uso de cartão de crédito e serviços, navegações em ambientes digitais), psicológicos (autodeclarações sobre personalidade, gosto), sociais (comunidades e amigos em ambientes digitais), entre outros" (ibid., p.5).

Uma vez construídos os bancos de dados, torna-se possível a construção de perfis, algoritmos derivados do tratamento das informações armazenadas nestes dispositivos de registro e que

passam a validar uma nova saída de dados. Isso significa que um perfil é, em suma, a criação de um modelo que visa analisar a pertinência ou a semelhança de um indivíduo ou comportamento a um grupo ou padrão em especial. Assim, podemos descrever sua instauração em duas etapas: a) a coleta de dados para a construção de um modelo computacional – seja baseado em uma investigação manual de dados de uma população específica (por exemplo, terroristas de uma determinada organização presos em um determinado período de tempo) ou com base em um processo informatizado, que usa uma população de treino (para adequação dos parâmetros do algoritmo); b) fase de validação, em que há a submissão de dados coletados de indivíduos particulares ao modelo criado, visando avaliar algum aspecto de sua existência. Na prática, esses perfis se tornam, como salienta Bogard (1996, p. 27), verdadeiras tecnologias de observação antes do fato. O que eles fornecem, através de suas análises, são prognósticos – antevisões capazes de instaurar realidades possíveis a partir de sua projeção. Desta forma, o perfil não é verdadeiro nem falso: ele é da ordem da simulação. E assim como o código, sua lógica é performativa: através de um achatamento temporal, ele transforma o presente a partir da efetivação transformadora daquilo que ele enuncia, intervindo no campo das atualizações possíveis a partir da conjectura de um futuro imaginável.

## REDES SOCIAIS E A REVELAÇÃO DE INFORMAÇÕES

Os sites de rede social não chamam a atenção apenas pela adesão majoritária em diferentes culturas e países do mundo, mas também, pela imensa quantidade de informações que os usuários parecem estar predispostos a revelar sobre si neste contexto (ACQUISTI; GROSS, 2005, p. 72). As pesquisas realizadas até o presente momento, referentes em sua maioria ao contexto americano de redes sociais como *Facebook* e o *MySpace* e focadas predominantemente no comportamento do público jovem, mostram que a quantidade de informações verdadeiras reveladas espontaneamente pelos usuários é significativa e que, de maneira geral, eles não costumam adotar as configurações de privacidade disponíveis para protegê-las (ACQUISTI; GROSS, 2005; JONES et. al.; SOLTREN, 2005; STUZMAN, 2006; GOVANI; PASHLEY, 2005; JONES, 2008; STRATER; RICHTER, 2007). À primeira vista, a impressão que temos é a de que os usuários dos sites de rede social não alimentam grandes preocupações acerca de sua privacidade. No entanto, Acquisti e Gross (2006) apontam a existência de uma discrepância exacerbada entre as atitudes destes usuários e as considerações

por eles reportadas acerca do tema, que indicam altos níveis de preocupação com o acesso de estranhos aos seus dados pessoais e com sua privacidade de maneira geral.

A facilidade de expansão e o crescimento exagerado dessas redes aumentam a probabilidade de que as informações disponibilizadas pelos usuários sejam expostas a um número cada vez maior e mais variado de pessoas, dificultando o controle de sua visibilidade pelos indivíduos que as publicam. Naturalmente, a amplitude deste processo depende do critério usado pelo site em questão para permitir o acesso ao perfil de terceiros. Assim, se os amigos podem ver seu perfil, quanto mais estranhos adicionados, maior o grau de exposição. Se os amigos dos amigos também podem ver seu perfil ou se todos os que participam das redes das quais você também participa podem visualizá-lo, as informações em jogo se tornam ainda mais disponíveis. Desta forma, quando usamos os sites de rede social, embora nem sempre tenhamos este fato em mente, estamos publicizando nossas vidas não apenas aos nossos amigos e conhecidos, mas a uma audiência potencialmente mais heterogênea e maior, que pode incluir, por exemplo, o site que as hospeda e em última instância, qualquer um que, com certo grau de esforço, deseje buscá-las (*hackers*, *spammers*, funcionários de agências governamentais, familiares, policiais, um possível empregador ou alguma autoridade na escola, na faculdade, etc).

A visibilidade das informações que os indivíduos disponibilizam nestes sites pode ser abordada através da noção de "públicos em rede", desenvolvida por Boyd (2007a, p. 8). A autora parte do princípio de que os sites de rede social representam o surgimento de um novo tipo de espaço público, que se caracteriza pela ausência de um contexto definido para a ação dos atores e pela amplitude das comunicações que nele ocorrem, esta última mais importante para a argumentação que visamos desenvolver aqui. Tradicionalmente, temos que, nas interações não-mediadas, ou face-a-face, a disseminação de um fato está limitada por restrições espaço-temporais (só quem o presenciou pode falar dele). O surgimento de tecnologias que subsidiem interações mediadas (TV, rádio, etc.) modifica este contexto porque elas potencializam a amplitude das audiências: os acontecimentos passam a ser registrados e podem ser reproduzidos em um contexto de dissociação espaço-temporal. No caso das redes sociais temos não apenas uma interação mediada, mas uma interação em rede, que modifica as circunstâncias do processo de interação social principalmente devido às características inerentes às linguagens digitais. Nestes sites, os dados, além de facilmente replicáveis e persistentes – o que você falou há 3 anos atrás ainda estará armazenado e disponível quando você tiver 30 – são buscáveis, o que significa que estarão disponíveis a qualquer momento a qualquer um que os encontre e queira acessá-los (BOYD, 2007b, p. 2-3).

Assim, a condição instaurada pelos sites de rede social nas dinâmicas da revelação de informações se torna, por natureza, contraditória. Boyd (2007a) se refere ao dilema dos jovens, que devem direcionar seus discursos ao mesmo tempo para audiências opostas; os pais, de quem querem ou precisam esconder tudo e os amigos, a quem querem mostrar tudo o que julgam interessante. As contradições experimentadas pelos interatores neste contexto são uma regra geral e estão longe de se configurarem como condição exclusiva do público jovem. Como ressaltam Acquisti e Gross (2005), muitas vezes queremos revelar algo às pessoas mais próximas, e não a estranhos. Outras, desejamos fazer o contrário. O fato é que as redes sociais aproximam e fazem coexistir todas as nossas diferentes redes de relacionamento, e com isso, demandam uma adequação difícil de encontrar: a de que as informações postadas sejam compatíveis com públicos tão diferentes quanto os amigos da balada da sábado à noite, os colegas de trabalho com quem você convive há alguns anos e o seu chefe, por exemplo. Assim, "ao tornar as conexões de uma pessoa visível para todas as outras, os sites de rede social removem as barreiras de privacidade que as pessoas mantêm entre os diferentes aspectos de suas vidas" (BOYD; DONATH, 2004, p. 78).[1]

A revelação de informações nos sites de redes social e os possíveis riscos associados a este processo também dependem da quantidade, veracidade e qualidade (considerada em termos de precisão ou acuidade) das informações publicadas. De maneira geral, as pesquisas revelam que, quando a proposta do site incentiva o *upload* de informações verdadeiras e o estabelecimento de conexões entre os indivíduos, é natural que as informações disponibilizadas sejam reais, corretas e precisas (ACQUISTI, GROSS, 2005).[2] No entanto, é importante ressaltar que o uso destes sites e que as práticas da construção e da exibição de si são processos intimamente relacionados à natureza social e pública de toda a informação ali disponibilizada. Consideremos novamente o estabelecimento das relações de amizade. Dado contexto de predominante anonimato das relações *online* e a facilidade de construção de uma identidade falsa, a rede de amigos funciona como um instrumento que permite a identificação e atesta a veracidade das informações publicadas pelos indivíduos (BOYD; DONATH, 2004, p. 73-74). Ainda que um indivíduo possa adicionar estranhos que são pessoas verdadeiras, ou criar vários *fakes* para simular uma rede de contatos em seu perfil, ou buscar ainda outras saídas, em geral, não faria sentido associar uma rede de conhecidos verdadeiros a um perfil próprio com informações falsas, pois o custo social de tal processo seria demasiadamente

[1] Tradução nossa para: "[…] by making all of one's connections visible to all the others, social networking sites remove the privacy barriers that people keep between different aspects of their lives".

[2] Esta premissa é predominante em sites cuja proposta é o *networking*, e não se aplica aos sites de relacionamento com o Match.com, que incentiva inclusive o uso de pseudônimos.

oneroso para a reputação daquele que mente dentro de seu próprio círculo social. Assim, a presença de amigos que sejam pessoas reais atesta, de maneira geral, a concordância com o comportamento predominante e aceitável dentro destes sites.

> O uso do nome verdadeiro e da rede (de amigos) implicam que se alguém mentir extensivamente em seu perfil, os verdadeiros conhecidos iriam verificar isso e presumidamente, repreendê-los – ou no mínimo, alguém poderia se sentir envergonhado de ser visto exagerando seus feitos diante dos amigos. Mentiras mais sérias, como uma pessoa casada se passando por uma solteira, seriam mais difíceis de executar em um site de rede social. (BOYD; DONATH, 2004).[3]

Assim, a conexão do perfil de um indivíduo à sua rede de amigos implica a ampliação do espectro espaço-temporal sobre o qual podem incidir as conseqüências das suas atitudes *online*. Enquanto o anonimato aumenta o grau de liberdade das relações – pois os indivíduos se vêem livres de qualquer problema futuro ou constrangimento presente – ele também fomenta o comportamento agressivo, desfavorecendo a sociabilidade e a comunicação entre os participantes. Neste sentido, a identificação, que pode ser considerada como perda de privacidade (BOYD; DONATH, 2004, p. 6) é também indispensável ao bom funcionamento da rede. Assim, essas conexões tornadas públicas implicam, cada vez mais, fornecer, em todos os aspectos e todas as interações, informações verdadeiras sobre si próprio, o que torna os indivíduos mais vulneráveis a uma série de riscos implícitos ao uso destes sites – riscos estes que, em geral, mesclam questões relacionadas à segurança e aos crimes cibernéticos, por um lado, e ao acesso dos dados disponibilizados a audiências indesejadas, por outro. Roubo de identidade, *phishing*,[4] *blackmailing*, vírus e *spywares*, assédio ou perseguição (*online* ou *offline*) e acesso inadequado a contas pessoais (bancárias, de e-mail ou *instant messaging*) se encaixam no primeiro grupo, enquanto problemas com pais, autoridades, futuros empregadores ou com aqueles interessados em coletar dados pessoais para *profiling*, por exemplo, fazem parte do segundo.

Os riscos inerentes ao uso do ciberespaço são potencializados pela lógica da associação de dados pessoais provenientes de diferentes fontes e bases de dados. Haggerty e Ericsson (2000) usam a noção de "agenciamento vigilante" para se referir a uma condição de convergência de

[3] Tradução nossa para: "The use of one's real name and the network both imply that if one were to prevaricate extensively in one's profile, real acquaintances would see this and presumably, make some rebuke — or at least, one would be embarrassed to be seen exaggerating accomplishments in front of one's friends. More serious deceptions, such as a married person posing as an available single, are far more difficult to perform in a networking site".

[4] O *phishing* acontece quando um agressor tenta adquirir informações relevantes de uma vítima se passando por alguma entidade confiável, como um site conhecido, um banco respeitado ou mesmo alguma agência governamental.

dispositivos outrora descontínuos, configurando uma vigilância que opera através da quebra dos fluxos comunicacionais que emanam do corpo (seja ele individual, coletivo, biológico ou social) e de sua recomposição para propostas de observação que visam o desenvolvimento de estratégias comerciais, de governo e controle. Assim, os dados disponíveis em redes sociais podem ser combinados àqueles presentes em diversas outras bases (de natureza estatal ou pública) que incluem informações sobre preferências de consumo (presentes em sites como eBay ou Amazon.com), sobre as instituições bancárias utilizadas (que podem ser "hackeados" através do históricos dos navegadores), sobre os termos digitados nos buscadores, etc. Este fato está na base das políticas de re-identificação que se tornam possíveis no ciberespaço, através das quais corpos de informações sem identificação explícita (de nome e endereço, principalmente), podem ser associados a dados cujo pertencimento pode ser estabelecido através da presença de atributos comuns.

Acquisti e Gross (2005) afirmam que a combinação do fornecimento de dados como endereço, data de nascimento e sexo pode ser uma ameaça aos usuários americanos de redes sociais. Associados ao fornecimento do número de telefone e da cidade em que mora o indivíduo em questão, eles podem subsidiar inclusive o roubo de identidade, além de permitirem a re-identificação de dados em relação a bases anônimas. Gross (2005) também mostra como softwares de reconhecimento facial podem rastrear as fotos disponíveis em perfis de um mesmo usuário em diferentes redes sociais, permitindo assim a identificar os demais dados disponibilizados. Assim, as informações reveladas de maneira anônima no Friendster podem ser somadas aos dados disponibilizados no Facebook, por exemplo. Outra forma de se levantar dados sobre indivíduos que usam redes sociais é através das ferramentas avançadas de busca. A partir da experimentação de diferentes critérios, a presença de um determinado perfil entre as listas de resultados de cada quesito procurado pode revelar dados sobre seu dono – como sexo, idade, status de relacionamento e preferência sexual (ACQUISTI, GROSS, 2005), além de outros menos óbvios relacionados ao uso de drogas e bebidas, por exemplo (JONES; SOLTREN, 2005, p. 27). Merecem destaque ainda os estudos de Jagatic et. al., que coletaram dados sobre as redes de relações de alunos da Indiana University disponíveis em sites de rede social e mostraram como essas informações podem aumentar o sucesso de um ataque *phising*.[5]

[5] Neste estudo, os autores enviaram um e-mail malicioso tanto de um remetente desconhecido da Indiana University quanto de um amigo da vítima. Este último e-mail foi quatro vezes mais eficiente em fazer com que o indivíduo clicasse no link malicioso e fornecessem seus dados de login e senha ao *phiser*.

Muitas hipóteses são levantadas para tentar explicar esta alta predisposição dos usuários de redes sociais em revelar informações apesar dos riscos envolvidos. Estudos prévios demonstram que esses indivíduos têm dificuldade em conceber e admitir sua vulnerabilidade (JAGATIC, et. al., 2007) e que, muitas vezes, eles não apresentam uma compreensão clara sobre o fato de que estes sites podem ser usados para propostas de coleta de dados que servirão às rotinas da publicidade direcionada ou subsidiarão atividades potencialmente ilegais, como crimes cibernéticos, *phishing*, etc. Hipóteses como o elevado grau de confiança nos serviços prestados por essas redes e no respeito de todos os usuários aos termos do serviço também são consideradas (ACQUISTI; GROSS, 2005, p.73). Um estudo mais aprofundado destas questões será realizado no próximo capítulo. Por hora, consideremos apenas que, quaisquer que sejam os motivos associados a este fenômeno, é importante que nosso olhar sobre as redes sociais considere que suas ferramentas de segurança e controle são permeáveis por natureza, "para alavancar seu valor enquanto utilidades em rede e promover seu crescimento, fazendo o registro, acesso e compartilhamento da informação descomplicados". (ACQUISTI; GROSS, 2006, p.2).[6] Assim, temos que os benefícios implícitos ao uso destes sites figuram, lado a lado, com riscos inerentes a sua configuração, modo de uso e estrutura.

## ANÁLISE DE PERFIS

Esboçadas as possíveis manobras de disponibilização, acesso, tratamento e uso dos dados individuais publicados no *Facebook*, passemos agora à nossa análise empírica sobre o comportamento dos usuários do site. No mês de setembro de 2008, realizamos um levantamento sobre a demografia do *Facebook* visando identificar os países com mais membros participantes. Este levantamento preliminar teve como objetivo orientar a composição da amostra utilizada nesta pesquisa. Os dados foram coletados diretamente do sistema de direcionamento de anúncios do *Facebook*, através do qual, com a ajuda de uma macro, consultamos o número de usuários maiores de 18 anos em cada um dos países disponíveis no sistema da empresa.[7] Os dados coletados em setembro de 2008 foram consultados novamente ao final desta pesquisa, no mês de fevereiro de 2009, utilizando-se a mesma metodologia, pois devido às significativas taxas de crescimento registradas pelo site

[6] Tradução nossa para: "to leverage their value as network goods and enhance their growth by making registration, access, and sharing of information uncomplicated".

[7] Interface disponível em: <http://www.facebook.com/ads/create/>. É importante ressaltar que o sistema disponibiliza dados sobre os países nos quais o número de usuários é significativo o suficiente para justificar o direcionamento de anúncios.

no último ano, tais dados se tornaram rapidamente desatualizados. Segundo os índices registrados pela primeira consulta realizada, pudemos identificar os países com maior número de usuários no contexto norte-americano e no contexto-latino americano: EUA e Canadá, com 33.718.780 e 10.065.720 membros, respectivamente, ocupavam o primeiro e o terceiro lugares no ranking geral de países por número de usuários; Chile, Colômbia, Venezuela, México e Argentina, com 3.410.140, 3.349.740, 1.572.740, 1.265.820 e 1.051.580 ocupavam, por sua vez, a oitava, nona, décima, décima terceira e décima nona posições no referido ranking. Assim, definimos estes cinco países como foco de nosso estudo do público latino-americano, principalmente pela falta de estudos que contemplassem esta parcela de usuários do site.

Outro fator considerado decisivo para esta escolha foi o crescimento do número de usuários dos países latino-americanos selecionados, observado durante o período de realização da pesquisa. Dados publicados pela *O'Reilly Research* em dezembro de 2008 (LORICA, 2008) comprovaram posteriormente esta tendência. Ainda que a maior parte dos usuários do *Facebook* esteja concentrada na América do Norte, nesta região o site cresceu apenas 17% nas 12 semanas que antecederam a publicação da medição realizada pela *O'Reilly Research*. Para a América do Sul, a taxa de crescimento foi de 33%, sendo que a região responde por apenas 10% dos usuários do site, atrás da Europa, com 31% e da América do Norte, com 40% (Fig. 3, Anexo 1). As taxas de crescimento para a Europa e para o Oriente Médio/Norte da África também foram maiores do que as registradas para a América do Sul. Outra contribuição interessante desta pesquisa é a faixa etária em que o site vem se expandindo nas diferentes regiões do mundo. Enquanto na América do Norte a maior parte dos novos usuários do *Facebook* tem entre 35 e 59 anos, na América do Sul a adesão de novos membros está distribuída com mais eqüidade entre as diversas faixas etárias. Além disso, nas faixas de 13-17 e 18-25 anos, o *Facebook* cresceu a taxas de apenas 4% e 8% na América do Norte, enquanto na América do Sul as taxas para essas duas faixas etárias são 39% e 32%, respectivamente (Fig. 4, Anexo 1). Por fim, a pesquisa revela que apenas no Oriente Médio/Norte da África o número de homens é maior do que o de mulheres entre os participantes do site. Na América do Norte, eles totalizam 42% e elas 54% dos usuários, enquanto na América do Sul 41% são homens e 49% são mulheres (Fig. 5, Anexo 1). A pesquisa da *O'Reilly Research* não traz dados específicos para a América Latina, e dentre os países que elegemos como foco de nosso estudo, os dados relativos ao México estão contabilizados na América do Norte.

Assim, a análise que se segue possui enfoque quantitativo e visa elucidar os padrões de revelação de informações dos usuários latino-americanos do *Facebook*. Nosso estudo visa identificar possíveis especificidades do contexto latino a partir de uma comparação com o contexto norte-americano. Neste sentido, circunscrevemos 10 redes, 8 latino-americanas e 2 norte-americanas, das quais recolhemos amostras significativas de perfis para análise. Um robô foi construído para realizar esta tarefa, usando a linguagem de programação *Perl* e *scripts* para o *parsing* das páginas HTML. O processo de coleta dos perfis se deu da seguinte forma. Primeiramente, uma nova conta era aberta no *Facebook* e cadastrada em uma das redes selecionadas para o estudo. Depois, uma busca aleatória realizada pelo robô no site retornava usuários integrantes desta rede. Por fim, estas páginas eram acessadas automaticamente, a partir do link disponível na página de busca. A página de perfil do usuário era então salva juntamente com as informações nela disponibilizadas, com exceção do nome e da foto do participante. Por fim, um banco de dados foi montado para organizar estas informações: dados como as redes das quais um usuário participava, sexo, idade, número de amigos e de fotos foram salvos. Os demais campos foram convertidos em variáveis dicotômicas: avaliamos apenas o preenchimento ou não preenchimento destas informações. Análises semelhantes foram realizadas no *Facebook* por Jones et. al. (2005) e Acquisti e Gross (2005), com foco no estudo de universidades americanas. Em nosso caso, como nosso objetivo é estudar o comportamento do público latino americano, avaliamos ser necessário considerar de antemão algumas questões relativas à forma como estes membros utilizam o site, principalmente no que diz respeito à participação em redes do *Facebook*. Tais diferenças devem considerar as condições em que surgiu o site e como se deu seu processo de expansão, focado primeiramente na expansão para outras universidades americanas a partir de Harvard. O suporte a redes de instituições de ensino superior fora dos EUA começou em outubro de 2005 e somente em setembro de 2006 o site abriu a participação a usuários comuns.

Desta forma, enquanto no contexto norte-americano o uso do site está predominantemente focado nas redes de instituições de ensino superior que exigem um e-mail da respectiva universidade para a participação, no contexto latino é comum a existência de redes abertas, que dispensam o cadastro de um e-mail institucional. Além disso, visto que no contexto norte-americano originalmente o uso do site começava com a adesão a uma rede de universidade e que hoje países como o Canadá e os EUA possuem redes geográficas para cidades, voltamos nossa atenção para como se dá o uso das redes de países na América Latina. Assim, dada a impossibilidade de acessar as redes fechadas, usamos em nosso estudo redes de universidades latino-americanas abertas, bem como as redes geográficas dos países correspondentes.

Usamos desta vez quatro países latino-americanos: Chile, Argentina, Colômbia e México. A Venezuela, por possuir número de usuários próximo aos da Colômbia segundo nosso levantamento preliminar, foi dispensada desta análise. Para subsidiar uma comparação com o público norte-americano, usamos o Canadá. Esta escolha foi motivada não só pelo significativo número de usuários do *Facebook* no país como pelo acesso a uma conta de e-mail que nos permitisse participar de uma rede universitária – depois de entramos em contato com várias instituições americanas e canadenses, identificamos a possibilidade de pagar pelo acesso a uma conta de e-mail da *University of British Columbia* (UBC).

Assim, o estudo que se segue será baseado em 20.682 perfis coletados em 10 redes do *Facebook*, a saber: Argentina, *Universidad Católica Argentina* (UCA); Chile, *Universidad de Viña Del Mar* (UVM); Colômbia, *Universidad Industrial de Santander* (UIS); México, *Universidad de Guadalajara* (UDG); Vancouver, *University of British Columbia* (UBC). A tabela abaixo mostra a divisão por gênero em cada uma das redes avaliadas. Os gráficos da distribuição por idade estão relacionados em anexo, e nos permitem constatar a primeira diferença de uso entre os públicos dos países latino-americanos e do país norte-americano. Enquanto em todas as redes de universidades latino-americanas estudadas a presença de representantes com mais de 27 anos é comum, variando em diferentes taxas até os 40 ou 42 anos, na rede canadense a freqüência de participantes decresce radicalmente a partir dos 27 anos, sendo praticamente inexistente a partir dos 31 anos. Não acreditamos que os participantes da rede estejam mentindo acerca de suas idades, visto que nosso questionário identificou que, em geral, os latino-americanos tendem a revelar informações verdadeiras no *Facebook*. Não podemos justificar esta diferença de comportamento, mas acreditamos que o fato de tais redes serem abertas pode facilitar que pessoas que tenham algum interesse em participar ou que tenham estudado nas respectivas instituições há mais tempo tenham acesso a elas mais facilmente do que os interessados em participar na rede canadense. Por fim, é importante considerar que as informações relativas a gênero e idade incluem apenas os que declararam esta informação em seus perfis.

| Rede | N | Masculino | Feminino |
|---|---|---|---|
| Argentina | 1795 | 54,64% | 45,20% |
| Universidad Católica Argentina (UCA) | 1052 | 46,96% | 53,03% |
| Chile | 3018 | 54,39% | 45,60% |
| Universidad de Viña Del Mar (UVM) | 1266 | 51,12% | 48,87% |
| Colômbia | 1421 | 58,96% | 41,03% |
| Universidad Industrial de Santander (UIS) | 2452 | 57,69% | 42,30% |

| | | | |
|---|---|---|---|
| México | 2939 | 57,12% | 42,85% |
| Universidad de Guadalajara (UDG) | 2146 | 55,58% | 44,41% |
| Vancouver | 2255 | 61,71% | 38,28% |
| University of British Columbia (UBC) | 2338 | 60,49% | 39,50% |

Analisamos o nível de uso de configurações de privacidade para cada uma das redes supracitadas de duas maneiras. Por *default*, um perfil no *Facebook* é visível pelos indivíduos que estão na mesma rede e pelos amigos. Assim, em um primeiro momento, avaliamos quantos indivíduos bloquearam o acesso ao seu perfil aos indivíduos de uma rede da qual faziam parte, deixando-o visível apenas aos amigos e/ou a outra rede da qual também fizessem parte. Como descrevemos acima, o *download* dos perfis era feito por um robô logado em uma das redes que circunscrevemos para este estudo. Assim, podemos apontar, entre os perfis que tentamos acessar, aqueles que não estavam disponíveis para leitura, ou seja, aqueles cujos donos restringiram o acesso aos integrantes da referida rede, usando suas configurações de privacidade. Como mostra a tabela abaixo, os canadenses foram os que mais usaram configurações de privacidade para restringir o acesso aos demais integrantes da rede aos seus perfis. Há uma diferença significativa entre a predisposição dos usuários da rede de ensino superior canadense e de redes latino-americanas no uso de configurações de privacidade para restringir o acesso a seus perfis. As porcentagens dos que liberam este acesso variam entre 77% e 92% para as redes de universidades latino-americanas, valor que cai para 38% na rede UBC. Para as redes geográficas a diferença observada foi menor. O percentual dos latinos que disponibilizam seus perfis girou entre 49% e 59%, contra 36% para a rede Vancouver.

Em todos os países estudados, a porcentagem de perfis acessíveis em redes de universidades foi significativamente maior do que para as geográficas. Isto pode indicar que a existência de um espaço real compartilhado de fato predispõe os indivíduos a liberarem seus perfis – obviamente, como não podemos acessar os perfis bloqueados, não podemos conjecturar sobre a influência de fatores como sexo e idade na predisposição do uso de configurações de privacidade. Somente entre os canadenses a diferença entre as porcentagens dos perfis acessíveis em cada tipo de rede foi pequena, o que aponta que a predisposição para o uso de configurações de privacidade, para este público, independe do contexto. Por fim, realizamos um teste nas redes Chile e Canadá circunscrevendo os usuários que participavam, ao mesmo tempo, das redes Chile e *Universidad de Viña Del Mar* (UVM) e Vancouver e *University of British Columbia* (UBC). Visamos avaliar se aqueles que haviam bloqueado o acesso aos seus

perfis aos demais integrantes da rede geográfica deixavam seus perfis abertos na rede da instituição de ensino superior. Encontramos que 16,3% dos canadenses que estavam nas duas redes e que fecharam seus perfis na rede Vancouver liberaram o acesso pela rede UBC. Para a interseção entre as redes Chile e UVM este valor sobre para 23,7%. Estes dados confirmam a tendência de que os canadenses tendem a bloquear o acesso aos seus perfis independente da rede, mas com leve predisposição a liberá-lo no contexto universitário, enquanto os chilenos estão comparativamente mais predispostos a liberar seus perfis para as redes de instituições de ensino superior do que para as geográficas.

| Nome | Total | Amostra (N) | Disponibilizam perfil | % Disponibilizam |
|---|---|---|---|---|
| Universidad Catolica Argentina (UCA) | 3193 | 1303 | 1052 | 81% |
| Argentina | 670229 | 3020 | 1795 | 59% |
| University of British Columbia (UBC) | 37390 | 6192 | 2338 | 38% |
| Vancouver | 863780 | 8647 | 3086 | 36% |
| Universidad de Viña Del Mar (UVM) | 2051 | 1545 | 1266 | 82% |
| Chile | 807673 | 7923 | 3844 | 49% |
| Universidad Industrial de Santander (UIS) | 4357 | 3164 | 2452 | 77% |
| Colômbia | 1133931 | 3062 | 1641 | 54% |
| Universidad de Guadalajara (UDG) | 7395 | 2334 | 2146 | 92% |
| México | 674512 | 5263 | 2939 | 56% |

Avaliamos também a publicação ou não de informações nos seguintes campos dos perfis coletados: telefone celular, endereço de e-mail, sobre mim, citações favoritas, livros de cabeceira, programas de TV favoritos, músicas favoritas, interesses, atividades, visão política, interessado em, status de relacionamento, religião, data de nascimento e gênero. Um perfil mínimo do *Facebook* deve ter pelo menos o nome, e-mail e no caso de uma rede de universidade, o status do participante (se aluno de graduação, funcionário, ex-aluno, etc.), sendo que o e-mail e o status podem ser configurados para ser ou não disponibilizados de acordo com as configurações de privacidade dos usuários. Assim, as informações que os usuários publicam para além desta quantidade mínima para a abertura de um perfil são reveladas por sua própria vontade. De maneira geral, considerando a média de todas as informações publicadas, temos que, para as redes geográficas, colombianos (m = 4,58) e argentinos (m = 4,90) exibem menos informações do que os chilenos (m = 5,80) e mexicanos

(m = 5,97). O comportamento dos usuários destes dois últimos países em relação à quantidade de informações reveladas em cada categoria é mais próximo do que entre os usuários dos dois primeiros. Os integrantes da rede geográfica canadense foram os que revelaram em média mais informações (m = 6,80).

A disponibilização de informações com valor comercial (livros de cabeceira, programas de TV favoritos, músicas favoritas, atividades e interesses) segue esta mesma tendência. O índice criado para calcular a média de publicação destas informações foi menor entre os colombianos (Ic = 0,93) e argentinos (Ic = 1,28) e maior entre mexicanos (Ic = 1,65) e chilenos (Ic = 1,66), sendo que a diferença entre os valores do índice para os dois últimos países não é estatisticamente significante. O maior grau de disponibilização de informações com valor comercial foi para a rede canadense (Ic = 2,16). Quanto à publicação de informações de contato, enquanto o número de telefone celular foi publicado por poucos em todas as redes geográficas (1% dos colombianos e argentinos, 2% dos chilenos e mexicanos, diferença não estatisticamente significante), a revelação do endereço de e-mail apresentou variação significativa. Enquanto no contexto latino-americano a porcentagem dos que publicava esta informação variou entre 13% e 20%, para a rede canadense este valor foi de 47%. Informações mais suscetíveis a maiores influências do contexto cultural, como visão política e religião, variaram em desacordo com esta tendência. Estes campos foram preenchidos, respectivamente, por 30% e 27% dos colombianos, 28% e 28% dos argentinos, 36% e 39% dos chilenos, 39% e 33% dos mexicanos, 35% e 32% dos canadenses. Outra informação que variou em desacordo com a tendência geral de comportamento em relação à revelação de informações foi o status de relacionamento. Disponibilizá-lo é mais comum entre mexicanos, chilenos e colombianos (63%, 60% e 57%, respectivamente) do que entre argentinos e canadenses (47% e 49%).

Consideremos agora o comportamento dos usuários das redes de instituições de ensino superior. Neste contexto, a predisposição dos indivíduos em revelar informações não equivale à observada acima, para o caso das redes geográficas. A predisposição de revelar informações foi menor entre os integrantes da *Universidad Católica Argentina* (m = 4,19). Em seguida, aparecem, com índices semelhantes, a *Universidad de Guadalajara* (m = 4,46) e *Universidad Industrial de Santander* (m = 4,55). No contexto latino, os chilenos, integrantes da *Universidad de Viña del Mar* foram os mais predispostos a revelar informações (m = 4,94). A coincidência com o comportamento nas redes geográficas foi constatada apenas para o caso do Canadá: a *University of British Columbia* registrou o maior índice entre as redes universitárias observadas (m = 6,79). Com exceção da Colômbia e do Canadá, nos quais a

média das informações reveladas foi igual para as redes geográficas e de universidades (m= 6,79 para a UBC e m = 6,80 para a Vancouver; m = 4,55 para a UIS e m = 4,58 para a Colômbia), nos demais países latino-americanos observamos que os usuários revelam menos informações nas redes de universidades do que na rede geográfica do país correspondente. Comparando o contexto entre os países. Com exceção do contexto colombiano, os usuários revelam, em média, menos informações com valor comercial em redes de universidades do que para as redes geográficas. Uma diferença sensível para os padrões de comportamento observados para as redes universitárias foi a alta predisposição dos usuários em revelar informações de contato em comparação com as redes geográficas. A publicação do telefone celular cresce ligeiramente e do endereço de e-mail em níveis muito significativos.

## A VIGILÂNCIA NAS REDES SOCIAIS E O ARGUMENTO PANÓPTICO

Para esclarecer melhor os contornos da vigilância que ocorre em sites de rede social, especialmente no *Facebook*, retomemos o argumento panóptico e sua arquitetura de visibilidade particular, considerando inicialmente apenas a divisão poucos-muitos implícita a este modelo, usando-o sem considerar os fatores implícitos ao contexto disciplinar da análise foucautiana. Como já ressaltamos ao longo deste trabalho, as redes sociais são projetadas para agregar o maior número de pessoas possível. Sua arquitetura de visibilidade é projetada para permitir a exposição e a observação generalizadas, através das quais todos se mostram a todos e todos observam todos, algo diferente do que pressupõe o modelo panóptico, através do qual alguns poucos observam muitos. Neste sentido, a arquitetura de redes do *Facebook*, apesar de tecnicamente frágil, representa uma tentativa de selecionar os campos de visão disponíveis aos usuários do sistema: todos vêem todos dentro de uma rede qualquer, todos os amigos vêem todos os amigos, o que é diferente de uma condição na qual todos os membros do site pudessem ver os perfis de todos os outros e expor seus perfis a todos os outros. No entanto, ainda assim, podemos considerar que o *Facebook*, como todo site de rede social, é um espaço para o exercício da exposição e do voyeurismo planificados e simétricos: tecnicamente, dentro da arquitetura das redes e de acordo com as configurações de privacidade dos usuários, é possível ver e ser visto. Esta condição de reversibilidade não impede, no entanto, que processos panópticos, em que poucos vêem muitos, não possam surgir dentro destes sites, com campos de visibilidade efetivamente assimétricos e programados para atender a interesses específicos.

Este nivelamento das hierarquias da vigilância e a emergência de uma condição em que todos observam todos não é exclusividade do contexto das redes sociais. E os contornos que este descentramento assume nestes sites também não é o mesmo que caracteriza, por exemplo, as políticas de segurança baseadas na ação do cidadão vigilante, fomentadas em larga escala nos EUA após os ataques às torres gêmeas, de acordo com as quais os indivíduos ordinários são responsáveis pela segurança pública e encarregados da função de observar e denunciar atos suspeitos. Se o efeito mais imediato aqui é a proliferação de uma cultura da suspeição e insegurança generalizadas, nas redes sociais a planificação da vigilância pode estar associada a efeitos bem menos funestos: olhar o outro pode estar ser um exercício de alteridade e de construção de si, um ato de troca, potencializado pela estrutura das redes e pela emergência das novas tecnologias. No entanto, seria uma atitude no mínimo ingênua ignorar que este ambiente esteja imune a efeitos panópticos, ou seja, que os dados aí publicados não possam servir a setores específicos, instaurando dinâmicas através das quais alguns coletam, manejam e colocam ao serviço de seus interesses as informações individuais disponíveis. Assim, nas redes sociais, a conectividade generalizada serve tanto aos objetivos sociais de uso do meio quanto a formas organizadas de vigilância de dados através das quais poucos observam muitos, utilizando para tal as habilidades computacionais aumentadas que subsidiam as políticas de coleta, registro e tratamento da informação.

Nas redes sociais, os canais de visibilidade distribuídos potencializam a vigilância social, fenômeno que não é exclusividade das tecnologias digitais nem das sociedades contemporâneas. No entanto, a exposição naturalizada e o espaço que esta prática ocupa nas estratégias de produção de subjetividade dos indivíduos é algo característico de nossa era, que em muito contribuiu para o sucesso e adesão maciços ao fenômeno das redes sociais. O olhar mediado se tornou lugar comum (MEYROWITZ, 1985). No entanto, como argumenta Lianos (2003), uma leitura possível para esta condição seria a de que não é a vigilância que avança, mas a sociabilidade que se torna cada vez mais institucionalizada, abrindo espaço, assim, para os mecanismos de controle contemporâneos que atuam sobre o comportamento humano, orientando condutas presentes freqüentemente a partir de conjecturas futuras. Neste sentido, lembramos que o consentimento ao olhar do outro implícito à exposição de si em redes sociais não é incondicional ou irrestrito. Assim, temos que o desejo de ser visto por alguns convive com o desejo de não ser visto por outros, conflito que os interatores destes sites tentam permanentemente apaziguar. No *Facebook*, podemos destacar, dentre estas formas indesejadas do olhar a figura da própria empresa se destaca enquanto uma audiência institucional silenciosa, em larga medida inesperadas por parte dos participantes destes sites,

cujo foco de atenção está na interação com os amigos e conhecidos. Assim, à medida que avançam a mediatização e a institucionalização da sociabilidade, o processo de interação social se complexifica: novos espaços podem se oferecer ao surgimento de arquiteturas panópticas, com alguns poucos se dedicando a observar muitos.

Assim como o panóptico é uma arquitetura que visa permitir ver tudo, no *Facebook*, o senso de intimidade do site e a consideração da privacidade dos usuários no desenvolvimento do sistema produziram o efeito de fomentar a revelação de informações, maximizando a visibilidade da empresa que hospeda os dados a partir da restrição da visibilidade disponível aos demais usuários. Estimular nos membros os sentimentos de segurança e familiaridade e permitir a eles escolher como e com quem compartilhar suas informações são fatores que fazem como que eles se sintam mais à vontade, menos preocupados ou que se torne mais importante e útil revelar informações verdadeiras sobre si. Outro ponto de semelhança com a arquitetura panóptica é a indecidibilidade vigilante. Assim como não é impossível atestar a presença ou ausência do vigia na torre em um determinado momento, no *Facebook* é impossível saber como e quando os dados individuais nele disponibilizados serão usados pela empresa ou por terceiros. Sabemos que as informações que publicamos estão potencialmente expostas a audiências diversas daquelas ditas aqui desejadas. No caso específico do uso dos dados individuais pela empresa, temos que inclusive os termos de uso do site atestam esse uso. Assim, sabemos que estas modalidades de acesso são possíveis, ainda que sua presença nos seja atualmente indecidível. Além disso, assim como para o prisioneiro seria impossível se furtar ao olhar controlador do vigia, em nosso caso a única alternativa seria deixar de usar a rede, algo tecnicamente válido, mas que implicaria a renúncia a todos os benefícios implícitos ao seu uso. Como resgatamos ao longo desse trabalho, nos casos em usuários se revoltaram contra novas funcionalidades no site ou com as políticas da companhia, as ameaças de que deixariam o site não foram cumpridas, o que nos leva a considerar que fugir a esse olhar em um mundo já tão acostumado a esta nova modalidade de comunicação seria algo difícil. Desta forma, vemos que é possível assinalar pontos de contato entre a vigilância que se passa no *Facebook* e aquela própria à arquitetura de visibilidade descrita pelo panóptico. No entanto, se algumas semelhanças existem, julgamos que a identificação de pontos de ruptura com esta lógica é mais importante para a perspectiva do trabalho que aqui visamos concretizar.

Ao considerarmos o panóptico não apenas como uma estrutura de visibilidade, mas em termos foucaultianos, como um mecanismo de controle social, vemos o quanto o fenômeno que se passa nas redes sociais diverge daqueles que se passavam nas sociedades modernas, não podendo ser abordado puramente sob uma perspectiva de continuidade com o modelo

disciplinar. Em primeiro lugar, o medo da sanção é aqui substituído pelo desejo de ver e ser visto. A revelação de si é voluntária e é vista por aqueles que se engajam nesta atividade como algo prazeroso, interessante e desejado. Além disso, ao invés de incidir sobre os desviantes, esta vigilância endereça os circuitos da sociabilidade e da inclusão. No entanto, se no modelo panóptico convive-se constantemente com o medo do vigia, aqui muitas vezes impera a falta de conhecimento acerca da visibilidade de outrem e mesmo das políticas da empresa que oferece o serviço. Afinal, temer o vigiar (ou o campo de sanções e punições a ele implícito) estava na base da estratégia de normalização que caracteriza o modelo disciplinar. Ao contrário, hoje, a vigilância não depende ou usa como premissa a internalização de valores ou normas. Lianos (2003, p. 424) propõe que a recepção desta racionalidade implícita aos sistemas sócio-técnicos com os quais interagimos para acessar os serviços dos quais desejamos exerce o efeito de controlar sem realizar esforços no sentido de estruturar as premissas do comportamento dos usuários. Assim, o que se objetiva – freqüentemente através do emprego de dispositivos tecnológicos - é promover e garantir o comportamento eficiente, i.e., aquele em acordo com os objetivos institucionais (LIANOS, 2003, p. 423).

## REFERÊNCIAS

ACQUISTI, Alessandro; GROSS, Ralph. Information Revelation and Privacy in Online Social Networs. Workshop on Privacy on Electronic Networks **(WPES)**, Alexandria, 2005. **Anais eletrônicos**. Disponível em: http://portal.acm.org/results.cfm?coll=GUIDE&CFID=16206531&CFTOKEN=76266819&query=Gross%20Acquisti&dl=GUIDE&dimval=4294832877.Acesso em:29/08/08.

ACQUISTI, Alessandro; GROSS, Ralph. Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. 6th Workshop on Privacy Enhancing Technologies (PET), Cambridge, Jun. 2006. **Anais eletrônicos**. Disponível em: < http://www.heinz.cmu.edu/~acquisti/papers/acquisti-gross-facebook-privacy-PET-final.pdf>. Acesso em 22/08/08.

ANDREJEVIC, Mark. **iSpy:** surveillance and power in the interactive era. Lawrence: University Press of Kansas, 2007.

BOGARD, William. Welcome to the Society of Control: The Simulation of Surveillance Revisited. In: HAGGERTY, K. D.; ERICSON, R. V. (eds.). **The new politics of surveillance and visibility**. Toronto: University of Toronto Press, 2006. p. 55-78.

BOYD, D. Why Youth (Heart) Social Network Sites: The Role of Networked Publics, in Teenage Social Life. **MacArthur Foundation Series on Digital Learning – Youth, Identity, and Digital Media Volume** (ed. David Buckingham). Cambridge, MA: MIT Press, 2007a.

_____. “None of this is real.” In **Structures of Participation**, edited by Joe Karaganis (in press, 2007b).

_____.; DONATH, J. Public displays of connection. **BT Technology Journal**, v. 22, n. 4, p. 71-82, 2004.

BRUNO, Fernanda. Dispositivos de vigilância no ciberespaço: duplos digitais e identidades simuladas. **Revista Fronteiras**, São Leopoldo, v. 8, n. 2, p. 152-9, mai./ago., 2006.

GOVANI, Tabreez; PASHLEY, Harriet. **Student Awareness of the Privacy Implications When Using Facebook**. Disponível em: < http://lorrie.cranor.org/courses/fa05/tubzhlp.pdf>. Acesso em: 16/10/08.

JAGATIC, Tom N.; JOHNSON, Nathaniel A.; JAKOBSSON, Markus; MENCZER, Filippo. Social phishing. **Communications of the ACM**. v. 50, n. 10, p. 94-100. Out. 2007.

JONES, Harvey; SOLTREN, José Hiram. **Facebook**: threats to privacy. Disponível em: <http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall05-papers/facebook.pdf >. Acesso em 18/08/08.

LIANOS, Michalis. **Le nouveau contrôle social:** toile institutionnele, normative et lien social. Paris: L’Harmattan, 2001.

_____. Social Control after Foucault. **Surveillance & Society**, v.1, n.3, p.412-30, 2003.

LORICA, B. “Facebook Growth By Country and the Slowdown in App Usage”, http://radar.oreilly.com/2008/07/facebook-growth-by-country-and.html, 2008.

MEYROWITZ, J. **No sense of place**:The impact of electronic media on social behavior. New York and Oxford: Oxford University Press, 1985.

POSTER, Mark. **The mode of information**: poststructuralism and social context. Chicago: The University of Chicago Press, 1990.

STRATER, Katherine; RICHTER, Heather. Examining Privacy and Disclosure in a Social Networking Community. 3rd Symposium on Usable Privacy and Security. Pittsburgh, Pennsylvania. July 18 - 20, 2007. **Anais eletrônicos**. Disponível em: < http://portal.acm.org/ft_gateway.cfm?id=1280706&type=pdf&coll=GUIDE&dl=GUIDE&CFID=15833498&CFTOKEN=79391213>. Acesso em: 11/09/08.