

Universidade Federal do Rio de Janeiro (UFRJ)
Centro de Filosofia e Ciências Humanas (CFCH)
Escola de Comunicação (ECO)

Liliane da Costa Nascimento

Participação e vigilância nos sites de rede social:
um estudo do Facebook.com

Rio de Janeiro
Março de 2009

**Participação e vigilância nos sites de rede social:
um estudo do Facebook.com**

Liliane da Costa Nascimento

Dissertação de mestrado apresentada ao
Programa de Pós-Graduação em Comunicação e
Cultura da Escola de Comunicação da
Universidade Federal do Rio de Janeiro, como
parte dos requisitos para a obtenção do título de
Mestre em Comunicação e Cultura.

Orientadora: Prof^ª Dr^ª Fernanda Glória Bruno

Rio de Janeiro
Março de 2009

Nascimento, Liliane da Costa

Participação e vigilância nos sites de rede social: um estudo do Facebook.com / Liliane da Costa Nascimento. – Rio de Janeiro, 2009.

214 f.

Dissertação (Mestrado em Comunicação e Cultura) – Universidade Federal do Rio de Janeiro, Escola de Comunicação, 2009.

Orientadora: Fernanda Glória Bruno

1. Cibercultura. 2. Tecnologias de vigilância. 3. Sites de rede social. 4. Facebook. 5. América Latina. I. Bruno, Fernanda (Orient.). II. Universidade Federal do Rio de Janeiro, Escola de Comunicação. III. Título.

Liliane da Costa Nascimento

Participação e vigilância nos sites de rede social: um estudo do Facebook.com

Dissertação de mestrado apresentada ao Programa de Pós-graduação em Comunicação e Cultura da Escola de Comunicação da UFRJ, como parte dos requisitos para a obtenção do título de Mestre em Comunicação e Cultura.

Rio de Janeiro, 30 de março de 2009.

Banca Examinadora

Prof.^a. Dr.^a. Fernanda Glória Bruno – Orientadora
Doutora em Comunicação e Cultura (UFRJ), ECO/UFRJ

Prof. Dr. André Luiz Martins Lemos
Doutor em Sociologia (Université Paris V), FACOM/UFBa

Prof. Dr. Henrique Antoun
Doutor em Comunicação e Cultura (UFRJ), ECO/UFRJ

Rio de Janeiro
2009

*Dedico este trabalho ao meu garoto
Thiago, pelo carinho e compreensão
incondicionais, pela ajuda imprescindível
com os códigos e planilhas e por me ouvir
pacientemente inúmeras vezes enquanto eu,
agitada, organizava em voz alta a confusão
de meus pensamentos.*

*Aos meus pais, Amadeu e Nelí, pela
presença, apoio e compreensão infinitos.
Pensar em vocês foi sempre a melhor
maneira de seguir em frente.*

AGRADECIMENTOS

Muitos contribuíram, cada qual à sua maneira, para a realização deste projeto pessoal. É chegada então a hora de agradecer. Antes de mais nada, à minha paciente e bem humorada orientadora, Fernanda Bruno, que soube me trazer calma e alegria nos momentos em que estive insegura e com quem pude compartilhar pensamentos interessantes e momentos únicos no decorrer dos últimos anos. Ao meu pai, Amadeu do Nascimento, pelos telefonemas e palavras de incentivo; à minha mãe, Nelí da Costa Nascimento e ao meu irmão Amadeu Jr., pela alegria certa das noites mineiras de sexta-feira e pelo apoio constante nas idas e vindas de volta pra casa; à minha irmã Aline Costa, que soube compreender e ajudar a seu modo. Àqueles que me ajudaram na difícil tarefa de mudar para o Rio de Janeiro: à amiga Ana Angélica Soares e ao seu pai, Canova, que gentilmente me cederam um lar para que tudo isso pudesse começar; à amiga Lívia Nascimento, com quem dividi muito mais que um apartamento ao longo do primeiro ano de mestrado. Aos colegas da pós, em especial às amigas Fernanda Gomes, Talitha Ferraz, Mariana Taborda e Paola Leblanc pelas conversas divertidas e pelo apoio mútuo. Igualmente, ao carinho e amizade de todos os que souberam se fazer presentes, apesar da ausência e da distância: Mariana Pelegrini, Dimas Tadeu, Letícia Perani, Vanessa Resende, Camila Wenzel, Flávia Paravidino, Luiz Felipe Stevenim e tantos outros. À divertida companhia carioca do casal None e Marcela, pelos fins de semana revigorantes que me ajudavam a arejar os pensamentos e preparar a volta ao trabalho. Ao Programa de Educação Tutorial da Faculdade de Comunicação da Universidade Federal de Juiz de Fora (PET-Facom/UFJF), onde tudo começou, especialmente aos professores Francisco Pimenta, Marta Pinheiro e Potiguara Mendes, a quem serei eternamente grata pelo conhecimento trocado e pelos momentos de amizade que me ajudaram a realizar escolhas importantes na vida. Aos professores do Programa de Pós Graduação da ECO/UFRJ, pelo aprendizado e por saberem respeitar meu desejo por horizontalizar minha formação e experimentar conhecimentos novos, em especial aos professores Paulo Vaz e Micael Herschmann. Ao imprescindível auxílio financeiro da Capes, sem o qual teria sido impossível a realização desta pesquisa. Aos funcionários da secretaria do PPGCOM/ECO/UFRJ, que além de desempenharem seu trabalho habitual, inúmeras vezes me ajudaram a driblar as dificuldades da distância, me auxiliando com atenção na entrega de trabalhos e no recebimento de documentos. Igualmente, aos funcionários das bibliotecas do Campus da Praia Vermelha da UFRJ, que tantas vezes me forneceram abrigo na hora de estudar. Por fim, um

agradecimento especial a todos os voluntários que tornaram possíveis as reflexões que aqui se apresentam, por terem tirado seu tempo para responder a minha pesquisa. A colaboração de cada um de vocês foi de valor inestimável para a concretização deste projeto.

There are no secrets here; all codes conform to one
code that decodes them all.
(*William Bogard, Welcome to the Society of
Control*).

Le contrôle forme ainsi un des composants de la
liberté postindustrielle. Il s'exprime dans les règles
de production et d'utilisation des systèmes, des
processus et des objets qui sont désirables comme
moyens consacrés à la construction autonome de la
biographie individuelle et de l'action collective.
(*Michalis Lianos, Le nouveau contrôle social*).

RESUMO

NASCIMENTO, Liliane da Costa. **Participação e vigilância nos sites de rede social: um estudo do Facebook.com**. Rio de Janeiro, 2009. Dissertação (Mestrado em Comunicação e Cultura) – Escola de Comunicação, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2009.

Esta dissertação visa analisar em que medida os processos referentes à publicação, acesso e uso das informações disponibilizadas através dos *sites* de rede social podem estar associados ao fenômeno da vigilância. Para alcançar este objetivo, nos lançamos ao estudo dos usuários latinos do *Facebook.com*, buscando compreender os fatores que influenciam seu comportamento em relação à revelação de informações, ao uso de configurações de privacidade e à autocensura dos dados postados no *site*. De maneira semelhante, investigaremos também como os usuários avaliam os riscos possivelmente associados às suas práticas de interação nestes ambientes, as possíveis audiências por eles conjecturadas como passíveis de acessarem seus dados através do *site* e o seu grau de conhecimento acerca das possíveis modalidades de uso destas informações. Para abordar estas questões, além de um levantamento bibliográfico sobre as práticas da empresa, conduziremos uma análise estatística de 262 questionários *online*, administrados em uma amostra de respondentes exclusivamente latinos. Este exame será complementado por uma investigação das diferenças comportamentais e demográficas entre usuários latino-americanos e norte-americanos do *Facebook* através da análise quantitativa de 23.458 perfis coletados em 11 redes do *site*, 3 canadenses e 8 latino-americanas, geográficas e universitárias. Neste percurso, colocaremos a própria noção de vigilância sob investigação e analisaremos suas relações com a participação e o controle, visando reunir e propor um escopo teórico capaz de lançar luz sobre as atividades vigilantes que encontram seu lugar nos *sites* de rede social, especialmente no *Facebook.com*.

Palavras-chave: Vigilância; *Facebook*; *Sites* de rede social; Revelação de Informações; América-Latina.

ABSTRACT

NASCIMENTO, Liliane da Costa. **Participation and surveillance on social network sites: a study of Facebook.com.** Rio de Janeiro, 2009. Dissertation (Master's Degree in Communication and Culture). Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2009.

This dissertation aims to analyse the extent to which the processes referable to the publication, access and use of information provided through social network sites can be associated with the surveillance phenomena. To achieve this goal, we engage ourselves in the study of Latin users of Facebook.com, trying to understand the factors that influence their behavior towards information revelation, usage of privacy settings and self-censorship of data posted on the site. In a similar way, we will also investigate how these users evaluate the potential risks associated to their practices of interaction in these environments, the possible audiences conjectured by them as liable to access their data through the website and their level of knowledge about possible modalities of use of these data. To approach these questions, added to a bibliographical research of the company's practices, we will conduct a statistical analysis of 262 internet-based questionnaires, administered to a sample of Latin respondents. This examination will be complemented by an inquire of behavioral and demographic differences between Latin Americans and North Americans users through quantitative analysis of 23.458 profiles collected from 11 Facebook networks, 3 Canadian ones and 8 Latin American ones, based around regions and colleges. Through this way, we will put the notion of surveillance under investigation and we will analyse their relations with participation and control, aiming to propose a theoretical scope able to highlight the surveillant activities which find their place on Facebook.com.

Keywords: Surveillance; Facebook, Social network sites; Information revelation; Latin America.

SUMÁRIO

INTRODUÇÃO	13
CAPÍTULO 1: A VIGILÂNCIA CONTEMPORÂNEA	19
1.1 As disciplinas: o olhar como armadilha	20
1.2 O controle	25
1.3 A vigilância digital	32
1.3.1 Vigilância e tecnologia: uma condição de reversibilidade	34
<i>1.3.1.1 Códigos e protocolos</i>	<i>40</i>
1.3.2 Vigilância, classificação e predição	46
<i>1.3.2.1 A estrutura temporal da vigilância: risco e predição</i>	<i>48</i>
<i>1.3.2.2 Classificação e individualização</i>	<i>51</i>
CAPÍTULO 2: AS REDES SOCIAIS	57
2.1 A evolução das redes sociais	59
2.2 Redes: estrutura e abordagem	61
2.3 A web 2.0 e as redes sociais	64
2.4 Estrutura e características principais	68
2.5 Redes sociais e a revelação de informações	72
2.6 Comunicação mediada e exposição de si	78
2.7 A publicidade direcionada e a mineração de dados nas redes sociais	83
2.8 Portabilidade: cada um tem a sua?	89
CAPÍTULO 3: REVELAÇÃO, ACESSO E USO DE DADOS INDIVIDUAIS NO FACEBOOK	95
3.1 Uma arquitetura de visibilidade particular	97
3.2 A publicação de informações do Facebook	100
3.3 A publicidade no Facebook	106
3.4 A portabilidade de dados no Facebook	116
3.5 Busca de pessoas e audiências indesejadas	123
CAPÍTULO 4: A VIGILÂNCIA NO FACEBOOK: RESULTADOS E APONTAMENTOS	130
4.1 Análise de questionários: o posicionamento dos usuários do sistema	132
4.2 Análise de perfis	147
4.3 Controle e vigilância: hierarquias em xeque?	157
4.4 O argumento panóptico, a normatividade e a participação	167
CONSIDERAÇÕES FINAIS	173

REFERÊNCIAS BIBLIOGRÁFICAS	180
ANEXO A: DADOS DEMOGRÁFICOS DO FACEBOOK	190
ANEXO B: QUESTIONÁRIOS APLICADOS	196
ANEXO C: ANÁLISE DE PERFIS	204

INTRODUÇÃO

Durante o ano de 2008, enquanto este trabalho era escrito, o *Facebook*¹ crescia a uma estrondosa taxa de 127% e se tornava o maior *site* de rede social da Internet, batendo com folga o *MySpace*, que até março do referido ano, vencia com apertada vantagem esta acirrada disputa (COMSCORE, 2009).² No mês de dezembro, o *site* registrou mais de 221 milhões de visitantes únicos, quase o dobro do alcance de seu maior rival, que contou com 125 milhões de visitantes únicos no mesmo período (ARRINGTON, 2009). Este excelente desempenho posicionou o *Facebook* como o sétimo *site* mais popular de toda a Internet, acessado por um em cada cinco internautas em todo o mundo no referido mês. No entanto, mais do que apenas um grande sucesso de público, o *Facebook* se destaca pela agressividade com que tem perseguido o tão sonhado modelo para a eficiente monetização das redes sociais. E é esta incessante busca pela conversão do tráfego de acesso em lucros concretos para a companhia que nos permite constatar um fato tão simples quanto importante, que colocamos aqui como o ponto de partida desta pesquisa. Os *sites* de rede social não são apenas espaços para o exercício aumentado da sociabilidade. Eles são, também, bases de dados amplas e poderosas, que podem se prestar a usos diversos e que encarnam com tranquilidade a premissa de que a geração de valor pode advir das dinâmicas horizontais da participação, da exibição de si e da construção da subjetividade. E são justamente o caráter público, a facilidade técnica de manejo e o valor dos dados disponibilizados nestes *sites* para diversas audiências que nos levam a suspeitar de uma possível convivência entre o ver descompromissado e o vigiar organizado nas modalidades de participação possibilitadas pelos *sites* de rede social, especialmente pelo *Facebook*.

Assim, as páginas que se seguem são orientadas pelo desejo de apreender as dinâmicas de transformação da relação entre as práticas vigilantes e o estatuto da sociabilidade no mundo contemporâneo. Elas sintetizam uma tentativa de compreender algo que chega a nós como o testemunho de um tempo. Enquanto lá fora nos esperam as ruas, com sua atmosfera particular, com suas práticas de convivência e modalidades de exercício do olhar, progressivamente, as fábulas de um mundo densamente interconectado invadem nossas vidas em espaços cujo aconchego outrora era atribuído e associado à esfera privada. Assim, nos lançamos à experimentação coletiva das maravilhas e delícias da conectividade generalizada,

¹ <http://www.facebook.com>.

² Segundo dados publicados em dezembro de 2008 pela *comScore*, disponíveis em: <http://www.comscore.com/press/release.asp?press=2698>. Cf. Anexo A, Fig. 1, p. 190.

interagindo em *sites* como o *Facebook*, *Orkut*, *LinkedIn*, *Friendster*, *Bebo*, dentre outros. Podemos caracterizar estes *sites* como serviços *online*, oferecidos, de maneira geral, por uma empresa, que nos permitem: a) mostrar aos outros fatos sobre nossas vidas e personalidades (seja através de textos, fotos ou vídeos); b) manter listas organizadas de contatos, os chamados ‘amigos’, que em geral podem ver o que publicamos sobre nós em nossas páginas e interagir conosco. O sucesso destes *sites* em diferentes países e culturas só faz reforçar os já evidentes benefícios e conveniências da sociabilidade mediada, do *voyeurismo* horizontalizado e da exibição de si, perseguidos por indivíduos comuns que publicam voluntariamente em seus perfis generosas quantidades de informação sobre suas vidas, gostos, interesses e personalidades. Em sua maioria completas³ e precisas, essas informações adquirem valores superlativos para públicos diversos – muitas vezes bem distantes da esperada audiência dos colegas e amigos – dentre os quais podemos elencar autoridades, familiares, anunciantes, empregadores e a própria empresa que oferece o serviço. Assim, podemos dizer que, nos *sites* de rede social, as práticas do ver e do ser visto se complexificam enquanto o ato social se depara com condições novas e desafiadoras.

Desta forma, diante dos variados mecanismos de acesso e uso das informações pessoais publicadas nos *sites* de rede social, nos questionamos sobre as possíveis relações deste fenômeno com a noção de vigilância. De maneira geral, o termo se refere ao processo através do qual populações são monitoradas e supervisionadas para propostas específicas (LYON e ZUREIK, 1996: 3). Historicamente, esta modalidade de olhar esteve atrelada à consolidação do Estado burocrático (GROEBNER, 2001; HACKING, 1999) e ao processo disciplinar de organização das forças produtivas, que visava extrair dos corpos inaptos condicionamentos produtivos e úteis (FOUCAULT, 1977). Mais recentemente, diversas transformações têm reconfigurado as dimensões deste fenômeno na contemporaneidade. Por um lado, consideremos as ameaças globalizadas do crime e do terrorismo, que resultaram em uma obsessão generalizada pela segurança a qualquer custo, postura que vem justificando frequentemente a ação de amplos mecanismos voltados à atividade de vigiar. Por outro, consideremos a progressiva informatização de nossas ações, transações e comunicações em um mundo no qual dependemos, a todo momento, de instâncias institucionais para realizar nossos planos de vida e escolhas. Esta condição – potencializada em grande medida pelas habilidades computacionais que tornam o registro praticamente infinito, o custo praticamente

³ O termo visa designar aqui que muitas informações são publicadas pelos usuários destes sites em sua totalidade: nome e sobrenome, dia mês e ano para o caso da data de nascimento, e assim por diante. Não queremos com isso denotar a abrangência destes dados em relação aos variados aspectos da vida de um indivíduo.

ínfimo e o processamento e recuperação de dados cada vez mais eficientes – justifica o uso do termo vigilância digital para nos referirmos às práticas contemporâneas através das quais “[...] alguma forma de atividade humana é analisada por um computador de acordo com alguma regra específica” (LESSIG, 2006: 209, tradução nossa).⁴

A principal regra desta nova condição é a de que interagimos constantemente com dispositivos para os quais o uso não mais se dissocia do registro. No contexto da vigilância contemporânea que ocorre no ciberespaço, nossas atitudes são imediatamente convertidas em informações sobre nós (BRUNO, 2006) e usadas para antever cenários futuros, gerando prognósticos que interferem sobre as escolhas e oportunidades presentes, de modo a maximizar a eficiência e minimizar o risco. Neste contexto, a abundância de dados individuais é organizada pelo uso de técnicas para a classificação dos indivíduos a partir da ação de algoritmos em amplos bancos de dados, visando dar sentido às massas informacionais anônimas acumuladas. Assim, gradativamente, vemos a vigilância deixar os porões da esfera estatal e o requinte das histórias de espionagem para se integrar progressivamente a outros contextos: o *marketing* e seus sistemas de recomendação de produtos e serviços; a vida cotidiana de indivíduos ordinários, que se valem da atual proliferação de dispositivos tecnológicos para se engajarem no trabalho de monitorar amigos e inimigos, conhecidos e desconhecidos, seja como forma de entretenimento ou com o objetivo de administrar a própria vida social (ANDREJEVIC, 2008). É neste sentido que nos lançamos, então, ao estudo do *site* de rede social *Facebook*, visando compreender e identificar as dinâmicas referentes à publicação, trânsito e uso de dados individuais que nele ocorrem.

O objetivo principal deste trabalho é investigar em que medida os processos que se passam nos *sites* de rede social podem ser associados ao fenômeno da vigilância. De maneira dinâmica, colocamos também a noção de vigilância sob investigação: se as atividades que se passam nestes *sites* podem ser denominadas vigilantes, de que vigilância essas práticas nos falam? Assim, visamos reunir contribuições que nos permitam propor um escopo teórico e empírico capaz de abarcar e qualificar os processos vigilantes que ocorrem no *Facebook*. Esta meta não poderia ser alcançada se não circunscrevêssemos aqui alguns objetivos específicos, a saber: a) conhecer como se dá e que fatores influenciam a revelação de informações (ACQUISITI e GROSS, 2005), a autocensura dos dados publicados e o uso de configurações de privacidade entre os usuários do *Facebook*; b) investigar em que medida os interatores atribuem riscos aos processos que se passam neste ambiente, identificar que riscos são estes e

⁴ Tradução nossa para: “[...] some form of human activity is analyzed by a computer according to some specified rule”.

como eles são endereçados pelos indivíduos em suas práticas de uso cotidianas; c) investigar as audiências consideradas ou pelo menos conjecturadas pelos usuários do *Facebook* como passíveis de acessarem suas informações através do *site* e buscar compreender em que medida há consciência ou conhecimento das possíveis modalidades de uso destes dados; d) identificar possíveis diferenças de uso do *site* entre canadenses e latinos, no que diz respeito à revelação de informações e ao uso de redes geográficas e universitárias.

Neste momento, se torna importante ressaltar que elegemos como foco desta pesquisa o público latino do *Facebook*, não só pela ausência de estudos que contemplassem essa parcela de usuários como também pelo expressivo crescimento da participação latino-americana no *site* no ano de 2008 (LORICA, 2008). Além disso, por motivos culturais – que não endereçaremos aqui, considerando as dimensões desta pesquisa – e históricos, acreditamos que existam diferenças de uso e de comportamento entre os usuários latinos e os norte-americanos do *site*, já que o *Facebook* surgiu como uma rede orientada a estudantes de instituições de ensino superior na universidade americana de Harvard e só se expandiu posteriormente para as demais regiões do mundo (o que justifica, por exemplo, a adesão em massa e a expressiva quantidade de usuários em países como os EUA e Canadá). Desta forma, a metodologia usada para a realização deste estudo concilia a pesquisa bibliográfica com a análise estatística de 262 questionários aplicados *online* em respondentes exclusivamente latinos e de 23.458 perfis coletados em 11 redes do *Facebook*, 8 latino-americanas e 3 canadenses, geográficas e de universidades. A partir destes dados, apresentaremos apontamentos sobre as posturas relativas à revelação de informações observadas para estes dois tipos de público.

Passemos, então, a uma breve descrição da estrutura deste trabalho.⁵ Em nosso primeiro capítulo, nos lançaremos ao estudo do fenômeno da vigilância, visando situá-lo historicamente e compreender suas relações com a noção de controle e com a existência de mecanismos de orientação da conduta dos indivíduos. Consideraremos inicialmente a analítica foucaultiana das sociedades disciplinares (FOUCAULT, 1977) e a arquitetura de visibilidade do panóptico, bem como suas implicações acerca dos processos de normatização e construção da subjetividade dos indivíduos. Em direção ao estudo das sociedades capitalistas contemporâneas, recuperaremos os argumentos de Gilles Deleuze (1992) acerca das sociedades de controle, bem como as noções de hipercontrole (BOGARD, 1996; 2006) e controle institucional (LIANOS, 2000; 2003). Estudaremos também as relações entre

⁵ Importante considerar também que, em termos estruturais, as decisões conceituais e metodológicas referentes a cada capítulo estão explicitadas na introdução de cada um deles, no decorrer deste trabalho.

vigilância, controle e tecnologia, de modo a situar o papel desempenhado pelos códigos e protocolos na ação e potencialização destes dispositivos (GALLOWAY, 2007; LESSIG, 2006). Por fim, elucidaremos as características da vigilância digital que acontece no ciberespaço: sua estrutura temporal, suas imediações com a esfera do risco, seus mecanismos classificatórios e suas estratégias de captura e formalização do comportamento humano. Esperamos, assim, lançar as bases teóricas com as quais dialogaremos ao longo deste trabalho, visando compreender as características que o fenômeno da vigilância assume no contexto dos *sites* de rede social.

No segundo capítulo nos dedicaremos a estudar os *sites* de rede social, buscando compreender suas características principais e os processos de publicação, trânsito e uso de dados pessoais por eles subsidiados. Inicialmente, situaremos historicamente o surgimento destes *sites* e consideraremos suas relações com a abordagem de análise das redes sociais (KNOKE e YANG, 2008) e com as dinâmicas de colaboração da *web* 2.0. A seguir, endereçaremos os processos de revelação de informações que se passam nessas redes e recuperaremos as contribuições de estudos prévios, que nos dão pistas de que os usuários do *Facebook* revelam grandes quantidades de informações verdadeiras sobre si e tendem a usar pouco as configurações de privacidade disponíveis (ACQUISTI e GROSS, 2006; JONES e SOLTREN, 2005; STUZMAN, 2006; GOVANI e PASHLEY, 2005). Consideraremos também neste capítulo as dinâmicas da exposição de si, fenômeno característico da cultura contemporânea que também se manifesta através da participação em *sites* de rede social. Por fim, voltaremos nossa atenção para o uso dos dados individuais publicados e consideraremos as políticas da publicidade direcionada e a construção de sistemas inteligentes capazes de recomendar anúncios, serviços e produtos a partir da mineração de gostos e interesses em redes sociais. Por fim, apresentaremos a recente discussão sobre a portabilidade de dados, movimento que visa promover a interoperabilidade e o trânsito de dados facilitado entre diversas mídias sociais a partir da adesão de diferentes serviços a padrões técnicos comuns.

O terceiro capítulo, por sua vez, é dedicado a situar o *Facebook* em relação às discussões efetuadas no capítulo anterior. Antes disso, no entanto, apresentaremos a estrutura do *site* e os mecanismos disponíveis aos usuários para a interação com os demais participantes e para a publicação de informações. Através deste processo, buscaremos delimitar as especificidades do *Facebook* em relação a outras redes sociais e explicitar como sua arquitetura de visibilidade particular predispõe a revelação de informações verdadeiras. Consideraremos também neste capítulo as reações dos usuários do serviço à introdução de novas ferramentas, como o *News-Feed*, o *Mini-Feed*, o *Beacon* e o *Social Ads* e focalizaremos

de perto as dinâmicas da publicidade no *site*, bem como os serviços de direcionamento de anúncios oferecidos pela empresa aos seus anunciantes. Igualmente, consideraremos as posturas da companhia em relação à portabilidade de dados e às dinâmicas de trânsito de informações inerentes ao *Facebook Platform* e ao *Facebook Connect*, que permitem aos indivíduos adicionar aplicativos externos ao seu perfil ou levar seus dados para outros *sites*. Por fim, identificaremos a ambição de diversas audiências em torno dos dados individuais publicados no *Facebook*: empresas de busca de pessoas, escritórios de admissão de instituições de ensino superior, futuros empregadores etc. Assim, trata-se de efetuar um levantamento preliminar com o intuito de direcionar nossos esforços na identificação de atividades que possam ser associadas ao fenômeno da vigilância.

Por fim, no quarto e último capítulo, selecionadas as evidências associadas preliminarmente à noção de vigilância, passaremos à apresentação dos resultados da investigação empírica desta pesquisa.⁶ A partir da análise dos questionários respondidos *online*, realizaremos apontamentos sobre a percepção dos latinos acerca das possíveis audiências e possíveis riscos implícitos ao uso do *Facebook*. Apresentaremos também os resultados encontrados para a investigação dos comportamentos relacionados à autocensura, à revelação de informações e ao uso de configurações de privacidade por esta parcela de usuários do *site*. A seguir, com base na análise dos perfis coletados, identificaremos tendências de comportamento dos públicos latino e canadense em relação ao uso de redes geográficas e de universidades e em relação à disponibilização de informações através do *Facebook*. Por fim, retomaremos a discussão sobre as hierarquias da vigilância e sobre como se conjugam as dimensões social e de controle (LIANOS, 2003) nas rotinas de uso dos dados individuais publicados no *site*. Completando nosso percurso, identificaremos, a partir de diversos grupos de audiências, os processos que podem ser associados à noção de vigilância no escopo dos *sites* de rede social. Concluiremos, por fim, apresentando nossa compreensão sobre as características e dimensões deste fenômeno a partir de um questionamento sobre contornos e limites da participação no contexto de interação destes *sites*. E o que podemos assim entrever no interstício em que a revelação prazerosa e voluntária de informações se articula a processos vigilantes são rotinas de integralização cujo modo operativo pretendemos elucidar nas páginas que se seguem.

⁶ Cf. Anexo B, p. 196 e Anexo C, p. 204.

1 A VIGILÂNCIA CONTEMPORÂNEA

Olhar de perto, olhar com atenção, ver e ser visto. Todas essas atividades, tão naturais para os homens e tão atreladas à própria constituição do ato social, possuem sentidos que integram o campo semântico da palavra vigilância. No entanto, tal como empregado no escopo deste trabalho, o termo se refere ao processo através do qual populações são monitoradas e supervisionadas para propostas específicas (LYON e ZUREIK, 1996: 3). As transformações sofridas por este fenômeno ao longo dos anos foram acompanhadas de perto pela evolução das forças capitalistas, pela ação das burocracias estatais e, mais recentemente, pelas novas estratégias de visibilidade decorrentes do surgimento das novas tecnologias de informação e comunicação. Neste percurso de transformações, o ato de ser vigiado adquire novas associações: implica ser governado, regulado, registrado, documentado, classificado, incluído em novos circuitos institucionais.

As práticas do ver e ser visto têm sua história, muitas vezes negada diante das intensas discussões em torno do papel das novas tecnologias na potencialização e na reconfiguração das atividades vigilantes. Podemos reconhecer formas ainda embrionárias de controle social nas práticas que acompanham o nascimento do Estado burocrático entre o fim da Baixa Idade Média e o início da Idade Moderna, quando a emergência de novas formas de vida pública veio acompanhada da necessidade de dispositivos e protocolos documentais – sistematizados enquanto categoria legal – para identificação dos cidadãos, permitindo assim o registro, a codificação e a verificação da identidade pelas instituições modernas, especialmente pelo Estado. Groebner (2001), ao situar as raízes do sistema estatal moderno entre os séculos XIV e XVI, descreve o surgimento de tais mecanismos de descrição, reconhecimento e autenticidade na Europa, em momentos diferentes e com características regionais peculiares, impulsionados em grande parte pela transcrição dos nomes da linguagem oral para a linguagem escrita.

Paralelamente à consolidação da identidade individual, surgem os dispositivos de coleta de dados em massa sobre as populações visando a enumeração dos indivíduos por parte das burocracias estatais. Relacionadas, em um primeiro momento, a finalidades militares e ao recolhimento de impostos, estas iniciativas, juntamente com o censo populacional, são apontadas por Lyon (2004) como formas simples e primordiais de vigilância, cujo principal objetivo não era o controle social, mas sim, o fortalecimento do poder do Estado em relação a outros Estados. De qualquer forma, um aspecto que merece destaque no tratamento da questão é a assertiva de que o processo de burocratização emergente nos Estados modernos é

ambíguo. Assim como a noção de democracia, a burocracia exige tratamento igual para todos, ou mais precisamente, o nivelamento dos cidadãos, a igualdade de todos perante a lei. Neste sentido, a inclusão dos indivíduos nos circuitos estatais do controle administrativo é uma medida democrática, que figura simultaneamente como forma de submissão ao olhar controlador do Estado e forma de aquisição de direitos através da inclusão nos circuitos da cidadania.

No entanto, ainda que em sua gênese a vigilância possa ser localizada como produto da burocracia dos Estados modernos, sua evolução mais recente, que podemos localizar a partir do final do século XX, é marcada por um processo de globalização (LYON, 2004) diante das ameaças generalizadas do crime e do terrorismo, da redução do papel do Estado na manutenção da lei e da ordem e da proliferação de novas tecnologias direcionadas ao monitoramento, registro e tratamento de dados sobre as condutas individuais. A partir dos anos 80, a significativa produção acadêmica na área indicou o nascimento de um novo campo de estudos, centrado na configuração e nas consequências do estabelecimento destes dispositivos em nossa sociedade. As preocupações voltadas à violação da privacidade, por um lado, e à sinergia destas novas práticas com os desígnios do mercado, por outro, têm polemizado o debate, que continua se desenvolvendo junto com questões sobre as dinâmicas de funcionamento dos dispositivos tecnológicos e sobre a reconfiguração do poder e do controle social na contemporaneidade.

As páginas que se seguem representam um esforço para delinear os contornos do fenômeno da vigilância na contemporaneidade, essencialmente aquela que acontece no ciberespaço. Por um lado, nos dedicaremos à identificação de tendências que indicam a emergência de novas formas de controle, diferentes da lógica das sociedades disciplinares descritas por Foucault (1977). Por outro, buscaremos as contribuições que os atributos técnicos dos dispositivos vigilantes podem fornecer para a compreensão de sua lógica operativa, de modo a compreendermos como atuam os mecanismos de registro, coleta, classificação, predição e individualização nas práticas contemporâneas da vigilância. Assim, esperamos localizar o atual estado da arte do debate sobre o tema, de modo a subsidiar, nos próximos capítulos deste trabalho, a nossa reflexão sobre a vigilância nos *sites* de rede social.

1.1 As disciplinas: o olhar como armadilha

Seria impossível – ou no mínimo leviano – contextualizar e compreender o *modus operandi* do controle social e o diagrama dos poderes envolvidos na configuração das

atividades vigilantes sem situar as contribuições de Michel Foucault, especialmente aquelas formalizadas na obra *Vigiar e Punir* (1977). Nela, Foucault descreve o grande passo das tecnologias de regulação da vida em direção ao refinamento, à sofisticação e à elegância analítica do método. Ao situar as sociedades disciplinares predominantemente nos séculos XVIII e XIX (elas emergem entre os séculos XVII e XVIII e vivem seu apogeu na primeira metade do século XX) ele descreve a disciplina como um aparelho normatizador que pode dispensar a propriedade dos corpos, a política do confisco e a violência do suplício para exercer uma coerção mecânica e calculada através de dispositivos tão suspeitos quanto sutis. Assim, Foucault analisa detalhadamente a emergência de uma nova anatomia política, baseada no investimento de poder empreendido sobre o corpo, no esquadramento minucioso do tempo, do espaço, dos movimentos e na ação detalhada e precisa sobre as forças atuantes – e não sobre os resultados dos processos: a disciplina define “como se pode ter domínio sobre o corpo dos outros, não simplesmente para que façam o que se quer, mas para que operem como se quer, com as técnicas, segundo a rapidez e a eficácia que se determina” (FOUCAULT, 1977: 127).

Através deste trabalho, Foucault descreve não somente como as instituições imediatamente coercitivas (como a prisão, o asilo, a justiça etc.) realizam a regulação da vida, mas também a forma através da qual aquelas outras que não possuem propósitos imediatamente ligados ao controle desempenham igualmente esta função (como a escola, o hospital, a fábrica etc.). Ele situa o papel das chamadas “tecnologias de confinamento”, espaços habitados por linhas de segmentaridade duras e regidos pelas regras disciplinares. Na modernidade, essas tecnologias proliferam e sua lógica se propaga por todo o corpo social, marcando a emergência de um novo modelo de Estado, baseado na construção e no uso de táticas e processos de normatização da vida e dos corpos. Assim, o século XVIII inaugura esquemas de docilidade/utilidade que deslocam a escala, o objeto e a modalidade das formas de controle até então existentes. As disciplinas submetem o corpo a uma mecânica do adestramento, trabalham-no através da religiosidade do exercício, ordenam a constituição de seus movimentos, organizam sua eficiência produtiva e esvaziam suas forças políticas. Efetam, enfim, investimentos táticos contínuos que visam “fabricar” indivíduos, extraindo de massas amorfas e inaptas condicionamentos produtivos e úteis.

A individualidade disciplinar depende de uma economia política do espaço, do tempo e das forças. Ela promove a distribuição espacial dos indivíduos, ordenando as multiplicidades e vinculando a ordem à codificação e hierarquização de seus redutos celulares. Trata-se de regular não somente o acesso, mas, sobretudo, as possibilidades de ação

dos indivíduos no interior das instituições: se é possível identificá-los e localizá-los, pode-se também vigiá-los e avaliá-los, individualmente e coletivamente. Assim, quadriculações produzem um ambiente imediatamente apreensível, organizado a partir do posicionamento preciso de unidades distintas e individualizantes, sobre as quais se pode, imediatamente, ao alcance do olhar, obter informações pertinentes à manutenção da obediência. Igualmente, o tempo disciplinar é serializado e graduado: um tempo linear, composto, evolutivo, organizado em fases múltiplas e sucessivas intermediadas por avaliações que permitem o controle e a intervenção sobre as capacidades dos indivíduos. Economia que visa dilatar o tempo útil, coibir os desvios e extrair o máximo de utilidade dos corpos disciplinados. E por fim, em sua organização, a disciplina busca pela composição ótima das forças, pelo arranjo preciso das peças móveis e flexíveis que devem ser articuladas corretamente para que se possa alcançar o máximo de efeito.

E qual seria o papel da vigilância na configuração deste modelo? Para Foucault (1977), o sucesso desta modalidade de poder e a economia de seus pequenos procedimentos só se tornaram possíveis pelo uso de três métodos igualmente simples: o olhar hierárquico, a sanção normalizadora e sua associação à prática do exame (FOUCAULT, 1977: 153). Por um lado, temos os regulamentos e micro-penalidades da disciplina, que permitem qualificar os comportamentos e performances dos indivíduos com base na referência de todos a uma regra comum, classificando-os, diferenciando-os, medindo-os, comparando-os, promovendo a adesão coletiva à homogeneidade da norma, da qual nasce todo um diagrama individualizante das diferenças. Por outro, temos a prática do exame, que subsidia a construção de um saber ao submeter os indivíduos a uma visibilidade programada e obrigatória: eles devem se mostrar ao poder, para que possam ser diferenciados, gratificados ou sancionados. Além de uma política de visibilidade, o exame pressupõe também uma dinâmica constante de acumulação documental sobre os indivíduos: as minúcias de suas doenças, as etapas de seu aprendizado, toda uma codificação de seus comportamentos e desempenhos, enfim, de sua individualidade. A partir dessas formalizações, se torna possível o surgimento de métodos de manejo e a dedução de assertivas provenientes destes registros, apresentadas sob a forma de categorias, médias e normas. Na modernidade, ser observado deixa de ser um privilégio social: enquanto o poder tenta tornar-se invisível, ele objetiva aqueles que visa submeter, investindo agora os indivíduos comuns – e mais ainda, os desviantes (os loucos, as crianças, os doentes, os delinquentes).

Para o funcionamento do aparato disciplinar, portanto, ver se torna algo imprescindível, pois só assim pode-se conhecer, sancionar e normalizar os indivíduos. Não

basta apenas garantir o confinamento: é necessário regular a existência no interior dos espaços a ele destinados através do controle das aberturas e canais que possibilitam observar e ser observado, tornando possível a objetivação cada vez mais eficiente do comportamento individual. Um vigiar intenso e contínuo, baseado em um saber que age através da hierarquização das relações e que é inscrito na materialidade dos espaços e nas regras previstas para sua habitação. De modo geral, podemos afirmar que a vigilância disciplinar é caracterizada basicamente por três princípios: a) o emprego do olhar em uma economia global do exercício do poder; b) a dissociação entre o ver e o ser visto através do estabelecimento de uma geometria calculada, que determina precisamente a rede de olhares e o mapa de visibilidades de um determinado espaço arquitetural; c) uma dissociação entre o centro onipresente e onisciente que tudo registra e a periferia, na qual os indivíduos, distribuídos em lugares fixos, estão constantemente submetidos ao olhar controlador do vigia.⁷

A utopia do controle disciplinar tem seu modelo ideal encarnado pelo panóptico, descrito por Jeremy Bentham⁸ e retomado por Foucault. Trata-se de um modelo generalizado de sujeição: o panóptico formaliza um diagrama de poder através de uma práxis arquitetural e óptica que pode ser aplicada a qualquer situação em que se pretenda gerenciar uma multiplicidade de indivíduos, impondo-lhes uma tarefa ou comportamento. No centro, um vigia e uma torre, com janelas para o interior. Ao redor, celas individuais, incomunicáveis, dotadas de duas janelas: uma para o interior e outra para o exterior, esta última funcionando como fonte de luz que projeta uma sombra através da qual a visão que o vigia tem da cela se completa. Tecnologia material do espaço, mas também tecnologia da luz e do visível. Isolados e dotados de visibilidade lateral, os sujeitos das celas não comunicam entre si e não vêem a torre, o que os torna incapazes de decidir sobre a presença ou a ausência do olhar vigilante. Desta dissociação deriva o efeito principal dos dispositivos panópticos: a internalização do olho do poder e seu funcionamento automático e contínuo. Isto porque o panóptico instaura uma relação de poder que é virtual e constante, pois a dominação subsiste mesmo se não há a atualidade de seu exercício ou de quem a exerce, já que, em última instância, o poder passa a ser exercido pelos próprios vigiados – vigias de si, fonte de sua própria sujeição; eis a sofisticação artificiosa introduzida por este dispositivo.

Alguns argumentos merecem destaque no tratamento da questão: a) o panóptico não deixa de ser uma máquina de prevenção, que visa, pela internalização da norma, dissuadir o

⁷ Importante ressaltar que tais princípios são separados aqui formalmente por uma licença didática; na prática eles não se configuram como instâncias independentes ou autônomas.

⁸ Jeremy Bentham (1748-1832), filósofo, economista, jurista e reformista social nascido em Houndsditch, Londres.

desvio de conduta antes mesmo que ele ocorra; b) o panóptico é também uma máquina de eficiência, pois permite a potencialização do poder disciplinar vigilante ao promover a economia de tempo, material e pessoal (nesta máquina, apenas um vigia é exigido para a observação de um grande número de pessoas); c) o panóptico é um dispositivo silencioso, pois age na direção da sofisticação e da leveza, dispensando a força bruta e a intervenção violenta: tudo se dá através de uma ficção que instaura uma vigilância real; d) o artifício da visibilidade constante da torre associado à indecidibilidade acerca da presença do vigia acaba por desindividualizar o poder, que passa a ser associado não mais a uma pessoa (governante, policial etc.), mas a um mecanismo que, em última instância, pode prescindir da presença atual de um humano, ainda que dela necessite virtualmente; e) por fim, o panóptico aponta para um mecanismo programável de normatização que estaria apto a difundir a vigilância por todo o corpo social através de uma rede de dispositivos que iriam “destrancar” a disciplina tal como concebida nos espaços fechados da era clássica, inaugurando um novo modelo de sociedade (FOUCAULT, 1977: 184).

Se a disciplina é uma tecnologia que instrumentaliza o poder, a vigilância é uma das técnicas à qual, neste ímpeto, ele recorre. Trata-se de uma inspeção habilidosa, que sabe integrar-se à eficácia produtiva dos aparelhos, que sabe responder aos desafios colocados pelo aumento do número de indivíduos a controlar, por um lado, e pelo desenvolvimento dos processos produtivos, por outro. Na passagem das disciplinas fechadas ao mecanismo global e ramificado do panoptismo forma-se uma sociedade baseada por uma nova lógica, por novos mecanismos de construção do saber, novas positivities, novas produções sociais. Elas são de ordem molecular, de natureza cotidiana, e encarnam dinâmicas mais sutis que aquelas presentes nas ações do poder soberano e nas técnicas da apropriação ou do confisco. Trata-se de um poder que não reprime, produz. Trata-se de um poder que não se exhibe, mas que quer tornar-se invisível – não mais sociedade do espetáculo, mas sim de vigilância (FOUCAULT, 1977: 190). Assim, o controle se ramifica não apenas através da proliferação de instituições na sociedade do século XVIII, mas, igualmente, através do processo de disciplinar os aparelhos já existentes.

No início deste capítulo, relembramos o surgimento dos modos de identificação dos indivíduos e citamos os direitos provenientes da esfera legal em que eram progressivamente incluídos pelas burocracias estatais. Aqui, vimos como a modernidade, com suas repartições individualizantes, não quer apenas marcar e identificar, mas, sobretudo, modificar as populações desviantes através do exercício cotidiano dos engenhos mínimos e habilidosos do poder disciplinar – por um lado, trata-se de um poder que determina (diz quem são os

indivíduos, onde devem se situar, como serão controlados etc.); por outro lado, trata-se de um poder que marca, que efetua uma divisão binária (a cisão entre normal e anormal, são e doente, perigoso ou não-perigoso etc.) (FOUCAULT, 1977: 176). A homogeneidade social da norma visa atuar como um fator de coesão social, diante do qual todas as diferenças são marcadas para que, assim, possa-se promover a economia dos gestos e comportamentos. E tudo isso sem recorrer à codificação dura da lei, pois basta aqui a sutileza cotidiana dos micro-poderes da disciplina. A vigilância, como vimos, não é uma invenção do século XVIII. No entanto, sua associação aos mecanismos de poder disciplinares faz com que possamos situar este como um importante momento nas transformações pelas quais passa este fenômeno através dos tempos.

1.2 O controle

Se o controle social não é uma instância fixa e imutável que se exerce de forma invariável através dos tempos, a questão que a contemporaneidade nos coloca é a de compreender como a regulação da vida vem sendo exercida nos dias de hoje. A sofisticação e a perspicácia da analítica foucaultiana é datada, e não pode ser simplesmente transferida para as análises efetuadas no presente. Desta forma, diversos autores têm realizado esforços para repensar os contornos deste fenômeno e identificar pontos de ruptura que nos permitam avançar em sua compreensão. O percurso que apresentaremos a seguir visa recolher nestas argumentações elementos que nos permitam compreender o que há neste ínterim que assinala a passagem das disciplinas às sociedades de controle (DELEUZE, 1992) e à inauguração de um novo controle social (LIANOS, 2001; 2003). Nosso objetivo não é teorizar e definir a natureza deste fenômeno, mas sim obter instrumentos que nos permitam pensar, ao longo deste trabalho, como a vigilância está associada ao controle em seu discurso e prática e em que medida ela se define por esta associação.

Depois da ação das tecnologias de confinamento, cuja lógica e cujo funcionamento são descritos por Michel Foucault (1977), vivemos hoje um tempo de crise das instituições que anuncia o surgimento de novos dispositivos. Gilles Deleuze (1992) descreve assim a emergência das sociedades de controle. Trata-se, sobretudo, de uma mutação do capitalismo, que passa de um modelo de concentração e propriedade, característico do século XIX, para um modelo de dispersão e sobre-produção. Esta passagem aponta para o surgimento de novas máquinas e novos acoplamentos: no lugar da mecânica dos movimentos, das séries regradas e precisas, da divisão funcional do tempo e do espaço, teríamos agora um controle sem escala,

modular, baseado, em grande medida, na imaterialidade das linguagens eletrônicas. Neste processo, originam-se novas construções sociais, responsáveis por sujeições de modalidade cada vez mais “*soft*”, que no lugar da disciplina do método, celebram o prazer das novas liberdades. Elas agenciam o desejo, oferecem as delícias do consumo e as alegrias do *marketing*, fomentam a escolha e capturam sua potência, “dominam”, enfim, sem se denunciarem, deixando como legado a ambigüidade da dúvida: onde acabam a diversão e a utilidade e onde começa controle?

De fato, a imbricação de estados é característica desta nova lógica. No regime das instituições de confinamento, ou dos “internatos”, como nos coloca Deleuze (1992), o indivíduo deve recomeçar sempre, a cada vez em uma nova instituição: elas figuram como variáveis independentes, governadas pelas linguagens analógicas. Já nos “controlatos” as variações são contínuas e governadas pelas linguagens numéricas (não necessariamente binárias). Na prática, isto implica dizer que, nas sociedades disciplinares, os indivíduos estavam submetidos à lógica da “quitação aparente” (DELEUZE, 1992: 222) – eles não cessavam de oscilar entre dois confinamentos, passando de uma instituição a outra e também de uma condição a outra, cada qual demarcada pelo campo de normalidade previsto para o papel social correspondente (o filho, o pai, o estudante, o professor, o trabalhador, e assim por diante). Já nas sociedades de controle, passamos à era da “moratória ilimitada”: a sensação aqui é a de nunca terminar nada (DELEUZE, 1992: 222), pois os limites entre as condições se tornam fluidos: onde acaba o tempo de trabalho e começa o tempo de lazer?; qual a diferença entre espaços como a escola e a casa?; e assim por diante. Adentramos a era da formação permanente, do salário por mérito, das metaestabilidades. Enfim, uma era regida por constantes modulações.

Os confinamentos são moldes, distintas moldagens, mas os controles são uma modulação, como uma moldagem auto-deformante que mudasse continuamente, a cada instante, ou como uma peneira cujas malhas mudassem de um ponto a outro (DELEUZE, 1992: 221).

Outro aspecto das sociedades de controle descrito por Deleuze (1992) diz respeito à identificação e manejo dos indivíduos pelos dispositivos do poder. Como vimos, o poder disciplinar visava individualizar e promover em cada um a internalização do controle através da referência ao corpo social homogêneo da norma. Neste contexto, o indivíduo precisava ser situado: sua assinatura indicava sua singularidade, enquanto seu número de matrícula indicava sua posição na massa. Já no que tange à emergência das sociedades de controle, Deleuze aponta para uma reconfiguração do par massa-indivíduo e para a escolha das cifras – ou

senhas – como o novo modo disponível para atestar e regular tanto o acesso aos circuitos informacionais (que também são econômicos, sociais etc.) quanto as modalidades possíveis de uso destes dispositivos. As senhas se tornam instâncias fundamentais em um contexto no qual os indivíduos e as massas são transformados em *bits*, inscritos em bancos de dados e manejados segundo aspectos específicos de sua individualidade a partir de comandos específicos expressos por trechos de códigos.

A linguagem numérica do controle é feita de cifras, que marcam o acesso à informação, ou a rejeição. [...] Os indivíduos se tornaram “dividuais”, divisíveis, e as massas tornam-se amostras, dados, mercados ou “*bancos*” (DELEUZE, 1992: 222).

Se as sociedades de controle operam em grande medida pela imbricação de limites e fronteiras, situar as diferenças entre sua lógica operativa e aquela própria às sociedades disciplinares exige cautela. É possível demarcar tendências – que se confundem e se misturam – e não situar um processo de sucessão simplificado, em que um modelo seria completamente e puramente substituído pelo outro. De fato, esta perspectiva pode ser deduzida da própria maneira através da qual as concepções foucaultianas e deleuzianas se dirigem aos processos sociais. Para Foucault, o poder pode ser concebido como uma “multiplicidade de correlações de força imanentes ao domínio onde se exercem e constitutivas de sua organização” (FOUCAULT, 1988: 88). Para Deleuze (1995), seríamos obrigados a considerar a ação constante de processos complementares de estratificação e desestratificação, povoados por duplas articulações que se dão tanto no nível do conteúdo quanto no da expressão. Assim, as singularidades, fluxos e intensidades aprisionadas levam à organização e formalização de estados, através de processos de codificação e decodificação, desterritorialização e territorialização que se alimentam mutuamente e continuamente. Estes modelos nos sugerem o cuidado redobrado na análise de como o controle hoje transforma, recria e se relaciona com as antigas estratégias da disciplina, voltando nossa atenção para as rupturas que caracterizam essa transição.

Grosso modo, a primeira grande diferença entre as sociedades disciplinares e as de controle está na ultrapassagem dos limites físicos dos quais dependiam as tecnologias de confinamento. Hoje, o controle deixa de ser exercido prioritariamente através da supressão dos nomadismos e da restrição à liberdade dos movimentos. Ao contrário, vivemos em uma sociedade que subsidiou, através da tecnologia, a superação da dicotomia dentro-fora e a porosidade de suas fronteiras, devido em grande parte ao regime de digitalização e virtualização dos corpos. No entanto, não podemos presumir a partir desta diferença que as

sociedades de controle estão em vias de extinguir os seus meios de confinamento – basta pensar em dispositivos como uma tornezeleira eletrônica para presos em regime condicional, por exemplo. Igualmente, seria de uma simplicidade leviana ignorar que a lógica panóptica já alimentava a ambição de “destrancar” as disciplinas em busca de uma dominação global, generalizando o controle para além dos espaços institucionais disciplinares. Este processo se dava através do estabelecimento de conexões entre as instituições ou da ação da polícia, encarregada do controle nos espaços “através”, fora dos limites dos confinamentos (FOUCAULT, 1977: 184-91).

Uma diferença fundamental advinda desta pulverização dos mecanismos de controle diz respeito à normatividade do controle social. Se o panoptismo quer “destrancar” as disciplinas, ele o faz essencialmente através de sua interiorização: libertar sua ação da dependência dos espaços de confinamento e colocá-la “dentro” dos indivíduos, para que a carreguem, assim, por toda parte. Ao contrário, a lógica vigente nas sociedades de controle não se alicerça mais sobre a interiorização do ideal da norma. Como vem sendo apontado por vários autores (HARDT e NEGRI, 2000; BOGARD, 2006), a polaridade binária normal-anormal cede espaço à multiplicação dos canais de afecção por parte das estratégias de poder, visando fomentar a adoção de identidades múltiplas (estilos, hibridismos tecnológicos, e assim por diante). Trata-se, portanto, de um controle que decodifica e recodifica a subjetividade para atuar não na supressão das diferenças, mas no gerenciamento das micro-identidades produzidas (HARDT e NEGRI, 2000: 180). Um controle que, no lugar do cálculo dos movimentos e da submissão dos corpos, elege como canais de atuação as formas de produção do conhecimento – a comunicação, a publicidade, o *marketing* e toda a rede de imaterialidades do capitalismo cognitivo.

Já para Lianos (2001; 2003), o controle social opera no sentido contrário à submissão, promovendo uma “de-sujeição” do indivíduo, que passa a ser abordado enquanto usuário de sistemas que consideram aspectos setorizados de sua existência (LIANOS, 2003: 12). Para o autor, na sociedade pós-industrial, a regulação das ações e atitudes não está mais ancorada na formação de uma consciência social orientada, como a da norma, mas se exerce através das dinâmicas procedimentais que devem ser percorridas por indivíduos autônomos em seu cotidiano institucional. Diferentemente do contexto moderno, o termo instituição denota aqui “[...] qualquer fonte de atividade mediada entre seres humanos” (LIANOS, 2003: 413, tradução nossa).⁹ Privadas ou públicas, elas se caracterizam pelo fato de que se interpõem

⁹ Tradução nossa para: “[...] any source of mediating activity between human beings”.

como fonte externa à negociação cultural envolvida – neste sentido, um *site*, uma loja ou um banco, por exemplo, são fontes institucionais, através das quais se dá um gerenciamento consciente e programado da atividade humana. Ao contrário do que ocorria no contexto moderno, o envolvimento dos indivíduos com estas instituições é planejado e desejado. Assim, o controle não é mais fruto de uma consciência internalizada, mas se dá através dos procedimentos e condições que moldam a interação de indivíduos soberanos com as instituições às quais escolheram ativamente se vincular para a obtenção de algum benefício, abstrato ou imediato.

Duas conseqüências importantes para a perspectiva deste trabalho decorrem desta nova condição. A primeira delas é a de que o controle social está deixando de se configurar como poder exclusivamente exercido por burocracias estatais bem equipadas para se pulverizar por uma série de instituições com as quais nos envolvemos cotidianamente e que passam a verificar aspectos cada vez mais setorizados de nosso comportamento (LIANOS, 2003: 414). E ainda mais importante: essas instituições não possuem como finalidade expressa ou imediata o controle ou a vigilância dos indivíduos. Assim, as rotinas da coleta e do tratamento de dados, por exemplo, são apenas efeitos acessórios inerentes ao funcionamento de redes institucionais eficientes, que nos fornecem serviços que nós mesmos julgamos cada vez mais indispensáveis. Desta forma, assim como não cabe pensar sistemas de poder unidirecionais e totalitários, que equacionem o controle social em termos de opressão ou repressão, trata-se de reconhecer aqui a presença de um novo controle, consensual, não intencional e não coercitivo (LIANOS, 2001: 17),¹⁰ que se dá na articulação com a autonomia individual e não à luz de uma retórica de cooptação das liberdades.

Isso não implica que o controle seja, em si, neutro, em termos de sua produção ou recepção, mas que não exista razão para acreditar em uma correspondência direta e uma simetria entre esses dois estágios. Isso é,

¹⁰ Lianos (2001; 2003) usa a expressão não-intencionalidade para se referir a uma condição na qual a produção de efeitos de controle não depende ou está previamente alicerçada no desejo de controlar, uma vez que aqui não se parte do projeto de estruturar as premissas do comportamento dos indivíduos, mas apenas de garantir, freqüentemente através do emprego de dispositivos tecnológicos, que as atitudes por eles tomadas se mantenham no campo do que é adequado e eficiente segundo os objetivos institucionais. Assim, à medida que somos abordados enquanto usuários de sistemas com os quais interagimos visando concretizar nossas escolhas e projetos, acabamos por nos envolver nas teias institucionais que gerenciam nosso comportamento através de nosso consentimento com os parâmetros de interação que nos são propostos. Como exemplifica Lianos (2001: 17), diante de um pedágio em uma rodovia, simplesmente pagamos e continuamos nosso caminho. O mesmo acontece com os sistemas de etiquetas magnéticas usados para evitar o roubo em grandes lojas. Eles não visam interiorizar nos consumidores juízos de valor capazes de dissuadir o roubo, mas simplesmente evitar que este comportamento e os prejuízos dele decorrentes prejudiquem os objetivos institucionais. Para tal, o sistema se vale apenas da simples detecção de que uma peça não paga está deixando os limites do ambiente protegido (LIANOS, 2003: 423). Conseqüentemente, se a assimilação de algum valor se dá através da interação com este sistema, trata-se de uma conseqüência do processo de gerenciamento institucional, e não de sua base operativa.

conseqüentemente, necessário ao reconhecimento da existência de tipos de atividade nas quais o controle surge de muitas maneiras que freqüentemente não foram concebidas visando a produção de efeitos de controle (LIANOS, 2003: 416, tradução nossa).¹¹

O outro ponto fundamental desta argumentação reside na relação do controle com a tecnologia. Lianos (2003) apresenta a idéia de que a mediação introduzida pelos dispositivos tecnológicos nos meios institucionais promove e apela para compatibilidade do comportamento dos indivíduos com aquele previsto para os ambientes sócio-técnicos previamente programados, propagando assim seus efeitos de normalidade não pelo apelo a uma consciência abstrata que fixe os limites do que é socialmente aceitável, mas sim através do consentimento às regras subjacentes ao funcionamento destes sistemas. Neste processo, os mesmos procedimentos e efeitos são estendidos igualmente a todos os que se submetem a uma dada rotina institucional tecnologizada. Desta forma, assim como no ciberespaço o uso não pode ser dissociado do registro, o uso de um sistema sócio-técnico não pode ser dissociado de seus efeitos normativos, embutidos nos aspectos técnicos de seu funcionamento. Neste cenário, a lógica moderna de se tratar os desviantes cede espaço a um contexto no qual o desvio nada mais é que um desafio organizacional – uma disfunção ou inadequação como qualquer outra do cotidiano institucional – que deve ser corrigida através da própria operação do sistema, e não com base na internalização de valores ou crenças nos indivíduos em questão (LIANOS, 2003: 423). Neste sentido, o autor sugere que:

[...] não é o controle que se torna dessocializado, mas a sociabilidade que se institucionaliza; não é a vigilância que se intensifica e se prolifera, mas a demanda por sistemas e redes que se propaga e favorece o fluir – ainda que atomizado – dos indivíduos (LIANOS, 2003: 425, tradução nossa).¹²

Assim, as reflexões do autor trazem o alerta de que a institucionalização da sociabilidade, por um lado, e a tecnologização crescente da mediação institucional, por outro, estariam gerando um decréscimo da necessidade de negociação social, o que tenderia a gerar também um decréscimo da motivação dos indivíduos para se apresentarem como sinceros, críveis ou insuspeitos. Nas rotinas do monitoramento generalizado e automatizado, a lógica é obedecer ao funcionamento do sistema e resolver setorialmente a condição vivenciada, e não

¹¹ Tradução nossa para: “This does not imply that control itself is ‘neutral’, in terms of its production or its reception, but that there is no longer any reason to believe in direct correspondence and symmetry between these two stages. It is, consequently, necessary to recognise the existence of types of activity where control arises in many ways that were often not intended to produce a controlling effect”.

¹² Tradução nossa para: “[...] it is not control that becomes desocialised, but sociality which institutionalises itself; it is not surveillance which intensifies and spreads, but the demand for systems and networks which propagates itself and favours the fluid – albeit atomised – channelling of individuals”.

negociar a condição imposta ou os valores a ela subjacentes, como era possível fazer diante de um vigia ou censor qualquer – mesmo porque se trata de um sistema e não de um humano (LIANOS, 2003: 420). A racionalidade embutida nesses dispositivos – compreendida pelos usuários do sistema como práxis necessária ao acesso a bens e serviços por eles visados, desejados e pretendidos – achata a complexidade das situações vivenciadas em um menu de opções restritas, só restando ao usuário desempenhar o seu papel e atender às regras pré-estabelecidas (LIANOS, 2003: 12).

Por fim, no que tange ao regime de atuação no tempo e à materialidade de suas ações, a disciplina visava esquadriñar o tempo, serializar etapas, intervir nos corpos e processos através de uma organização probabilística que favorecesse a busca pela performance ótima, *i.e.*, mais eficiente. Neste contexto, a observação dos indivíduos visava à intervenção sobre uma realidade material imediata (basta lembrarmos das práticas da sanção normalizadora e do exame nas sociedades disciplinares). Segundo Bogard (2006), neste aspecto, a tônica da mudança que caracteriza as formas de controle contemporâneas está na imaterialidade e na virtualidade de suas formas de intervenção – não se trata mais de “remediar” o real, mas de nele intervir por antecipação, a partir da projeção de um futuro provável. Aqui, a observação dos comportamentos não é mais deduzida das localizações celulares e das posições ocupadas pelos indivíduos nas séries disciplinares: neste novo contexto, se as formulações numéricas e comparações subsidiadas pelos cálculos estatísticos permanecem, o foco de sua incidência é modificado radicalmente.

A natureza do controle, no entanto, está mudando. O controle não é mais mera questão de probabilidade ou eficiência. O controle estatístico, sem dúvidas, ainda está muito presente entre nós. Mas ele não é mais direcionado ao problema do possível e do real. Quem se importa com o que é possível, ou com os meios eficientes que existem para realizá-lo, quando se pode comandar o virtual? (BOGARD, 2006: 60, tradução nossa).¹³

Com esta proposição, a velha premissa de patrulhar territórios e controlar o movimento das massas é direcionada ao patrulhamento dos regimes do possível. A lógica recorrente do controle é a da predição e nela, observar e conhecer adquirem sentido na medida em que permitem a construção de modelos matemáticos capazes de classificar os indivíduos com a finalidade de subsidiar operações antecipatórias: impedir o crime antes que ele ocorra,

¹³ Tradução nossa para: “The nature of control, however, is changing. Control is no longer merely a question of probability or efficiency. Statistical control, no doubt, is still very much with us. But it is no longer mired in the problem of the possible and the real. Who cares what is possible, or what efficient means exist to realize it, when one commands the virtual?”.

identificar as doenças antes que elas apareçam, identificar o produto certo antes de realizar a oferta, e assim por diante. Bogard (1996) denomina esta situação de hipercontrole, característica das sociedades telemáticas, marcada pela atuação no regime do tempo. Na argumentação do autor, esta assertiva levaria à idéia de que o controle, em última instância, deixaria de existir e se transformaria em um imenso aparelho de gerenciamento de possibilidades – não haveria mais crimes a se punir ou desviantes para se curar, pois tudo seria engenhosamente previsto e remediado antes mesmo de acontecer. Em suma, o autor propunha que o regime da simulação é marcado pelo controle absoluto sobre as modalidades de produção de realidade, o que originaria uma condição mais controladora que o controle: o hipercontrole, engendrado e dissolvidos em práxis operacionais cotidianas e transparentes (BOGARD, 2006: 70). No entanto, revisitando mais recentemente este conceito, Bogard (2006: 71) reafirma a lógica operativa subjacente a estas práticas, mas reconsidera a possibilidade de uma desmaterialização do controle. Desta vez, o autor prefere ressaltar que a análise do controle social na contemporaneidade não deve ser concebida como um processo unidirecional de abandono da lógica disciplinar, mas considerar “[...] da maneira mais detalhada possível os mecanismos concretos de estratificação e desestratificação em ação, e como eles transformam as práticas tradicionais do confinamento institucional” (BOGARD, 2006: 76, tradução nossa).¹⁴

1.3 A vigilância digital

De modo geral, a vigilância digital pode ser definida como “[...] o processo através do qual alguma forma de atividade humana é analisada por um computador de acordo com alguma regra específica” (LESSIG, 2006: 209, tradução nossa).¹⁵ Ela diz respeito a formas de monitorar e classificar as ações ou comunicações dos indivíduos com finalidades diversas: seja para o direcionamento de anúncios publicitários, para a personalização de ofertas de produtos, para a customização do conteúdo de *sites* ou para o que mais sugerirem a retórica da informação relevante e da maximização da eficiência. Trata-se, portanto, de um dispositivo silencioso e pouco visível: na maior parte das vezes, não sabemos quando ou como nossas informações pessoais estão sendo coletadas e muito menos com que finalidades serão usadas em um futuro mais ou menos próximo. No entanto, o que se pode afirmar com certeza é que a

¹⁴ Tradução nossa para: “[...] in as detailed a way as possible the concrete mechanisms of stratification and desestratification at work, and how they transform the traditional practices of institucional confinement”.

¹⁵ Tradução nossa para: “[...] the process by which some form of human activity is analyzed by a computer according to some specified rule”.

coleta de dados pessoais é uma atividade rotineira no ciberespaço. Enquanto você usa a Internet para se comunicar com seus amigos; para comprar livros, passagens ou qualquer outro tipo de produto; para simplesmente mandar um *e-mail* ou realizar uma busca sobre um assunto qualquer, suas conexões momentâneas e preferências manifestas estão sendo submetidas às rotinas do cálculo e do registro.

Para verificar este fato, basta “seguir a inteligência”. Frequentemente, aqueles dispositivos que se propõem a fazer algo por você, a automatizar e otimizar tarefas, em algum momento, foram nutridos com dados sobre seu comportamento *online*: a sua livreria virtual que lhe indica constantemente novos produtos, o *banner* no topo do seu *webmail* que apresenta anúncios relacionados ao conteúdo das suas mensagens, o seu *site* de rede social que apresenta possíveis novos amigos e comunidades de seu interesse. Estes acontecimentos só se tornaram possíveis porque você forneceu a estes sistemas – direta ou indiretamente – informações sobre suas preferências, sobre seus gostos e interesses, sobre sua rede de relacionamentos, além de outras menos prováveis como o número do seu cartão de crédito, o destino para o qual você pretende viajar nas próximas férias, o número que você calça ou veste, e assim por diante. A rotina do registro é um labirinto: não escapamos dela uma vez que estamos na rede. O seu navegador guarda *cookies*; o seu provedor de acesso pode guardar informações sobre seus padrões de uso da rede; o seu buscador pode registrar e usar suas *queries* de busca, e assim sucessivamente. E neste processo, o labirinto em que se enreda o internauta comum é convertido, através do emprego de meios técnicos de armazenamento e tratamento da informação, em um verdadeiro “mapa do tesouro” para as empresas que passam a usufruir destes dados: nascem assim sistemas extremamente eficientes que permitem a organização destas massas de informação, tornando-as utilizáveis, apreensíveis aos sentidos humanos e passíveis de geração de valor.

A vigilância contemporânea possui pontos de continuidade e ruptura com aqueles processos próprios à modernidade disciplinar, representados pelo imperativo do controle totalitário e autoritário, pelas metáforas do Estado controlador e do *Big Brother*. A nosso ver, o principal ponto de ruptura com esta antiga ordem está no engendramento de estratégias de poder essencialmente “liberadoras”, que agem através da captura e da capitalização da autonomia dos indivíduos. Assim, a vigilância que ocorre no ciberespaço se exerce menos através do olhar do que através de mecanismos de coleta, registro e classificação dos indivíduos; ela não mais objetiva o corpo, mas sim rastros informacionais despersonalizados; ela não visa mais remediar ou curar os desviantes, mas sim, projetar antevisões e instaurar realidades possíveis (BRUNO, 2006). Aqui, a dissociação entre o ver e o ser visto,

característica dos regimes panópticos, é substituída por uma outra, marcada pela retórica da visibilidade e exposição máximas (equacionadas através do fomento constante à colaboração) e da transparência mínima, segundo a qual a privacidade que é constantemente violada pelas práticas de monitoramento também é usada para justificar a propriedade privada dos bancos dados acumulados e para negar a transparência necessária nas políticas de registro e uso dessas informações (ANDREJEVIC, 2007: 7-8).

Assim, as reflexões apresentadas a seguir são uma tentativa de compreender como operam os dispositivos de vigilância no ciberespaço. Em um primeiro momento, concentraremos nossos esforços em avaliar as conseqüências da influência tecnológica sobre a reconfiguração das atividades vigilantes. Em um segundo momento, passaremos à análise do modo de operação desses novos dispositivos e das formas de controle e exercício do poder implícitas a seus processos de classificação, predição e individualização. Neste percurso, a utopia da comunicação libertária e descentralizada cede espaço para uma realidade bem menos revolucionária, mas nem por isso, menos divertida ou menos sedutora. Assim, a vigilância emerge enquanto um fenômeno marcado por regiões de ambigüidades e hibridismos que articulam perigos e prazeres em potencial, como é próprio das estratégias de controle contemporâneas.

1.3.1 Vigilância e tecnologia: uma condição de reversibilidade

A technological system is by definition a system of control of a certain environment. When this environment has a direct link with socialised human behaviour, the social universe is faced with new constraints.
 Michalis Lianos¹⁶

Não existe novidade alguma em reafirmar que as mudanças mais profundas pelas quais passamos nas últimas décadas estão intimamente relacionadas com o fenômeno da tecnologia e com as formas através das quais ela influencia os processos econômicos, políticos e sociais. Da revolução digital, possibilitada pela popularização das interfaces gráficas, passando pela disseminação dos computadores pessoais e finalmente pelo estabelecimento da rede mundial de computadores, diversas transformações reconfiguraram nossa cultura, a maneira como nos relacionamos com os outros e com o mundo ao nosso

¹⁶ LIANOS, Michalis. Social Control after Foucault. **Surveillance & Society**, v. 1, n. 3, 2003, p. 418.

Tradução nossa: “Um sistema tecnológico é por definição um sistema de controle de um certo ambiente. Quando esse ambiente tem uma ligação direta com o comportamento humano socializado, o universo social se depara com novos constrangimentos”.

redor. Este processo pode ser descrito como uma rede de acontecimentos que se alimentam: novos protocolos e novas evoluções técnicas engendram novos comportamentos e modos de ação que, por sua vez, realimentam o circuito, fomentando novas necessidades tecnologicamente orientadas. E não acreditamos que alguma força – interna ou externa – seja capaz de paralisar ou reverter este ciclo. Nós somos, enfim, seres por demais tecnologizados: não apenas porque usamos estes dispositivos ou porque dependemos deles, mas, sobretudo, porque acreditamos neles. E é justo esta crença na neutralidade dos processos tecnológicos e dos dispositivos vigilantes que abre o espaço para o exercício de novas formas de controle.

Uma vez que a vigilância no ciberespaço opera com base na coleta, uso, tratamento e troca de informações em padrão digital, não é difícil elencar motivos para argumentar o quanto esta linguagem potencializou características necessárias ao funcionamento e à eficácia dos dispositivos vigilantes. Dentre elas, podemos citar a facilidade da produção e a exatidão da reprodução de conteúdos, o armazenamento permanente e ampliado a limites praticamente infinitos e, sobretudo, a emergência de possibilidades inéditas para a recuperação e o tratamento da informação inserida nessas redes. Através desta nova linguagem, tarefas humanamente impossíveis – como localizar algo na imensa massa de dados que constitui a Internet ou deduzir assertivas de bancos dados cuja quantidade informacional tende ao infinito – se tornaram não só possíveis como rotineiras. Além disso, agora, o dispositivo vigilante não é mais independente e exterior aos fluxos monitorados: se na sociedade disciplinar, as acumulações documentais que arquivavam dados sobre as performances e competências dos indivíduos nas diversas instituições pelas quais passavam consistiam de arquivos produzidos paralelamente aos diversos sistemas de avaliação aos quais eram submetidos, hoje, o dispositivo vigilante e o aparato comunicacional não podem mais ser dissociados (BRUNO, 2006).

Segundo Marx (2002), as características da informação nos ambiente digitais nos ajudam a apontar uma série de tendências para a distinção entre as táticas disciplinares e a vigilância contemporânea. Dentre elas, podemos listar a inauguração de um estado de mobilização ampla dos sentidos, e não apenas do olhar; a ausência da exposição voluntária implícita na lógica do exame e a emergência de uma vigilância silenciosa, desconhecida e ignorada, em grande parte, pelos indivíduos a ela submetidos; a operação remota e não presencial de seus dispositivos e o acesso em tempo real aos dados coletados de maneira contínua; a inexpressividade do custo associado ao armazenamento das unidades de informação; a introdução das rotinas da simulação para além da representação dos indivíduos etc. Definitivamente, as mesmas tecnologias que adquirem cada vez mais importância em

nosso cotidiano são as mesmas que estão atuando na quebra das barreiras naturais (como a limitação dos sentidos humanos) e artificiais (como muros, lacres e paredes) que antes protegiam a informação pessoal.

Para esclarecer melhor estas nuances, consideremos a diferenciação proposta por Lessig (2006) entre a privacidade nos espaços privados e nos espaços públicos. Segundo o autor, a privacidade nos espaços privados, de natureza legal, pode ser associada ao direito de ser deixado só. Ela é complementada por barreiras físicas que delimitam a propriedade privada (ninguém entrará em sua casa para espionar documentos seus). Por outro lado, nos espaços públicos, nada impede que o seu comportamento seja observado. O que até bem pouco tempo atrás garantia a privacidade nestes espaços era simplesmente a impossibilidade técnica de construir sistemas capazes de produzir registros, organizar e tratar essa imensa de massa de informações de maneira rápida e eficiente. Assim, no que tange à vigilância nos espaços públicos, o autor diferencia monitoramento e busca. Segundo ele, somos monitorados enquanto andamos na rua, por exemplo – podemos ser notados ou não; mas, sobretudo, podemos ser (e freqüentemente somos) esquecidos logo em seguida, pois o único registro proveniente desta ação é aquele que fica na mente das pessoas que cruzam meu caminho. Por outro lado, o que pode ser buscado é aquela parte das nossas vidas que está gravada, como ocorre facilmente com nossas ações no ciberespaço. Esses dados podem ser re-acessados, tratados, e assim por diante (LESSIG, 2006: 202).

Assim, podemos deduzir das assertivas de Lessig (2006) que as linguagens eletrônicas subsidiam duas diferenças fundamentais no estabelecimento das práticas contemporâneas da vigilância. Antes, as informações monitoradas, ainda que existissem em algum lugar (mesmo que este lugar fosse a mente de uma pessoa) não podiam ser extraídas com facilidade, sem muito esforço e principalmente, sem custos. Hoje, na Internet, temos um mundo imediatamente palpável, tangível, manipulável, reconhecível, formado por arquivos, textos, linhas de códigos e pacotes trafegando segundo protocolos conhecidos. Como veremos a seguir, formatar tecnologias para o reconhecimento e o tratamento de dados neste ambiente não é uma tarefa difícil. Além disso, na rede, o monitoramento pode ser realizado de maneira invisível, sem incômodo algum aos usuários. Teoricamente, é como se um homem invisível pudesse adentrar sua casa sem que você sequer o notasse; ou então, que você soubesse que iria receber esta visita, mas não se importasse, já que, efetivamente, é impossível saber quando, como ou mesmo se efetivamente esta visita se concretizou. Trata-se de uma invisibilidade tecnologicamente subsidiada, freqüentemente usada para argumentar que, em última instância, não há invasão de privacidade: que perigo haveria no fato de máquinas lerem

meus *e-mails* ou monitorarem meus dados pessoais? Afinal, elas não são inteligentes, não possuem opiniões ou sentimentos. Desta forma, como nos coloca Bruno (2008), as medidas tomadas em prol da defesa privacidade, freqüentemente, permitem que, ainda assim, ela seja violada. Trata-se de uma retórica cruel, que nos estimula a acreditar em uma segurança ilusória, cujos possíveis danos seriam insignificantes perto dos benefícios envolvidos no uso dos serviços gratuitamente oferecidos. Em certa medida, há uma incitação à idéia de que, ainda que o olhar vigilante seja impreciso, sutil e indecível, ele não é o censor que pretende lhe punir e normalizar, mas uma ferramenta que promete lhe ajudar no desempenho de tarefas cotidianas e sociais sem deixar, em momento algum, de respeitar suas vontades e os limites de sua privacidade.

A emergência das comunicações em rede reconfigura também o papel desempenhado pela informação no seio do sistema capitalista. Como pontua Poster (1990), a digitalização dissociou textos, imagens e vídeos não apenas das coerções espaço-temporais a que outrora estiveram submetidos, mas, também, do custo material de sua reprodução analógica. A imaterialidade veio acompanhada de uma lógica marcada pelo excesso, e trouxe consigo um novo problema no que tange à geração do valor. Se o sistema capitalista depende da escassez para gerar valor, na rede, instaura-se um paradoxo: o valor depende da livre circulação, o que se opõe radicalmente à noção de propriedade. Pontuamos apenas que, neste contexto, deter a propriedade da informação se torna cada vez mais difícil para o sistema capitalista. E para os internautas, da mesma maneira, manter a propriedade sobre suas informações pessoais vem se tornando algo cada vez mais impossível. No entanto, o que nos parece é que dados pessoais têm se afirmado como a contrapartida da gratuidade: uma espécie de cobrança simbólica, paga com informações sobre quem você é, do que você gosta, o que você pensa e consome, está invisivelmente embutida como condição de uso aos inúmeros sítios e serviços de acesso gratuito que são oferecidos aos internautas. Através deste processo, a chamada economia da informação vem privatizando informações pessoais em uma escala inédita (ANDREJEVIC, 2007), e assim o capitalismo parece estar encontrando uma nova forma de exercer controle sobre a linguagem, depois do abalo sofrido com o fim de sua fase industrial.

O que parece é que na era da sociedade industrial a relação do capitalismo com a linguagem exigia uma certa combinação complexa através da qual a linguagem só poderia ser reproduzida se ela fosse transformada em pesadas, inertes formas de matéria que o capitalismo era especialmente projetado para controlar. Uma vez que este arranjo foi desmantelado pelos dispositivos de comunicação eletrônica, o capitalismo perdeu sua habilidade de controlar a linguagem e isto aconteceu ao mesmo tempo em que ele se tornou dependente da linguagem no processo de produção (ciência),

consumo (anúncios publicitários) e controle (pesquisas de *marketing*, teoria dos sistemas, cibernética, teoria dos jogos etc.) (POSTER, 1990: 74-5, tradução nossa).¹⁷

As brigas pelo controle da informação que caracterizam tanto as lutas pelo direito à propriedade intelectual por parte dos capitalistas quanto os protestos acerca do direito à privacidade por parte dos internautas identificam o ciberespaço a uma grande guerra informacional. Esta questão vem sendo freqüentemente equacionada em termos do direito à interatividade, capaz de conferir às redes informáticas, à primeira vista, um potencial eminentemente democrático, a partir do qual todo receptor seria também um emissor em potencial. O termo interatividade se refere, de modo geral, à capacidade de aproveitamento do *feedback* do receptor pela fonte emissora em tempo real. No entanto, seu significado se pulverizou e banalizou a tal ponto que alguns autores dizem preferir inclusive evitá-lo (MANOVICH, 2001: 55). O que nos interessa aqui é notar como o discurso sobre a noção de interatividade traz implícita uma discussão sobre a questão do controle nas redes informacionais. Ainda que cibernética possa ser acusada de comparar o comportamento humano ao de máquinas como aquecedores e termostatos, como ressalta Andrejevic (2007: 18-21), Norbert Wiener já antevia, nos processos de captura contínua e uso da informação para a produção de respostas a fenômenos e condições dinâmicas, conseqüências futuras decorrentes da concentração de poder gerada pela possibilidade de controle destes processos. Além disso, de maneira semelhante, ainda que a teoria matemática da informação, de Shanon e Weaver, apresente uma visão unilateral e linear do processo comunicativo, na qual o *feedback* seria usado apenas para comprovar o recebimento adequado da mensagem pelo receptor, ela dialoga com muitas das atuais críticas à celebração do potencial interativo das redes, que vêm alicerçadas na idéia de que a agência¹⁸ dos interatores nestes ambientes é limitada e muitas vezes, se resume a uma condição reativa,¹⁹ que os condena a percorrer a

¹⁷ Tradução nossa para: “It appears that during the epoch of industrial society the relationship of capitalism to language required a certain complex combination by which language could only be reproduced if it was transformed into heavy, inert shapes of matter that capitalism was preeminently designed to control. Once this arrangement was broken by electronically mediated communication devices, capitalism lost its ability to control language and it did so at the same moment that it became dependent upon language in the process of production (science), consumption (advertising) and control (market research, systems theory, cybernetics, game theory etc.)”.

¹⁸ Para a autora, o conceito de agência, ao lado das noções de imersão e transformação, se colocam como os responsáveis pela implicação física e psicológica dos interatores em um ambiente digital. A agência diz respeito à estrutura de gratificação advinda da visualização imediata por parte dos participantes das conseqüências de seus atos e ações. Cf. MURRAY, 2003: 127.

¹⁹ Primo divide os sistemas interativos entre “reativos” e de “interação mútua”, estes últimos caracterizados por “verdadeiras trocas, em que todos os agentes possam experimentar uma evolução de si na relação e da relação propriamente dita” (PRIMO, 2000: 7).

roteirização fechada de parâmetros pré-programados em busca de caminhos determinados a priori.

As consequências políticas do controle interativo residem no fato de que, hoje, freqüentemente, as dinâmicas da colaboração, vendidas como eminentemente revolucionárias e participativas, são o substrato de formas cada vez mais sutis e sofisticadas de vigilância. Andrejevic (2007: 2) usa o termo “*digital enclosure*” para se referir a um espaço interativo no qual toda e qualquer ação é, inexoravelmente, matéria de registro ou monitoramento imediato, como se passa com a Internet. Podemos considerá-los como espaços em que as transações estão condenadas a uma espécie de metalinguagem, a gerar constantemente informações sobre si próprias. O componente mais interessante da argumentação do autor é a associação do termo *enclosure* com o processo de transição do regime feudalista ao regime capitalista, contexto no qual se deu a consolidação da propriedade privada e a cisão entre os detentores dos meios de produção e aqueles obrigados a vender sua força de trabalho em nome do uso destes meios. Andrejevic (2007) considera que este processo guarda semelhanças com a situação em que se encontram os internautas hoje, que em troca do uso dos vários sítios e serviços gratuitos da *web* submetem-se a um monitoramento caracterizado pela captura dos espaços interativos como geradores de um valor secundário, derivado das informações por eles fornecidas. “Este *feedback* se torna propriedade de companhias privadas que podem armazenar, reunir, classificar, e, em muitos casos, vender a informação a outros na forma de um banco de dados ou de uma *commodity* cibernética” (ANDREJEVIC, 2007: 2, tradução nossa).²⁰

Por fim, como nos lembra Manovich (2007), ainda que a discussão sobre as novas mídias enfatize prioritariamente aspectos como a interatividade, a comunicação em rede e a pluralidade de códigos presentes na linguagem multimídia, um dos conceitos mais fundamentais relacionados ao computador digital é o da computação propriamente dita. É sob esta égide que podemos compreender a atuação de tecnologias como o *data matching*²¹, a simulação, o *profiling*²², dentre tantas outras. Como ressalta o autor, além das interfaces

²⁰ Tradução nossa para: “This feedback becomes the property of private companies that can store, aggregate, sort, and, in many cases, sell the information to others in the form of a database or a cybernetic commodity”.

²¹ O *data matching* é uma técnica computacional que permite a integração total ou parcial de duas ou mais bases de dados (NATIONAL STATISTICS, 2004: 5), tornando possível tanto comparar uma mesma informação com aquelas presentes em diferentes conjuntos quanto comparar lateralmente bancos de dados inteiros, visando identificar tendências, informações duplicadas etc. Assim, esta técnica pode servir tanto para verificar quanto para reunir informações diversas sobre um mesmo indivíduo, como seus gostos, interesses, hábitos de consumo etc.

²² O *profiling* envolve a descoberta de padrões em amplas bases de dados, capazes de representar pessoas a partir do uso de algoritmos e técnicas computacionais e matemáticas.

gráficas, dos bancos de dados e do ciberespaço, a visualização dinâmica de dados desponta como mais uma realidade possibilitada pela ciência da computação.²³ Empregando métodos variados, que vão da estatística clássica ao *data mining*,²⁴ os computadores possibilitaram mapear conjuntos mais complexos de dados, alimentados em tempo real. Esta ampliação do poder de cálculo dessas máquinas, que veio acompanhada de novos paradigmas nas ciências puras e aplicadas contemporâneas, parece estar agora emprestando suas virtudes de processamento, visualização e mapeamento de dados a aspectos que antes pareciam bem menos afeiçoados a formalizações, como o comportamento humano, suas preferências, tendências e interesses.

Concluimos assim que as características da linguagem digital conferem à vigilância no ciberespaço uma condição de reversibilidade, expressa em através de duas maneiras principais. A primeira delas pode ser assim enunciada: se a vigilância tem como matéria prima, seja na modernidade ou na contemporaneidade, a coleta e o uso de informações sobre populações, grupos e indivíduos, o padrão digital instaura neste contexto, em que a informação opera como um tradutor universal, uma reversibilidade entre a violação e a proteção dos dados visados pelos cidadãos ou pelos dispositivos vigilantes. Toda informação é protegida ou violada por algoritmos, e todo código, uma vez elaborado, possui implícita a possibilidade de sua quebra. A segunda condição de reversibilidade diz respeito ao fato de que, no ciberespaço, o uso não pode ser dissociado do registro, o que faz como que a utilização das ferramentas disponíveis e os benefícios imediatos buscados pelos internautas através deste processo tragam sempre, embutidos, um potencial vigilante, pois implicam a disseminação de informações que podem ser largamente usadas com outros objetivos, não previstos ou sequer conhecidos pelos usuários de um determinado sistema. Assim, sempre que um internauta perde o controle sobre um corpo de informações, alguém, em um outro lado do mundo ou da tela, pode estar adquirindo este controle e apropriando-se dos dados em questão.

1.3.1.1 Códigos e protocolos

A estrutura e a história da Internet já trazem implícitas relações estreitas com formas

²³ Como nos coloca Manovich (2007), a visualização de dados diz respeito a situações em que informações que por natureza não são visuais – como o fluxo de dados na Internet, o funcionamento dos mercados financeiros etc. – são convertidas em imagem. Assim, os computadores são máquinas que facilitam a conversão de uma representação em outra a partir de técnicas de mapeamento, processo facilitado pela representação digital de informações de diferentes naturezas em uma linguagem comum: a do código.

²⁴ O *data mining* é uma técnica computacional que envolve a aplicação de algoritmos em bases de dados para extrair padrões úteis de amplos corpos de informações (FAYYAD *et al.*, 1996).

de monitoramento e com questões acerca do acesso e da proteção de dados. Afinal, a rede mundial de computadores, em sua origem entre o fim da década de 50 e início da década de 60, surgiu como uma tecnologia militar destinada não só a resistir a potenciais ataques como também a proteger dados considerados estratégicos pelo governo americano. A idéia era que os arquivos, uma vez salvos em um computador ou máquina local, pudessem ser disseminados e replicados em tempo hábil para diferentes máquinas ao redor do mundo. Assim, a destruição de uma informação se tornaria impossível, pois devido a ausência de um comando central (que se ofereceria como alvo fácil aos inimigos), um dado só poderia ser destruído se todo o sistema se extinguisse. No entanto, com a evolução desta tecnologia, passamos a descobrir, cada vez mais, que sua arquitetura, tão celebrada por seu potencial supostamente democrático e anárquico, possui pontos de concentração e estruturas de organização que implicam diversos graus de centralização e controle (BARABÁSI, 2003; GALLOWAY, 2004; GALLOWAY e THACKER, 2007; LESSIG, 2006). Para compreendermos este fato, devemos considerar inicialmente as características dos substratos materiais que subsidiam a formação das redes informáticas: o código e os protocolos.

Os protocolos são padrões que prescrevem, através de algoritmos, a forma como os dispositivos se comunicam. Eles estabelecem parâmetros comuns de conectividade e representam uma solução operacional para que a comunicação em rede possa ocorrer. Assim, nas palavras de Galloway (2004: 39, tradução nossa), “[...] protocolos são a linguagem comum que todos os computadores em uma rede falam”.²⁵ Sabemos que a Internet é, em suma, uma rede de redes, formada por computadores dispersos ao redor do mundo, interconectados na arquitetura cliente/servidor. Nela, o conjunto de protocolos que desempenha esta função é o TCP/IP (respectivamente *Transmission Control Protocol* e *Internet Protocol*). Podemos descrevê-lo como um modelo de camadas, no qual um nível inferior tem sempre o papel de organizar um conjunto de procedimentos para o protocolo da camada superior. Temos assim uma camada física de *hardware* com seus protocolos materiais (cabos, conectores etc.); uma camada de rede que se ocupa do “roteamento” de pacotes, efetuando o seu tráfego entre a origem e o destino, comumente através do protocolo IP; temos uma camada de transporte, que se ocupa do estabelecimento de uma conexão e da integridade e confiabilidade do transporte de dados, garantindo que eles cheguem ao destino proposto (freqüentemente através do protocolo TCP ou UDP); e por fim temos a camada de aplicação, responsável pelo nível semântico ou pelo conteúdo da transação em questão, seja ela o acesso

²⁵ Tradução nossa para: “[...] protocols are the common languages that all computers on the network speak”.

a uma página *www* (protocolo HTTP), o uso de *e-mail* (protocolo SMTP), e assim por diante. Como ressalta Galloway (2004: 42), estes protocolos, funcionando em conjunto, garantem que a Internet seja uma rede robusta e eficiente graças à flexibilidade de seu modo de funcionamento: usando os mesmos protocolos, qualquer servidor pode se comunicar com qualquer cliente na rede, e assim, ela pode se readaptar para corrigir a rota de pacotes, falhas eventuais em suas sub-redes, e assim por diante.

A utilidade de tratar a lógica dos protocolos não está apenas na descrição material das formas de funcionamento da *web*, mas também na dedução dos subtextos políticos e principalmente no conhecimento de uma lógica operativa que acreditamos povoar não só o imaginário contemporâneo como o exercício das práticas vigilantes no ciberespaço. Corpos de informações que se separam aqui e se recompõem acolá, camadas que particionam práxis operativas e que conferem ampla flexibilidade para se lidar com massas de dados significativas, a operação de um controle distribuído e efetuado por agentes autônomos, a interação entre elementos humanos e não-humanos, além de uma inexorabilidade tecnologicamente subsidiada: uma vez codificado, um protocolo descreve o destino imediato e certo das informações que o atravessam. Ele não visa interpretá-las nem julgar as possibilidades implícitas a seus próprios processos (GALLOWAY, 2004: 52-3). Um protocolo recebe dados, os descodifica, recodifica, e os fornece à camada superior. Assim, tal como abordados por Galloway e Thacker (2007), os protocolos se referem à emergência de uma nova forma de controle: não mais a burocracia ou a hierarquia, não mais as estratégias disciplinares e sim uma nova modalidade, própria aos sistemas distribuídos, marcada por sua modularidade e flexibilidade.

Abstraído em um conceito, o protocolo pode ser definido como aparato de controle horizontal, distribuído, que guia tanto a formação técnica quanto política das redes de computadores, sistemas biológicos e outras mídias (GALLOWAY e THACKER, 2007: 28, tradução nossa).²⁶

Mais uma vez, consideremos a estrutura da Internet. Um bom exemplo de sua modularidade pode ser dado pelo fato de que ela não opera através de uma estrutura pré-estabelecida de “lincagens”, mas sim através de uma conectividade distribuída: rotas mutantes são criadas a partir da seleção de caminhos que só existem temporariamente a partir das definições estabelecidas pelo protocolo IP. Neste processo de conexões sucessivas e

²⁶ Tradução nossa para: “Abstracted into a concept, protocol may be defined as a horizontal, distributed control apparatus that guides both the technical and political formation of computer networks, biological systems, and other media”.

dinâmicas, o próximo nó (ou a próxima máquina da rede) nunca sabe o destino final de um pacote, mas apenas a regra simples que o protocolo IP determina: que o pacote “X” deve ser enviado na direção “Y”. Assim, como cada nó desconhece também a localização exata dos clientes com os quais pode se conectar, ele transporta o pacote na direção mais próxima do destino apontado, e assim sucessivamente, até que ele chegue ao seu destino. Assim, podemos considerar que os protocolos fazem da própria Internet uma tecnologia modular, uma grande máquina que orchestra ao vivo o som de diferentes instrumentos na construção de uma composição harmônica e espontânea. E esta espontaneidade não significa a ausência completa de controle ou regulação, mas antes o nascimento de uma espontaneidade regulada. Em resumo, a ausência de uma instância central que exerce um controle hierárquico, ou *top-down*, não quer dizer que outras formas de regulação não sejam possíveis. Galloway e Thacker (2007: 46) usam a noção de “soberania distribuída” para se referir à idéia de que o controle e a organização podem ser disseminados por uma série de pequenas decisões locais.

Por fim, uma última questão importante no tratamento dos protocolos diz respeito ao fato de que eles dependem, em larga medida, de tecnologias de identificação e monitoramento. O protocolo DNS, por exemplo, traduz os endereços da *www* tais como os conhecemos, enquanto nome, para o número de IP para os quais eles apontam. Por outro lado, o protocolo TCP além de estabelecer a comunicação entre dois computadores (através de um processo comumente denominado *handshake*), deve constantemente rastrear os pacotes para verificar como está ocorrendo o tráfego de dados. Se algum dado se perde ou é corrompido, o protocolo deve acusar a falha para que ele possa ser reenviado. De maneira semelhante, o tráfego de pacotes, efetuado pelo protocolo IP, prevê um número máximo de “saltos” no “roteamento” dos pacotes. A cada salto, o tempo de vida do pacote é subtraído de um, e ele é apagado automaticamente se o seu tempo de vida chega a zero. E todas estas decisões locais são tão necessárias quanto indispensáveis ao bom funcionamento da rede. Desta forma, para assegurar a eficácia e a robustez do sistema, qualquer desvio deve ser acompanhado de perto, para que as medidas necessárias – já pré-estabelecidas pelos protocolos – sejam tomadas. De uma camada a outra, o poder de controle sobre a informação é potencializado.

Consideremos agora a análise do papel do código e sua atuação, principalmente na camada de aplicação. Páginas *web* são linhas de código que estruturam não só a maneira como a informação é exibida como também os limites da agência dos interatores neste contexto. Toda informação que circula na rede (ela própria um grande aglomerado de arquivos dispostos em servidores dispersos ao redor do mundo) é traduzida em linhas de código que podem ser facilmente armazenados, transportados e tratados para gerar novos

dados, segundo finalidades determinadas por qualquer um que a eles tenha acesso. As características do código e de sua linguagem, naturalmente, podem fornecer algumas explicações e, em outros casos, valiosos *insights* sobre a vigilância na era das novas tecnologias. O código é uma linguagem formal, em suma, uma forma de classificação. Qualquer *software*, a despeito da linguagem de que ele se utilize, é um conjunto de instruções denominadas algoritmos, estruturadas e precisas o suficiente para serem executadas por uma máquina. Diferente de uma receita de bolo, ou de qualquer outra formalização que descreva as etapas da execução de uma tarefa, os códigos computacionais possuem uma particularidade: eles são, ao mesmo tempo, uma descrição, uma classificação, um esboço e uma execução. “A programação de computadores reúne em uma só, ao que parece, a segunda e a terceira das três etapas de um conceito, a notação do conceito e a sua execução” (CRAMER, 2002: *online*, tradução nossa).²⁷

Neste sentido, Arns (2005) considera que o código é uma linguagem performativa. Partindo do princípio de que a linguagem não se limita apenas à sua função referencial ou descritiva, ele destaca que, muitas vezes, um enunciado possui como dimensão inerente e predominante uma ação, e não apenas uma intenção. Considere, por exemplo, um veredito. Ao ser proferido por um juiz, ele instaura uma nova ordem: algumas palavras cometem fatos, e isso também é verdadeiro para o caso do código, uma linguagem executável, e que só faz sentido quando é executada, subsidiando a existência do ambiente cujas regras ele formalizou. Grosso modo isto quer dizer que quando eu digito em um bloco de notas um trecho de código HTML qualquer e salvo o arquivo na extensão “.htm”, ele irá exibir, quando solicitado, não mais um arquivo de texto e sim uma página *web* com as características formalizadas através do código redigido (escrever *backgroundcolor = “blue”* quer dizer que, efetivamente, eu terei a minha página *web* com o fundo azul). Assim, uma vez que um *software* ou um ambiente *web* tenha sido codificado e executado, ele carregará as funcionalidades para ele planejadas, instaurando como realidade efetiva os objetivos e potencialidades de uso previstos por sua codificação.

Quando eu falo da performatividade do código, eu quero dizer que esta performatividade não deve ser entendida como sendo puramente técnica, *i.e.*, ela não acontece apenas no contexto de um sistema técnico fechado, mas possui implicações estéticas, políticas e sociais. Códigos de programação são caracterizados pelo fato de que aqui, “dizer” coincide com “fazer”. [...] Esta performatividade do código possui consequências imediatas e políticas em espaços atuais e virtuais (dentre outros, a Internet),

²⁷ Tradução nossa para: “Computer programming collapses, as it seems, the second and third of the three steps of concept, concept notation and execution”.

para os quais estamos cada vez mais nos direcionando e vivendo: isso significa, em última instância, que esta performatividade do código *mobiliza* ou *imobiliza* seus usuários (ARNS, 2005: 7, grifo do autor, tradução nossa).²⁸

Desta forma, como nos propõe Lessig (2006), uma maior regulação da Internet – regulação esta que depende da identificação das pessoas, do que elas estão fazendo, e de onde elas podem ser encontradas – acontece, igualmente, através das regras e das leis, ou seja, do código que regulamenta um determinado espaço. E por outro lado, o código, entendido agora em seu sentido técnico, carrega, através das funcionalidades que permite, as regras traçadas de acordo com os objetivos previstos para cada espaço. Neste sentido, se em sua estrutura e arquitetura originais, a Internet dificultava o controle e a localização dos indivíduos, presenciamos, hoje, o surgimento acelerado de novas formas, tecnologias e espaços de controle. E dando um passo adiante, elas permitem diversos e complexos graus de vigilância dos indivíduos sem que isso signifique incomodá-los, identificá-los ou imputá-los por coisas funestas como crimes cibernéticos ou operações ilegais. A lógica do controle envolve os indivíduos em estratégias prazerosas, inclusivas, amplamente disponíveis e úteis a todos os que delas podem usufruir. E todos querem integrar esses novos ciclos de consumo, interação e civilidade.

Acreditamos que uma perspectiva que considera os aspectos técnicos da comunicação em rede como fatores que atuam de maneira exclusiva no processo que molda o alcance social destes meios pode ser acusada de recair facilmente na armadilha do determinismo tecnológico. Por outro lado, ignorar as características, relações e contradições estabelecidas neste processo seria empobrecer o debate sobre as possibilidades de uso, as interações e as formas de controle colocadas em jogo com a inserção das novas tecnologias na sociedade e no mercado. Seja no que diz respeito às suas características mais tangíveis, seja no que aponta para uma certa lógica e um imaginário próprios ao nosso ambiente tecnologizado, devemos reconhecer certos pontos de contato entre as características deste novo meio e os fenômenos que nele encontram seu lugar. Desta forma, o modo de operação das interfaces não pode ser dissociado dos objetivos a que este determinado funcionamento está servindo, pois sabemos que, na era da flexibilidade das linguagens, o caminho poderia sempre ser outro. Esta

²⁸ Tradução nossa para: “When I speak of the performativity of code, I mean that this performativity is not to be understood as a purely technical performativity, i.e., it does not only happen in the context of a closed technical system, but affects the realm of the aesthetic, political and social. Program code is characterised by the fact that here “saying” coincides with “doing”. [...] This “coded performativity” has immediate and political consequences on the actual and virtual spaces (amongst others, the Internet), in which we are increasingly moving and living: it means, ultimately, that this coded performativity *mobilises or immobilises* its users”.

reversibilidade é a mesma que pode conferir poder ora a *hackers*, ora a criminosos, ora aos gurus do *marketing*, e assim por diante. Desta forma, trata-se, sobretudo, de conhecer os modos de operação das interações e processos vigentes e operar, em cada caso, uma busca pelo valor dos valores.

1.3.2 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: 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: 69). Trata-se, portanto, de uma resposta inconsciente, automatizada e não-direcional (POSTER, 1996: 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 reclassificados 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 (1996: 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 simulações 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 (POSTER, 1996: 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, 2008). Ao invés dos dados estáveis, referentes a categorias geodemográficas, biométricas, relativos a gênero etc., que praticamente não se alteram com o curso do tempo, as informações e aspectos visados por esses dispositivos hoje são predominantemente 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” (BRUNO, 2008: 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: 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.

1.3.2.1 A estrutura temporal da vigilância: risco e predição

Para compreender em detalhes como este dispositivo opera, analisemos a noção temporal subjacente ao seu modo de operação. Neste sentido, é importante ressaltar que o imaginário da predição está intimamente relacionado à emergência da sociedade de risco. A passagem desta noção dos domínios da matemática e da teoria dos jogos a alicerce de organização do corpo social na contemporaneidade diz respeito a configuração de um mundo globalizado, no qual os perigos se potencializaram e no qual os indivíduos, sem o respaldo do Estado de bem estar social, assumem para si a tarefa de atingir a felicidade e o sucesso (BECK, 1992; DOUGLAS, 1992). Neste cenário, a ciência foi eleita como forma através da qual os indivíduos devem medir os limites do que é seguro, de modo correr riscos sem colocar os outros em risco. Assim, a cisão entre leigos e especialistas – na base dos cálculos que

guiam a prevenção do crime, que certificam nossos produtos, orientam nossa alimentação e acabam assim por determinar nossos comportamentos – marca a entrada da ciência e o afastamento da política tradicional dos processos através dos quais se legisla acerca do permitido e proibido, ou melhor, do que é ou não recomendável segundo o risco que lhe é cientificamente atribuído. E naturalmente, o cálculo do risco exige a coleta de dados pessoais.

As práticas vigilantes e as rotinas do cálculo de risco apontam para novos modos de gerenciar e classificar os indivíduos, que visam orientar suas ações para certos fins. E no exercício desta forma de poder, há uma obstinação generalizada pela prevenção que nos dá a seguinte pista: a de que estamos vivenciando o curso de uma mudança na forma através da qual nos relacionamos com o futuro, com o presente e com o passado. Neste sentido, cabe resgatar a argumentação de Koselleck (2006) acerca das categorias que ele denomina “espaço de experiência” e “horizonte de expectativa”. Ancoradas fundamentalmente na generalidade, elas permitem entrelaçar passado e futuro, produzindo a própria história e as condições de seu conhecimento. Sob o ponto de vista deste trabalho, tais categorias são interessantes na medida em que permitem precisar a diferença existente entre a presença do passado e a presença do futuro. Desta forma, o autor define a experiência como

[...] o passado atual, aquele no qual acontecimentos foram incorporados e podem ser lembrados. Na experiência se fundem tanto a elaboração racional quanto as formas inconscientes de comportamento, que não estão mais, ou que não precisam mais estar presentes no conhecimento. Além disso, na experiência de cada um, transmitida por gerações e instituições, sempre está contida e é conservada uma experiência alheia. Nesse sentido, também a história é desde sempre concebida como conhecimento de experiências alheias (KOSELLECK, 2006: 309-10).

Por outro lado, a expectativa:

[...] é ao mesmo tempo ligada à pessoa e ao interpessoal, também a expectativa se realiza no hoje, é futuro presente, voltado para o ainda-não, para o não experimentado, para o que apenas pode ser previsto. Esperança e medo, desejo e vontade, a inquietude, mas também a análise racional, a visão receptiva ou a curiosidade fazem parte da expectativa e a constituem (KOSELLECK, 2006: 310).

Neste sentido, Koselleck (2006) caracteriza a modernidade por uma condição em que, essencialmente, o espaço de experiência se descola do horizonte de expectativas. A superação constante, tecnologicamente subsidiada, fez com que a aceleração do tempo rompesse drasticamente uma condição própria ao mundo camponês ou ao mundo urbano dos artesãos, em que as experiências transmitidas de geração em geração sempre eram suficientes para se

dar conta do ritmo do mundo, de modo a haver sempre continuidade entre as experiências acumuladas e as expectativas alimentadas. Assim, fundamentalmente, o contemporâneo é marcado por uma inversão temporal que nos leva a projetar possíveis futuros para agirmos no presente de modo a evitar as consequências meléficas, por um lado, e promover aquelas que são desejadas, por outro. Vivemos hoje um desejo constante por fazer coincidir passado e futuro, como se uma experiência pudesse ser completamente deduzida de uma expectativa. Parecemos ter abandonado aquela premissa simples, segundo a qual o futuro histórico sempre é diferente do passado histórico. Afinal, como argumenta Koselleck (2006), um prognóstico é sempre um prognóstico, ou seja, o futuro não pode ser experimentado antecipadamente.

[...] os prognósticos também são determinados pela necessidade de se esperar alguma coisa. Voltada para um campo de ação mais amplo ou mais estreito, a previsão libera expectativas, a que se misturam também temor e esperança. As condições alternativas têm que ser levadas em conta, pois sempre entram em jogo possibilidades que contêm mais do que a realidade futura é capaz de cumprir. Assim, um prognóstico abre expectativas que não decorrem apenas da experiência. Fazer um prognóstico já significa modificar a situação de onde ele surge. Noutras palavras: o espaço de experiência anterior nunca chega a determinar o horizonte de expectativa (KOSSELLECK, 2006: 313).

Da mesma maneira, a vigilância visa conhecer e classificar os indivíduos de acordo com seus hábitos e estados presentes de modo a fabricar ou prever cenários futuros. No entanto, se o horizonte é um espaço novo que só podemos antever, e não precisar, o que dizer das exaustivas tentativas de prever o crime e eventualmente punir os indivíduos baseando-se em especulações? Ou de identificar por antecipação a oferta correta de modo a maximizar o consumo? O elemento mais importante desta nova lógica é que, ainda que o futuro seja incerto, um prognóstico é sempre atual: uma previsão sempre afeta o presente em que é concebida. Por isso, podemos dizer que os perfis, ao obedecerem a esta lógica da predição, são performativos: eles não são nem verdadeiros, nem falsos – são da ordem da simulação – e ao enunciarem uma conjectura possível, se tornam efetivos em relação ao tempo presente, pois nele interferem de maneira imediata e real. Considere, por exemplo, a estrutura de um sistema de recomendação. Você vai a uma livraria, faz uma compra, e todos os seus registros passam a integrar um banco de dados que será usado para gerar novas recomendações de produtos a partir de medições de semelhança do seu gosto com o estoque disponível.²⁹ Em um determinado momento, você encontra dentre essas recomendações um produto que você

²⁹ A loja virtual amazon.com possui um sistema de recomendação que perfila indivíduos para fomentar suas vendas. Uma descrição detalhada do sistema pode ser encontrada em Çentimentel *et al.*, 2000 e em Linden, 2003.

desconhecia até alguns segundos atrás, se interessa, e acaba por comprá-lo. Lógica semelhante está implícita também ao caso da adolescente de 16 anos e filha de imigrantes muçulmanos que, após ter sua navegação na Internet monitorada pelo FBI, foi convidada a sair dos EUA por se encaixar em um perfil de “menina-bomba”.³⁰

1.3.2.2 Classificação e individualização

Este achatamento temporal efetuado pela projeção do futuro no presente só se torna possível a partir da operação de uma grande máquina de classificação dos indivíduos, operante em uma cultura que já se acostumou à indistinção entre imagem e referente, modelo e realidade (BOGARD, 1996). Em função do papel que desempenha na estruturação dos mecanismos contemporâneos da vigilância, entendemos a noção de classificação como o processo através do qual as extensas massas de dados coletados adquirem sentido, *i.e.*, se tornam palpáveis aos sentidos humanos, permitindo a dedução de assertivas que subsidiarão o governo da conduta e a intervenção sobre as escolhas dos indivíduos. As rotinas da estatística, do *data mining*, da amostragem, da dedução de padrões, do cálculo de proximidade, semelhança e afinidade não são mero fruto dos avanços tecnológicos recentes. Ao contrário, elas possuem sua história, que entrelaça a origem das iniciativas de enumeração em massa dos cidadãos com o processo de construção de identidades coletivas, com o estabelecimento de guias classificatórias que subsidiaram a emergência da norma e o desenvolvimento das formas de classificação social.

Antes da centralização dos esforços de enumeração dos cidadãos por parte das burocracias estatais modernas, alguns censos já haviam sido realizados em diferentes datas e lugares do mundo por aventureiros ou visionários. As mesmas províncias italianas em que teve origem o conceito moderno de Estado protagonizaram esforços para a realização de levantamentos estatísticos antes mesmo de qualquer outra cidade européia (HACKING, 1999). No entanto, na era moderna, a realização de censos era uma iniciativa mais comum entre metrópoles como Espanha, França e Inglaterra, com o objetivo de conhecer melhor suas colônias. O uso da estatística pelo poder público começa com os ingleses, e mais tarde, os alemães são os responsáveis por consolidar a idéia de que “[...] o Estado-nação é essencialmente caracterizado por sua estatística, e desta forma, demanda um ministério de estatística para se definir enquanto tal e para definir seu poder” (HACKING, 1999: 18,

³⁰ Cf. Bruno, 2006: 158.

tradução nossa).³¹

Assim, os escritórios designados à coleta de dados sobre os indivíduos se tornaram peça integrante da maquinaria estatal. No entanto, o momento mais importante no curso deste processo se dá com o fim da Era Napoleônica, quando a enumeração dos indivíduos e de seus hábitos subsidiou a emergência de um “espírito quantificador” (CAPLAN e TORPEY, 2000: 3), a partir do qual a questão “Quem é esta pessoa?” passa a se confundir, gradualmente e em grande medida, com uma outra – “Que tipo de pessoa é essa?”. Na virada do século XVIII para o século XIX, os dados coletados pelas burocracias estatais deixam de ser matéria de acesso exclusivo do rei e de seus administradores e ganham o domínio público (HACKING, 1999: 3). E este processo está intimamente relacionado a dois outros que se desenvolvem de maneira paralela no século XIX: a emergência das leis da probabilidade e da noção de normalidade. Se o século XVIII e a crença exacerbada na razão e na ciência fizeram o homem acreditar que o mundo seria explicado exclusivamente por leis de causalidade – lógica segundo a qual a probabilidade era um efeito colateral da ignorância humana, ou uma tentativa de dar conta do que a razão ainda era incapaz de explicar – no século XIX o determinismo é subvertido pelas leis do acaso (HACKING, 1999: 3). E este indeterminismo probabilístico acaba por potencializar o engenho do controle social.

Como argumenta Hacking (1993), a coleta de dados em larga escala, o cálculo de médias e a identificação dos desvios acabam por se tornar instrumentos para uma espécie de engenharia social calcada na idéia da norma. A dedução de leis estatísticas a partir de dados coletados, tabulados e tornados públicos se torna então uma forma de conhecer melhor e controlar populações desviantes. Ao longo do século XIX, a habilidade de lidar com números se desenvolve, e através deste processo, as formas de controle ligadas à identificação passam a se ligar cada vez mais a processos de classificação derivados do estabelecimento de identidades: a história das regras a que se submetem os cidadãos não pode ser desvinculada da identificação que permite imputar penas nem da classificação que permite a formalização do comportamento desejável. Desta forma, o controle social é indissociável dos mecanismos de estabelecimento de tipos, da classificação dos indivíduos a partir do estabelecimento de identidades coletivas, processo que por sua vez, tem conseqüências profundas na maneira como percebemos a sociedade a nossa volta, na forma através da qual nos relacionamos com os outros e os concebemos em nosso meio social.

³¹ Tradução nossa para: “[...] the nation-states is essentially characterized by its statistics, and therefore demands a statistical office in order to define itself and its power”.

Eu afirmo que a enumeração requer categorização, e que definir novas classes de pessoas para novas propostas da estatística tem consequências para os modos através dos quais concebemos os outros e pensamos acerca de nossas próprias possibilidades e potencialidades (HACKING, 1999: 6, tradução nossa).³²

Duas questões se tornam pertinentes quando resgatamos a história dos mecanismos de enumeração dos cidadãos e de classificação social. A primeira delas diz respeito à dispersão das habilidades vigilantes pelo corpo social. Se antes estes processos se davam predominantemente sob a tutela do Estado burocrático, hoje, eles estão ao alcance de qualquer um que possua meios técnicos (amplamente disponíveis e de baixo custo) e conhecimento necessário para tal. Os bancos de dados que proliferam na contemporaneidade não são necessariamente estatais ou ligados a uma figura de autoridade pública e científica (BRUNO, 2008: 5). Eles são também privados e servem igualmente aos desígnios do *marketing*, do consumo, a empresas de seguros, e assim por diante. A segunda diz respeito ao uso e à inserção social das generalizações obtidas através da classificação dos indivíduos. Na modernidade este processo visava a identificação de padrões regulares e a dedução de médias que promoviam uma formalização do comportamento desejado a partir de uma classificação predominantemente binária (normal-anormal), levando assim à incorporação da norma. Na contemporaneidade, a lógica dos perfis não visa formalizar uma lei, própria ao homem médio ou normal, mas tendências e potencialidades dos mais variados tipos de indivíduos. Não cabe mais identificar o desvio para efetuar a sanção, e sim, incorporá-lo ao perfil para que ele responda também a mais este padrão circunstancial da conduta.

Diferentemente, os perfis encarnam múltiplas micro-regularidades no seio de inúmeras variáveis heterogêneas e, de modo algum, apresentam-se como regulamentos. A divisão norma/desvio não se aplica aos perfis, pois eles são padrões resultantes de combinatórias e regras associativas de tipo não valorativo entre muitas variáveis, podendo ser aplicáveis a potencialmente todas as qualidades e comportamentos humanos. O perfil não é nem uma medida nem um valor, mas um padrão de ocorrência de um certo fator (comportamento, interesse, patologia) num dado conjunto de variáveis. As médias e normas eram a referência comum das massas; os perfis são as micro-regularidades dos nichos, tribos, grupos (BRUNO, 2008: 8).

Neste sentido, os processos de individualização inaugurados pela vigilância contemporânea diferem daqueles que caracterizaram a modernidade. A lógica aqui vigente não é mais a da causalidade, mas a da correlação; não mais o modelo centralizador na norma

³² Tradução nossa para: "I claim that enumeration requires categorization, and that defining new classes of people for the purposes of statistics has consequences for the ways in which we conceive of others and think of our own possibilities and potentialities".

com sua cisão operativa binária, mas o gerenciamento de modulações conjunturais identitárias. As séries disciplinares intermediadas pela prática do exame e acompanhadas pelos registros detalhados da performance dos indivíduos possuíam uma lógica “evolutiva”, historicamente determinada. Ao contrário, hoje, esta unidade cede lugar à dinâmica fluida da combinação de estados transitórios que querem dizer não de uma unidade profunda, mas de uma tendência predominante. Assim, atitudes e comportamentos que não são capazes de justificar um ao outro passam a ser relacionados enquanto portadores de uma conexão superficial, que não pode nem precisa ser explicada, apenas identificada, pois o interesse está no fato de que ela possa, eventualmente, se repetir. Assim, uma combinação como “pessoas que escolhem a profissão “x” gostam de filmes alternativos” passa possuir valor – não um valor meramente conceitual, que se limite a demonstrar relações ou constatar sua existência, mas operatório, visto que estas conjunções irão alimentar sistemas que visam tornar mais eficientes processos associados ao *marketing* ou à busca por serviços e produtos.

Assim, enquanto grande parte do discurso contemporâneo sobre vigilância associa esta prática a uma questão de privacidade – conceito de dimensões extremamente amplas e um tanto quanto abstratas, uma vez que envolve a formalização de uma sensação subjetiva de desrespeito e violação em uma categoria legal – a análise das práticas de classificação social a identificam mais como uma questão de justiça social. Estes sistemas funcionam como dispositivos de poder na medida em que passam a decidir, no presente, sobre as possibilidades e escolhas disponíveis aos indivíduos de acordo com a avaliação efetuada e com o grupo em que são inseridos. Assim, Lyon (2004) explica que essas categorias de classificação social são responsáveis pela concessão de um tratamento direcionado e preconizado. De maneira semelhante, Gandy (1996) confere a essas tecnologias um poder discriminatório, e usa o termo *panoptic sort* para se referir a uma condição em que nossas interações com os sistemas do mercado, estatais, dentre outros, passa a ser pautada pelo registro e processamento de dados sobre nossas buscas, compras, comunicações e transações, em um esforço analítico para diferenciar, classificar e segmentar indivíduos. Por um lado, isso implica dizer que a vigilância contemporânea, ao contrário da moderna, não incide sobre os desviantes de modo a curá-los ou recuperá-los, mas se associa aos circuitos do consumo e da sociabilidade. Por outro, neste processo, ela também fomenta novas cisões sociais e novos modos de discriminação.

A panoptic sort é uma complexa tecnologia discriminatória. Ela é panóptica por considerar toda informação sobre o estado e comportamento individual como potencialmente útil na produção de inteligência sobre o valor

econômico de uma pessoa. Ela é uma tecnologia discriminatória porque é usada para classificar pessoas em categorias baseando-se nessas estimativas (GANDY, 1996: 133, tradução nossa).³³

Enfatizando as rotinas da publicidade direcionada e do *marketing*, Gandy (1996) ressalta também que a classificação tem como objetivo manifesto a eficácia. Assim como na modernidade ela visava disciplinar os indivíduos, reduzindo as incertezas sobre seu comportamento futuro, hoje ela é usada para manter no limite do programável as taxas de lucro das empresas, que usam as informações pessoais coletadas para prever e calcular a resposta de um dado indivíduo a uma determinada oferta ou sua inserção em um determinado segmento do mercado. Esta classificação, portanto, ao informar processos de tomada decisão, determinará, por exemplo, o acesso ou não de um indivíduo a uma promoção ou informação específica. Assim, amostras pontuais do comportamento passam a informar atitudes concretas e a virtualidade do modelo encontra seu lugar na efetividade do real. Neste contexto, o autor ressalta que todo processo de classificação é também uma generalização: ele depende da redução da complexidade do fenômeno analisado para a produção de um conhecimento que ele descreve como sendo da ordem da racionalidade instrumental (GANDY, 1996: 136). Assim, baseando-se em amostras de indivíduos e de seus comportamentos, os processos de *social sorting* dispensam inumeráveis outros aspectos de suas existências e personalidades para efetuar suas correlações empíricas e imediatas.

Neste sentido, como explicitam Bowker e Star (1999: 278), um sistema de classificação é uma forma de gerenciamento coletivo da memória e, sobretudo, do esquecimento: “um sistema de classificação diz a você o que esquecer e como esquecer” (BOWKER e STAR, 1999: 278, tradução nossa).³⁴ Ele opera uma reorganização a partir da qual apagar alguns registros permite a instauração de uma lógica nova na operação e na produção do conhecimento. Esta concepção traz implícita a idéia de que toda classificação é também um mecanismo de visibilidade. Há aqui uma suposição de que toda categorização valoriza alguns aspectos e silencia outros. Assim, a classificação está sempre associada a um poder que legitima, institucionaliza e reconhece uma prática, ao mesmo tempo em que a insere, como contrapartida, em um campo de visibilidade e também de controle, tornando a vigilância possível. E como toda categorização, assim como qualquer codificação molar,

³³ Tradução nossa para: “The panoptic sort is a complex discriminatory technology. It is panoptic in considers all information about individual status and behavior to be potentially useful in the production of intelligence about a person’s economic value. It is a discriminatory technology because it is used to sort people into categories based upon these estimates”.

³⁴ Tradução nossa para: “The classification system tells you what to forget and how to forget it”.

instaura zonas de sombra, ela ancora sua eficiência nesta pretensa invisibilidade. Assim, Bowker e Star (1999) explicitam que a compreensão das implicações morais de um determinado sistema de classificação depende de ferramentas que permitam ver o invisível e questionar a organização tranquilizadora que ele instaura. Afinal, “para qualquer indivíduo, grupo ou situação, classificações e padrões conferem vantagem ou conferem sofrimento” (BOWKER e STAR, 1999: 7, tradução nossa).³⁵ Essas políticas de representação encerram escolhas e conseqüências nas quais deve residir o próprio questionamento de seu processo de construção e atuação.

³⁵ Tradução nossa para: “For any individual, group or situation, classification and standards give advantage or the give suffering. Jobs are made and lost; some regions benefit at the expense of others”.

2 AS REDES SOCIAIS

Os *sites* de rede social, como o *MySpace*,³⁶ *Facebook*,³⁷ *Friendster*,³⁸ *LinkedIn*,³⁹ *Bebo*,⁴⁰ *Orkut*⁴¹ e tantos outros, caíram definitivamente no gosto popular. Eles são espaços que permitem aos indivíduos construir redes “hiperlincadas” de amigos e conhecidos, que de acordo com os critérios de visibilidade de cada *site*, podem ser percorridas por outros usuários, seja por uma curiosidade motivada ou por mero divertimento. Eles integram a onda das novas tecnologias colaborativas que têm se multiplicado na Internet nos últimos anos e praticamente todo o seu conteúdo é produzido pelos próprios usuários, que neles encontram novos canais para a expressão pessoal, para a troca de informações e compartilhamento de fotos, vídeos, jogos e interesses. Muitos benefícios estão latentes a este novo modo de interação social: para alguns usuários, eles podem ser úteis na hora de achar um novo emprego; para outros, na hora de encontrar um namorado. E para a maioria deles, estes *sites* representam, no mínimo, uma forma divertida de interagir e potencializar suas conexões sociais. Assim, através das interações que subsidiam, eles se tornam fonte de informação sobre os mais variados assuntos, pessoas e lugares, e acabam por transformar nosso cotidiano, nossa visão de mundo e as oportunidades que nos estão disponíveis.

A idéia de instrumentalizar uma rede de indivíduos através da tecnologia computacional para permitir a interação e a comunicação entre elas não é algo novo. Acquisti e Gross (2005) identificam a presença dos precedentes deste conceito na construção do *Plato*, ferramenta desenvolvida na Universidade de Illinois na década de 60 para fins educacionais e que passou a dar suporte a dispositivos de comunicação para troca de *e-mail*, construção de fóruns, salas de *chat* e *instant messaging*. Ao longo dos anos, as ferramentas para suportar comunidades virtuais evoluíram, passando pelos antigos BBS's, pela *Usenet* e pelos clássicos canais de IRC, populares nas décadas de 80 e 90. Muitas diferenças técnicas, estruturais e culturais separam estas primeiras formas de comunicação em rede e o surgimento dos *sites* de rede social que conhecemos hoje. Mas de maneira geral, pode-se afirmar que foi só com o boom da *www* e com o surgimento comercial da Internet que estas redes puderam crescer em alcance e importância, se tornando um fenômeno mundial que agrega hoje a participação de milhões de pessoas. Assim, adotando um modelo que sucede a construção das antigas páginas

³⁶ <http://www.myspace.com/>.

³⁷ <http://www.facebook.com/>.

³⁸ <http://www.friendster.com/>.

³⁹ <http://www.linkedin.com/>.

⁴⁰ <http://www.bebo.com/>.

⁴¹ <http://www.orkut.com/>

pessoais, vários destes *sites* surgiram, com sofisticação de propostas e padrões de uso variados, visando a participação de um público geral ou se especializando em um segmento específico (a música no *MySpace*; atividade profissional no *LinkedIn*; o namoro no *Match.com* etc.).⁴²

É difícil precisar em que reside, afinal de contas, a fórmula de tamanho sucesso. Seja ela qual for, é indiscutível o fato de que estes *sites* acabaram por se tornar grandes estruturas de concentração na paisagem atual da Internet: muitos outros documentos apontam para eles; muitos dos usuários da rede os acessam diariamente, o que equivale a dizer que se tornaram grandes *hubs* ou pólos – nós com uma quantidade excepcional de *links* (BARABÁSI, 2003). Aliado ao fato de que estes *sites* tornam grande parcela de nossas vidas matéria pública – *i.e.*, publicamente arquivada – podemos dizer que eles configuram um novo e potente campo para a exposição e também para a coleta de dados sobre os comportamentos, performances, interações e interesses dos indivíduos.

O casamento quase perfeito entre a visibilidade maximizada e a grande predisposição dos indivíduos em revelar informações pessoais nesses *sites* forma uma conjuntura ambígua, que oferece os benefícios imediatos da sociabilidade em rede, que atende à demanda contemporânea pela exposição de si, mas que, ao mesmo tempo, subsidia as rotinas do acesso e do tratamento de dados por parte de uma audiência desconhecida, colocando em jogo questões sobre os riscos e sobre a nebulosidade das políticas de uso de dados pessoais que hoje trafegam livremente pelo ciberespaço.

Assim, o objetivo deste capítulo é situar o fenômeno das redes sociais, abordando suas características principais e voltando nossa atenção para as questões que envolvem a publicação e o uso dos dados pessoais nelas disponibilizados. Neste sentido, nossa argumentação vai de um questionamento do estatuto e das condições de participação na *web* 2.0 às dinâmicas da revelação de informações e da exposição de si nestes *sites*, passando pelos riscos subjacentes a estes processos. Neste sentido, vemos emergir toda a ambigüidade deste novo contexto, no qual os benefícios imediatos da participação e as dinâmicas da exposição de si figuram lado a lado com a possibilidade constante do acesso de terceiros a dados pessoais, subsidiando as rotinas da publicidade direcionada ou até mesmo o crime. Por fim, veremos como estas contradições se relacionam com a luta pela institucionalização dos formatos e práxis ligados ao trânsito de dados pessoais nas mídias sociais, encerradas nas discussões sobre as políticas da portabilidade. Desta forma, consideraremos como a interação

⁴² As redes sociais existentes somavam 380 em 2005 de acordo com o *Social Software Weblog*. Cf.: <http://socialsoftware.weblogsinc.com/2005/02/14/home-of-the-social-networking-services-meta-list/>.

em redes sociais agencia as delícias da compatibilidade e a tirania dos filtros em um universo mediado.

2.1 A evolução das redes sociais

Usamos aqui o termo “rede social” como simplificação da expressão “*site* de rede social”, emprestada da literatura em língua inglesa e assim definida por Boyd e Ellison (2007):

Definimos *sites* de rede social como serviços oferecidos através da rede mundial de computadores que permitem aos indivíduos (1) construir um perfil público ou semi-público dentro de um sistema delimitado, (2) articular uma lista de outros usuários com os quais ele compartilha interesses, e (3) visualizar e percorrer suas listas de conexões e aquelas disponibilizadas por outros dentro do sistema (BOYD e ELLISON, 2007: *online*, tradução nossa).⁴³

A origem desta nova modalidade de comunicação pode ser situada em 1997, quando foi lançado o *SixDegrees.com*, apontado como o primeiro *site* de rede social da Internet. No ano de 2000, apesar do sucesso de público, o *site* acabou por extinguir seus serviços devido à falta de viabilidade econômica do negócio. De lá pra cá, no entanto, o fenômeno das redes sociais só fez consolidar seu sucesso e de acordo com a argumentação de Boyd e Ellison (2007), podemos identificar três fases neste processo. Na primeira delas, de 1997 a 2000, vários *sites* que articulavam comunidades virtuais começaram a integrar progressivamente ferramentas de redes sociais, permitindo aos usuários que construíssem perfis e navegassem através das listas de amigos (este foi o caso de sítios como o *LiveJournal*,⁴⁴ o coreano *Cyworld*⁴⁵ ou os asiáticos *AsianAvenue*,⁴⁶ *BlackPlanet*⁴⁷ e *MiGente*⁴⁸). A segunda fase começou com o surgimento do *Ryze.com*⁴⁹ em 2001, e marcou o estreitamento dos laços das redes sociais com o mundo dos negócios. Surgiram assim o *Tribe.net*⁵⁰, o *LinkedIn* e o *Friendster*, todos a partir de iniciativas de pessoas profissionalmente e pessoalmente ligadas,

⁴³ Tradução nossa para: “We define social network sites as web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system. The nature and nomenclature of these connections may vary from site to site”.

⁴⁴ <http://www.livejournal.com/>.

⁴⁵ <http://www.cyworld.com/>.

⁴⁶ <http://www.asianave.com/>.

⁴⁷ <http://www.blackplanet.com/>.

⁴⁸ <http://www.migente.com/>.

⁴⁹ <http://www.ryze.com/>.

⁵⁰ <http://www.tribe.net/welcome>.

atuantes na cena das novas tecnologias e dos negócios de San Francisco. Por fim, depois do sucesso absurdo do *Friendster* e do declínio da rede devido tanto a divergências com usuários do *site* quanto à falta de estabilidade do serviço, temos um verdadeiro “boom” na cena das redes sociais: *sites* com estrutura baseada na centralidade dos perfis pipocam em diversos países, destinados a amplas audiências ou públicos especializados.

As duas redes sociais mais usadas em todo o mundo atualmente nascem depois do declínio do *Friendster*. O *MySpace*, lançado em 2003, tentou reproduzir o sucesso de seu antigo rival permitindo a participação de menores e principalmente oferecendo um espaço para as bandas de *indie rock* que estavam sendo banidas do *Friendster* na onda de tolerância zero com os *fakesters*.⁵¹ Junto com as bandas, vieram os fãs adolescentes e seus amigos, além do público adulto que migrava de outros *sites* (BOYD, 2006). O *site* se tornou um sucesso de público e, em julho de 2005, foi comprado pela *News Corporation* do magnata Rupert Murdoch, por US\$580 milhões. Ao contrário do *MySpace*, que visava integrar qualquer participante em qualquer lugar do mundo, os objetivos e a abordagem do *Facebook* foram bem diferentes. Ele surgiu em 2004, criado por Mark Zuckerberg e focado em atender às demandas de um público específico: alunos da universidade americana de Harvard. Assim, ele se diferencia por ter sido projetado para atender a uma comunidade local pré-existente, que compartilhava um espaço físico comum nos campus, refeitórios, dormitórios e salas de aula (CASSIDY, 2006: *online*). Depois de proliferar por outras instituições de ensino superior e chegar também às escolas de ensino médio e às empresas, o *site* tornou a participação aberta a qualquer um em setembro de 2005, e tem experimentado um crescimento significativo no número de participantes desde então.

Com tantos *sites* e tantas opções, a briga pela liderança na cena das redes sociais nunca esteve mais acirrada. Em março de 2007, enquanto o *MySpace* já sustentava mais de 100 milhões de visitantes únicos/mês, o *Facebook* contava com modestos 30 milhões, e perdia de longe para o seu grande rival também em relação ao número de usuários cadastrados. Nesta época, seria difícil prever que, depois de crescer a uma estrondosa taxa de 3% por semana,⁵² no mês de maio de 2008, pela primeira vez, o *Facebook* bateria o *MySpace*

⁵¹ O termo designa os perfis *fakes* que invadiram o *Friendster* no decorrer do desenvolvimento do *site*. Eles incluíam celebridades, personagens, objetos, ícones, instituições e idéias. Permitiam, assim, o estabelecimento de conexões entre os indivíduos a partir do compartilhamento de interesses comuns. Ao mesmo tempo, satisfaziam o interesse dos usuários de ter mais amigos e acessar mais perfis, driblando a limitação técnica segundo a qual só era possível visualizar perfis que se localizassem até a quatro graus de distância de um usuário qualquer (amigos de amigos de amigos de amigos). Esta prática irritou a empresa, que acabou por extinguir todos os *fakesters* do *site* (BOYD, 2006: *online*).

⁵² Segundo dados do *Forrester* citados pelo *Techradar*, disponíveis em: <http://techradar1.wordpress.com/2008/01/11/facebookmyspace-statistics/>.

em número de visitantes únicos: de acordo com os dados da *comScore*, o *site* registrou a marca de 123,9 milhões de visitantes únicos no referido mês, contra 114,6 milhões do seu rival.⁵³ O número de páginas visualizadas no *Facebook* também foi maior: 50,6 bilhões contra 45,4 bilhões do *MySpace*. Segundo dados do próprio *Facebook*⁵⁴, o *site* tem hoje versões traduzidas para 35 línguas e mais de 140 milhões de usuários ativos, que gastam juntos 2,6 bilhões de minutos no *site* a cada dia. Assim, mais que um gigante em terra de gigantes, o *Facebook* se tornou, simplesmente, o *site* de rede social com o maior número de visitantes únicos no ano de 2008, figurando entre os sítios mais acessados da Internet em todo o mundo.

2.2 Redes: estrutura e abordagem

A definição matemática do termo rede aponta para um grupo de elementos, denominados nós ou vértices, conectados por arestas ou *links* (NEWMAN, 2003: 168). O estudo deste fenômeno possui precedentes em diversas áreas do conhecimento. Historicamente, seus conceitos fundamentais foram tomados da teoria dos grafos, introduzida pelo matemático Leonhard Euler (1707-1783) e da mecânica estatística, especialmente a partir do interesse dos cientistas na compreensão da cinética dos gases. Foi por volta de 1930 que as redes se tornaram objeto de análise também na área da sociologia,⁵⁵ marcando a evolução de um processo que culmina hoje com uma mudança fundamental: ao longo dos anos, o foco do estudo das redes passou da consideração da topologia e propriedades de *links* e nós, concebidos enquanto estruturas estáticas, para a abordagem das regras e da estrutura de funcionamento, criação e evolução de redes dinâmicas, que se auto-organizam e se modificam ativamente (BARABÁSI, 2003). Esta evolução nos trouxe a compreensão global de que vivemos em um mundo densamente interconectado, no qual diferentes fenômenos, da interação social à organização do tráfego aéreo, podem ser estudados, modelados e usados para explicar um ao outro por possuírem uma estrutura comum.

Neste contexto, a emergência da Internet – pela sua capacidade de registro e pela

⁵³ Os dados estão reproduzidos em: http://news.cnet.com/8301-13577_3-9973826-36.html. Cf. Anexo A, Fig. 2, p.190.

⁵⁴ Estes dados estão disponíveis em: <http://www.facebook.com/press/info.php?statistics>.

⁵⁵ Ainda que as relações entre o campo da sociologia e o estudo das redes tenham se aprofundado a partir da década de 30 do século XX, é importante ressaltar que as ciências sociais já se interessavam por esta temática pelo menos desde o século XIX. Neste período, merecem destaque os trabalhos de Saint Simon (1760-1825), que concebia a cidade como um organismo vivo, permeado por redes materiais (que direcionavam fluxos de energia e matéria-prima) e espirituais (através das quais circulava o dinheiro). Segundo Lemos (2005:14), seus trabalhos acabaram por influenciar não só a sociologia urbana da Escola de Chicago no início do século XX como também a atual emergência das redes telemáticas.

conseqüente facilidade no tratamento de dados referentes à sua composição e estrutura – representa uma possibilidade inédita de compreensão do fenômeno das redes, suas características e padrões, que uma vez conhecidos, podem ser aplicados a todos os sistemas cuja estrutura seja recorrente, sejam eles sintéticos ou naturais. E não seria diferente para o caso dos *sites* de rede social. Ainda que, obviamente, a interação tecnologicamente mediada introduza novos elementos ao convívio social, podemos dizer que estes *sites* encerram mapeamentos espontâneos do comportamento humano e da vida em sociedade. Eles fornecem uma estrutura visual para as redes de relações existentes entre os indivíduos e permitem a terceiros navegarem por esses *links* sociais, constatando a direção das ligações estabelecidas e a presença ou a ausência de focos de pertencimento ou interesses comuns que as sustentem. E uma vez que a maior parte destes *sites* são públicos, à medida que os indivíduos revelam informações sobre seus gostos, interesses e sobre como eles se sentem em relação a si próprios e ao mundo em que se inserem, um grande espaço se abre seja para cientistas interessados na estrutura do fenômeno social ou para empresas interessadas em compreender seus padrões de gosto e consumo.

Grande parte dos conceitos usados hoje para a abordagem dos *sites* de relacionamento vem da metodologia de análise de redes sociais, um campo de estudos multidisciplinar com raízes nas áreas da sociologia, psicologia e antropologia. Ela se caracteriza pelo foco de estudo dirigido aos padrões de relacionamento estabelecidos entre pessoas ou entidades. Em oposição a uma abordagem individualista, na qual considera-se que os indivíduos tomem suas decisões sem nenhum grau de afetação decorrente do meio social em que se inserem, este tipo de análise visa precisar e descrever a formação, o fluxo de informações e os padrões emergentes nas estruturas em rede, de modo a considerar como o comportamento individual é afetado pela participação dos indivíduos no contexto social. (KNOKE e YANG, 2008: 4; GARTON, HAYTHORNTHWAITE e WELLMAN, 1997: *online*). Assim, ao estudar as relações estruturais – porque elas ocorrem e quais suas conseqüências – a abordagem de redes sociais se interessa não pelos atributos ou valores dos indivíduos que conferem coesão à estrutura social mas sim, pelas regularidades presentes em seus padrões de relacionamento e pela maneira através da qual comportamentos e escolhas locais podem gerar mudanças estruturais macro-observáveis (KNOKE e YANG, 2008: 5-6).

Consideremos agora a relação entre a noção de rede e o processo de comunicação que encontra seu lugar nos *sites* de rede social. Uma rede social possui dois elementos fundamentais: atores (indivíduos, grupos formais ou organizações informais) e relações (conexões estabelecidas entre os indivíduos) (KNOKE e YANG, 2008: 6-7). Para o contexto

dos *sites* de rede social, consideremos que “assim como uma rede de computadores é um conjunto de máquinas conectadas por uma série de cabos, uma rede social é um conjunto de pessoas [...] conectadas por uma série de relações sociais como amizade, relações de trabalho ou troca de informações” (GARTON, HAYTHORNTHWAITHE e WELLMAN, 1997: *online*, tradução nossa).⁵⁶ Wasserman e Faust (1994: 18) denominam estas conexões de laços sociais, responsáveis por estabelecer as ligações entre os pares de atores. Esses laços podem descrever diversos tipos de relações e possuírem diferentes graus de intensidade. No contexto de um *site* de rede social, por exemplo, os laços podem se caracterizar pelo pertencimento a um mesmo tópico de interesse (na estrutura das comunidades e grupos), pela troca de mensagens (privadas ou através das ferramentas de comentário) e, é claro, pelo estabelecimento de uma relação de amizade.

Ainda que nossa análise não esteja centrada no uso de ferramentas de análise de rede, acreditamos que os conceitos e a abordagem da análise estrutural podem contribuir para o direcionamento das questões deste trabalho. Inicialmente, consideremos que a vigilância nas redes sociais depende de dois fatores principais: a) a revelação de informações pelos indivíduos e, por conseguinte, os fatores que a influenciam; b) as formas através das quais os dados disponibilizados podem fluir de um nó a outro da rede, assim como as motivações que podem levar à sua captura e/ou uso para determinadas propostas. Desta forma, acreditamos que a estrutura dos *sites* de rede social também deva ser considerada nesta dinâmica, afinal, ela influencia tanto o comportamento dos indivíduos quanto o fluxo de informações que se dá através dela. Inicialmente, podemos considerar esta assertiva com um embate entre as escolhas e objetivos dos indivíduos, por um lado, e o controle exercido pela rede, por outro. No entanto, na visão da análise estrutural (DEGENNE e FORSÉ, 1999), tanto o comportamento dos indivíduos e grupos influencia a estrutura da rede quanto a própria estrutura da rede, emergente a partir das interações entre estes indivíduos e grupos, lança constrangimentos e restrições sobre os comportamentos individuais.

Normas derivam da posição estrutural de indivíduos e grupos, porque esta posição é suficiente para determinar as oportunidades e limitações que influenciam a alocação de recursos e para explicar as regularidades de comportamento observadas. E isto ocorre não por conta de uma relação abstrata com o todo, mas por conta das relações concretas entre indivíduos que moldam a estrutura e explicam porque alguns têm acesso mais

⁵⁶ Tradução nossa para: “Just as a computer network is a set of machines connected by a set of cables, a social network is a set of people [...] connected by a set of social relationships, such as friendship, co-working or information exchange”.

facilitado a certos recursos do que outros (DEGENNE e FORSÉ, 1999: 3, tradução nossa).⁵⁷

Neste sentido, ao preterir tanto pela primazia das escolhas individuais autônomas e atomizadas quanto por uma ditadura do contexto social sobre as ações e escolhas humanas, a análise estrutural de redes sociais pode voltar nossa atenção para este processo de relações mútuas através do qual tanto as dinâmicas de revelação de informações quanto o fluxo e a visibilidade das informações na rede influenciam e são influenciados por sua estrutura. Desta forma, como pretendemos explorar no decorrer deste trabalho, acreditamos que este processo pode ser relacionado com as formas de controle que podem se tornar possíveis nestas redes.

2.3 A web 2.0 e as redes sociais

Não seria exagero afirmar que a sociedade em que vivemos foi tomada por uma verdadeira “panacéia colaborativa”. As empresas descobrem o poder de modelos mais abertos e menos hierárquicos de gestão (TAPSCOTT e WILLIAMS, 2007). A ciência avança e a compreensão do fenômeno das redes nos prepara para um mundo em que devemos perceber as relações, seja na Física, na Biologia ou na Matemática (BARABÁSI, 2003). E a comunicação, por sua vez, se vê às voltas com o discurso da participação e do empoderamento dos antigos espectadores, agora convertidos em sujeitos ativos e autônomos prontos a emitir suas mensagens graças ao poder libertador das novas tecnologias digitais e em rede. Assim, a colaboração se tornou uma tendência recorrente no discurso e abordagem sobre as características e potencialidades da rede mundial de computadores, seja no contexto das comunidades virtuais, da produção de conhecimento ou de outros tipos de interação mediada por computador. O que nos interessa, para a perspectiva deste trabalho, é questionar em que medida a premissa da participação e a configuração do que se convencionou chamar *web 2.0* (O'REILLY, 2005) influenciam e modificam a estrutura das comunidades virtuais e como esta transformação se relaciona com as formas de vigilância que nelas se tornam possíveis.

Como nos relembra Antoun (2008: 11), o debate acerca das transformações que o modelo de comunicação distribuído da Internet estaria instaurando no tradicional aparato da

⁵⁷ Tradução nossa para: “Norms arise from the structural position of individuals or groups, because this position is sufficient to determine opportunities and constraints which influence the allocation of resources and to explain the behavioural regularities observed. And this is so not because of an abstract relation to the whole, but because of concrete relations between individuals which shape the structure and explain why some have easier access to certain resources than others”.

mídia massiva remonta aos anos 80 e 90. Com o passar dos anos, uma visão libertadora – e porque não dizer libertária – veio consolidar e celebrar a anarquia das trocas, as subversões dos ativistas, as criações do *net.artistas*, a engenhosidade dos *hackers* e, sobretudo, a autonomia da participação disponível ao cidadão comum. Agora, subitamente, todos nós somos importantes, quase famosos. Opinamos e ajudamos a pautar a grande mídia, nos exibimos nas redes sociais e somos confrontados a todo instante com a lógica do “colabore, por favor”: “mande sua foto”, “conte-nos a sua experiência”, “ajude-nos a aperfeiçoar nossos serviços e produtos”. No entanto, um olhar mais cuidadoso sobre a evolução recente da *web* nos confronta com um arsenal de dúvidas. Com quem estamos, de fato, colaborando? O que há por trás dos benefícios imediatos de uma interação proposta? Diante destas perguntas, fica mais clara a idéia de que a natureza desta onda participativa guarda relações com formas de controle próprias à estrutura das redes e características das sociedades contemporâneas (GALLOWAY e THACKER, 2007; ANDREJEVIC, 2007).

A discussão sobre a *web 2.0* (O'REILLY, 2005) pode ser situada na passagem dos anos 1990 ao início do século, em discussões concentradas no *site Cluetrain Manifesto*, que se propôs pensar as transformações que as comunicações e o mundo dos negócios estavam sofrendo neste novo meio (ANTOUN, 2008: 11). Embora não exista consenso sobre o uso do termo, a idéia básica é de que a Internet estaria experimentando um processo de evolução através do qual os *websites* estáticos e autônomos estariam dando lugar a uma plataforma global para a colaboração, compartilhamento e gestão coletiva da informação. Segundo Primo (2008: 101), “a *web 2.0* é a segunda geração de serviços *online* e caracteriza-se por potencializar as formas de publicação, compartilhamento e organização de informações, além de ampliar os espaços para a interação entre os participantes do processo”. De modo geral, a acepção empírica do termo gira em torno da idéia de que, em um *site* tradicional, o internauta poderia ter acesso às informações, mas não poderia interagir com elas, ou seja, não poderia modificá-las, complementá-las ou comentá-las. Como resumem Tapscott e Williams (2007: 53), “[...] estejam as pessoas criando, compartilhando ou socializando, a nova *web* significa, sobretudo, participar em vez de receber passivamente informações”.

Algumas características dessa nova *web* nos permitem associá-la à questão da vigilância no ciberespaço e ao trânsito de dados individuais. A primeira diz respeito à premissa da *web* como plataforma (O'REILLY, 2005), um indicativo de que as funções que antes dependiam da instalação de *softwares* específicos em uma determinada máquina local podem agora ser realizadas *online* através de servidores remotos. As contas de *webmail* são um caso clássico. O subtexto de tal premissa é que, apesar das vantagens aparentes deste

processo – afinal, para que gastar espaço em disco no meu computador se posso armazenar dados em servidores de terceiros? – tal atitude significa deixar cada vez mais informações sobre suas comunicações e transações registradas em locais que, em parte, você desconhece. A segunda característica diz respeito à arquitetura da participação e à ação da inteligência coletiva: na *web 2.0*, o uso agrega valor, de modo que os serviços oferecidos se tornam melhores quanto mais as pessoas os usam (O'REILLY, 2005). Assim, ao imperativo da circulação, inerente à *web 1.0*, acrescenta-se o da participação, de modo a se deduzir valor para a coletividade enquanto bi-produto do trabalho realizado em rede. Para o caso dos *sites* de rede social, o uso do serviço, que significaria também seu aprimoramento, pode ser praticamente equacionado em termos de revelação de informações. Quanto mais você experimenta os novos aplicativos do *Facebook* e as novidades do *site*, mais informações sobre você estão sendo disponibilizadas a uma audiência virtual, que pode incluir agentes do *marketing*, *spammers*, e assim por diante.

A *web 2.0* significa também a adição de novas formas de mediação aos processos comunicativos que se passam na rede. A facilidade de se publicar informações sem depender de conhecimentos técnicos apurados e da manipulação direta de códigos de programação, que está na base de sua abrangência, significa a adição de novas camadas de *software* que estabelecem as regras para a interação dos indivíduos. Por um lado, esta mudança pode estar associada a maior grau de controle das ações no ciberespaço, pois os modelos usados são pré-programados e seus padrões de interação não são questionados ou colocados em jogo por aqueles que os usam. Por outro lado, desta facilidade de produção de conteúdos resulta o crescimento vertiginoso da própria Internet e da massa de informações que a compõe, o que significa que mais pessoas estão revelando mais informações sobre suas preferências, tendências, interesses e histórias de vida, seja de maneira direta, em seus *weblogs* ou nos *sites* de rede social, ou de maneira indireta, ao realizar compras e transações na rede.

Além disso, a *web 2.0* é marcada por um trabalho colaborativo de natureza meta, ou seja, que diz respeito a inúmeras formas de organização e recuperação da informação baseadas em classificações que surgem a partir da interação dos próprios usuários. Em geral, esses procedimentos de classificação permitem a seleção, segundo determinados critérios, desta grande massa informativa e a posterior recuperação da informação segundo determinados padrões. É o que acontece, por exemplo, quando um usuário do *Facebook* resolve “marcar” um usuário em uma foto de seu álbum, transformando-a em um *link* que dá acesso ao perfil da pessoa que aparece na imagem considerada. Neste caso, a inserção de uma *tag* tem a ver com a reprodução das redes de relações dos indivíduos também através das

fotos que eles colocam em seus perfis, o que se torna possível a partir de um mecanismo de identificação e estabelecimento de “lincagens” que não é *top-down*, mas *bottom-up*. Afinal, esta rede de relações emerge de iniciativas descentralizadas de indivíduos diversos que querem dizer algo sobre si próprios ao mostrarem suas conexões sociais ou facilitarem o processo de identificação daqueles presentes em uma determinada foto por terceiros. Assim, trata-se de uma modalidade de disponibilização de informações indireta e colaborativa, através da qual se torna possível a qualquer participante publicar dados sobre terceiros e contribuir para o reconhecimento e associação de todos os usuários às suas imagens que estão espalhadas pela rede, quer eles saibam de sua existência quer não.

No contexto da *web 2.0*, as comunidades virtuais também se reconfiguram, e deixam de girar em torno de interesses comuns (RHEINGOLD, 1993), do compartilhamento de interesses em torno de um tema específico, como nos antigos BBS's (*Bulletin Board Systems*)⁵⁸ e nos clássicos grupos de discussão e fóruns da rede. No lugar deste modelo, emergem as redes egocêntricas do *buzz*⁵⁹ e do *marketing* viral. Grosso modo, é a lógica das correntes: um apelo para que alguém repasse uma informação baseando-se não no fato de o conteúdo ser adequado ou interessante àquela determinada pessoa, mas em uma suposição de que ela estaria interessada em recebê-lo simplesmente porque é seu amigo (BOYD, 2006: *online*).

A emergência dos *sites* de rede social indica uma mudança na organização das comunidades *online*. Ainda que os *sites* dedicados a comunidades de interesse ainda existam e prosperem, os *sites* de rede social são primeiramente organizados em torno de pessoas, e não de interesses. As primeiras comunidades *online* como a *Usenet* e os fóruns de discussão eram estruturados por tópicos ou de acordo com hierarquias, mas os *sites* de rede social são estruturados como redes pessoais (ou egocêntricas), nas quais o indivíduo é o centro de sua própria comunidade (BOYD e ELLISON, 2007: *online*, tradução nossa).⁶⁰

⁵⁸ Os BBS's forneciam interfaces textuais para o *download* de dados e *softwares*. Ofereciam também serviço de *chat* e de troca de mensagens entre seus participantes. Atividades como jogos *online* e participação em fóruns de discussão também eram possíveis nestas redes, que estão entre as primeiras comunidades virtuais da Internet. O sistema era acessado via linha telefônica ou via TELNET (*TELEtype NETwork* – protocolo computacional que permite o acesso remoto e em tempo real a um computador interligado à rede). Assim, dado o alto custo das ligações telefônicas de longa distância, os BBS's congregavam, em sua maioria, pessoas de uma mesma localidade. Muito populares nas décadas de 80 e 90, essas redes declinaram a partir da popularização da *World Wide Web*. Cf. WIKIPEDIA: *online*.

⁵⁹ Uma tradução literal para *buzz* seria “burburinho”. Na esfera do *marketing*, o termo designa estratégias que visam promover a multiplicação espontânea ou planejada de uma mensagem através do corpo social, visando o crescimento exponencial do alcance de um serviço ou produto. De acordo com Lima (2008: *online*) o termo se aproxima da definição de *marketing* viral na medida em que também visa promover o espalhe eficiente de vírus de informação. No entanto, para ele, o *buzz* pode ser difundido por qualquer meio, físico ou digital, enquanto o *marketing* viral é distribuído pela Internet.

⁶⁰ Tradução nossa para: “The rise of SNSs indicates a shift in the organization of online communities. While websites dedicated to communities of interest still exist and prosper, SNSs are primarily organized around people, not interests. Early public online communities such as Usenet and public discussion forums were

Neste percurso, a *web* que esteve intimamente associada ao zapatismo e às lutas de *Seattle* no fim dos anos 90 e que reunia movimentos em torno de uma luta comum ou de uma atividade comum (AUNTOUN, 2008: 20) cedeu espaço ao modelo dos *blogs* e redes sociais, um *playground* para a relação harmônica e cooperativa das empresas com seus mercados autônomos e genuinamente interessados (LEVINE, LOCKE, SEARKS e WEINBERGER, 2000). Neste processo, a gestão coletiva dos meios apropriados e criados pelos usuários no antigo modelo da *web* dá lugar à participação com menu, à customização de formas comuns (o seu *weblog*, o seu perfil) que são “suas”, mas que lhe são oferecidas por empresas para a qual a *web* também é um negócio, e que como tal, deve ser lucrativo. Isso nos faz lembrar dos antigos canais de IRC (*Internet Relay Chat*)⁶¹ e de sua substituição pelas redes sociais. Guardadas as devidas diferenças, visto que o IRC era um protocolo para comunicação sincrônica (*instant messaging*) e que as redes sociais colocam em jogo um novo formato e novas formas para a expressão pessoal, temos a passagem de um modelo em que a mediação proprietária era praticamente invisível para um modelo em que os serviços são pagos com a exposição personalizada a conteúdos publicitários a partir de técnicas de mineração de dados e *profiling*.⁶²

2.4 Estrutura e características principais

Três estruturas principais caracterizam os *sites* de rede social, a saber, os perfis, as listas de amigos e as ferramentas de comentários (BOYD, 2007a: 2). De maneira geral, a participação começa com o cadastro e o direcionamento dos usuários para a criação de sua página pessoal, na qual se representarão a partir das ferramentas disponíveis. Comumente, um perfil possui guias de informação que abarcam dados pessoais como idade e localização, dados sobre preferências e interesses (filmes, músicas, programas de TV) e um campo mais subjetivo, de preenchimento livre, no estilo “*about me*”. A liberdade de customização do *layout* e de adição de módulos ao perfil (os chamados aplicativos) varia de *site* para *site*,

structured by topics or according to topical hierarchies, but social network sites are structured as personal (or ‘egocentric’) networks, with the individual at the center of their own community”.

⁶¹ O IRC é uma forma de comunicação sincrônica através da Internet (*chat*), que permite a interação entre os participantes basicamente através de um canal – que funciona como um fórum público de discussão no qual todas as mensagens são vistas por todos os demais participantes – e de mensagens privadas, trocadas por dois indivíduos.

⁶² No Brasil, por exemplo, nos anos 90, os servidores de IRC eram mantidos por provedores que visavam apenas fomentar o uso da Internet e ganhar indiretamente através da adesão de novos usuários. Raramente anunciavam seus serviços no canal, enviando uma mensagem visível a todos os usuários. Já o alto custo de banda envolvido no tráfego de vídeos, fotos e dados nas redes sociais exigiu um modelo proprietário, em que grandes companhias mantêm os serviços oferecidos, atuando como uma mediação mais presente e visível.

assim como a liberdade para publicar vídeos e fotos. É importante esclarecer que, muitas vezes, o termo perfil é usado de maneira genérica, para indicar a página de um usuário em uma rede social, com todas as ferramentas que a integram e todas as informações publicadas através das interações possibilitadas por cada uma delas. Esta denominação, aliás, faz todo sentido, uma vez que a representação dos indivíduos nestes *sites* não deriva apenas das informações concentradas no formulário de autodescrição, e sim de todos os signos presentes na página de cada um deles.

Além do perfil, os *sites* de rede social também se caracterizam pela presença das listas de amigos e das ferramentas de comentário. Uma vez que o usuário tenha criado o seu perfil, é possível adicionar ou aceitar outros usuários como amigos. A relação de amizade exige, na maior parte dos casos, confirmação bi-lateral, o que significa que uma das partes faz o convite e a outra pode recusá-lo, aceitá-lo ou ignorá-lo, conforme sua predisposição. Cada vez que um novo *link* é estabelecido, uma nova pessoa é adicionada às listas dos amigos, exibidas na página de cada usuário. E cada vez que um usuário acessa a página de um amigo, são exibidos os amigos que eles possuem em comum. A liberdade para percorrer essas listas e visualizar os perfis para os quais elas apontam varia de acordo com as configurações de privacidade dos usuários e com a arquitetura de visibilidade do *site* em questão. Por fim, os *sites* de rede social também se caracterizam pela presença das ferramentas de comentário, inicialmente projetadas com a função de permitir aos usuários escreverem testemunhos sobre seus amigos para que estranhos pudessem ler. No entanto, sua apropriação pelos usuários indicou uma nova forma de uso, a de conversação pública sobre assuntos cotidianos. Ainda que muitos *sites* de rede social possuam também recursos para a troca de mensagens privadas entre seus usuários, esta forma de uso do recurso de comentário é predominante na maioria deles.

De maneira geral, a criação de um perfil em um *site* de rede social passa pelo processo de compreensão dos códigos sociais vigentes – *i.e.*, dos limites do que é ou não bem-vindo e aceitável enquanto comportamento esperado por aquela comunidade – e por estratégias de exposição de si – *i.e.*, pela escolha de como se apresentar aos outros neste novo ambiente. Goffman (1959), usando a noção de performance, tal como concebida em sua dimensão teatral, desenvolve o conceito de *impression management* para se referir às estratégias empregadas cotidianamente pelos indivíduos para produzir uma boa impressão naqueles com quem interagem. Segundo o autor, esta noção se refere aos esforços – conscientes ou inconscientes – empenhados pelos atores para controlar as informações colocadas em jogo em um processo de interação social, de modo a gerenciar e influenciar positivamente a opinião dos seus interlocutores. Ainda que o fator tecnologia esteja ausente das análises do autor, que

remontam à década de 1950 e foram pensadas considerando a interação como um fenômeno co-presencial, alguns pontos de continuidade e rupturas podem ser assinalados.

Nas redes sociais temos um contexto de comunicação assíncrona, no qual as ferramentas disponíveis para a interação entre os atores se modificam. Nelas, os gestos, a expressão facial e outras características próprias às situações co-presenciais cedem espaço para estratégias comunicativas que vão do uso de um simples *emoticon* ao compartilhamento de mídia (fotos, vídeos, jogos e aplicativos). Assim, nas redes sociais, o “*personal front*” – termo usado por Goffman (1959: 24) para se referir às características fixas que acompanham o indivíduo, como a idade, sexo, tipo físico etc. – é recriado. Agora, estes atributos são transmitidos através de fotos e da descrição textual presente na guia de informações do perfil, enquanto as características mutáveis são agora comunicadas não mais de maneira imediata, mas de maneira assíncrona através do *upload* de status ou de aplicativos como o *SuperPoke* (que permite aos usuários expressarem sentimentos e mudanças de humor). No entanto, ainda assim, podemos dizer que as redes sociais permitem aos indivíduos o gerenciamento de impressões, por três motivos principais: a) os perfis permitem a expressão dos atores e as inferências sobre sua personalidade por parte da sua audiência; b) os perfis permitem aos atores receberem *feedback* sobre suas performances (o que acontece através das ferramentas de comentário, por exemplo, através da qual amigos escreverão o que acharam da mudança da foto de seu perfil, por exemplo).

Neste sentido, os perfis desempenham a função de performances virtuais identitárias (BOYD, 2007a: 11-2). Através deles, os atores visam produzir realidades sobre si e fazê-las críveis para suas audiências. Boyd (2007a: 12) ressalta dois aspectos importantes deste processo. Por um lado, podemos afirmar que, nos *sites* de rede social, os indivíduos têm mais controle sobre suas performances, uma vez que eles podem escolher como se comunicar com os outros e que tipo de informação revelar sobre si (freqüentemente excluindo fatos desagradáveis sobre suas vidas e personalidades). Por outro lado, a autora considera que, comparados à atuação presencial dos indivíduos, os perfis são representações limitadas, o que faz com que enganos e erros de comunicação possam ocorrer. Isto aconteceria porque, enquanto nos ambientes concretos nosso corpo, voz, postura e expressões desempenham a função imediata de transmitir aos outros nossas predisposições, intenções, sentimentos e personalidade, nos ambientes digitais estas dicas fornecidas pelo contexto não são comunicadas facilmente pelos indivíduos (DWYER, 2007: 1).

O estabelecimento de relações entre os membros é outro componente fundamental dos *sites* de rede social. Os tipos de pessoas que marcamos como amigos e as razões pelas quais

fazemos isso variam imensamente, de modo que nossas conexões podem ser resultado de um convite interessante vindo de um completo desconhecido ou significar a reafirmação de uma amizade de longos anos (BOYD e DONATH, 2004). Assim, no contexto dos *sites* de rede social, a noção de amizade adquire novo sentido. No mundo *offline*, tendemos a separar nossos amigos (aqueles com quem realmente contamos em momentos de adversidade e que julgamos ser pessoas bem próximas a nós) dos que são apenas nossos conhecidos. No entanto, em um *site* de rede social, todas as nuances dos diferentes graus de envolvimento que podemos estabelecer com as pessoas são reduzidas a uma relação binária: amigo ou não amigo (BOYD e DONATH, 2004). Uma única categoria passa então a englobar relações diversas, à medida que adicionamos ou não nossos familiares, antigos amigos da escola ou da faculdade, professores, colegas de trabalho, desconhecidos e até mesmo pessoas públicas que admiramos (bandas, celebridades etc.).

Os componentes técnicos do sistema, o custo social de rejeitar alguém quando se é adicionado como amigo e a arquitetura de visibilidade do *site* em questão influenciam o comportamento dos usuários em relação à noção de amizade. No entanto, como em uma rede social o estabelecimento de laços é sempre uma escolha tornada pública, podemos afirmar que esta decisão está implicada nos processos de construção da imagem dos indivíduos, uma vez que suas conexões sociais são apresentadas enquanto parte do ritual de mostrar-se aos outros (BOYD e DONATH, 2004). Assim, ao serem exibidas nas páginas dos usuários, as listas de amigos, assim como as guias de informação do perfil, fornecem informações sobre suas personalidades, permitindo aos seus pares julgá-los de diversas formas, avaliando ou não o seu pertencimento a um determinado tipo de comportamento, atitude ou grupo, em um processo que reforça as guias de identidade coletiva, operando e reafirmando cisões dentro destes *sites* (BOYD e DONATH, 2004).

Assim, a expressão de gostos e interesses subsidia processos de reconhecimento mútuo e associação, através dos quais os indivíduos articulam o seu senso de pertencimento e constroem sua percepção global de como é e como se articula a comunidade em que interagem. Afinal, já que é impossível conhecer toda a extensão deste novo ambiente e precisar o público ao qual se dirigem, os usuários destas redes precisam imaginar a sua extensão, a fim de que possam direcionar seus esforços no processo de construir-se digitalmente. Assim, como ressaltam Boyd e Donath (2004), uma diferença fundamental dos *sites* de rede social em relação às interações *offline* é o fato de que, neles, o contexto – responsável por ditar as predisposições dos indivíduos sobre como agir em determinado ambiente – é dado pelas listas de amigos, das quais se pode inferir muita informação sobre

suas personalidades, seu estilo ou sua “tribo”. Como resumem Boyd e Donath, “[...] status social, crença política, gosto musical etc., podem ser inferidos da companhia que mantemos” (2004: 72, tradução nossa).⁶³ E como veremos a seguir, este processo de conceber a amplitude da rede e da audiência com a qual interagimos e à qual se dirigem nossas performances é fundamental para a mensuração das conseqüências do processo de revelar informações nos *sites* de rede social.

2.5 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 e GROSS, 2005: 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 e GROSS, 2005; JONES e SOLTREN, 2005; STUZMAN, 2006; GOVANI e PASHLEY, 2005; JONES *et al.*, 2008; STRATER e 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.

Em primeiro lugar, a revelação de informações nos *sites* de rede social está ligada ao alcance e à visibilidade dos dados em questão. Neste sentido, como ressaltam Acquisti e Gross (2005: 3), é importante considerar que as redes sociais são, por natureza, mais amplas do que as redes que sustamos em nosso convívio social cotidiano, *i.e.*, *offline*. Citando Strahilevitz (2004) e Boyd e Donath (2004), os autores argumentam que, enquanto uma rede *offline* sustenta, em geral, algumas dezenas de laços significantes (estabelecidos com aqueles que nos são mais íntimos) e cerca de 1000 a 1700 laços fracos (estabelecidos com aqueles que

⁶³ Tradução nossa para: “[...] social status, political beliefs, musical taste, etc., may be inferred from the company one keeps”.

são apenas nossos colegas ou conhecidos), um *site* de rede social nos conecta em média a um número bem maior de pessoas. Isto se deve, em parte, à facilidade estrutural de fazer novas conexões e ao baixíssimo esforço necessário ao estabelecimento de uma relação de amizade – afinal, bastam apenas alguns poucos cliques. Além disso, a pretensa segurança derivada da idéia de que a amizade é apenas uma conexão virtual – e, portanto, sem maiores consequências sobre nossas vidas “reais” – pode contribuir para que os possíveis benefícios de aceitar um estranho como amigo pareçam maiores do que os possíveis riscos associados a este processo. E a cada novo amigo, temos novos amigos de amigos, e assim por diante, o que faz nossas conexões se multiplicarem rapidamente. Neste sentido, Boyd e Donath lançam a hipótese de que:

[...] o número de laços fortes que um indivíduo é capaz de manter pode não ser significativamente aumentado pelas tecnologias de comunicação [...], mas que o número de laços fracos que alguém pode formar e manter é capaz de crescer substancialmente, por conta do tipo de comunicação que passa a acontecer de maneira mais barata e fácil com as novas tecnologias que são bem adequadas para estes laços (BOYD e DONATH, 2004: 80, tradução nossa).⁶⁴

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 que terceiros acessem um dado perfil. 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).

⁶⁴ Tradução nossa para: “[...] the number of strong ties an individual can maintain may not be greatly increased by communication technology [...], but that the number of weak ties one can form and maintain may be able to increase substantially, because the type of communication that can be done more cheaply and easily with new technology is well suited for these ties”.

A visibilidade das informações que os indivíduos disponibilizam nestes *sites* pode ser abordada através da noção de “públicos em rede”, desenvolvida por Boyd (2007a: 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, potencializando 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: 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 vezes, 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 e DONATH, 2004: 78, tradução nossa).⁶⁵

⁶⁵ 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”.

A revelação de informações nos *sites* de rede 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 e GROSS, 2005).⁶⁶ No entanto, é importante ressaltar que o uso destes *sites* e 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 o 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 e DONATH, 2004: 73-4). 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 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 e DONATH, 2004: 74, tradução nossa).⁶⁷

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 consequências 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

⁶⁶ 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.

⁶⁷ 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”.

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 e DONATH, 2004: 76) 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*,⁶⁸ *blackmailing*, vírus, *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 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 histórico 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

⁶⁸ 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.

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 identificar os demais dados disponibilizados. Desta forma, 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 e GROSS, 2005), além de outros menos óbvios relacionados ao uso de drogas e bebidas, por exemplo (JONES e SOLTREN, 2005: 27). Merecem destaque ainda os estudos de Jagatic *et al.* (2007), que coletaram dados sobre as redes de relações de alunos da Universidade de Indiana disponíveis em *sites* de rede social e mostraram como essas informações podem aumentar o sucesso de um ataque *phishing*.⁶⁹

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 e GROSS, 2005: 73).

Um estudo mais aprofundado destas questões será realizado no próximo capítulo. Por ora, 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 e GROSS, 2006: 2, tradução

⁶⁹ Neste estudo, os autores enviaram um *e-mail* malicioso tanto de um remetente desconhecido da Universidade de Indiana 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 *phisher*.

nossa).⁷⁰ 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.

2.6 Comunicação mediada e exposição de si

Dentre as hipóteses levantadas para explicar as dinâmicas da revelação de informações nos *sites* de rede social, Leonard (2004: *online*) retoma a premissa de que haveria uma suposta diferença cultural de uso da Internet entre gerações, que separaria os *geeks* que a construíram – para os quais a privacidade era matéria importante – e aqueles que hoje a usam maciçamente e já cresceram acostumados a este novo meio. Neste sentido, ele considera o surgimento das novas tecnologias e de suas dinâmicas participativas como um dos motivos pelos quais para estes jovens a exposição seria um comportamento natural. Para eles, a vida pessoal seria concebida como matéria de exposição pública, esvaziando, conseqüentemente, a noção de privacidade tal como concebida por gerações anteriores. Ainda que a questão da exposição de informações sobre si em redes sociais esteja associada também – e principalmente – a fundamentos mais amplos e complexos do que a noção de privacidade é capaz de sugerir, é impossível negar que nossa sociedade é hoje permeada pelo ímpeto de se expor. E os meios de comunicação figuram hoje, ao mesmo tempo, como os agentes e os sintomas privilegiados desta grande mudança, que pretendemos explorar a seguir (BRUNO, 2005: 56).

As práticas da exposição de si proliferam não só na Internet, mas constituem um fenômeno endêmico na cultura contemporânea, cujas manifestações mais características podem ser encontradas nos *weblogs* confessionais, nos *reality shows*, nos *fotologs* pessoais e nos *sites* de rede social. Nestas práticas, o olhar do outro é requisitado e o que outrora era abrigado sob a égide da esfera da vida privada (pessoal ou íntima) agora é exposto ao olho público, “ao mesmo tempo de todos e de ninguém” (BRUNO, 2005: 56). Neste novo contexto, a vida – não mais apenas a das celebridades, mas a do homem comum – se torna matéria prima para a produção midiática no que ela tem de mais trivial e cotidiana, instaurando as dinâmicas fluidas do ver e do ser visto, do desejo por se mostrar nestas novas vitrines do *voyeurismo* contemporâneo e também por observar aqueles que nelas se exibem. O estatuto desta visibilidade requisitada é de inserção e de reconhecimento do outro, de modo que ser fonte da atenção alheia figura quase que como um direito contemporâneo (BRUNO,

⁷⁰ Tradução nossa para: “[...] to leverage their value as network goods and enhance their growth by making registration, access, and sharing of information uncomplicated”.

2005). Nas redes sociais, tal direito está associado a um sentimento diferente do desejo pela fama, mas intimamente associado ao sucesso, a uma necessidade de apresentar aos que conhecemos e àqueles com quem venhamos a nos relacionar em um futuro próximo fatos sobre nossa existência no que ela tem de mais interessante e excitante: os melhores momentos, as melhores fotos, as melhores performances.

A compreensão deste processo passa pela premissa de que a gênese da subjetividade, quando historicamente situada, pode ser associada a variações no estatuto do olho público. Sibilia (2008), a partir da obra de David Riesman (1950), resgata a ocorrência de uma mutação nos processos através dos quais os sujeitos se definem, situada em meados do século XX. Trata-se da passagem de um modelo de subjetividade “introdiregida” a um modelo “alterdiregido”, ou mais precisamente, do nascimento de uma forma de estilização da existência que se daria a partir de “um deslocamento daquele núcleo do eu situado nas profundezas íntimas do ‘caráter’ individual em direção a tudo aquilo que os outros podem enxergar como sendo a ‘personalidade’ do sujeito que se mostra” (SIBILIA, 2008: 243). Bruno (2005), apoiando-se nos trabalhos de Elias (1994) e Vigarello (1996), desloca-se a um passado ainda mais remoto, e mostra a relação histórica do cuidado de si e do decoro corporal (em suma, da atenção ao que é publicamente visível) com a gênese da subjetividade. A autora relembra que estes elementos se relacionam não apenas com a instauração do processo civilizatório ou com a codificação das relações sociais, mas com a hipótese de que, “a atenção e o cuidado com o olhar do outro vão sendo progressivamente interiorizados e constituindo todo um campo de cuidados consigo, de autocontrole, autoregramento e autovigilância que passam a reger a esfera íntima e privada” (BRUNO, 2005: 57).

No entanto, a relação que hoje se estabelece no âmbito das novas tecnologias de comunicação entre a construção da subjetividade dos indivíduos e o campo de visibilidade ao qual eles se expõem se modifica substancialmente, e é justamente o estatuto desta mudança que nos interessa aqui acompanhar. Bruno (2005: 8) mostra que, na modernidade, o estatuto do olhar público está associado à lei e ao ideal da norma, o que o coloca em atrito com a esfera privada, que neste diagrama de poder, passa a se caracterizar como lugar de fuga, como refúgio para as liberdades do corpo e elocubrações da intimidade (BRUNO, 2005: 60). A atuação desta modalidade de olhar, que impõe a renúncia aos desejos e requisita constantemente a consciência moral interiorizada, é associada pela autora à instância psíquica do superego, assumindo as funções de promover a censura e proibir a transgressão. No entanto, na contemporaneidade, temos um cenário no qual a existência é individualizada e cada um, longe da tutela do estado e dos regimes de seguridade que o amparavam, deve

assumir para si a tarefa de promover o seu próprio sucesso, calculando os riscos de suas escolhas e planejando sua própria felicidade (BECK, 1992). Dado o esvaziamento da esfera política e das instituições que outrora suportavam a ação coletiva (o sindicato, a família etc.), as trajetórias individuais se tornam indicativos cada vez mais claros de uma competência cruel, que se dá na superação e não na aceitação dos limites e que pode ser lida ou traduzida em termos de uma auto-realização que ganha sentido na exposição das atitudes e performances que a indicam. Neste contexto, Bruno (2005: 61), associa o olho público contemporâneo à instância do ideal de ego.

Se considerarmos o que hoje se entende como a via do sucesso e da realização pessoal, veremos que ela está mais ligada à superação de limites e à alta performance individual do que à aceitação de limites, a interdições superegóicas e à adequação a normas coletivas. [...] E este ideal de realização é inseparável de um cuidado com a imagem e com o olhar do outro, que é menos da ordem da interdição (que limita ou impede fazer o que se deseja) do que da ordem da performance (que incita estar à altura do seu desejo, do seu ideal) (BRUNO, 2005: 62).

Os ideais de inovação constante, perfeição a qualquer custo, formação permanente e superação individual marcam este cenário, no qual correr riscos – sem, no entanto, colocar os outros em risco (BECK, 1992) – se torna um comportamento almejado e admirado. Assim, Sibilia (2008) e Bruno (2004) mostram como esta nova subjetividade se dá no ato de se fazer visível e de expor a intimidade na busca da aprovação alheia. “No império das subjetividades alterdirigidas, tudo o que se *é* deve ser visto para poder realmente *ser*. Cada um *é* tudo aquilo que mostra de si, e tão somente isso” (SIBILIA, 2008: 245). Por isso, o alto grau de investimento sobre a aparência e a busca da autopromoção através do consumo e da gestão cuidadosa da reputação da própria marca. Não é à toa que, no que tange à temática das redes sociais, a exposição de si é frequentemente relacionada à noção de capital social, que se refere aos recursos implícitos às relações sociais mantidas pelos indivíduos através de sua inserção em grupos (RECUERO, 2005). Neste sentido, o capital social depende de uma mobilização que pode ser caracterizada pelo custo do investimento necessário à construção e à manutenção das relações entre os indivíduos, o que os permitirá, no futuro, usufruir dos recursos associados à rede em que se inserem visando satisfazer seus interesses e atingir seus objetivos. Assim, mostrar-se em uma rede social implica negociar com as impressões que os outros terão sobre você e com a confiança que eles depositarão nesta relação, seja ela *online* ou *offline*. Afinal, como já esclarecemos aqui, um dos papéis desempenhado pelo perfil é o de promover uma apresentação performática, capaz de influenciar positivamente nossas relações e

conexões. Neste sentido, como ressalta Sibilia (2008: 235), a *web* fornece um espaço para a concretização das metáforas das citações dos indivíduos e da volatilidade de suas reputações.

É importante ressaltar que, neste novo contexto, a expressão da intimidade é marcada por seu caráter superficial, por uma modalidade de exposição que não deixa entrever nada através, por representações do ‘eu’ que deixam a sensação de transparência total. Afinal, experimentamos também uma mudança do estatuto do que existe para além do que está relatado, escancarado, publicado, publicizado. Assim, essas narrativas de si não implicam a exteriorização de um ‘eu’ profundo, mas apontam para uma subjetividade que se dá no ato de se expor, e que, nem por isso, pode ser tomada como irreal, menos verdadeira ou menos autêntica. Como explicita Bruno (2005: 65), “[...] na superficialidade estética contemporânea o que é deixado para trás ou por trás da imagem, da aparência e do artifício não é mais verdadeiro que o que se mostra”. Trata-se, portanto, de uma mudança no foco daquilo que merece a atenção dos indivíduos. Neste sentido, Sibilia ressalta como essas novas práticas da exposição de si se encontram em um limiar de publicidade total (2008: 246), assertiva que fica bem clara quando consideramos a iniciativa do *Facebook* de exibir na lateral direita do *site*, em seu espaço destinado a publicidade, um ‘anúncio’, que a cada vez mostra a foto e as atualizações de status de um de seus amigos.

As dinâmicas da exposição de si nas redes sociais, acreditamos, possuem algumas particularidades em relação às práticas cujo lugar é a mídia de massa (como os *reality shows*) e a outras próprias também ao ambiente da Internet (como os *weblogs* e *fotologs*). A principal delas é a freqüente associação com o contexto de relações que os indivíduos mantêm em sua vida *offline*. Ainda que um *weblog* ou *fotolog* possa ser visitado também por aqueles que nos são mais próximos, nas redes sociais as informações reveladas são imediatamente visíveis a todos os que adicionamos como amigos, visto que é comum nestes *sites* a implementação de ferramentas de *feed*, que indicam àqueles com que mantemos conexões as nossas atualizações recentes. Outra questão interessante é a necessidade de novidade que cerca o *update* dos perfis: fatos novos, sensações novas, experiências novas são narradas em um espaço que permite conjugar o que os indivíduos dizem sobre si próprios com o que eles fazem. Diferentemente do que ocorre nos *weblogs*, entre os quais é mais comum que o foco da narrativa seja textual (ainda que ela venha acompanhada de vídeos e fotos), os fatos em redes sociais são freqüentemente narrados através dos álbuns de fotos, que associam as imagens a legendas criativas e comentários dos amigos ou daqueles que nelas aparecem. Já as atividades e sentimentos mais cotidianos vêm no formato *microblogging* das atualizações de status (diga-nos o que você está fazendo agora) e são freqüentemente utilizados para a expressão de

toda sorte de sensações, gostos e predisposições, configurando um espaço aberto para a expressão pessoal cuja amplitude dificilmente conseguiríamos descrever aqui. Por fim, um remix de mídia e de referências – letras de músicas ou trechos de livros, vídeos caseiros, trechos de clipes e todo tipo de produção cultural – ajudam a revelar o gosto e o momento pessoal vivido pelo dono do perfil.

Nas redes sociais o protagonista ‘eu’ vem acompanhado daqueles que sua personalidade permite conquistar, que falam sobre suas virtudes nas ferramentas de testemunho e com quem eles trocam mensagens através das estruturas de comentário. E nestes *sites*, a exposição exagerada de detalhes íntimos sobre a vida dos indivíduos, ainda que presente, não é tão freqüente quanto nas escritas de si próprias aos *weblogs* confessionais, devido, principalmente, a esta proximidade exagerada com o contexto de relações *offline* mantidas pelo indivíduo que se mostra. Este fato fez emergir em muitos *sites* um contexto de exposição mais controlado e cuidadoso, que preza pela reputação dos indivíduos e no qual aqueles que se vêem exagerando na dose – publicando fotos picantes ou mantendo álbuns que mais parecem *books* fotográficos, por exemplo – acabam ridicularizados pelos demais.⁷¹ É importante mostrar sucesso e beleza, mas é igualmente importante que esta artificialização venha em um contexto o mais natural e autêntico possível: o da vida cotidiana. Assim, se as atitudes adquirem sentido quando publicizadas a outrem, as experiências mais comuns passam a ser vivenciadas considerando este novo campo de visibilidade virtual. Há então uma condição em que a atenção se volta não apenas ao que é visível ao olhar do outro, mas ao que pode se tornar visível, através da transformação de si próprio em uma narrativa midiática.

Assim, as redes sociais se tornam um lugar privilegiado para a exposição de fatos, momentos e conversas cotidianas que permitam a exibição de nossos feitos, experiências, aquisições, trocas, relações e transformações (físicas e psíquicas), narradas em uma construção que, freqüentemente, tolera algumas fraquezas e defeitos, mas exclui de maneira precisa o insuportável e tudo o que pode ser sinônimo de limitação ou fracasso. O foco destas narrativas está, portanto, na ficcionalização regulada de si através de relatos particulares que usam toda a sorte de recursos disponíveis. Neste sentido, cabe ressaltar o quanto este campo de expressão pessoal é expandido pelo uso de aplicativos, que podem ser escolhidos e instalados pelos usuários em seus perfis e servem para engajá-los em ações tão variadas quanto mostrar aos outros produtos que você compraria ou as causas que o mobilizam; mostrar seus sentimentos em relação às pessoas com quem você se relaciona; os presentes que

⁷¹ Um bom exemplo pode ser dado pelo popular *weblog* “Pérolas do Orkut”, que se dedica a relatar as gafes e exageros dos usuários do site. Disponível em: <http://www.perolasdoorkut.com.br/>.

você daria a elas; a sua proximidade delas em termos de gosto musical ou cinematográfico etc. A revelação de informações através dos aplicativos e hipóteses acerca dos impulsos que levam os indivíduos a se mostrarem nas redes sociais serão consideradas no próximo capítulo, para o caso específico do *Facebook*.

2.7 A publicidade direcionada e a mineração de dados nas redes sociais

Os perfis não são apenas espaços para a exposição de si. Na abordagem dos sistemas de recomendação e da *web* personalizada, eles são formas de realizar buscas continuamente, de alimentar sistemas com dados sobre nossos comportamentos a partir de um monitoramento contínuo que subsidiará o retorno de informações relevantes (ÇENTIMENTEL *et al.*, 2000). A argumentação que se segue é baseada pela premissa de que os *sites* de rede social não revolucionaram apenas a maneira como interagimos e atuamos socialmente. O seu desenvolvimento pode ser igualmente descrito como o nascimento de uma nova bolha no cenário da rede: o alto valor de mercado destes *sites* é apenas um indicativo de um casamento perfeito entre a potência do alto tráfego de usuários e a grande quantidade de informações disponíveis sobre aqueles que os acessam. Em resumo, os *sites* de rede social se oferecem como um espaço perfeito para a realização de todos os sonhos do *marketing* contemporâneo e de sua nova geração de serviços publicitários personalizados, para a qual conhecer o público-alvo, suas predisposições, gostos e interesses permite oferecer o produto e a oferta certos, aumentando a possibilidade de que o anúncio cumpra seu papel de aumentar as vendas e os lucros. E como é fácil perceber, estes são justamente os dados que os usuários de redes sociais disponibilizam voluntariamente nestes *sites*, o que nos permite associar o seu valor de mercado ao de uma *commodity* cada vez mais valorizada nos dias de hoje: informações pessoais.

Hoje, cerca de 6% do dinheiro gasto com publicidade nos EUA é direcionado à Internet (URSTADT, 2008a). As formas de se anunciar *online* evoluíram muito nos últimos anos: o tradicional *banner* cedeu espaço para o *contextual advertising* – aquele associado aos mecanismos de busca, que nos é exibido separadamente dos resultados orgânicos na página do buscador – e posteriormente para o *behavioral targeting*, termo que descreve uma série de métodos para se coletar informações sobre o comportamento dos internautas de modo a gerar modelos que orientem os anunciantes sobre como aumentar as possibilidades de atingir os consumidores (RÖHLE, 2007: *online*). Podemos considerar o *targeting* como uma forma de predição do comportamento dos indivíduos, interpelados enquanto consumidores. A idéia

básica é conhecer seus hábitos, tendências e interesses de modo atingi-los com serviços, ofertas e produtos que eles considerem relevantes. Assim, a eficiência desta proposta depende da quantidade e precisão das informações coletadas sobre os alvos que se deseja atingir.

No entanto, em um cenário econômico cada vez mais competitivo, as preocupações em torno da privacidade são freqüentemente deixadas para segundo plano e burladas sob a argumentação de que não há comportamento abusivo ou ameaça aos indivíduos cujos dados e atitudes *online* são sujeitos às rotinas da coleta e tratamento de dados. Afinal, como afirmam os anunciantes, o monitoramento é feito por máquinas e a identidade dos indivíduos suprimida. No entanto, para “quebrar o código dos consumidores” (TUROW, 2006), ou seja, para entendê-los e encontrar formas de fazer com que eles percebam os anúncios veiculados, essas empresas estão vigiando suas ações no ciberespaço, inaugurando uma condição na qual a observação maquínica é usada na tentativa de produzir a atenção humana. E a partir destes sistemas, os consumidores podem ser classificados, classificação essa que preconiza o tratamento diferenciado: vantagens para determinados grupos, programas de fidelidade, promoções direcionadas e assim por diante. Assim, essa vigilância que se diz inofensiva produz efeitos reais sobre a vida destes consumidores.

Os anunciantes gostam de abordar a questão pela lógica do custo benefício – porque os consumidores se revoltariam com algo que traz benefícios a eles, impedindo-os de ter que procurar pelos produtos que desejam e ainda obtendo vantagens (TUROW, 2005: 114)? A tônica é sempre a de que estes sistemas do *marketing* contemporâneo não implicam invasão de privacidade e devem ser vistos “[...] não como intrusos comerciais, mas como uma assistência de vendas precisa para os consumidores em um mundo complicado” (TUROW, 2005: 119, tradução nossa).⁷² Porém, “esta relação aparentemente inofensiva pode levar rapidamente a sentimentos de discriminação, raiva e suspeição se os espectadores acreditam que eles não estão ganhando os descontos ou as oportunidades que os outros recebem” (TUROW, 2005: 119, tradução nossa).⁷³ Segundo Turow (2005), há uma crença, por parte das empresas no fato de que as possíveis reações negativas geradas por esta nova condição podem ser controladas através da responsabilização dos próprios consumidores. O argumento utilizado para esta manobra seria o de que a ausência de vantagens seria um atestado da ineficácia destes indivíduos em interagir com os trâmites institucionais da companhia e com

⁷² Tradução nossa para: “[...] not as commercial intrusion but as pinpoint selling help for frenetic consumers in a troubling world”.

⁷³ Tradução nossa para: “Such seemingly benign relationships can quickly lead to feelings of discrimination, anger, and suspicion if viewers believe that they are not getting the discounts, or the opportunities to attend to material, that others receive”.

seu sistema de vantagens, o que situaria a questão na esfera individual, na relação empresa-consumidor, disfarçando sua real abrangência. No entanto, apesar desta retórica amistosa e dos benefícios implícitos ao uso destes sistemas, eles permitem às empresas gerenciar melhor e com mais eficácia seus consumidores: através deles pode-se recompensar e valorizar os comportamentos vistos com bons olhos pelas políticas corporativas ou afastar os indesejados. Como resultado final, para Turow (2005), esta condição produziria nos indivíduos a insegurança e a ansiedade sobre seu posicionamento nestas políticas de classificação e sobre sua exclusão de preferências associadas à permanência em um certo grupo.

Para o caso dos *sites* de rede social, o uso de dados pessoais para o *targeting* publicitário também é uma realidade. Desenvolvimentos recentes no campo da computação – especialmente nas técnicas de *data mining* e aprendizado de máquina – vêm subsidiando o surgimento de métodos para o estudo de dados estruturados em rede (JENSEN e NEVILLE, 2002). Assim, os *sites* de rede social representam hoje uma possibilidade inédita de aprender mais sobre as pessoas – especialmente sobre grandes grupos de pessoas (LEONARD, 2004) – a partir do estudo de seu comportamento e de suas conexões. As informações disponibilizadas pelos usuários nestes *sites* podem então ser usadas para produzir mapas que reproduzam a estrutura da comunidade estudada e relacionem os *links* da rede aos interesses dos indivíduos entre os quais eles se estabelecem. E tudo isso sem empenhar esforço algum para recolher estas informações. Afinal, nos *sites* de rede social elas estão amplamente disponíveis, além de reunidas de uma maneira extremamente organizada: os *links* são as relações de amizade, enquanto os interesses e características dos indivíduos estão distribuídos nas guias de informação dos perfis, sortidos por gêneros e apresentados sob a forma de palavras-chaves.

Bons exemplos sobre como os dados de redes sociais podem ser usados são encontrados em Liu *et al.* (2005) – que visam produzir o que eles intitulam “fábricas do gosto”, matrizes de correlações capazes de especificar o grau de afinidade entre quaisquer dois itens de interesses – e Adamic *et al.* (2003) – que visam apontar como a personalidade e os interesses dos indivíduos influenciam a estrutura da rede social que se constitui a partir do estabelecimento das relações de amizade. Uma contribuição importante que se pode depreender destas análises é a de como o emprego de técnicas computacionais permite o mapeamento de relações efêmeras e instáveis, conjunturais, cuja natureza é marcada por uma superficialidade diagnóstica que não visa interpelar os indivíduos em toda a sua complexidade ou interioridade psíquica. Liu *et al.* (2005: 2, tradução nossa) denominam este campo de inferências semânticas de *taste ethos*, “[...] um agrupamento efêmero de interesses da fábrica

do gosto”.⁷⁴ A idéia é conseguir medir a chance de conexões improváveis, como a de que alguém que goste de praticar *yoga* goste também da música de Mozart e de comer *sushi*. Assim, não se trata de classificar os indivíduos em categorias estabelecidas *a priori*, mas de identificar correlações conjunturais que delineiem tendências, que permitam deduzir comportamentos prováveis.

De maneira semelhante, Adamic *et al.* (2003) buscaram calcular as correlações existentes entre a manifestação dos itens de personalidade e as preferências listados pelos usuários do *site Clube Nexus*, uma comunidade virtual fundada na universidade americana de Stanford em 2001. Assim, os pesquisadores visavam realizar medições que permitissem indicar, por exemplo, qual a probabilidade de que alguém que se julgasse engraçado (traço de personalidade) gostasse do gênero comédia (interesse). A pesquisa identificou que tendências aparentemente sem relação alguma eram recorrentes, e se mostravam significativas para os padrões de comportamento das pessoas. É esperado que as pessoas que se julgam atraentes julguem a aparência algo importante. No entanto, a mineração de dados nessas redes permite traçar correlações menos óbvias: aqueles que gastam seu tempo livre em casa são mais comuns entre os que cursam História, enquanto aqueles que se julgam engraçados são mais comuns entre os que cursam Biologia (ADAMIC *et al.*, 2003). Segundo os autores, poucos dos possíveis pares encontrados para os dados disponibilizados apresentaram medições nas quais o valor encontrado para que se dessem ao acaso foi significativo.

Vejamos agora como tem ocorrido a publicidade nas redes sociais. Consideremos, inicialmente, esta equação simples: “na Internet, tráfego é igual a dinheiro” (BERNOFF e LI, 2008: 11, tradução nossa).⁷⁵ Ela pode nos ajudar a compreender a corrida das empresas de redes sociais na busca por monetizar seus serviços e converter suas astronômicas audiências em lucros concretos. No entanto, os resultados não têm sido muito animadores. Consideremos, por exemplo, o caso do *Facebook*. Em 2007, a *Microsoft* comprou 1,6% da empresa por 240 milhões de dólares, o que deu ao serviço o duvidoso valor de 15 bilhões de dólares. No entanto, as previsões são de que o *site* tenha um prejuízo de 150 milhões de dólares no ano de 2008, decorrente dos custos de operação, incluindo novos servidores (URSTADT, 2008b). Sergey Brin (*apud*. URSTADT, 2008b), co-fundador da *Google*, que pagou 900 milhões de dólares por uma parcela de tráfego do *MySpace* em 2006, considera que ainda não foi descoberto o jeito certo de anunciar e monetizar as redes sociais. De maneira geral, o preço do custo por 1000 impressões de um anúncio em um desses *sites* (*cost*

⁷⁴ Tradução nossa para: “[...] an ephemeral clustering of interests from the taste fabric”.

⁷⁵ Tradução nossa para: “On the Internet, traffic equals money”.

per mille - CPM) é menor do aquele cobrado por *sites* jornalísticos ou por aqueles com público mais restrito e definido. No entanto, nem mesmo os baixos custos têm sido suficientes para atrair uma grande quantidade de anunciantes.

Urstadt (2008b), afirma que a publicidade em *sites* de rede social tem três problemas fundamentais. O primeiro deles é a falta de atenção dos usuários aos anúncios veiculados nestes ambientes. A justificativa mais comum é a de que os anúncios são tomados como intrusos em um contexto no qual as pessoas estão interessadas e ocupadas, interagindo socialmente. Isto justificaria o baixo número de cliques nestas peças publicitárias, ao contrário do sucesso do *AdWords* da *Google*, por exemplo, no qual a publicidade é veiculada em relação ao conteúdo de uma busca. O segundo problema diz respeito ao conteúdo do contexto em que um anúncio será mostrado. Como um *site* de rede social é construído por seus usuários, seu conteúdo é enormemente variado, o que dificulta a previsão do que será exibido lado a lado com um determinado anúncio. Naturalmente, a repulsa dos anunciantes em ver seus anúncios dividindo espaço com conteúdos considerados “inapropriados” é um grande incentivo ao controle do comportamento dos usuários por parte das empresas provedoras deste tipo serviço, como é o caso do *Facebook*, que visa aperfeiçoar cada vez mais seu sistema de moderação dos materiais publicados no *site* (URSTADT, 2008a).

Por fim, o problema da publicidade em redes sociais está relacionado também à questão da privacidade. Recentemente, diversas companhias se engajaram na idéia de que neste novo meio a publicidade também deveria envolver nossas redes de relações, de modo a se tornar interessante e chamar a atenção do público ao qual ela se direciona. Um bom exemplo pode ser dado pelos programas *Social Ads* e *Beacon*, lançados pelo *Facebook* em 2007. O primeiro usa ações que você execute no site relacionadas a determinada marca ou produto para anunciá-lo através de seu perfil. Já o *Beacon* notifica toda a sua lista de amigos sobre suas ações executadas em *sites* parceiros: você compra algo no *eBay*, por exemplo, e o *Beacon* se encarrega de incluir sua compra nos *feeds* que aparecem no seu perfil e no perfil dos seus contatos. O sistema não era *opt-in*, ou seja, ele foi ativado a despeito da vontade e do conhecimento dos usuários do *Facebook*, o que gerou reações extremamente negativas por parte do público, fazendo com que a empresa chegasse inclusive a se desculpar publicamente pela invasão de privacidade provocada pelo funcionamento do programa.

Outro exemplo de publicidade direcionada em redes sociais é o sistema *HyperTargeting*, lançado pelo *MySpace* em 2007. Ele percorre os perfis dos usuários do *site* e coleta dados sobre seus interesses e demografia. “Ele classifica os perfis em dez categorias mais gerais, tais como esportes e entretenimento – que são subdivididas em mais de 1000

categorias mais precisas, como beisebol ou um filme específico” (URSTADT, 2008b: *online*, tradução nossa).⁷⁶ O *targeting* no *Facebook* também já é uma realidade: qualquer anúncio que você deseje veicular no *site* pode ser direcionado segundo critérios demográficos, de escolaridade etc. Neste sentido, vale lembrar que a literatura relacionada à privacidade e ao comércio eletrônico tem encontrado em suas medições altos níveis de preocupação dos usuários em oferecer dados que permitam às empresas construir seus sistemas de recomendação. No entanto, nas redes sociais, estas informações são reveladas com boa vontade e, de maneira geral, são verdadeiras e precisas, o que faz com que elas tenham mais valor do que aquelas oferecidas por companhias como a *ChoicePoint* e a *Acxiom*, que construíram negócios de bilhões de dólares vendendo bases de dados de informações pessoais (JONES e SOLTREN, 2005).

Podemos dizer, desta forma, que o cenário das redes sociais vêm experimentando uma mudança semelhante àquela descrita por Röhle (2007) para o mercado dos buscadores. Ele afirma que, atualmente, os anúncios não são mais uma forma de gerar receitas para melhorar os sistemas de busca. Diferentemente, estes *sites* estão se tornando plataformas para o *advertising*, enquanto a busca assume apenas a função de gerar o tráfego de usuários. No caso das redes sociais, de maneira semelhante, a interação social funciona duplamente, como aquilo que gera tráfego e aumenta a predisposição dos usuários em revelar informações. Assim, os dados que você coloca em seu perfil, as comunidades, redes ou grupos aos quais você se junta, os aplicativos que você adiciona, em suma, toda a informação publicada se torna uma forma de produzir conhecimento sobre você, conhecimento este que irá atuar como um filtro mediador de suas relações *online*: “[...] sua rede se torna o seu filtro no mundo, e quanto mais cuidado você empenha em cultivar e nutrir esta rede, melhor o filtro se torna” (LEONARD, 2004: *online*, tradução nossa).⁷⁷ Evidentemente, existe uma grande vantagem em receber ofertas relevantes, em deixar que um sistema lhe ajude a se orientar em um ambiente de excesso informacional. No entanto, estes filtros podem também figurar como dispositivos de controle que segmentam consumidores e legislam no presente sobre as possibilidades futuras que a eles estarão disponíveis. Lado a lado, convivem assim os benefícios e tiranias de um mesmo universo mediado.

⁷⁶ Tradução nossa para: “It sorts the profiles into 10 rough categories--such as sports and entertainment--that are subdivided into more than 1,000 narrower categories, such as baseball or a specific film”.

⁷⁷ Tradução nossa para: “[...] your network becomes your filter on the world, and the more carefully you cultivate and nurture that network, the better the filter becomes”.

2.8 Portabilidade: cada um tem a sua?

A discussão sobre a portabilidade de dados tem a ver com o processo de construção de padrões que permitam a evolução da *www* em direção ao que se convencionou chamar *web* semântica, um modelo no qual a rede seria alimentada com informações a respeito do sentido do conteúdo nela abrigado de modo a retornar dados relevantes aos seus usuários.⁷⁸ A portabilidade é um movimento que surgiu em torno da idéia de permitir e fomentar a interoperabilidade e o trânsito facilitado de dados entre os diversos serviços ou mídias sociais que utilizamos cotidianamente na rede.⁷⁹ Em resumo, trata-se, por um lado, da busca por facilitar o remix e o compartilhamento de dados pessoais e por outro, de permitir que os usuários sejam de fato donos das informações que publicam, conferindo-lhes poder de ação sobre como elas devem fluir na rede e a quem elas devem estar disponíveis. O enfoque da portabilidade é múltiplo e atinge simultaneamente os interesses de três grupos distintos: os usuários, as empresas e os desenvolvedores. Uma vez que estes setores, principalmente os dois primeiros, possuem, comumente, interesses opostos, a idéia da portabilidade tem levantado muitas polêmicas acerca do impacto da iniciativa sobre os padrões de segurança e privacidade vigentes na rede.

À primeira vista, os benefícios da portabilidade são para todos. Por um lado, para as empresas provedoras de serviços, esta iniciativa permitiria, teoricamente, arrebatar mais usuários, pois agora, com a participação automatizada e facilitada, eles não mais necessitariam preencher formulários de inscrição e postar novamente as informações que querem publicar se já o fizeram em algum outro contexto. Assim, ficaria mais fácil para as empresas oferecer seus serviços ao público e obter constantemente informações atualizadas sobre seus usuários mesmo se eles não visitam periodicamente o *site* daquele serviço, por exemplo: basta que eles concordem em compartilhar as informações e elas serão automaticamente publicadas em todos os *sites* autorizados.

Por outro lado, para os consumidores finais, a portabilidade significaria: a) a simplificação das rotinas de uso da rede e b) o direito de exercer controle sobre os corpos de

⁷⁸ A *web* semântica deriva das idéias de Tim Berners-Lee acerca de uma *web* mais inteligente, na qual computadores se tornariam capazes de analisar os dados da rede e atender com mais precisão às solicitações dos usuários. A iniciativa do desenvolvimento dos conceitos e padrões técnicos para esta nova *web* giram principalmente em torno do *World Wide Web Consortium* (W3C), criado por Berners-Lee em 1994 e encarregado de garantir a compatibilidade dos padrões usados para a navegação na rede.

⁷⁹ O *DataPortability Project* (DPWG) vem coordenando e formalizando os esforços de diferentes iniciativas em direção ao desenvolvimento da portabilidade e em prol da adoção de padrões livres. Hoje, grandes empresas o *Digg*, *Facebook*, *Google*, *Microsoft* e *Yahoo!* também estão envolvidas com este movimento. Mais informações sobre o *DataPortability Project* podem ser encontradas no site: <http://www.dataportability.org/>.

informações disponibilizados, escolhendo quando, com quem e o que compartilhar. Atualmente, grande parte dos usuários da Internet utiliza diferentes serviços ou mídias sociais: eles possuem *weblogs*, *fotologs*, perfis em diferentes *sites* de rede social, e assim por diante. Cada vez que eles desejam fazer um comentário no *blog* de um amigo ou abrir um perfil em um novo *site* de rede social, eles precisam executar novamente uma série de tarefas: preencher formulários de cadastro, disponibilizar o conteúdo desejado etc. Neste contexto, a portabilidade lhes daria o direito de conectar e replicar informações automaticamente, eliminando os custos de reproduzir manualmente o que já foi publicado.

Com a portabilidade de dados, você pode trazer sua identidade, amigos, conversas, arquivos e histórias com você, sem ter que adicioná-los manualmente a cada novo serviço. [...] À medida que suas experiências se acumulam e você adiciona ou modifica dados, essas informações serão automaticamente atualizadas em outros *sites* e serviços se você permitir, sem ter que revisita-los ou recolocar os dados em questão (BIZANES, 2008: *online*, tradução nossa).⁸⁰

Como já abordamos anteriormente, no ambiente da Internet, a compatibilidade é alcançada através de protocolos, ou seja, do desenvolvimento e/ou adoção de padrões comuns que permitam o trânsito de dados e a conversação harmônica entre máquinas que se compreendam mutuamente. De maneira semelhante, a portabilidade depende de soluções que garantam esta pretensa interoperabilidade dos serviços distribuídos. Dentre eles estão o RSS (*Really Simple Syndication*), que permite aos usuários receber as atualizações das fontes de informações por eles escolhidas; o *OpenID*, sistema gerenciado pela *OpenID Foundation* que visa fornecer aos usuários um login transversal e único para o acesso a variadas fontes de serviços; o *OAuth*, um sistema de autenticação através do qual as autorizações dadas pelos usuários para que aplicativos e *sites* acessem seus dados podem ser verificadas; o RDF (*Resource Description Framework*), que permite o cadastro de quantidades significativas de metadados para o aprimoramento das ferramentas de busca e o SIOC, tecnologia apresentada pelo *Semantically-Interlinked Online Communities Project* ao *World Wide Web Consortium* que forneceria suporte para a integração de listas de discussão, fóruns e *weblogs* (HAYMAN, 2006: 13-4; PICK, 2007: *online*). Ainda que a concretização do ideal da portabilidade e a implementação de seus serviços distribuídos dependa da operação de todos esses protocolos, três deles são particularmente importantes para a argumentação que desenvolveremos aqui.

⁸⁰ Tradução nossa para: “With data portability, you can bring your identity, friends, conversations, files and histories with you, without having to manually add them to each new service [...]. As your experiences accumulate and you add or change data, this information will update on other sites and services if you permit it, without having to revisit others to re-enter it”.

As políticas da portabilidade dizem respeito a qualquer tipo de conteúdo criado e postado em mídias sociais por seus usuários. Estes conteúdos, muitas vezes, se referem a pessoas: são dados de contato, de identificação, informações sobre seus gostos, preferências, interesses etc. Neste contexto, três padrões específicos desenvolvidos através deste movimento visam suportar a indexação, a criação de metadados e a recuperação de dados sobre pessoas. O primeiro deles, os *Microformats*, são uma forma de reaproveitar *tags* HTML e XHTML para integrar à codificação das estruturas *web* a produção de metadados específicos sobre eventos (*hCalendar*)⁸¹; revisões de produtos, serviços, pessoas, lugares, *websites* etc. (*hReview*)⁸²; dados pessoais, incluindo nome, endereço, país, foto, telefone, *e-mail* etc. (*hCard*)⁸³; e relações entre as pessoas, incluindo grau de parentesco ou amizade, relação romântica, proximidade geográfica etc. (XFN).⁸⁴ Assim, ao mesmo tempo em que criamos as estruturas *web*, podemos dar informações precisas sobre o conteúdo produzido, de uma só vez, a humanos e máquinas. O uso dos microformatos funciona, desta forma, como uma *tag* que pode atestar a natureza e o pertencimento da informação, permitindo seu reconhecimento em diferentes *sites*, *softwares* e dispositivos: assim, dados podem ser extraídos, indexados, buscados, salvos ou referenciados cruzadamente (HAYMAN, 2006).

Para o caso dos *sites* de rede social, o uso combinado do *hCard* e do XFN permite, dependendo da compatibilidade dos serviços usados, exportar parte das suas informações de perfil e listas de amigos.⁸⁵ Se, por exemplo, um usuário possui um *weblog* que também suporta tais padrões, ele pode trafegar dados entre ele e o seu perfil de rede social: basta estabelecer que aquelas URL's são controladas pela mesma pessoa e o trânsito de informações se torna possível. É importante ressaltar também que os microformatos, ao serem reconhecidos pelos navegadores, devem apresentar uma interface padrão – ícones ou outras marcações, dependendo do *browser* utilizado – à qual estará associada a possibilidade de executar ações como a edição, importação/exportação etc. dos dados em questão.⁸⁶

É importante ainda diferenciar dois padrões: o XFN e o FOAF⁸⁷. O XFN permite a um autor fornecer informações sobre a natureza de uma relação a partir de um *link*. Ainda que, segundo Meyer (*online*), seja provável que seu uso se torne mais popular em *blogs*, ele serve para designar a relação entre pessoas no estabelecimento de qualquer *link* que aponte para

⁸¹ Disponível em: <http://microformats.org/code/hcalendar/creator>.

⁸² Disponível em: <http://microformats.org/code/hreview/creator>.

⁸³ Disponível em: <http://microformats.org/code/hreview/creator>.

⁸⁴ Disponível em: <http://www.gmpg.org/xfn/creator>.

⁸⁵ A lista dos serviços que já suportam tanto o XFN quanto o *hCard* pode ser encontrada em: <http://microformats.org/wiki/hcard-xfn-supporting-friends-lists>.

⁸⁶ Cf.: <http://microformats.org/wiki/user-interface>.

⁸⁷ Cf.: <http://www.foaf-project.org/>.

uma página pessoal. Nele, a relação declarada por um autor deve ser confirmada pela pessoa referida, de modo que a falta desta confirmação já pode servir como um indicativo de que se trata de algo inverídico. Já o *Friend of a Friend* (FOAF) – um padrão de geração de metadados específico para a descrição de pessoas, suas atividades, interesses e relações – permite tanto que um autor dê informações sobre si próprio quanto a outros que escrevam metadados sobre ele, sem depender, no entanto, de uma confirmação bi-lateral, o que pode resultar em informações falsas. Além disso, o FOAF é bem mais aberto, e tem como objetivo descrever com detalhes as pessoas e suas relações a partir dos *links* existentes entre elas.

Por fim, consideremos ainda o *Attention Profiling Markup Language* (APML), que permite o monitoramento, registro e compartilhamento do seu *attention data*, *i.e.*, daquilo que define o seu perfil de interesse e seus hábitos de navegação na *web* (PICK, 2007). Pense, por exemplo, no sistema de recomendação da *Amazon.com*. Imagine agora que você pode compartilhar as informações que compõem o seu histórico de interesses no *site* com outras livrarias virtuais, para obter recomendações de produtos e ofertas elaboradas a partir das suas compras, buscas e *ratings* de itens específicos. Pense agora que isso se aplicaria não apenas às livrarias virtuais, mas a toda *web*. Esta é a pretensão do APML, um padrão que permitiria aos usuários compor e compartilhar seus perfis de interesse visando receber conteúdos personalizados. Todos os dados coletados enquanto você usa a *web* – as músicas que você ouve, as URL's que você acessa, os termos pelos quais você busca, as *tags* que você registra, irão compor um arquivo XML, que armazena suas preferências, gostos, tendências e o seu grau de interesse nos campos de ação registrados. Acessando um *site* qualquer, você tem a opção de compartilhar com ele o seu perfil de interesse, personalizando sua vida virtual.

Esta iniciativa parte de dois pressupostos fundamentais. O primeiro é o de que a quantidade de informações presente na *web* é um obstáculo à sua eficiência e dificulta a vida do internauta comum. E o segundo considera que é melhor controlar como nossos dados estão sendo coletados para subsidiar sistemas de recomendação do que permitir que as empresas continuem fazendo isso indiscriminadamente. Todos os padrões até aqui descritos ainda estão em fase de desenvolvimento e implantação, e é difícil equacionar agora os possíveis benefícios e os potenciais riscos associados a este processo. No entanto, é importante ressaltar que muita polêmica e um certo grau de suspeita giram em torno destas iniciativas. Por um lado, os advogados da portabilidade defendem que devolver aos usuários o controle sobre suas informações fomentará a competição entre os *sites* de rede social existentes e criará uma *web* mais inteligente e bem estruturada. Afinal, se os usuários podem facilmente levar consigo suas informações, a lógica é a de que eles escolham o serviço que julgarem melhor.

No entanto, como apontam os mais céticos em relação a esta nova tendência, por que motivo as empresas facilitariam o trânsito dos dados que os usuários postam em seus serviços, entregando a seus rivais o seu maior patrimônio, depois de anos de esforços no sentido de aprimorar-se e conseguir mais adeptos? Afinal, como argumenta Heyman (2008: 13), fazer com que os usuários tenham que postar novamente todas as suas informações cada vez que eles desejem usar um novo serviço seria também uma forma de desencorajá-los a deixar de usar um determinado *site* – o que significaria menos usuários e menos receita para a empresa preterida. Seja como for, é indiscutível que, quando analisamos a situação do ponto de vista dos usuários, vemos que ajudá-los a replicar automaticamente suas informações na rede e a usá-las como eles bem entenderem significa também propagar e estruturar cada vez mais estas informações, o que inevitavelmente gera preocupações em torno de como esses dados serão usados e acessados e sobre as políticas de privacidade que regularão estes processos.

Na cena das redes sociais, a portabilidade tem sido adotada e apresentada pelas empresas através de um discurso bem intencionado e amigável, que luta pela concessão de direitos aos usuários destes serviços. No entanto, o que temos visto até agora não passa da emergência de uma compatibilidade limitada, que ainda não diz respeito à construção de padrões abertos e universais e na qual o controle sobre os dados se refere estritamente ao direito de publicá-los em outros lugares. Sob a argumentação de que um sistema completamente aberto ameaçaria a privacidade dos usuários, pois deixaria seus dados sujeitos ao acesso e uso de qualquer um, *sites* como o *Facebook* defendem padrões próprios, por exemplo. Neste contexto, é importante ressaltar que só existem duas formas de fazer com que a cena das redes sociais seja uma estrutura aberta: ou as empresas existentes concordam em adotar padrões comuns ou uma única empresa controlará todo o mercado.

Alguns analistas dizem que o fracasso dessas empresas em fornecer aos seus adeptos uma portabilidade real poderia desestimular o uso de seus serviços (HEYMAN, 2006: 13). Por outro lado, muitos argumentam que o conceito de portabilidade não está em discussão, mas sim a forma através da qual ele será implementado, inaugurando a próxima fase da *web*: a *web* social (HEYMAN, 2006). No próximo capítulo examinaremos como a rede social *Facebook* tem concebido a idéia da portabilidade. Por ora, encerremos com as considerações de Chirs Saad (*apud*. NAONE, 2008: *online*), co-fundador do *DataPortability Project*. Ele argumenta que, até agora, as empresas parecem querer que a portabilidade seja uma via de mão única, pois “alguns querem receber dados de outros *sites* sem conceder dados a ninguém, enquanto outros querem disponibilizá-los sem recebê-los – cada um na esperança de que o seu

site se tornará a ferramenta de uso primordial do usuário” (NAONE, 2008: *online*, tradução nossa).⁸⁸

⁸⁸ Tradução nossa para: “[...] many companies want data portability to be a one-way street. Some want to receive data from other sites without giving any up, while others want to provide data without receiving it – each hoping that its site will become a user's primary social tool”.

3 REVELAÇÃO, ACESSO E USO DE DADOS INDIVIDUAIS NO FACEBOOK

Como nos deixam entrever as evidências recolhidas no capítulo anterior, as redes sociais constituem um fenômeno complexo que coloca em jogo a revelação de informações, por um lado, e o acesso de diversas audiências aos dados individuais disponibilizados, por outro. Endereçar este conflito para o caso específico do *Facebook* é o objetivo deste capítulo, o que faremos a partir do recolhimento de evidências presentes na produção acadêmica e no discurso jornalístico relacionados, aliados à observação participante e ao uso do referido *site*. Antes, no entanto, dois esclarecimentos se tornam necessários. O primeiro deles visa justificar o uso da expressão dados individuais, usada em substituição ao termo dados pessoais, que a nosso ver, poderia restringir a compreensão dos leitores acerca da amplitude e da variedade de informações publicadas pelos usuários do *Facebook*. No entanto, o uso da palavra “individual” não quer dizer que estes dados só possuem valor de uso quando atrelados à identidade dos indivíduos. Como já ressaltamos no primeiro capítulo, este argumento é excessivamente empregado, de forma que julgamos leviana, para afirmar que, uma vez excluído o nome do detentor de uma determinada informação, o uso que dela se fará não implicará em invasão de privacidade (BRUNO, 2006). Portanto, o uso dos dois termos, dados pessoais e individuais, servem aqui para designar o conjunto de informações que são voluntariamente disponibilizadas pelos indivíduos nos *sites* de rede social, através do processo de revelação de informações (ACQUISTI e GROSS, 2005).

Um outro esclarecimento necessário diz respeito à iniciativa de elencar ao longo deste capítulo processos possivelmente associados à noção de vigilância. Ao mesmo tempo em que nosso objetivo é investigar a ocorrência – ou não – deste fenômeno nos *sites* de rede social, precisamos associar, de antemão, sua existência a um certo conjunto de fatos e evidências que nos possibilitem circunscrever nossa atenção e concentrar nossos esforços na condução da investigação pretendida. Esta licença metodológica será concretizada ao longo deste capítulo, no qual desenvolveremos um estudo detalhado do *Facebook*, visando compreender como funciona o *site* e como se dá a publicação, o acesso e a proteção dos dados individuais nele disponibilizados. Sob o ponto de vista do usuário comum, abordaremos a publicação de informações no *site*. Paralelamente, identificaremos em diversos setores tendências de uso destes corpos de dados para diferentes propostas, que incluem desde a seleção de candidatos em processos de admissão de universidades americanas a pais excessivamente cuidadosos e preocupados. Assim, esperamos recolher evidências que direcionem nossos esforços na condução das análises dos questionários respondidos e dos perfis coletados, que serão

apresentadas no próximo capítulo.

Desde já, é importante explicitar que enfatizaremos os usos comerciais e de audiências institucionais (policiais, empregadores etc.) e tenderemos a não nos deter em fenômenos já amplamente aceitos, como o uso social das informações disponibilizadas por amigos, curiosos etc. Partimos da perspectiva de que as características estruturais da rede impactam não somente as modalidades de interação entre os indivíduos no *Facebook* como também as formas de controle que nele podem emergir (GALLOWAY e THACKER, 2007). De maneira semelhante, acreditamos também que a estrutura de visibilidade de uma rede tem consequências sobre a percepção dos indivíduos acerca do ambiente em que interagem e sobre as formas de uso e expectativas que eles nutrem em relação ao meio. Assim, começaremos com uma descrição detalhada da estrutura do *Facebook*, buscando elucidar sua arquitetura de visibilidade particular e suas características, bem como as opiniões dos usuários e suas reações a novas funcionalidades implementadas. Em suma, nos lançaremos aqui a um trabalho de reconhecimento do papel desempenhado neste contexto pelos protocolos (GALLOWAY, 2004), que mediam as formas de interação existentes no *site*.

Além disso, buscaremos enfatizar as políticas da própria companhia acerca dos dados de seus usuários, formalizadas através de suas políticas de privacidade e termos de uso ou explicitadas através de suas atitudes, principalmente aquelas associadas aos serviços publicitários por ela oferecidos aos que desejam anunciar seus produtos e marcas no *site*. Abordaremos também o posicionamento da empresa acerca da portabilidade de dados e elucidaremos algumas das dinâmicas de trânsito e uso de informações individuais implícitas ao *Facebook Platform* e ao *Facebook Connect*, considerando especialmente os interesses das empresas desenvolvedoras, dos usuários de aplicativos e da própria empresa. Por fim, abordaremos também as estratégias de proteção dos dados individuais oferecidas aos usuários do *site*. Ao longo deste percurso, identificaremos a paradoxal condição através da qual um *site* cujos dados são efetivamente públicos se converte em um reduto familiar e habitual. Paralelamente, compreenderemos como este senso de proximidade entre os participantes e a ampla variedade de configurações de privacidade disponíveis desempenham o papel de fomentar a revelação de informações. Por fim, veremos como os dados publicados se prestam a usos nem sempre conhecidos ou visados por aqueles que interagem cotidianamente no *site* e apontaremos, assim, que os usuários do *Facebook* parecem ter às mãos uma nova tarefa: gerenciar não apenas sua imagem e reputação, mas os riscos inerentes aos silenciosos processos de uso de suas informações que emergem no *site*.

3.1 Uma arquitetura de visibilidade particular

Reunir grandes quantidades de informações pessoais verdadeiras em diretórios públicos, como acontece no *Facebook*, não é tarefa fácil, e a própria história do *site* é uma prova disso. Originalmente, o termo *facebook* designa um catálogo dado aos calouros universitários com informações sobre sua classe, contendo uma foto de cada integrante e dados sobre cada um, incluindo nome, data de nascimento, cidade e escola na qual cursaram o *high school*. Segundo Cassidity (2006: *online*), colocar o *facebook online* era um projeto da própria universidade de Harvard. No entanto, a realização de tal tarefa de maneira hierárquica e centralizada, com a criação de um departamento responsável por publicar as informações de todos os alunos, seria algo extremamente trabalhoso. Nas palavras do próprio Mark Zuckerberg, o *Thefacebook.com*, que surgiu na referida universidade em janeiro de 2004, era uma ferramenta que permitiria aos universitários realizar esta tarefa de maneira descentralizada, mantendo o controle sobre suas informações e escolhendo ativamente o que seria publicado. E ao que tudo indica, o então estudante de Psicologia estava correto. O *site* foi um sucesso instantâneo no campus universitário à época de seu lançamento, e segundo narra a história, apenas vinte e quatro horas depois de entrar no ar, ele já contava com cerca de 12 a 15 mil usuários, número que se expandiu para abranger três quartos da população de Harvard já no final do mês de fevereiro (CASSIDITY, 2006).

Dentre as possíveis razões para esta adesão em massa, uma nos é particularmente cara. O que diferenciava o ainda *TheFacebook.com* de outros *sites* de rede social já existentes, como o *Friendster* e o *MySpace*, era o fato de que ele possibilitava a construção de comunidades virtuais que compartilhavam previamente um espaço concreto e cotidiano. Isso mobilizava os usuários e fomentava um interesse de natureza diferente no uso do *site*. Olívia Ma, uma ex-estudante de Harvard e uma das primeiras pessoas a se cadastrar no *site*, descreve assim esta condição: “Eu me lembro do forte sentimento despertado pelo fato de que aquela pessoa cujo perfil você teria visitado na noite anterior poderia estar sentada tomando café na mesa próxima a você no refeitório na manhã seguinte” (MA, *apud.* CASSIDITY, 2006: *online*, tradução nossa).⁸⁹ Outro fator importante diz respeito ao fato de que a participação não era aberta a qualquer um: o cadastro era realizado utilizando o endereço de *e-mail* da

⁸⁹ Tradução nossa para: “I remember the buzz of excitement around the fact that that kid whose profile you had checked out the night before might be sitting at the table next to you in the dining hall the next morning at breakfast”.

universidade,⁹⁰ o que conferia aos usuários a idéia de estar interagindo em um ambiente mais familiar e, por conseguinte, mais confiável e seguro. “Porque os usuários do *Facebook* deveriam ter um endereço de *e-mail* válido de Harvard, a maioria eram estudantes e muitos estavam dispostos a publicar seus endereços de *e-mail* e residenciais, seu celular, e até mesmo sua orientação sexual” (CASSIDITY, 2006: *online*, tradução nossa).⁹¹ Definitivamente, a segurança não era uma preocupação mobilizadora da atenção dos participantes nestes primórdios.

Naturalmente, o *site* cresceu e se expandiu para outras universidades: em janeiro de 2004, ele já estava presente em 40 instituições (CASSIDITY, 2006). Neste momento, uma terceira decisão foi crucial para preservar o seu caráter exclusivista e intimista. Sua arquitetura de visibilidade foi construída para permitir que os perfis só pudessem ser acessados por estudantes da mesma instituição, ou no jargão do *Facebook*, dentro da mesma rede. A única alternativa a esta regra era o *link* de amizade: uma vez estabelecido, ele tornava os perfis dos amigos mutuamente visíveis, independente da universidade por eles freqüentada. Para fazer frente ao *MySpace*, seu concorrente principal, o *site* acabou abrindo a participação a qualquer usuário no ano de 2006. No entanto, a arquitetura das redes permanece. Hoje, elas totalizam mais de 175 mil,⁹² e podem ser de universidades, escolas de ensino médio, empresas ou geográficas (estas últimas agregam usuários por países, sendo que apenas EUA, Canadá e Reino Unido possuem redes para cidades). A participação em redes geográficas é livre, mas os usuários do *site* só podem mudar seu cadastro neste tipo de rede a cada 60 dias. De maneira geral, até hoje, a maior parte das redes de universidades, escolas e empresas exigem um *e-mail* da instituição ou organização para o cadastro dos participantes, que uma vez efetuado, passa a depender da aprovação de um moderador.

Desta forma, podemos concluir que a estrutura do *Facebook* é mais fechada do que a de outros *sites* de rede social hoje existentes. No *MySpace* e no *Orkut*, por exemplo, os perfis são visíveis a qualquer usuário do *site*, ainda que esta configuração possa ser alterada para torná-los disponíveis apenas aos amigos. O *Facebook* representa o avesso desta tendência.

⁹⁰ É comum entre as universidades americanas – e também em vários outros países do mundo – conferir aos novos alunos, no ato de seu registro, um endereço de *e-mail* da instituição (@cmu.edu para a *Carnegie Mellon*; @nyu.edu para a *New York University* etc.).

⁹¹ Tradução nossa para: “Because Facebook users were required to have a valid Harvard e-mail address, most were students, and many were willing to post their e-mail and home addresses, their cell-phone numbers, and even their sexual orientation”.

⁹² Levantamento realizado a partir dos dados disponibilizados pelo próprio *Facebook* em: <http://www.facebook.com/networks/networks.php?view=hs#/networks/networks.php?view=geographies>. De acordo com nossa medição, são 531 redes geográficas, 9.805 de ensino superior, 129.197 de ensino médio e 35.636 redes de empresas. Hoje, o próprio site convida seus usuários a sugerirem a criação de novas redes através do *link*: <http://www.facebook.com/help/suggestions.php>.

Nele, se um novo usuário se cadastra no *site* e não entra em nenhuma rede, ele só poderá ver o perfil dos seus amigos. Além disso, mesmo quando o usuário participa de uma rede, o acesso às informações dos demais participantes desta rede não é facilitado pela estrutura do *site*: enquanto o perfil dos amigos é eventualmente exibido diretamente na página daqueles com quem se mantém uma relação de amizade, os perfis daqueles que participam das mesmas redes só podem ser acessados por um caminho mais longo, que inclui o uso de ferramentas de busca ou o acesso às configurações da conta do usuário, na qual é possível editar e visualizar as redes das quais ele participa. Assim, a necessidade de possuir um *e-mail* da instituição para que se torne possível acessar os perfis dos participantes da respectiva rede, aliado à existência de um espaço real compartilhado, são fatores cruciais no estímulo à confiança dos usuários em seus pares, o que influencia diretamente a quantidade e a qualidade das informações por eles disponibilizadas (ACQUISTI e GROSS, 2005).

Outro fator que atua em sentido semelhante é o direcionamento que o *site* confere aos novos usuários no ato do cadastro, encorajando-os a publicar informações verdadeiras. Os termos do serviço também reforçam esta diretriz. Segundo este documento,⁹³ os usuários concordam em “fornecer informações precisas, atualizadas e completas sobre si assim que sejam requisitadas pelo *Site*” (FACEBOOK: *online*, tradução nossa).⁹⁴ Um contraponto a este modelo pode ser oferecido pelos *sites* para namoro, como o *Match.com*, no qual os usuários são incentivados a usar pseudônimos e a não fornecer informações de contato, por exemplo, preservando suas identidades. Assim, seja através de especificações técnicas, das regras do próprio serviço ou das normas sociais compartilhadas entre os usuários (ACQUISTI e GROSS, 2005: 72), o *Facebook* se propõe a ser um reduto para relacionamentos entre pessoas reais, que compartilhem um determinado espaço, que se conheçam ou que potencialmente possam vir a se conhecer. E neste contexto, o estabelecimento de relações entre os indivíduos é considerado como dependente da confiança estabelecida entre os membros: relações verdadeiras pedem que as informações reveladas sejam verdadeiras. Assim, os benefícios sociais implícitos ao uso do *site* se encontram vinculados a um grau de exposição considerável dos seus participantes.

No entanto, apesar da arquitetura de visibilidade restrita e da atmosfera de familiaridade e segurança que ela fomenta, o *Facebook* possui uma estrutura frágil, como qualquer outro *site* de rede social. Como argumentam Acquisti e Gross (2006: 3), para

⁹³ Disponível em: <http://www.facebook.com/terms.php?ref=pf>.

⁹⁴ Tradução nossa para: “[...] provide accurate, current and complete information about you as may be prompted by any registration forms on the Site”.

promover o contato entre as pessoas e aumentar seu valor de mercado, essas redes precisam facilitar o registro de novos usuários, a publicação e o acesso aos dados ali disponibilizados. Assim, apesar de sua arquitetura de visibilidade particular, devemos considerar que os dados publicados no *Facebook* são efetivamente públicos. O mecanismo de validação de *e-mails* para o cadastro em uma rede é altamente passível de fraudes. Afinal, como os processos de registro e de confirmação do *e-mail* são rápidos, basta o acesso temporário de um indivíduo a uma conta válida para que seja possível ter acesso aos perfis de todos os integrantes da rede considerada. Como ressaltam Acquisti e Gross (2005: 79), esta tarefa pode ser realizada através do acesso remoto a máquinas infectadas com vírus ou mesmo do acesso presencial a computadores de uso coletivo, nos quais eventualmente algum usuário possa ter fechado seu *webmail* sem se descadastrar. Para os casos em que não se requer um endereço de *e-mail* válido, como para o cadastro nas redes geográficas, a fraude fica ainda mais fácil: a criação de uma conta *fake*, ainda que em desacordo com os termos de uso do serviço, resolveria rapidamente o problema.

3.2 A publicação de informações do Facebook

No que diz respeito à publicação de informações, consideremos que ela pode acontecer: a) de maneira direta, ou seja, os dados são postados pelo próprio usuário; b) de maneira indireta, quando os dados sobre um indivíduo são publicados pelos amigos ou por ferramentas automatizadas do próprio sistema. Podemos distinguir em dez categorias, listadas abaixo, as principais formas de disponibilização de informações pessoais no *Facebook*:

- *Perfil*: inclui os dados presentes na guia de informações da página do usuário, como cidade, sexo, atividades, interesses, músicas, livros, informações de contato, formação e atuação profissional, além dos grupos e páginas dos quais ele participa/é fã. Aqui, as informações são adicionadas e editadas pelo dono da conta.

- *Wall*, ferramenta que passou a integrar o *site* ainda em 2004 e que constitui um espaço no qual os amigos de um usuário podem escrever para o dono do perfil, possibilitando a troca de mensagens públicas – elas ficarão visíveis àqueles que puderem acessar a página do usuário em questão.

- *Fotos*, ferramenta adicionada em 2005, que permite aos usuários construírem em suas páginas álbuns temáticos que ficarão visíveis aos que podem visualizar seu perfil. Além disso, o dispositivo permite que os usuários identifiquem aqueles que aparecem nas fotos, o que é feito através da inserção de um *link* que relaciona a imagem da foto ao perfil da pessoa

que nela aparece. Essa *tag* de identificação é, portanto, adicionada por terceiros (de maneira indireta) e não pode ser bloqueada automaticamente. Assim, só resta ao indivíduo que foi marcado em uma foto indesejada remover manualmente a *tag* inserida.⁹⁵

- *Vídeos*, ferramenta que permite aos usuários “uploadar” arquivos de vídeo de seus computadores, adicionando-os ao seu perfil.⁹⁶

- *Eventos*, ferramenta que permite aos usuários criarem em seu perfil um evento, adicionando informações sobre ele e convidando amigos para participar.⁹⁷

- *Grupos*, ferramenta lançada ainda em 2004 que permite que usuários com interesses semelhantes se agreguem em torno de um determinado tema. Nos grupos, eles podem trocar idéias no *discussion board*, postar itens e *links* para discussão e manifestar comunhão de interesses e visões de mundo.⁹⁸

- *Status*, ferramenta de *microblogging* presente no perfil do usuário, que o permite publicar informações sobre seu humor, sentimentos, afazeres etc. a cada vez que ele entra no *site*, em resposta à pergunta: “O que você está fazendo agora?”.⁹⁹

- *Mini-Feed* e *News-Feed*, ferramentas introduzidas no *site* em 2006, que fornecem históricos sobre as atualizações dos usuários do serviço. O *News-Feed* aparece na página inicial dos usuários e traz notificações sobre as ações recentes de seus amigos, permitindo que se possa visualizar com facilidade, acessando apenas uma página, o que tem acontecido em seu círculo social, *i.e.*, na vida de todos os contatos adicionados no *site*. Já o *Mini-Feed* é centrado em apenas um usuário, e aparece em seu perfil, listando históricos sobre suas atualizações: fotos adicionadas, páginas das quais ele se tornou fã, as novas relações de amizade por ele estabelecidas, os novos aplicativos por ele adicionados etc. É possível incluir no *Mini-Feed* também históricos das atividades recentes executadas em outros *sites*, como o *YouTube*, *Del.icio.us* etc. Vale ressaltar que, ao contrário de outros *sites* de rede social, nos quais ao entrarmos na página de nossos amigos, visualizamos diretamente as informações da guia de perfil, no *Facebook*, ao clicarmos no *link* da página de um amigo qualquer, somos direcionados imediatamente para uma página em que aparecem o *Wall* e o *Mini-Feed* do

⁹⁵ Segundo dados do próprio *Facebook*, mais de 700 milhões de fotos são postadas no *site* todo mês.
Cf.: <http://www.facebook.com/press/info.php?timeline#/press/info.php?statistics>.

⁹⁶ Segundo dados do próprio *Facebook*, mais de 4 milhões de vídeos são postados no *site* todo mês.
Cf.: <http://www.facebook.com/press/info.php?timeline#/press/info.php?statistics>.

⁹⁷ Segundo dados do próprio *Facebook*, mais de 2 milhões de eventos são criados no *site* mensalmente.
Cf.: <http://www.facebook.com/press/info.php?timeline#/press/info.php?statistics>.

⁹⁸ Segundo dados do próprio *Facebook*, o *site* possui hoje mais de 19 milhões de grupos ativos.
Cf.: <http://www.facebook.com/press/info.php?timeline#/press/info.php?statistics>.

⁹⁹ Segundo dados do próprio *Facebook*, mais de 13 milhões de usuários do *site* atualizam seu status no *Facebook* pelo menos uma vez por dia.
Cf.: <http://www.facebook.com/press/info.php?timeline#/press/info.php?statistics>.

usuário. De maneira semelhante, quando entramos no *site*, a primeira coisa que visualizamos é o *News-Feed*, com as ações recentes de nossos amigos.

- *Comentários*, ferramenta que permite ao próprio usuário ou aos seus amigos postar comentários sobre as fotos postadas, as novas amizades estabelecidas, sobre as atualizações de status etc. Em geral, quase todos os históricos do *Mini-Feed* suportam essa funcionalidade. Os comentários adicionados também são públicos, e ficam disponíveis no perfil do usuário para serem lidos por aqueles que podem visualizá-lo.

- *Aplicativos da plataforma*, ferramentas responsáveis por complexificar e levar a limites quase insondáveis as dinâmicas da revelação, do trânsito de informações e da expressão pessoal no *site*. O *Facebook* permite que qualquer desenvolvedor possa criar um aplicativo novo para o *site* e disponibilizá-lo para que os usuários que assim desejarem possam adicioná-los aos seus perfis. Mais de 52 mil aplicativos estão disponíveis no *Facebook Platform*, que recebe cerca de 140 novos aplicativos por dia.¹⁰⁰

Naturalmente, os processos de revelação de informações diretos oferecem aos usuários a possibilidade de controlar, escolher e censurar empiricamente o que é ou não publicado. Neste sentido, podemos constatar que os processos indiretos, aqueles nos quais as informações são publicadas através de terceiros ou de processos automatizados, são os mais controversos, como acontece no caso do *News-Feed* e do *Mini-Feed*. Essas ferramentas monitoram constantemente todos os perfis existentes no *site* e representam uma instância onipresente e onisciente em relação às ações dos indivíduos no *Facebook* e em sítios parceiros, conferindo uma visibilidade imediata e descomplicada às suas atitudes e mapeando-as com precisão em um sistema textual de históricos curtos que facilita sua apreensão por parte da audiência. Seria uma tarefa dispendiosa entrar no perfil de cada um de nossos amigos e verificar a cada dia suas atualizações. No entanto, com o *News-Feed*, basta logar o *Facebook* e nossa página inicial nos fornecerá as atualizações de todos eles, munidas de *links* para seus perfis, para que as novidades possam ser contempladas com mais detalhes. Essas ferramentas desconhecem o esquecimento, registram e arquivam tudo e permitem reconstruir com requintes barrocos nossa história no *site*, da abertura da conta ao estabelecimento das mais recentes relações de amizade.

¹⁰⁰ Atualmente, mais de 95% dos usuários do site usam pelo menos um aplicativo disponibilizado através da plataforma. Cf.: <http://www.facebook.com/press/info.php?timeline#/press/info.php?statistics>.



Fig. 1: Guia de informações de um perfil no *Facebook*.



Fig. 2: Wall e Mini-Feed. Note, no campo de endereço do navegador, o ID do usuário.

A reação dos usuários do *Facebook* à introdução do *News-Feed* e do *Mini-Feed*, na época de sua adição ao *site*, não foi das melhores. Elas foram consideradas uma ameaça à privacidade dos membros do serviço e uma onda de protestos invadiu o *site*, pedindo que elas fossem desativadas ou que o *opt-out* fosse permitido. Milhares de pessoas enviaram *e-mails* para a companhia e um grupo, aberto no *Facebook* na manhã daquele dia 5 de setembro, intitulado *Students Against Facebook News Feed*,¹⁰¹ já contabilizava mais de 100 mil membros no final do dia. Estudantes na Flórida planejavam um boicote ao *site* no dia 12 de

¹⁰¹ Disponível em:

<http://www.facebook.com/s.php?ref=search&init=q&q=students+against+facebook+news+feed&sid=4e2136b1f01bbae8a88c61a7c0461f6b#/group.php?sid=4e2136b1f01bbae8a88c61a7c0461f6b&gid=2208288769>.

setembro daquele ano (LACY, 2006: *online*) e uma petição *online* contra os novos dispositivos chegou a ser assinada por 113.550 internautas.¹⁰² Por fim, Zuckerberg (2006: *online*) se desculpou publicamente através de um post no *weblog* da empresa pela falta de clareza no lançamento dessas funcionalidades e pelo fato de elas não terem vindo acompanhadas por controles de privacidade adequados. Posteriormente, a página de configurações de privacidade passou a incluir o controle dos tipos de históricos que apareceriam no *News-Feed* e no *Mini-Feed*, além de listar as informações que nunca são compartilhadas através destes dispositivos. Com o tempo, muitos daqueles usuários furiosos desistiram dos protestos e mudaram de idéia: hoje, eles dizem gostar das ferramentas de *feeds*, sintoma de uma profunda mudança de postura e comportamento.

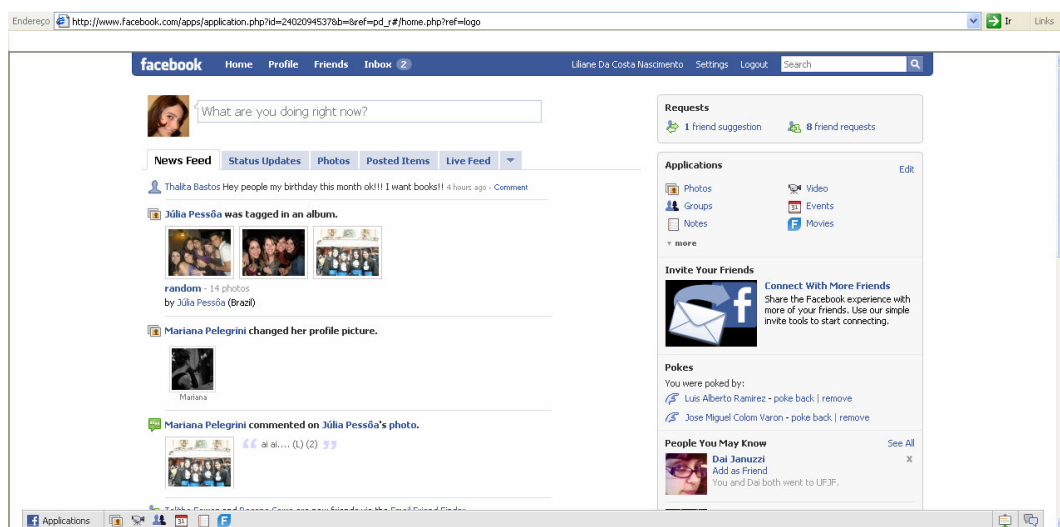


Fig. 3: Página inicial dos usuários no *site*, com o *News-Feed*.

No ano de 2008, novos reclames em relação a esses mesmos dispositivos surgiram, agora baseados no fato de que a possibilidade de excluir manualmente históricos do *Mini-Feed* postados no perfil na verdade não os excluía do *News-Feed*, que é entregue a todos os amigos de um determinado usuário. Na verdade, esta mudança só pode ser efetuada se o usuário visita as configurações de privacidade da sua conta e define que, dali em diante, toda a categoria de mensagens entre as quais se encontra a que para ele é indesejada deixarão de ser postadas nos *feeds*. No entanto, desta vez, os protestos vieram sem a mesma força de antes,¹⁰³ seja porque o *Facebook* se tornou mais eficiente em ouvir seus usuários ou porque

¹⁰² Disponível em: <http://www.petitiononline.com/faceb00k/petition.html>.

¹⁰³ Ver o grupo "If I hide something in my mini-feed it shouldn't show in my friends's news", disponível em: <http://www.facebook.com/group.php?gid=7967973537>.

aqueles jovens se acostumaram a este ambiente de exposição naturalizada. Ben Parr, o garoto que abriu o primeiro grupo de protesto contra o *Facebook* em 2006, afirma hoje categoricamente que não se importa mais com sua privacidade e que, neste meio tempo, “[...] nossas visões sobre o que deveria ser compartilhado, o que não deveria ser compartilhado, e com quem compartilhamos nossas vidas mudaram ao máximo” (PARR, 2008: *online*, tradução nossa).¹⁰⁴ Consideramos que estes episódios são emblemáticos por dois motivos. O primeiro deles tem a ver com a importância crucial da implantação do *News-Feed* e do *Mini-Feed* para a evolução do *Facebook*, já mencionada pela porta-voz da companhia, Melanie Deitch (*apud*. LACY, 2006: *online*) na ocasião da revolta de 2006. Essas ferramentas não só deram ao *site* uma funcionalidade única dentre os *sites* de rede social na época como subsidiaram muitas das futuras tentativas de monetização do serviço por parte da companhia. O segundo motivo pelo qual este episódio nos interessa envolve uma questão um pouco mais complexa, que pensaremos no decorrer deste trabalho: o que, de fato, incomodou esses usuários furiosos e qual a natureza das reivindicações embutidas nestes reclames por privacidade?

Uma vez que as informações disponibilizadas já eram públicas, mas protegidas pelo senso de familiaridade e proximidade fomentado pela estrutura do *site* e alimentado pelos usuários, pensamos que, nesta ocasião, o que mais feria a liberdade dos internautas era a idéia de que o controle empírico – *i.e.*, no ato da postagem – sobre o que era publicado a respeito de suas vidas em suas vitrines virtuais não estava mais sob o toque do teclado, mas nas mãos de um sistema de monitoramento que transformava suas atitudes em informações sobre eles. O aqui e agora deste momento de decisão, assim como as certezas e hesitações vivenciadas pelos usuários, foram suprimidos por um cálculo diferente, ao qual eles deveriam se acostumar dali em diante: se eu fizer isso, esta ação será notificada da forma ‘x’ ou ‘y’ nos meus *feeds*. Essas ferramentas abrem então um primeiro caminho em direção às rotinas do controle indireto da informação, através de configurações de privacidade cada vez mais refinadas e que implicam formas de manejo mais custosas e complicadas para os usuários. No entanto, tais configurações se mostram cada vez mais frágeis em um ambiente no qual a exposição voluntária figura lado a lado com as ambições de diversos setores sobre os dados individuais, inclusive as da própria empresa que os hospedam.

¹⁰⁴ Tradução nossa para: “Our views on what should be shared, what shouldn’t be shared, and with whom we share our lives are what have changed the most”.

3.3 A publicidade no Facebook

Analisemos agora as dinâmicas do uso de informações pessoais dentro dos novos programas para a publicidade social e direcionada hoje existentes no *site*. Começamos pelo sistema *Facebook Ads*, lançado pela companhia em 2007. Três funcionalidades conferem corpo a este novo sistema. A primeira delas são as *Facebook Pages*, através das quais os anunciantes podem construir perfis para suas marcas, empresas e produtos.¹⁰⁵ Assim como ocorre na criação de uma página pessoal, trata-se aqui de escolher a que aspectos da marca dar visibilidade e de que maneira. A segunda funcionalidade do *Facebook Ads* é um novo sistema de anúncios chamado *Social Ads*, que combina as peças publicitárias com ações de amigos sobre um produto, serviço ou marca. A idéia é associar o direcionamento de anúncios relevantes com referências confiáveis provenientes de nosso círculo social.¹⁰⁶ Por fim, o *Facebook Ads* conta ainda com o *Facebook Insights*, uma interface que fornece aos anunciantes dados sobre as atividades, tendências, demografia dos fãs e desempenho dos anúncios veiculados, permitindo-os ajustar o *targeting* de suas mensagens. O serviço é disponível para todas as páginas de anunciantes e anúncios sociais.

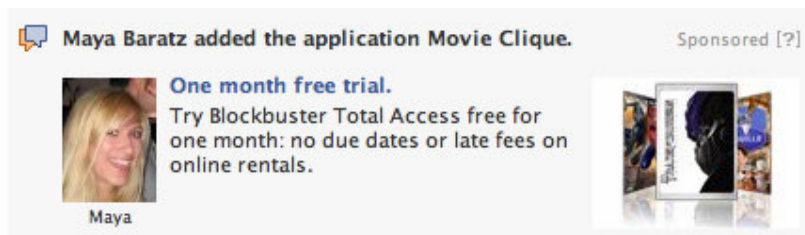


Fig. 4: Imagem de anúncio social do *Facebook* (*Social Ads*). Fonte: MCCARTHY, 2008: online.

Podemos notar que o *Facebook Ads* agencia duas idéias fundamentais: a) a de que os anunciantes possam usar informações sobre os usuários do *site* e sobre como eles interagem com suas peças publicitárias para maximizar a eficácia de seus anúncios; b) a de usar a estrutura social dos laços de amizade para fomentar o consumo, concebendo os amigos como fonte de recomendação segura e propagadores de referenciais e tendências que levem ao

¹⁰⁵ A idéia é a de que os usuários possam se associar e interagir com esses perfis institucionais assim como interagem com seus amigos, escrevendo no mural da página, usando os aplicativos nela inseridos, adicionando fotos e vídeos etc. Todas essas ações podem ser integradas no *News-Feed* e no *Mini-Feed* dos usuários.

¹⁰⁶ Se um anunciante deseja usar esta modalidade de anúncios, o primeiro passo é definir as ações sociais que devem ser consideradas (por exemplo, o fato de um usuário adicionar um aplicativo ou se tornar fã de um perfil institucional). Quando esta ação é executada, ela é associada pelo site ao anúncio da campanha, que aparecerá lado a lado a um histórico da ação e da foto do usuário que a executou. Este tipo de anúncio é mostrado então aos amigos do usuário em questão, aparecendo no *News-Feed* ou na lateral do site, no espaço tradicionalmente destinado à publicidade.

desejo pela compra de novos produtos e serviços. Como se pode claramente notar, a iniciativa é a de usar a estrutura gerada pelas redes de relações mantidas entre os indivíduos para direcionar os esforços de publicidade e alavancar o consumo. Nas palavras de Zuckerberg (*apud*. FACEBOOK, 2007: *online*, tradução nossa), o sistema é baseado na idéia de que pessoas influenciam pessoas: “Não se trata mais apenas de mensagens que são veiculadas aos espectadores pelas companhias, mas cada vez mais de informações que são compartilhadas entre amigos”.¹⁰⁷ No entanto, as reações dos usuários a este novo sistema de publicidade mostram que, para eles, ter sua imagem e seus dados individuais usados para promover produtos e marcas pode estar bem longe do que Zuckerberg considera compartilhar informações, constituindo uma prática abusiva.

Consideremos, especialmente, o *Social Ads*. A maior parte das queixas relacionadas ao sistema são provenientes do fato de que a ferramenta não pede permissão ou notifica os usuários no momento em que eles executam no *site* as ações que, em um futuro próximo, serão associadas aos anúncios publicitários. O release de lançamento do produto se limita a dizer que “nenhuma informação pessoal é compartilhada com o anunciante que cria um *Social Ad*”¹⁰⁸ e que “os usuários do *Facebook* só verão os *Social Ads* na medida em que seus amigos estão compartilhando informações com eles” (FACEBOOK, 2007: *online*, tradução nossa)¹⁰⁹. No entanto, como ressaltam Solove (2007: *online*) e Hansell (2007: *online*), existe uma grande diferença entre expressar no próprio perfil algo positivo em relação a uma marca e ter esta ação usada para anunciá-la aos seus amigos. O fato de que os indivíduos resolvam manifestar de maneira pública sua relação com serviços e produtos não pode ser tomado como consentimento para a publicação desta ação em outro contexto – principalmente quando nele o usuário em questão aparece dando credibilidade a um anúncio publicitário (MCGEVERAN, 2007a: *online*).¹¹⁰ A estratégia do *Facebook* é captar a atenção do público através da associação com o círculo social dos usuários, em uma tentativa de impedir que os anúncios publicitários sejam ignorados, como é comum acontecer nos *sites* de rede social. No entanto, como nos relembra Hansell (2007), para os usuários destes *sites*, a associação a artistas e

¹⁰⁷ Tradução nossa para: “It’s no longer just about messages that are broadcasted out by companies, but increasingly about information that is shared between friends.”

¹⁰⁸ Tradução nossa para: “No personally identifiable information is shared with an advertiser in creating a Social Ad”.

¹⁰⁹ Tradução nossa para: “Facebook users will only see Social Ads to the extent their friends are sharing information with them”.

¹¹⁰ Para McGeeveran, professor da *University of Minnesota Law School*, a manobra do *Facebook* pode ser compreendida como invasão de privacidade pela lei americana, por implicar a apropriação do nome desses usuários em benefício das marcas anunciadas. O autor lembra que a lei do estado de Nova York, por exemplo, considera que o nome, a foto ou a voz de uma pessoa não podem ser usados para propostas comerciais sem prévio consentimento por escrito do referido indivíduo (MCGEVERAN, 2007b: *online*).

produtos é uma forma de expressar a personalidade e o gosto, donde podemos dizer que essas ações estão envolvidas nas complexas estratégias de construção da imagem pessoal e da exposição de si. E justamente por isso, esses usuários não se mostram felizes quando alguma informação pessoal é exposta de maneira que não corresponda exatamente a sua vontade.

Outra iniciativa que registrou níveis de desaprovação semelhantes foi o sistema de anúncios *Facebook Beacon*, lançado em 2007. Trata-se de uma ferramenta que informa os seus amigos sobre ações que você executa em *sites* parceiros do *Facebook*. Suponhamos que você vá ao *site* da *Blockbuster* e alugue um filme, ou faça uma compra no *Overstock.com*. Caso você esteja logado no *Facebook*, o *site* afiliado exibirá uma notificação que lhe confere a possibilidade de publicar um histórico dessas ações no seu *Mini-Feed* e no *News-Feed*, exibindo-a a todos os seus amigos. O *Beacon* notificava os indivíduos de que as ações que estavam realizando em *sites* externos seriam enviadas ao *Facebook* através de uma pequena janela que aparecia no canto inferior da página por apenas 20 segundos. Decorrido este tempo, a ausência de uma resposta negativa era tomada como consentimento explícito, e a ação era reportada ao *Facebook*.¹¹¹ Logo, muitos começaram a reclamar do fato de que as notificações eram imperceptíveis.¹¹² Depois das primeiras reações negativas, a ausência de resposta à mensagem de alerta que aparecia no *site* afiliado passou a implicar na publicação do histórico no prazo de 2 dias. No entanto, a principal falha do sistema estava no fato de que o *Beacon* foi lançado no sistema *opt-out*, ou seja, os usuários eram automaticamente incluídos no programa e surpreendidos por essas mensagens abusivas.

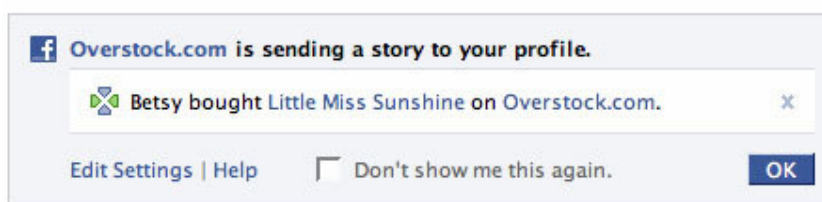


Fig. 5: Imagem de uma notificação do *Facebook Beacon*. Fonte: SCHIFFMAN, 2007: *online*.

A organização *Move.On.org* entrou com uma ação civil contra o *site* e em apenas 10 dias, uma petição que apoiava a iniciativa foi assinada por mais de 50 mil usuários do serviço

¹¹¹ Uma segunda chance era dada aos usuários quando logavam sua conta no site, no entanto, este segundo aviso poderia passar igualmente despercebido se o indivíduo fosse diretamente checar suas mensagens ou o perfil de um amigo.

¹¹² Entre os dias 6 (quando o sistema foi lançado) e 29 de novembro, o alerta para impedir a publicação de históricos *Beacon* foi mudado 4 vezes pelo *Facebook*. Em todas essas versões, as opções para publicar o histórico e para permitir permanentemente a publicação são as mais visíveis. Cf. STORY, 2007.

(STONE e STORY, 2007: *online*). Igualmente, muitos grupos pipocaram no *Facebook* protestando contra o *Beacon*.¹¹³ Por fim, a companhia admitiu os erros com a implantação do programa e mudou a forma de operação do *Beacon*. A partir de então, os usuários que ignoravam os alertas não tinham mais suas ações exibidas no *Facebook*.¹¹⁴ No entanto, por um bom tempo, a empresa insistiu em não permitir uma configuração universal de exclusão do programa alegando que os usuários precisavam experimentar o *Beacon* antes de decidir por não participar: assim como no caso da revolta do *News-Feed*, a aposta era a de que, com o tempo, os usuários se apaixonariam pela novidade (STORY, 2007: *online*). No entanto, as propostas dessas duas ferramentas são bem diferentes. Enquanto o *News-Feed* visa monitorar o que acontece no círculo social dos usuários, os históricos produzidos pelo *Beacon* visam fundar um contexto favorável para a inserção de anúncios publicitários, nos quais os participantes do *site* figurariam como fonte de recomendação segura para seus amigos. Assim, finalmente, a companhia acabou cedendo e lançou um controle de privacidade que permite desligar completamente o programa (ZUCKERBERG, 2007: *online*).

O fato mais importante acerca do *Beacon* e talvez o menos comentado é que, enquanto os usuários se revoltavam com a visibilidade que o programa conferia às suas ações, uma prática silenciosa da empresa passava despercebida: o rastreamento das atividades dos usuários do *Facebook* fora dos limites do *site*. Como reporta Stefan Beteau, engenheiro do *CA's Threat Research Group*, ao contrário do que afirmava o *Facebook*,¹¹⁵ o *site* estava coletando informações sobre as ações dos usuários em *sites* afiliados mesmo quando esses indivíduos optavam por não compartilhar os históricos e mesmo quando eles não estavam logados no *Facebook* (BETEAU, 2007: *online*).¹¹⁶ Quando um *site* se torna um afiliado *Beacon*, linhas de *Javascript* são incluídas em seu código fonte. Elas são responsáveis por

¹¹³ Dois dos mais expressivos são os grupos *Facebook users against Facebook Beacon* e *Petition: Facebook, stop invading my privacy!* – com respectivamente 1974 e 71904 membros em 15/01/09.

¹¹⁴ Hoje, esta publicação depende de uma confirmação dada pelo usuário em resposta a uma mensagem que é exibida diretamente em seu perfil. Caso ele ignore também este alerta, o histórico *Beacon* fica armazenado. Da próxima vez que um novo histórico for enviado ao *Facebook*, a notificação exibida listará também os históricos antigos, que poderão ser removidos definitivamente ou publicados.

¹¹⁵ Posteriormente, a companhia admitiu que coletava informações sobre as atividades de usuários não “logados” e daqueles que optavam por não compartilhar seus históricos (PEREZ, 2007: *online*).

¹¹⁶ Para comprovar que as afirmações da companhia acerca do funcionamento do seu novo sistema não eram verdadeiras, Beteau (2007: *online*) realizou um teste simples. O engenheiro executou uma ação em um *site* parceiro em três condições: logado no *Facebook* e com o *site* aberto, com o *site* fechado sem antes realizar *logout* e depois de se desconectar do *site* e reiniciar a seção do *browser*. Em todos os três casos, ele optava por não enviar o histórico ao seu perfil. Ao verificar com um *sniffer* o tráfego da rede ele descobriu, para sua surpresa, que em todos os três casos as informações foram repassadas ao *Facebook*. No terceiro caso, o mais espantoso, se a máquina nunca foi usada para logar o *Facebook* ou se o usuário nunca marcou a opção “*remember me*” (para evitar que ele tenha que digitar novamente seu *login* toda vez que deseja acessar o *site*), os dados são enviados mas não são associados ao ID do usuário no *Facebook*.

enviar ao *Facebook* uma série de variáveis, como a *url* dos itens visitados e as informações buscadas pelo usuário no *site* parceiro. Uma vez que essas variáveis tenham sido preparadas, elas chamam uma página do *Facebook* e repassam estes parâmetros. Só aí, então, o sistema verifica a presença do *cookie* que aponta se o usuário está logado para então lhe exibir o alerta que o notifica que um histórico está sendo enviado ao seu perfil. Mas como enfatiza Berteau (2007), a essa altura, toda a informação coletada sobre as atividades dos indivíduos no *site* afiliado já foram enviadas ao *Facebook*.

Note, assim, que o trânsito de dados em questão envolve muito mais do que a publicação de um histórico ao seu grupo de amigos, mas uma coleta bem mais ampla de dados, que somados àqueles já disponibilizados pelos usuários em seus perfis, podem fornecer padrões acurados do comportamento, tendências, preferências e interesses destes internautas. Assim, pouco importa que o *Beacon* nos pergunte se queremos ou não enviar um histórico de nossas ações ao nosso perfil. Quando esta pergunta nos é direcionada, informações muito mais relevantes já foram coletadas sem que sequer soubéssemos. Segundo o *Facebook*, esses dados, enviados com o intuito de saber se o usuário está logado e gerar o alerta de notificação, são devidamente apagados se ele decide não compartilhar o histórico.¹¹⁷ No entanto, fica uma pergunta: porque o caminho adotado não poderia ter sido verificar se o usuário está logado primeiro e enviar os dados depois? Assim, podemos concluir que o problema do *Beacon* não é a publicação, mas a coleta silenciosa de dados efetuada pelo *site* em seus afiliados, fato que permanece fora do foco de atenção e do controle dos usuários do serviço.

Consideremos agora como se dá o *targeting* dos anúncios publicitários no *Facebook*. Quando os usuários logam sua conta, o *Facebook* coleta dados sobre o tipo de *browser* usado e o IP da conexão. Como claramente explicitado na política de privacidade do *site*, ele se reserva também o direito de coletar informações dos perfis de todos os usuários e de fontes externas e usá-las para direcionar anúncios aos seus usuários.

O *Facebook* pode usar a informação do seu perfil sem identificá-lo individualmente a terceiros. Nós fazemos isso para propostas como reunir quantas pessoas em uma rede gostam de uma banda ou filme e personalizar os anúncios e promoções que podemos fornecer a você no *Facebook*. Nós acreditamos que isso o beneficia. Você pode saber mais sobre o mundo ao seu redor e, onde existem anúncios publicitários, é mais provável que eles o interessem. Por exemplo, se você coloca um filme favorito em seu perfil, nós podemos servi-lo com um anúncio sobre a exibição de um filme similar

¹¹⁷ Esta informação é explicitada com clareza na FAQ *How does Beacon work?*, disponível em: <http://www.facebook.com/beacon/faq.php>. As afirmações da companhia sobre o fato de que não há coleta de dados de usuários não logados e daqueles que optam por não compartilhar os históricos podem ser encontradas tanto nesta FAQ quando nos *e-mails* trocados por Berteau (2007: *online*) com representantes da empresa.

em sua cidade. Mas nós não dizemos à empresa cinematográfica quem você é (FACEBOOK: *online*, tradução nossa).¹¹⁸

Além disso, ainda segundo a política de privacidade do *site*:

O *Facebook* pode coletar também informações sobre você de outras fontes, como jornais, blogs, serviços de *instant messaging*, e de outros usuários do *Facebook* através da operação do serviço (por exemplo, *tags* em fotos) para oferecer a você informações mais úteis e uma experiência mais personalizada (FACEBOOK, *online*, tradução nossa).¹¹⁹

No ato da contratação de uma campanha publicitária, os anunciantes podem definir as características demográficas e possíveis campos de interesse da audiência que desejam alcançar: sexo, idade, localização geográfica, instituições de ensino superior e palavras-chave podem ser selecionados através do sistema de anúncios do *site*.¹²⁰ As possibilidades que podem emergir desta associação de informações são infinitamente amplas. Se uma pessoa vive em uma determinada cidade, pode receber propaganda de eventos que ocorrerão na região; pessoas interessadas em um determinado estilo musical, autor ou diretor podem receber anúncios de produtos que correspondem ao seu gosto (livros, ingressos, CD's, DVD's etc.); aquelas listadas como noivas supostamente estariam interessadas em serviços para a festa de casamento e de acordo com a trajetória educacional e com a área de atuação do indivíduo, até mesmo oportunidades de formação profissional podem ser direcionadas. Com os avanços das pesquisas realizadas na área, correlações ainda menos óbvias – traçadas, por exemplo, através de medições de semelhança entre os indivíduos ou dos cliques de interesse (LIU *et al.*, 2005) – permitirão associar, no futuro, um contexto de preferências manifestas com uma estética ou padrão particular (a música do artista “x”, a pintura de “y” e o tipo “z” de comida poderiam corresponder a um estilo latino, por exemplo) a partir do qual outros gostos poderão ser inferidos, potencializando os mecanismos de recomendação existentes.

¹¹⁸ Tradução nossa para: “Facebook may use information in your profile without identifying you as an individual to third parties. We do this for purposes such as aggregating how many people in a network like a band or movie and personalizing advertisements and promotions so that we can provide you Facebook. We believe this benefits you. You can know more about the world around you and, where there are advertisements, they're more likely to be interesting to you. For example, if you put a favorite movie in your profile, we might serve you an advertisement highlighting a screening of a similar one in your town. But we don't tell the movie company who you are”.

¹¹⁹ Tradução nossa para: “Facebook may also collect information about you from other sources, such as newspapers, blogs, instant messaging services, and other users of the Facebook service through the operation of the service (e.g., photo tags) in order to provide you with more useful information and a more personalized experience”.

¹²⁰ A localização é rastreada pelo IP do usuário, enquanto os demais dados são retirados de seus perfis. As palavras-chave são baseadas em ocorrências dos campos atividades, interesses, músicas favoritas, programas de TV, filmes e livros da guia de informação dos perfis.

Por fim, no mês de agosto de 2008 o *Facebook* lançou sua última novidade: o *Engagement Advertisements*, baseado na idéia de levar os usuários a interagir com os anúncios publicitários e compartilhar as ações realizadas com seus amigos. Com o sistema, eles poderão se tornar fãs de um perfil institucional a partir de um anúncio, enviar presentes relacionados a uma marca ou produto para os seus amigos (comportamento já popularizado no *site* através dos aplicativos da plataforma) e comentar os anúncios exibidos, sendo que esta última ação será integrada no *News-Feed*, que entregará históricos a todos os contatos do usuário no *site* (OWYANG, 2008: *online*). Ao invés de direcionar os usuários para um *site* externo, estes anúncios visam produzir ações sociais em torno deles dentro do *Facebook*. Este arsenal de opções oferecidas aos anunciantes é um indício da insistente busca da companhia por um modelo adequado para a monetização do *site*. No entanto, os resultados obtidos no último ano não são animadores, isso sem levar em conta os embates freqüentes com os usuários por conta das inovações muitas vezes consideradas abusivas. Este é um fator importante, pois a tendência é a de que quanto mais positivos forem os resultados, menos significantes se tornarão os protestos dos usuários. Como afirma a analista da *Jupiter Research*, Emily Riley (*apud*. ELKINS, 2007: *online*), mesmo que alguns resolvam deixar o serviço revoltados com estas inovações, sendo o *Facebook* um *site* suportado pela renda de publicidade, só o restará considerar que esta perda é inevitável.

Top 10 Online Display Advertising Publishers in the US, Ranked by Total Display Ad Views, June 2008

	Total display ad views (millions)	Share of display ads	Advertising-exposed unique visitors (millions)
1. Fox Interactive Media	52,228.0	15.9%	83.7
2. Yahoo! sites	34,675.0	10.5%	130.7
3. AOL LLC	19,004.0	5.8%	96.5
4. Microsoft sites	15,485.0	4.7%	87.7
5. Google sites	5,075.0	1.5%	81.9
6. Facebook	3,650.0	1.1%	30.7
7. eBay	3,512.0	1.1%	52.2
8. Viacom Digital	3,114.0	0.9%	36.4
9. Comcast.net	2,644.0	0.8%	11.9
10. Glam Media	2,237.0	0.7%	33.5
Total Internet	329,828.0	100.0%	180.6

Note: home, work and university locations
Source: comScore Ad Metrix as cited in press release, August 26, 2008
097853 www.eMarketer.com

Fig. 6: Dados da *comScore* (2008: *online*) para o mercado de anunciantes americanos.
Fonte: *eMarketer.com* (2008: *online*).

A companhia afirma que 70 dos 100 maiores anunciantes americanos já veicularam publicidade no *site* desde 2007 (VASCELLARO, 2008: *online*). No entanto, segundo dados publicados em junho de 2008 pela *comScore*, o *site* foi apenas o sexto maior veiculador de

publicidade *online* nos EUA no mês de junho de 2008, com uma parcela de apenas 1,1% do número total de anúncios exibidos no país no referido período. O *MySpace* permanece à frente, com 15,9% deste total. A medição da *comScore* não contempla, por exemplo, os novos formatos de anúncios, como os que integram o *Engagement Advertisements*. Assim, as expectativas são de que os resultados da companhia cresçam com a incorporação destas novas parcelas, nas quais o *site* tem concentrado seus esforços nos últimos anos (E-MARKETER, 2008: *online*). Mas, por enquanto, Owyang (2008: *online*), analista da *Forrester Research*, estima que os usuários do *Facebook* cliquem nos anúncios do *site* a uma taxa menor que 1%. Para ele, este baixo retorno é decorrente dos objetivos e do foco de atenção dos usuários, que ao usarem um *site* de rede social, estão preocupados em se expressar e interagir com os outros, e não em procurar por produtos, anúncios ou informações (OWYANG, 2008). O autor ainda apresenta dados que comprovam essa hipótese e lista os comportamentos mais comuns dos jovens em *sites* de rede social: a) Ver o que os amigos estão fazendo: 86%; b) Mandar uma mensagem a alguém: 79%; c) Postar ou atualizar o próprio perfil: 70%; d) Olhar perfis de pessoas desconhecidas: 65%.¹²¹

As discussões em torno destas controversas iniciativas do *Facebook* nos permitem listar alguns fatos e argumentos recorrentes. O primeiro deles é o de que, ainda que seja difícil precisar a adesão dos usuários a estes protestos, podemos afirmar que, em geral, o número de pessoas que demonstrou sua indignação em grupos abertos contra o *Beacon*, o *Social Ads* e contra as políticas de coleta, mineração e trânsito de dados no *site* é pequeno em relação ao número total de usuários do serviço.¹²² No entanto, é interessante notar que estes grupos possuem temáticas amplas e variadas, abrangendo fenômenos tão diversos quanto o acesso a informações pessoais por parte de autoridades como empregadores, agências governamentais etc. até as práticas de publicidade direcionada do próprio *Facebook*. Para muitos estas mobilizações são vistas com descrédito, dado o passado de ameaças não cumpridas por parte de militantes furiosos prometendo – e apenas prometendo – fechar suas contas e deixar o *site*. Isto aconteceu na ocasião dos protestos no *News-Feed*; nos protestos contra a abertura do *site* à participação de qualquer um (e não mais apenas a estudantes de escolas e universidades

¹²¹ Segundo dados da *North American Technographics Retail And Marketing Online Youth Survey, Q4 I*, realizada em 2007 pela *Forrester Research*.

¹²² *Petition: Facebook, stop invading my privacy!*, 71904 membros; *Facebook users against Facebook Beacon*, 1974 membros; *Facebook, don't use my conversations for commercial purposes, or I'll leave*, 1943 membros; *Stand Up! Don't Let Facebook Invade Your Social Life With Ads!*, 528 membros; *Facebook Users Against Personally Targeted Advertising and Data Mining*, 359 membros; *We will leave Facebook if you start bombarding us with advertisements*, 311 membros; *Help stop Facebook's Beacon: hacks personal info for marketing purposes!!*, 308 membros; *We don't want information from Facebook sold and spread to outsiders!*, 206 membros. Consulta em 15/01/08.

cadastradas, em 2006) e também nos casos mais recentes do *Beacon* e do *Social Ads*. Para o estudante Tony Gingrasso (apud. ELKINS, 2007: *online*), com o tempo, as pessoas aceitarão o *Social Ads* como parte do *site*, expectativa semelhante à da diretoria da empresa em relação ao *Beacon* (STONE e STORY, 2007: *online*). No entanto, ainda que não tenham fechado suas contas, muitos usuários do serviço já deram provas suficientes de que estão de olho nas políticas da empresa.

Neste complicado debate, as opiniões se dividem. Para usuários como o australiano Anthony Baken, os anúncios são o preço que se paga pelo uso gratuito do serviço.¹²³ Enquanto muitos se sentem desrespeitados, outros afirmam que receber anúncios direcionados é algo interessante, como é o caso do americano Cameron Battle.¹²⁴ Para ele, a mudança significa que agora veremos anúncios de produtos que queremos comprar, e não apenas “lixo randômico”. Outros reclamam de erros no direcionamento dos anúncios, como é o caso do australiano Chris Kettle: “estou doente de ver anúncios para *gays* – eu defini meu interesse em mulheres – ALÔ?!”.¹²⁵ Esta reclamação pode assumir contornos ainda mais complexos, como relata Rachel Beckman (2008: *online*) em matéria ao *Washington Post*, na qual a autora narra sua revolta contra a insistência do *site* em direcionar-lhe anúncios sobre dietas e perda de peso. Ela afirma que, como o *Facebook* sabe muitas informações sobre seus usuários, nele o *targeting* publicitário fica completamente diferente daquele outrora realizado pelas empresas de TV, por exemplo, que mostram anúncios de brinquedos junto com os programas infantis. Ela considerou ofensivo o anúncio com o título “*muffin top*”,¹²⁶ em que aparecia uma mulher vestida em um jeans justo e com culotes à mostra. Depois de reportar o anúncio e atualizar o seu perfil dizendo que estava noiva, ela passou a receber coisas do tipo “Você quer ser uma noiva gorda?”, considerados tão ofensivos pela autora quanto aqueles que ela diz receber hoje, depois do casamento, perguntado se ela deseja engravidar e recomendando clínicas para tratamento contra a infertilidade.

Ainda que Rachel (2008: *online*) exagere um pouco na maneira como considera o fato de receber anúncios direcionados – em seu relato altamente personalizado, ela usa termos como “minha página do *Facebook* me chamou de gorda”, por exemplo – e que, em seu caso específico, o teor ofensivo se deva, em grande medida, à abordagem e não apenas ao conteúdo da publicidade recebida, sua argumentação nos deixa entrever uma questão interessante

¹²³ Em post ao grupo “We will leave Facebook if you start bombarding us with advertisements”.

¹²⁴ Em post ao grupo “Stand Up! Don't Let Facebook Invade Your Social Life With Ads!”.

¹²⁵ Tradução nossa para: “Am sick of seeing the Gaymen one - I ticked my interest is in WOMEN - hello?!”, em post ao grupo “We will leave Facebook if you start bombarding us with advertisements”.

¹²⁶ O *muffin* é um tipo de bolinho doce, comum na culinária americana.

associada ao tema. Consideremos um caso hipotético em que o direcionamento de um anúncio para perda de peso seja feito corretamente, *i.e.*, para uma pessoa gorda. Neste caso, o indivíduo acima do peso será, a todo o momento, pressionado pelos diversos anúncios a contemplar um padrão social desejado: ser belo e magro. Além de reproduzir esta fórmula contemporânea, o fato de os anúncios serem direcionados potencializa seu poder de controle social: define-se, de antemão, que o que está disponível aos gordos não são os anúncios sobre belas roupas, mas os de dietas, feitos para ajudá-los a perder peso, exacerbando clivagens sociais e pré-determinando neste ambiente suas opções de consumo. Hoje o sistema do *Facebook* conta inclusive com um mecanismo através do qual o público pode votar e definir a relevância do anúncio recebido, de modo a tornar as recomendações mais inteligentes. No entanto, nem a ausência de erros nem o aprimoramento técnico e social das recomendações enviadas serão capazes de evitar este tipo de problema, gerado pela segmentação apriorística de indivíduos em grupos para o recebimento de tratamento preconizado e diferenciado, fórmula para o equacionamento de um novo controle social. Mais uma vez, são colocados lado a lado os benefícios de se receber conteúdo relevante – o que facilitaria o trabalho de um consumidor assoberbado e sem tempo para procurar o que precisa – e os potenciais riscos das políticas de classificação implícitas a este processo.

Já no caso do *Social Ads*, consideremos inicialmente o argumento do canadense Greg Benedetto, fundador do grupo *Stand Up! Don't Let Facebook Invade Your Social Life With Ads!*. Ele afirma no tópico de abertura do grupo que não se importa em receber anúncios direcionados, mas que o *Facebook* simplesmente passou dos limites e que não suportará ter sua imagem usada para vender produtos aos próprios amigos.¹²⁷ Enquanto isso, outro integrante do grupo, o alemão Bas Grasmayer, opina a favor da nova ferramenta, dizendo que agora as pessoas poderão contar com novas fontes de informação sobre os produtos que lhes interessam e receber recomendações genuínas de seus conhecidos ao invés de anúncios falsos de empresas. Para ele, os históricos associados aos anúncios no programa *Social Ads* se limitam a reportar fatos como “Liliane comprou o produto X” ou “Liliane escreveu um *review* do produto Y”, e não significam que o indivíduo esteja anunciando ou endossando o produto relacionado (GRASMAYER, 2007: *online*). Sabemos que a intenção da companhia ao lançar o *Social Ads* era realmente a de apresentar produtos enquanto recomendações seguras de amigos, fato confirmado pelo próprio *layout* do anúncio e pela maneira como a foto do indivíduo é posicionada na peça. No entanto, a possibilidade apresentada por Bas pode ser

¹²⁷ Disponível em: <http://www.facebook.com/group.php?gid=7284881147>.

considerada em um contexto no qual os usuários do *site*, já acostumados ao sistema, compreendam que o anúncio é produzido involuntariamente e de maneira automatizada pelo *site* e que a aparição de um amigo ao lado de uma peça publicitária não significa que ele tenha uma opinião favorável em relação ao produto ou serviço anunciado.

Em todas essas discussões, um argumento é recorrente. As pessoas querem escolher ativamente o que aparece em seus perfis e como isso aparece. Consideremos novamente as queixas acerca do *Beacon*. Além da mais óbvia e direta – a de que a ferramenta contava a todos os seus amigos, inclusive para sua namorada, sobre o presente que deveria ser uma surpresa para ela – as chances de que a ferramenta publicasse algo embaraçoso era algo preocupante. Suponhamos que um usuário tenha alugado filmes eróticos em um dos *sites* afiliados no final de semana. De repente, ele pode se deparar com a desgostosa surpresa de que um histórico desta ação foi entregue a todos os seus contatos no *site*. Além disso, como argumenta a estudante Annie Kadala (*apud.* STONE e STORY, 2007: *online*, tradução nossa), “só porque uso um *site*, isso não significa que eu queira dizer aos meus amigos sobre isso”.¹²⁸ Como ela exemplifica, “talvez eu o tenha usado porque ele era mais barato”.¹²⁹ Na verdade, os motivos pelos quais as pessoas não desejam publicizar tudo o que acontece em suas vidas são amplamente variados. Essas restrições são inerentes ao próprio ato social, e o acompanham em diferentes épocas e situações, sejam elas *online* ou *offline*. Por ora, nossas observações preliminares nos permitem levantar as seguintes hipóteses: a) a de que alguns dos principais motivos por trás das queixas associadas pelos usuários à questão da privacidade são provenientes de alguma interferência nos processos de exibição de si, levados tão a sério pelos interatores nos *sites* de rede social; b) a de que tais interferências e sua ligação com os processos de exibição de si podem aborrecer os indivíduos tanto por sua projeção social (*i.e.*, o fato de um usuário não querer que outros saibam, por exemplo, que ele alugou um determinado filme) quanto pela associação desta projeção social a um contexto institucional (*i.e.*, o fato de um indivíduo se sentir contrariado ou invadido justamente por aparecer ao lado de uma determinada marca para seus amigos).

3.4 A portabilidade de dados no Facebook

Consideremos agora a posição do *Facebook* em relação à portabilidade de dados nas redes sociais. É importante ressaltar, de antemão, que a companhia foi pioneira na realização

¹²⁸ Tradução nossa para: “Just because I use a Web site, doesn’t mean I want to tell my friends about it”.

¹²⁹ Tradução nossa para: “Maybe I used that Web site because it was cheaper”.

de esforços no sentido de permitir a integração do seu serviço com fontes externas. No mês de agosto de 2006, ela lançou a primeira versão da *Facebook Platform API (Application Programming Interface)*, que permitia a programadores externos usar as informações proprietárias do *site* para construir aplicativos *web*, *desktop* e *mobile*. Os dados que poderiam ser compartilhados através do *Facebook Developers* incluíam aqueles postados pelos indivíduos na guia de informações de seu perfil, suas fotos, eventos e sua rede de amigos. Para a companhia, a idéia era a de permitir que os usuários pudessem usufruir da experiência social proporcionada pelo *site* onde quer que estivessem (VORA, 2007: *online*). Posteriormente, em maio de 2007, enquanto o *MySpace* se esforçava para banir ou adquirir os *widgets* criados dentro do *site* (ARRINGTON, 2007: *online*), o *Facebook* lançou a versão mais recente da *Facebook Platform*, desta vez abrindo o próprio *site* a receber aplicativos produzidos por terceiros, que podem ser instalados pelos próprios usuários em seus perfis. As informações que podem ser disponibilizadas aos desenvolvedores abrangem, de acordo com os termos de uso da plataforma, todas aquelas declaradas na guia de informações do perfil, o ID associado ao usuário e qualquer dado visível através do *site*, incluindo:

[...] seus planos para o verão, sua rede de relações no *Facebook*, seu histórico educacional, seu histórico profissional, informações sobre seu curso, cópias de fotos de seus álbuns do *Facebook*, metadados associados com seus álbuns de fotos (por exemplo, data de criação, nome do álbum, comentários em suas fotos etc.), o número total de mensagens enviadas e/ou recebidas, o número total de mensagens não lidas em sua caixa de mensagens, o número total de *pokes* enviados e/ou recebidos, o número total de *posts* em seu *Wall* [...] (FACEBOOK: *online*, tradução nossa).¹³⁰

No que diz respeito ao trânsito de dados pessoais através da plataforma, o acesso dos programadores e empresas a essas informações depende de uma autorização explícita do dono da conta que requisita a adição de um novo aplicativo. Ao executar esta ação, ele é perguntado claramente se deseja conceder a fontes externas acesso aos seus dados pessoais. Em caso afirmativo, o aplicativo por ele autorizado se torna apto a acessar não apenas os seus dados individuais, mas também as informações de todos aqueles cujo perfil ele também pode visualizar. Isto depende da visibilidade arquitetada pela estrutura das redes e das configurações de privacidade definidas pelos usuários, fatores que permitem ou limitam o

¹³⁰ Tradução nossa para: “[...] your summer plans, your Facebook user network affiliations, your education history, your work history, your course information, copies of photos in your Facebook Site photo albums, metadata associated with your Facebook Site photo albums (e.g., time of upload, album name, comments on your photos, etc.), the total number of messages sent and/or received by you, the total number of unread messages in your Facebook in-box, the total number of “pokes” you have sent and/or received, the total number of wall posts on your Wall™ [...]”.

acesso dos indivíduos a um determinado perfil. O acesso aos dados individuais concedido aos desenvolvedores da plataforma também é restringido pelo *Facebook*. Em termos contratuais, conforme expresso nos termos do serviço do *Facebook Developer*, é vetado aos programadores de aplicativos da plataforma “(...) exibir ou disponibilizar (ou ajudar terceiros a exibir ou disponibilizar) a qualquer pessoa quaisquer *Facebook Properties*¹³¹ que esta pessoa não seja capaz de acessar adequadamente através do *Site Facebook*” (FACEBOOK: *online*, tradução nossa).¹³² Além disso, o documento dos termos de uso da plataforma proíbe claramente que os desenvolvedores efetuem “venda, revenda, redistribuição, sublicenciamento ou transferência de qualquer parcela das *Facebook Properties*, ou o uso e armazenamento de quaisquer *Facebook Properties* para qualquer proposta diversa das especificamente autorizadas aqui” (FACEBOOK: *online*, tradução nossa).¹³³

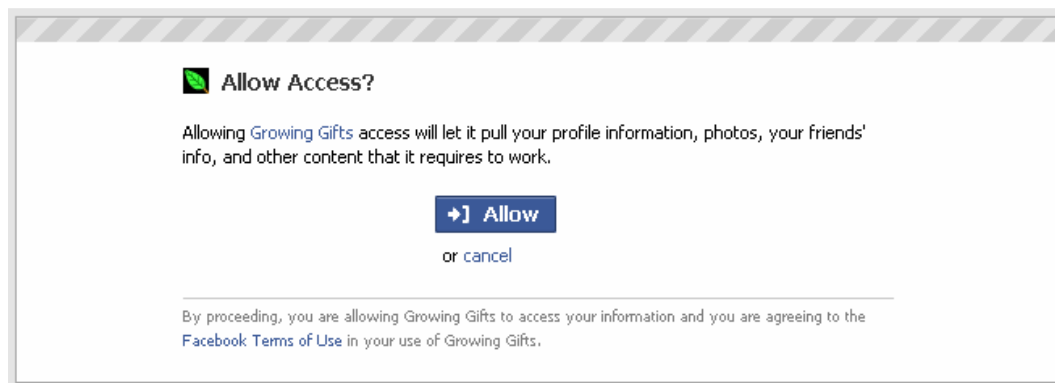


Fig. 7: Aviso através do qual os usuários do *site* permitem a um aplicativo acessar os dados de seu perfil.

É importante considerar também que cada aplicativo possui sua política de privacidade, que irá legislar sobre o uso dos dados que podem ser acessados através da conta de um usuário para além das restrições previamente impostas pelo *Facebook*. Neste sentido, a empresa exige que, caso o aplicativo disponibilizado através de seu serviço colete diretamente qualquer tipo de informação identificável de qualquer usuário, isto deve estar claramente explicitado em sua política de privacidade. No entanto, de acordo com a política de privacidade do *Facebook*, ainda que o *site* imponha restrições contratuais e técnicas aos

¹³¹ O termo *Facebook Properties* é usado no documento dos termos de uso da plataforma para designar as informações que podem ser exportadas para os Aplicativos e Repositórios de Dados.

¹³² Tradução nossa para: “[...] otherwise display or provide (or assist any third party to display or provide) to any person any Facebook Properties that such person would not properly have been able to access through the Facebook Site”.

¹³³ Tradução nossa para: “You may not sell, resell, lease, redistribute, license, sublicense or transfer all or any portion of the Facebook Properties, or use or store any Facebook Properties for any purpose other than as specifically authorized herein”.

desenvolvedores da plataforma, autorizar um aplicativo implica sempre em disponibilizar a terceiros os dados do seu perfil e de todos aqueles usuários cujos perfis você também pode visualizar. Apesar da cautela, este acesso é um ponto de vulnerabilidade na arquitetura de visibilidade do *site*, pois é difícil garantir que os desenvolvedores da plataforma estejam agindo corretamente.

Por favor, note que o *Facebook* não filtra ou aprova os Desenvolvedores da Plataforma e não pode controlar como esses Desenvolvedores da Plataforma usam qualquer informação pessoal que eles possam obter através dos Aplicativos da Plataforma. Além disso, os Desenvolvedores da Plataforma podem requerer que você assine seus próprios termos do serviço e políticas de privacidade, o que pode dar a eles direitos adicionais ou impor obrigações adicionais a você, então, por favor, tenha certeza de que você analisou esses termos e políticas com cuidado antes de usar qualquer Aplicativo da Plataforma (FACEBOOK: *online*, tradução nossa).¹³⁴

Assim, a proteção das informações pessoais e as dinâmicas da revelação de informações se tornam mais complexas neste novo contexto, marcado por novas modalidades de remix social, em que dados são recuperados e combinados com aplicativos de fontes externas para permitir novas formas de customização da expressão pessoal e dos processos de interação interpessoais.¹³⁵ A forte adesão dos usuários a esses aplicativos mostra sua importância na atual estrutura do *site* e chama nossa atenção para os processos de revelação, apropriação e uso das informações aí disponibilizadas.¹³⁶ Dentre os inúmeros tipos e propostas de aplicativos existentes, chamam a nossa atenção aqueles que usam dados sobre características, preferências e interesses para realizar medições de semelhança e afinidade entre usuários, associando ou não este processo à recomendação de serviços e produtos. Um

¹³⁴ Tradução nossa para: "Please note that Facebook does not screen or approve Platform Developers and cannot control how such Platform Developers use any personal information that they may obtain in connection with Platform Applications. In addition, Platform Developers may require you to sign up to their own terms of service, privacy policies or other policies, which may give them additional rights or impose additional obligations on you, so please make sure to review these terms and policies carefully before using any Platform Application".

¹³⁵ Como grande parte dos aplicativos da plataforma permite realizar ações relacionadas aos amigos, eles contam com uma funcionalidade para o envio de um convite a outros usuários. Além disso, a adição de um aplicativo e as ações realizadas através dele aparecem no *News-Feed* e no *Mini-Feed*, o que fomenta uma cultura de trocas sociais constantemente renovadas pela dispersão dessas ferramentas.

¹³⁶ Dentre os aplicativos de mais sucesso no site, encontramos propostas as mais variadas possíveis: oferecer e receber drinques de amigos, como no caso do *Pass a Drink* (7.267.762 usuários ativos/mês); atuar contra o aquecimento global através de um jogo cujos patrocinadores doam dinheiro para salvar florestas à medida que você usa o aplicativo, como no *(Lil) Patch Green* (5.674.705 usuários ativos/mês); descobrir qual de seus amigos é o mais inteligente através de um jogo, como no caso do *Who has the biggest brain?* (3.740.764 usuários ativos/mês); descobrir que está interessado em você, como no caso do *Are you interested?* (3.534.710 usuários ativos/mês); comprar seus amigos e descobrir quanto você vale no mercado do site através do aplicativo *Owned!* (2.266.270 usuários ativos/mês); criar um mapa interativo de todas as cidades que você já visitou no mundo, através do *Cities I've visited* (1.607.589 usuários ativos/mês); receber mensagens anônimas de seus amigos e descobrir o que eles realmente acham de você, através do *Honesty Box* (1.409.921 usuários ativos/mês) etc.

dos representantes mais populares desta tendência é o aplicativo *Movies*, da *Flixster* (6.200.492 usuários ativos/mês), que permite comparar o gosto cinematográfico de um determinado usuário com o de seus amigos através de um teste de compatibilidade denominado *Movie Compatibility Test*. Resenhas, *ratings* e listas dos filmes que um usuário deseja assistir podem ser compartilhadas através do aplicativo, que também permite a comparação do conhecimento dos usuários através de um teste chamado *Never-Ending Movie Quiz*. Através destes testes, o aplicativo reúne dados suficientes para calcular a similaridade e construir *rankings* de participantes e de seus filmes preferidos. E segundo a política de privacidade do *Movies*, as informações dos participantes são submetidas a rotinas de coleta, armazenamento e análise estatística. A empresa também se reserva o direito de “compartilhar informações que incluem seus Dados Pessoais, Informações Não-Identificáveis e Dados de *Logs* com terceiros para análises industriais e perfilação demográfica e para direcionar anúncios publicitários sobre outros produtos e serviços” (FLIXSTER: *online*, tradução nossa).¹³⁷

Uma outra modalidade de aplicativos em que estas medições de semelhança também estão presentes são aqueles destinados a permitir que os usuários listem itens de seu interesse e revelem aos outros o seu estilo. O *StyleFeeder* (41.078 usuários ativos/mês) é um aplicativo que funciona como um sistema de recomendação de produtos (roupas, móveis, jóias, bolsas, maquiagem, utensílios para o lar, para animais de estimação, eletrônicos etc.). Ele permite aos usuários dar *ratings* em diversos itens, adicioná-los aos seus perfis, marcá-los com *tags*, fazer comentários e compartilhar suas compras e artigos desejados com os amigos. Todos os itens listados possuem um *link* para o *site* no qual se pode comprar o produto. E com base no estilo e nas preferências dos usuários, bem como nos *ratings* dados por outros usuários em itens semelhantes, o aplicativo retorna recomendações periódicas aos interatores. A idéia é fazer com que a atividade de comprar e mostrar o que se deseja seja, por um lado, interessante àqueles que querem afirmar seu estilo e por outro, capaz de incentivar o consumo através da rede social de recomendações que o aplicativo estabelece. Naturalmente, o uso deste tipo de aplicativos implica o fornecimento de um amplo espectro de informações sobre o gosto dos indivíduos participantes. E neste caso específico, trata-se de dados que possuem valor comercial imediato, pois revelam preferências diretamente ligadas a hábitos de consumo. Segundo os termos de uso do aplicativo, estas informações são públicas, e ao postá-las, os

¹³⁷ Tradução nossa para: “[...] share aggregated information that includes your Personal Information, Non-Identifying Information and Log Data with third parties for industry analysis and demographic profiling and to deliver targeted advertising about other products and services”.

usuários estão concedendo aos desenvolvedores “[...] permissão para usar, exibir, modificar, distribuir e de qualquer forma explorar esses itens, informações, mensagens e comentários em conexão com o *Site* e com o nosso negócio” (STYLEFEEDER: *online*, tradução nossa).¹³⁸

Consolidando e expandindo o seu serviço, o *Facebook* decidiu abrir sua plataforma a outros *sites* de rede social em dezembro de 2007. Com esta iniciativa, outras redes passaram a oferecer a terceiros a oportunidade de desenvolver aplicativos através da *Facebook Platform*, disponibilizando-os aos usuários destes *sites*. Esta decisão foi anunciada pouco tempo depois do lançamento do projeto *Open Social*, da *Google*, lançado em novembro de 2007.¹³⁹ O *Open Social* foi anunciado pela *Google* como uma plataforma que opta por padrões abertos – *JavaScript* e *HTML (Hyper Text Markup Language)* – ao contrário do *Facebook*, que opta por padrões fechados – o *FQL (Facebook Query Language)* e o *FBML (Facebook Markup Language)*, dentre outros. O uso de padrões abertos evita que os programadores devam aprender a realizar as mesmas ações em uma nova linguagem cada vez que queiram construir aplicativos para um determinado *site*. No entanto, muitos questionam a natureza aberta desta iniciativa. Como afirma o programador Dare Obasanjo em seu *weblog*, apesar do uso do prefixo *open*, a plataforma da *Google* não teve um processo de desenvolvimento aberto e possui seus segredos como qualquer outra tecnologia proprietária. Esta opinião é compartilhada por Shelley Powers em seu *weblog*:

Talvez o mundo irá ler os termos de uso da API, e perceber que ela não é uma API aberta; ela é uma API gratuita, pertencente a e controlada por uma única companhia: *Google*. [...] Talvez o mundo também perceba que a funcionalidade é dependente da tecnologia de hospedagem da *Google*, que tem seus próprios termos de serviço (incluindo a adição de anúncios conforme as determinações da *Google*), e que construir um aplicativo *OpenSocial* liga o *Google* ao seu aplicativo e a qualquer *site* de rede social que compre este sonho. (POWERS, 2007: *online*, tradução nossa).¹⁴⁰

Em maio de 2008 foi lançada a mais nova forma de interação do *Facebook* com fontes externas, desta vez invertendo a idéia da plataforma. Com o *Facebook Connect*, se torna

¹³⁸ Tradução nossa para: “[...] permission to us to use, display, modify, distribute and otherwise exploit such items, information, messages and comments in connection with the Site and otherwise in connection with our business”.

¹³⁹ De maneira semelhante, o objetivo deste projeto é disponibilizar um conjunto de API’s que possam ser usadas por programadores para construir aplicativos compatíveis com todos os sites que aderirem ao projeto, como é o caso do *Hi5*, do *LinkedIn*, do *Orkut* etc.

¹⁴⁰ Tradução nossa para: “Perhaps the world will read the terms of use of the API, and realize this is not an open API; this is a free API, owned and controlled by one company only: Google. [...] Maybe the world will also take a deeper look and realize that the functionality is dependent on Google hosted technology, which has its own terms of service (including adding ads at the discretion of Google), and that building an *OpenSocial* application ties Google into your application, and Google into every social networking site that buys into the Dream”.

possível levar sua identidade e rede de amigos para *sites* externos, que podem agora desenvolver seus sistemas pensando em permitir que seus usuários integrem os dados do *Facebook* ao invés de ter que postá-los novamente.¹⁴¹ Os dados que podem ser compartilhados incluem as informações básicas de perfil, foto, eventos, grupos, amigos etc. (MORIN, 2008: *online*). Além disso, o *Facebook Connect* permite que os controles de privacidade dos usuários e a atualização de suas informações sejam repassados automaticamente aos *sites* externos. Para os desenvolvedores, fica mais fácil adicionar contexto social aos seus *sites* e reconhecer, inclusive, quais amigos de um determinado usuário no *Facebook* também estão presentes em seu *site*. A iniciativa foi acompanhada de perto pelo *MySpace*, que lançou quase que concomitantemente sua plataforma *Data Availability*, permitindo igualmente a incorporação de dados do *site* em fonte externas. No entanto, assim como no caso do *Facebook Platform* e do *Open Social*, muitas críticas têm sido direcionadas a essas iniciativas.



Fig. 8: Aviso que permite aos usuários do *Facebook* conectar os dados por eles disponibilizados em seus perfis com *sites* externos. Fonte: MORIN, 2008: *online*.

De maneira geral, o que se percebe é que todas as empresas querem engendrar meios para permitir que os usuários possam levar seus dados para outros *sites* ou usufruir de outros *sites* sem precisar deixar seus serviços. Assim, essas iniciativas são promotoras de uma compatibilidade limitada e não representam com fidelidade os ideais do *DataPortability*. Existe sempre uma empresa que quer deter o controle sobre as informações dos seus usuários, ainda que permitindo que eles as compartilhem desta ou daquela forma, com este ou com aquele serviço. Assim, os indivíduos podem usar outros *sites* sem que eles precisem dar a

¹⁴¹ Um exemplo simples seria o cadastro para a postagem em um fórum ou *weblog*, que em geral exige que o indivíduo preencha um formulário com nome, foto etc. Caso o site no qual se deseja fazer o comentário esteja integrado ao *Facebook*, basta que o usuário escolha conectar seus dados, fornecendo a identificação solicitada.

outras companhias o controle sobre suas informações pessoais. Não nos cabe comparar ou julgar aqui as pretensões de cada um dos *sites* de rede social hoje existentes, mas é importante ressaltar que, como esta interoperabilidade entre serviços só pode ser alcançada pela adoção de um único padrão por todas essas redes, o *Facebook*, por seu pioneirismo, possui hoje plataformas mais consolidadas e com mais chances de prevalecer caso o ideal do desenvolvimento de protocolos abertos não seja alcançado. Por fim, vale ressaltar que, ironicamente, as principais justificativas do *Facebook* para a construção de seus próprios padrões são a privacidade e a segurança de seus usuários. Nas palavras de Dave Morin (*apud*. NAONE, 2008: *online*), não se trata apenas de *Data Portability*, mas também de *Privacy Portability*. “Porque o *Facebook* quer colocar os usuários no controle do que acontece com as informações compartilhadas, diz Morin, ele é cauteloso acerca de padrões abertos; ele quer ter certeza de que eles são seguros antes de integrá-los ao *site*” (NAONE, 2008: *online*, tradução nossa).¹⁴²

3.5 Busca de pessoas e audiências indesejadas

Um outro fenômeno associado à coleta e ao tratamento de dados provenientes de redes sociais vem de uma nova geração de serviços que têm surgido na Internet, designados pela expressão *people search engines* ou buscadores de pessoas. O exemplo que aqui nos interessa é uma companhia chamada *Rapleaf*,¹⁴³ baseada em San Francisco, cujos investidores incluem também o lendário Peter Thiel¹⁴⁴ e que oferece seus serviços através de dois *sites*: o *Rapleaf.com*, uma engine de busca de pessoas que permite descobrir o nome, idade e as redes sociais das quais uma pessoa qualquer faz parte e o *Upscoop.com*,¹⁴⁵ que permite, de maneira semelhante, descobrir em que redes sociais sua lista de contatos de *e-mail* participa (para isso, você deve fornecer ao serviço a senha de sua conta *Gmail*, *Yahoo* ou equivalente). A *Rapleaf* surgiu visando construir um sistema de reputação alternativo ao do *e-Bay*, que pudesse fornecer informações sobre as pessoas e informar decisões na hora de contratar um

¹⁴² Tradução nossa para: “Because Facebook wants to put users in charge of what happens to shared contact information, says Morin, it’s cautious about open standards; it wants to make sure they’re secure before integrating them into its site”.

¹⁴³ Disponível em: <http://www.rapleaf.com>.

¹⁴⁴ Peter Thiel, um curioso e bem-sucedido investidor do Vale do Silício, foi o primeiro a investir no *Facebook*. Ao ser procurado pelos ainda estudantes de Harvard Zuckerberg, Dustin Moskowitz e Chris Hughes em junho de 2004, ele injetou 500 milhões de dólares na então nascente companhia. Ele é também co-fundador da *Pay-Pal* e de dois outros fundos de investimento, o *Clarium Capital Management* e o *Founders Fund*. Graduado em Filosofia pela *Stanford University*, é dono de uma ideologia futurista e libertária com relação às maravilhas do mundo virtual e ativista do grupo *TheVanguard.Org*, criado para fazer frente à *MoveOn.org*.

¹⁴⁵ <http://www.upscoop.com>.

profissional ou escolher um prestador de serviços, por exemplo. Assim, a *Rapleaf* construiu uma base de dados com mais de 50 milhões de perfis, que incluem dados como idade, nome, endereço, rede de contatos, visão política, músicas, filmes e livros favoritos, hábitos *online*, aplicativos adicionados e redes sociais usadas pelos indivíduos avaliados. Estes dados são provenientes de suas contas em *sites* como o *Facebook*, *MySpace*, *LinkedIn*, *Bebo*, *Classmates.com* etc. (OLSEN, 2007: *online*).

As evidências existentes são de que os perfis acumulados pela *Rapleaf* são repassados à *TrustFuse*, detentora da companhia. O serviço prestado pela *TrustFuse* funciona da seguinte maneira: seus clientes levam listas de endereço de *e-mail* à empresa e compram perfis das pessoas listadas. Estes corpos de informações irão ajudá-las a direcionar publicidade a estes indivíduos com base em seus hábitos, gostos, preferências e interesses. E segundo a política de privacidade que orienta os serviços da *TrustFuse*, “as informações coletadas através do *Rapleaf* podem ser usadas para assistir os serviços da *TrustFuse*. Adicionalmente, informações coletadas pela *TrustFuse* no curso de seus negócios podem ser igualmente reveladas ao *Rapleaf* para perfis buscados por *e-mail*” (TRUSTFUSE: *online*, tradução nossa).¹⁴⁶ Assim, a questão que permanece sem resposta é a de como a *Rapleaf* obtém acesso aos endereços de *e-mail* dos usuários de *sites* como *Facebook*, no qual, ainda que seja imprescindível o uso de um endereço de *e-mail* no ato do cadastro no serviço, fica a critério do usuário publicar ou não em seu perfil esta informação, que só estará visível àqueles que podem ver sua página, de acordo com suas configurações de privacidade. Ao contactar o *Facebook*, Olsen (2007: *online*) foi informada de que a companhia não tem nenhum acordo com a *Rapleaf* para fornecer acesso aos endereços de *e-mail* de seus usuários.

Segundo o CEO da *Rapleaf*, Auren Hoffman, alguma manobra especial é usada para obtenção destes dados, aos quais a empresa não possui nenhum tipo de acesso privilegiado ou intermediado por contratos de concessão.¹⁴⁷ Além deste agravante, duas questões importantes são levantadas quando analisamos de perto este e outros serviços semelhantes como o *WikiWorldBook*¹⁴⁸ e o *Spokeo*¹⁴⁹. As pessoas não sabem que estão sendo buscadas ou que alguém pode ter acessado os dados de seus perfis através da consulta a outros *sites*. Além

¹⁴⁶ Tradução nossa para: “Information captured via Rapleaf may be used to assist TrustFuse services. Additionally, information collected by TrustFuse during the course of its business may also be displayed on Rapleaf for given profiles searched by e-mail address”.

¹⁴⁷ Olsen (*op. cit.*) argumenta que uma das possíveis técnicas utilizadas poderia ser a derivação do nome a partir do endereço de *e-mail*, usando combinações possíveis.

¹⁴⁸ Trata-se de um buscador que retorna dados de um determinado indivíduo com base em seus perfis em redes sociais. Disponível em: <http://wikiworldbook.com/>.

¹⁴⁹ Trata-se de um buscador que agrega dados de 41 fontes, incluindo o *Facebook*. Disponível em: <http://www.spokeo.com/>.

disso, é interessante notar também o argumento usado por essas empresas para justificar a natureza de seus serviços: o de que elas não estão fazendo nada além de reunir dados cuja natureza já é pública, como afirma a *TrustFuse* (*apud.* OLSEN, 2007: *online*). Auren Hoffman (*apud.* OLSEN, 2007: *online*, tradução nossa) apresenta uma opinião ainda mais polêmica: “Nós estamos ajudando as pessoas a controlar sua privacidade. Você não poderia sequer saber que existem todas essas coisas sobre você por aí. [...] E agora você pode gerenciar todas essas informações”.¹⁵⁰ De qualquer forma, a existência desta modalidade de buscadores é uma prova da consolidação do uso dos *sites* de rede social enquanto fonte de informação sobre pessoas. Estes serviços são uma indicação clara de que a necessidade de conhecer os dados disponibilizados nestes *sites* pode constituir um negócio tão lucrativo quanto invasivo, justificado por argumentos no mínimo duvidosos e pelo amplo interesse de diversos setores sobre estes corpos de dados individuais (JONES e SOLTREN, 2005; ACQUISTI e GROSS, 2006).

O ecossistema de ferramentas para a revelação de informações existente em *sites* como o *Facebook* se relaciona também com outros campos de visibilidade problemáticos para os usuários: pais, autoridades, empregadores etc. Ainda que a arquitetura de visibilidade do *site* dificulte o acesso destas audiências aos perfis de seus usuários, os relatos sobre ocorrências desta natureza não param de crescer. Uma pesquisa realizada pela *Kaplan Test Prep* nos meses de julho e agosto de 2008 revelou que, entre 320 importantes instituições de ensino superior americanas, 10% admitem checar perfis de candidatos à admissão usando *sites* de rede social. Deste total, 38% afirmam que as informações encontradas afetaram negativamente suas impressões sobre os candidatos (KAPLAN, 2008: *online*). Apesar da maioria das escolas entrevistadas não possuir diretrizes para a consulta e uso deste tipo de dados, alguns profissionais afirmaram ter inclusive rejeitado estudantes por conta do conteúdo de seus perfis. Como naturalmente não há tempo para avaliar a vida virtual de todos os candidatos, em geral, as escolas realizam este tipo de checagem no caso do recebimento de denúncias de algum concorrente ou quando o histórico do candidato lista algum comportamento suspeito. Thomas Griffin (*apud.* HECHINGER, 2008: *online*), diretor de admissões na *North Carolina State University*, relata um caso recente em que um estudante cujo histórico registrava punições por brigas acabou preterido quando os avaliadores encontraram em seu perfil do *Facebook* uma foto segurando uma arma. Por outro lado, Sandra Starke (*apud.* HECHINGER, 2008: *online*), da *State University of New York* em

¹⁵⁰ Tradução nossa para: “We’re helping you manage your privacy. You might not even know there’s all these things about you out there. [...] And now you can manage all this information”.

Binghamton, diz aconselhar a sua equipe a ignorar dados provenientes destes *sites*, cujas informações ela considera serem de caráter casual, como as conversas que temos cotidianamente com outros.

Seja qual for a opinião das autoridades com as quais estes jovens se relacionarão no curso de suas vidas, o fato é que este é apenas um primeiro momento em que eles terão que se deparar com julgamentos provenientes das informações que eles revelam em *sites* de rede social. Jones e Soltren (2005) relatam como administradores de universidades americanas têm utilizado o *Facebook* para saber mais sobre seus alunos e eventualmente punir atitudes em desacordo com suas diretrizes de conduta e comportamento. Um bom exemplo é a expulsão do então aluno da *Fisher College* em Boston, Cameron Walker, em outubro de 2005. Ele foi acusado de manter um grupo em prol da demissão de um oficial da segurança do campus que ele considerava ultrapassar os limites de sua função, se dedicando exacerbadamente a vigiar os estudantes (JONES e SOLTREN, 2005: 26). Casos similares, em que estudantes foram investigados, punidos ou até expulsos não param de se multiplicar, e incluem o uso de fotos, comentários ou associação a grupos considerados inadequados ou em desacordo com as políticas disciplinares de suas instituições. Evidências de uso de álcool e drogas, realização de festas em dormitórios estudantis e até mesmo grupos para a troca de informações e dicas na resolução de exercícios têm sido usados para justificar sanções (SMITH, 2005: *online*; PERRY, 2006: *online*). De maneira semelhante, investigações policiais também têm se beneficiado deste tipo de informações. Um exemplo recente é o do cineasta de 29 anos Mark Andrew Twitchell, preso por assassinato. Uma das evidências usadas pela polícia foi o status de seu perfil do *Facebook* do dia 15 de agosto de 2008, no qual ele dizia ter muito em comum com Dexter Morgan, uma referência ao *serial killer* do seriado de TV (REID, 2008: *online*).

Outra modalidade de uso dos dados disponibilizados em perfis de rede social é apontada por uma pesquisa realizada pela *Harris Interactive* a pedido da *CareerBuilder.com* entre maio e junho de 2008 com mais de 3.100 empregadores nos EUA. A análise revelou que 22% deles checam os perfis de candidatos em *sites* de rede social (CAREERBUILDER, 2008: *online*). O valor é exatamente o dobro dos 11% encontrados pela pesquisa realizada em 2006, também pela *CareerBuilder.com*. Dois outros dados interessantes encontrados pela pesquisa: 9% dos entrevistados disseram estar planejando integrar a busca de perfis em seus processos de contratação e 34% dos que afirmaram já realizar este tipo de consulta admitiram já ter encontrado nestes *sites* conteúdos que os levaram a desistir de um candidato. Dentre os conteúdos mais penalizados pelos empregadores, 41% dos entrevistados apontaram o fato de o candidato publicar informações sobre o uso de drogas ou álcool; 40% desaprovam a

postagem de conteúdos ou fotos inapropriados ou ofensivos; 29% apontam a falta de habilidades comunicativas dos indivíduos pesquisados; 28% relatam o fato de o candidato falar mal da empresa anterior; 27% constataram que o candidato mentiu sobre sua qualificação; 22% encontraram conteúdo discriminatório (em relação à raça, religião ou sexo); os mesmos 22% citaram que o nome virtual do candidato era pouco profissional; 21% apontam a ligação do indivíduo com comportamento criminoso e 19% desaprovaram o fato de o candidato ter publicado informações confidenciais do emprego anterior. Os empregadores também ressaltaram fatores positivos encontrados em perfis de candidatos, como gosto eclético, criatividade, boas referências de terceiros, adequação à empresa ou ao cargo pretendido e boas habilidades comunicativas.

O que podemos constatar é que, em todos esses casos, audiências capazes de exercer algum poder sobre determinados indivíduos, aplicando sanções ou legislando sobre as possibilidades que lhes estão disponíveis, recorrem aos corpos de informações que compõem seus perfis, visando informar seus processos de tomada de decisão ou manter a ordem adequada ao funcionamento de suas instituições. Por um lado, estes processos podem aumentar a eficácia de alguns aparatos como o policial e o escolar. No entanto, o uso dessas informações será sempre marcado por um certo grau de subjetividade em sua interpretação, o que pode levar a pré-julgamentos equivocados, gerando sanções descabidas ou antecipando cenários e riscos futuros através do controle das possibilidades presentes. Naturalmente, este risco é inerente a qualquer processo que inclua julgamento e escolha. No entanto, as tecnologias digitais adicionam novos elementos a estas dinâmicas ao funcionarem como uma memória praticamente infinita que armazena pensamentos e atitudes de diferentes tempos, sejam eles duradouros ou efêmeros. Enquanto nas modalidades de uso efetuadas pela polícia e pelas universidades o foco está na constatação e na prevenção – encontrar fatos que corroborem ou denunciem transgressões presentes, visando punir e evitar transgressões futuras – nos usos feitos pelos departamentos de admissão e pelas empresas em seus processos de contratação as decisões informadas não visam aplicar sanções aos indivíduos: nem a prisão, nem a expulsão. Nestes casos, ainda que não haja modelos computacionais para informar os processos de escolha, a eleição subjetiva dos marcadores de comportamento usados por aqueles encarregados de triar as informações acessadas constituem um mecanismo de antecipação: negar o aluno que exibe uma foto em que aparece armado seria uma forma de impedir o crime ou a presença de um futuro atirador dentro da universidade; de maneira semelhante, negar o funcionário com esta ou aquela atitude *online* é evitar a presença de um funcionário possivelmente inadequado ou desqualificado dentro da empresa. Estas atitudes

implicam legislar sobre as oportunidades futuras dos indivíduos, usando agora não apenas uma singela carta de recomendação de um emprego anterior, mas todo o arsenal de informações que se pode encontrar sobre eles virtualmente.

Por fim, seria do interesse dos usuários destes *sites* impedir a determinadas audiências o acesso a suas informações. No que diz respeito à proteção dos dados disponibilizados através do *Facebook*, podemos afirmar que, de maneira geral, o *site* permite aos seus usuários um alto grau de controle das informações publicadas através de um amplo e refinado espectro de configurações de privacidade.¹⁵¹ Não é difícil encontrar Mark Zuckerberg reafirmando que este é um diferencial do serviço prestado por sua empresa, perseguido desde os primórdios de sua concepção. Para ele, o *site* pode ser uma nova fonte de informações sobre o mundo. “E a melhor forma de fazer isso é ter as pessoas compartilhando o máximo de informações que elas se sintam confortáveis em compartilhar. E a maneira de fazer com que elas se sintam confortáveis é dar a elas controle sobre exatamente quem pode ver o que” (ZUCKERBERG, *apud*. CASSIDITY, 2006: *online*, tradução nossa).¹⁵² No entanto, apesar do amplo espectro de opções disponíveis, estudos prévios apontam que os membros do *site* utilizam pouco ou não utilizam as configurações de privacidade para proteger suas informações (JONES e SOLTREN, 2005; AQUISTI e GROSS, 2005).¹⁵³

Por fim, uma consideração se faz importante. Apesar dos termos de uso do *Facebook* permitirem que os usuários requisitem o não compartilhamento de suas informações pessoais com terceiros, nenhuma configuração de privacidade foi implementada para suportar a ação de maneira direta e automática. Hoje, esta solicitação só pode ser feita através do

¹⁵¹ A página de configurações de privacidade do site permite aos indivíduos: a) definir quem pode ver seu perfil, suas informações de contato e cada um dos campos de sua guia de informação de perfil; b) definir quem pode buscar por seu perfil, as informações que estarão disponíveis em seu anúncio público de busca (para aqueles que buscarem por seu nome fora do *Facebook*, usando um buscador como o *Google*, por exemplo) e os tipos de informações que estarão disponíveis nestas buscas (foto, lista de amigos, páginas das quais sou fã, *link* para enviar mensagem e *link* para adicionar como amigo); c) definir as ações que serão reportadas no *Mini-Feed* e no *News-Feed* dos usuários e fazer o *opt-out* para o uso destes históricos no programa *Social Ads*; d) definir os dados que os aplicativos adicionados por seus amigos podem acessar em seu perfil através do *Facebook Platform* (foto, atividades, interesses, *wall*, notas, eventos para os quais se é convidado etc.); e) bloquear alguém, impedindo que esta pessoa busque por seu perfil ou entre em contato através de qualquer um dos canais do *site* (*wall*, mensagens etc.). Os grupos de informações acima descritos podem ser disponibilizados às redes e amigos do usuário, apenas à sua rede primária e amigos, aos amigos de amigos, apenas aos amigos ou a públicos ainda mais específicos, usando controles ainda mais refinados.

¹⁵² Tradução nossa para: “The way you do that best is by having people share as much information as they are comfortable with. The way you make people comfortable is by giving them control over exactly who can see what”.

¹⁵³ É importante considerar que nem mesmo as configurações de privacidade impedem que o site seja usado para descobrir informações sobre os indivíduos. As ferramentas de busca avançada dentro de uma das redes das quais eles fazem parte podem relacioná-los a conteúdo inadequados (uma pesquisa pela palavra bêbado pode listar os perfis em que a palavra aparece, mesmo que não se tenha acesso aos seus conteúdos para a verificação do contexto em que foi usada a palavra, por exemplo).

encaminhamento de uma mensagem à companhia, que em geral permanece sem uma resposta formal ou confirmação por parte da empresa. Assim, os indícios são de que, no *Facebook*, a privacidade é arquitetada como um valor que permita aos indivíduos revelar cada vez mais informações. No entanto, se as configurações disponíveis servem para impedir que outros usuários visualizem os dados em questão, as mesmas regras não se aplicam às modalidades de acesso que podem ser exercidas pela própria companhia.

4 A VIGILÂNCIA NO FACEBOOK: RESULTADOS E APONTAMENTOS

Esboçadas as possíveis formas de disponibilização, acesso 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 *site*, através do qual, com a ajuda de uma macro,¹⁵⁴ consultamos o número de usuários maiores de 18 anos em cada um dos países disponíveis no sistema da empresa.¹⁵⁵ 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* no último ano, tais dados se tornaram rapidamente desatualizados.¹⁵⁶ 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*.¹⁵⁷ 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: *online*) comprovaram posteriormente esta tendência. Ainda que a maior

¹⁵⁴ A macro aqui mencionada se refere à gravação de uma seqüência de ações de teclado e mouse utilizadas na interação entre aplicativos para a realização de determinada tarefa, de forma que possam ser repetidas um certo número de vezes de maneira autônoma.

¹⁵⁵ 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.

¹⁵⁶ Cf. Anexo A, Fig. 3, p. 191 e Fig. 4, p. 193.

¹⁵⁷ O Brasil, em nosso levantamento preliminar, ocupou a quadragésima sétima posição no ranking de países por número de participantes, com 167.220 usuários ativos. Dada a nossa escolha por privilegiar os países latino-americanos com os maiores números de usuários no *Facebook* e também a predominância do uso da rede social *Orkut* no país, descartamos o Brasil de nossa análise. Ressaltamos, no entanto, que a participação brasileira no *site* vem crescendo: de setembro de 2008 a fevereiro de 2009, 73.800 novos usuários aderiram ao serviço no país.

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%.¹⁵⁸ 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 equidade 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.¹⁵⁹ 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 representam 42% e elas 54% dos usuários, enquanto na América do Sul 41% são homens e 49% são mulheres.¹⁶⁰ 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, justificado nosso interesse no estudo do público latino, apresentaremos agora os resultados da observação empírica desta pesquisa, que se subdivide em duas etapas: a análise de 262 questionários aplicados *online* em respondentes latino-americanos e a análise de dados coletados de cerca de 20 mil perfis de 11 redes do *Facebook*, geográficas e de universidades, 3 norte-americanas e 8 latino-americanas. É importante ressaltar que com exceção da rede de ensino superior canadense, nenhuma das redes latino-americanas selecionadas exigia o *e-mail* da instituição para a participação, escolha motivada pela nossa inacessibilidade a uma conta de *e-mail* que nos permitisse participar das redes fechadas. A análise dos questionários utiliza uma amostra reduzida de respondentes e é usada para fornecer apontamentos sobre as rotinas de uso do *site* e a percepção das diferentes modalidades de vigilância que nele ocorrem. Ao contrário, a análise de perfis utiliza amostras das quais se pode extrair valores com níveis de significância aceitáveis. A partir dos resultados observados, apresentaremos nossas conclusões sobre como se dá a vigilância nos

¹⁵⁸ Cf. Anexo A, Fig. 5, p. 195.

¹⁵⁹ Cf. Anexo A, Fig. 6, p. 195.

¹⁶⁰ Cf. Anexo A, Fig. 7, p. 195.

sites de rede social. Partiremos de uma discussão sobre as possíveis modalidades de ver¹⁶¹ associadas ao uso destes *sites* e teceremos considerações sobre as hierarquias da vigilância e a conjugação das dimensões social e de controle nas rotinas de uso destas redes.

4.1 Análise de questionários: o posicionamento dos usuários do sistema

Paralelamente à definição de nosso foco de estudo, um *website* foi produzido com a intenção de hospedar o questionário *online* que seria aplicado aos voluntários participantes. Como forma de incentivo, quatro prêmios foram sorteados entre os respondentes, a saber, quatro vale-compras da loja virtual *Amazon.com* no valor de U\$40.00 (quarenta dólares) cada um. Com o intuito de impedir fraudes motivadas pelo interesse dos usuários em concorrer ao prêmio, alguns mecanismos de segurança foram implementados no *site*.¹⁶² Dados como o IP dos participantes e o tempo que cada um levou para responder à pesquisa foram registrados para evitar possíveis fraudes e auxiliar no posterior descarte de questionários respondidos inadequadamente. Visamos garantir ao máximo o anonimato dos participantes, para que eles se sentissem livres de constrangimentos na hora de responder o questionário: tanto as suas respostas quanto os registros auxiliares coletados não envolviam nem sua identificação nem o uso de seus perfis do *Facebook* para a checagem do comportamento por eles reportado. Ao completar o preenchimento do questionário, os que desejassem concorrer ao prêmio eram encaminhados a um formulário no qual deveriam deixar seu *e-mail*. Automaticamente, o sistema enviava ao endereço registrado um número de identificação que posteriormente seria usado no sorteio do prêmio. Para o recrutamento de voluntários, depois de algumas tentativas, o método utilizado foi a criação de anúncios no *Facebook*, direcionados a pessoas de qualquer sexo e idade nos seguintes países: Canadá, Estados Unidos, Argentina, México, Colômbia, Chile e Venezuela. Dada a receptividade do público latino, os anúncios nos países norteamericanos foram suspensos e os respondentes destes países eliminados da amostra tabulada.

A pesquisa e todas as demais informações existentes no *site* foram traduzidas para três

¹⁶¹ O termo modalidades de ver denota, no contexto desta pesquisa, a conjunção das diferentes audiências e dos diferentes interesses que as movem na direção dos dados individuais disponibilizados em redes sociais, caracterizando modos de acessar e ler perfis diferenciados, de acordo com o momento, os objetivos e as intenções daquele que vê.

¹⁶² O uso de prêmios se justifica aqui como forma de incentivo aos voluntários participantes. Uma das principais dificuldades enfrentadas na pesquisa foi justamente mobilizar pessoas desconhecidas em países distantes a nos ajudarem, respondendo corretamente as questões propostas. Ainda que o oferecimento de prêmios implique o risco de possíveis fraudes, acreditamos que sem eles seria mais difícil conseguir um número razoável de respondentes. Dado o contexto não presencial e a impossibilidade de remunerarmos todos os participantes, optamos por um prêmio de caráter impessoal, cuja retirada não prescindisse de dados como conta bancária ou nome completo dos participantes.

línguas: inglês, português e espanhol. Para atingir um número razoável de respondentes, subdividimos o questionário em dois, cada um com cerca de dez questões e tempo médio de resposta de cerca de 7 minutos. Algumas questões, consideradas essenciais para calibrar as demais respostas, foram repetidas em ambos. Por fim, após o período de testes para encontrar o melhor método de recrutamento, as respostas contabilizadas foram aquelas registradas durante o mês de dezembro de 2008. No total, cerca de 2000 pessoas acessaram o *site* e 279 questionários completos foram registrados. Não houve nenhum caso de usuário usando IP de *proxy* ou IP já registrado no sistema. Aqueles com respostas contraditórias ou que foram respondidos em menos de 3 minutos foram descartados. Depois de dispensarmos 17 questionários, fechamos nossa amostra em 262 respondentes, sendo 127 de um tipo e 135 de outro. Os questionários de respondentes latino-americanos registrados com a utilização de métodos de recrutamento anteriores – a saber, divulgação em grupos do *Facebook*, através de amigos e de um grupo aberto para a pesquisa – não foram descartados. Os resultados desta pesquisa foram analisados com a utilização do *software* Open Office Calc e alguns scripts PHP,¹⁶³ codificados com objetivos específicos para atender a nossas necessidades. Utilizamos, predominantemente, a exemplo de Acquisti e Gross (2006), variáveis categóricas, contínuas e dicotômicas. Dentre os testes realizados, usamos testes-*t*¹⁶⁴ para as variáveis categóricas, dicotômicas e médias. As correlações produto-momento de *Pearson*¹⁶⁵ foram empregas para o estudo das relações entre as variáveis contínuas e categóricas e também para a investigação das relações entre diferentes as variáveis categóricas. Devido ao tamanho reduzido da amostra em comparação à totalidade da população latino-americana dos países selecionados no *site*, que soma hoje mais de 13 milhões de usuários ativos, não é possível atribuir aos percentuais observados um bom intervalo de confiança. No entanto, de acordo com os testes estatísticos realizados, foi possível aceitar algumas hipóteses, demonstradas no decorrer desta análise. Nossa amostra foi selecionada de maneira aleatória e, apesar de seu número reduzido, consideramos que ela pode nos trazer valiosos dados e *insights* sobre como o público latino-

¹⁶³ PHP *Hypertext Preprocessor*, linguagem de programação muito utilizada para a criação de páginas HTML dinâmicas, executadas em um servidor.

¹⁶⁴ Em estatística, quando se deseja verificar a veracidade de uma dada hipótese, realizam-se alguns cálculos baseados nas características encontradas em uma amostra da população que se deseja analisar. Um dos testes mais utilizados é o *teste-t*, que nos fornece um valor (*t-value*) a partir do qual se pode verificar, de acordo com o tamanho da amostra, a probabilidade de erro em aceitar ou rejeitar a hipótese investigada. Cf. LAPPONI, 2005.

¹⁶⁵ A correlação mencionada mensura o quanto uma variável está relacionada com outra variável. Quando o coeficiente de correlação é igual a 1 (um) dizemos que as variáveis estão perfeitamente correlacionadas de forma positiva, ou seja, sempre quando uma variável cresce a outra também cresce, e quando uma decresce a outra também decresce. Quando encontramos um coeficiente de valor -1 (um negativo) as variáveis estão perfeitamente correlacionadas de forma negativa, *i.e.*, o comportamento da segunda variável é o oposto ao comportamento da primeira. Cf. LAPPONI, 2005.

americano utiliza o *site*, abrindo espaço para questões e investigações futuras.

Conteste la encuesta **INGLÉS** **ESPAÑOL** **PORTUGUÉS**

SURVEY

ENCUESTA

Por favor, conteste las preguntas siguientes dando solo informaciones verdaderas. No identíquese en ninguno de los campos del formulario.

Muestra usted lo rellena, está concordando con la utilización de las informaciones para fines científicos. En contrapartida, nos comprometemos a preservar su identidad y no asociarla a las informaciones que usted nos dá.

Después de rellenar toda la encuesta podrá participar del sorteo de cuatro vale-compras de US\$40.00 en la tienda virtual amazon.com. Para conocer las reglas del sorteo [clique aquí](#).

Usted solo puede contestar la encuesta se tiene un perfil personal en el Facebook (FB): (www.facebook.com).

Por favor, seleccione correctamente sus datos demográficos.

Fig. 1: *Site* produzido para hospedar a pesquisa realizada.

Consideremos abaixo os dados demográficos de nossos 262 respondentes. A idade média de nossos voluntários foi de 24,2 anos ($sd = 9,53$). No gráfico relativo ao país em que residem, a legenda ‘outros’ inclui participantes da Bolívia, Brasil, República Dominicana, Equador, Paraguai e Uruguai. Em relação à divisão de gênero para a América do Sul reportada pela *O’Reilly Research* (LORICA, 2008: *online*), 41% dos participantes da região são homens, 49% mulheres e 10% optaram por não revelar esta informação. Logo, dos que revelaram esta informação, 46% são homens e 54% são mulheres. Em nossa amostra, excluídos os representantes para o México e a República Dominicana, a porcentagem de homens sul-americanos é 38,5% e de mulheres 61,5%. Assim, temos que nossa amostra super-representa indivíduos do sexo feminino e sub-representa os do sexo masculino, pois a diferença encontrada para a divisão de gênero na América do Sul medida por um teste-*t* foi estatisticamente significativa ($t = 4,801$; $Pr = 0,00\%$).¹⁶⁶

¹⁶⁶ Para subsidiar a compreensão dos testes posteriores, expliquemos o procedimento aqui realizado. Neste caso, estamos testando a hipótese de que a divisão de gêneros seja idêntica, *i.e.*, que a diferença entre os percentuais de pessoas em cada sexo seja nula. O resultado do teste foi de 0,00% de aceitar a hipótese investigada, o que nos permite concluir que a diferença entre as divisões de gêneros é significativa. O teste-*t* possui dois resultados, sendo que o *t-value* (*t*) é um resultado intermediário e necessário para a obtenção da probabilidade (*Pr*) que é o resultado final do teste. Para valores de probabilidade inferiores a 5% adotamos que a hipótese é falsa, ou seja, neste caso, a proporção entre os sexos é diferente.

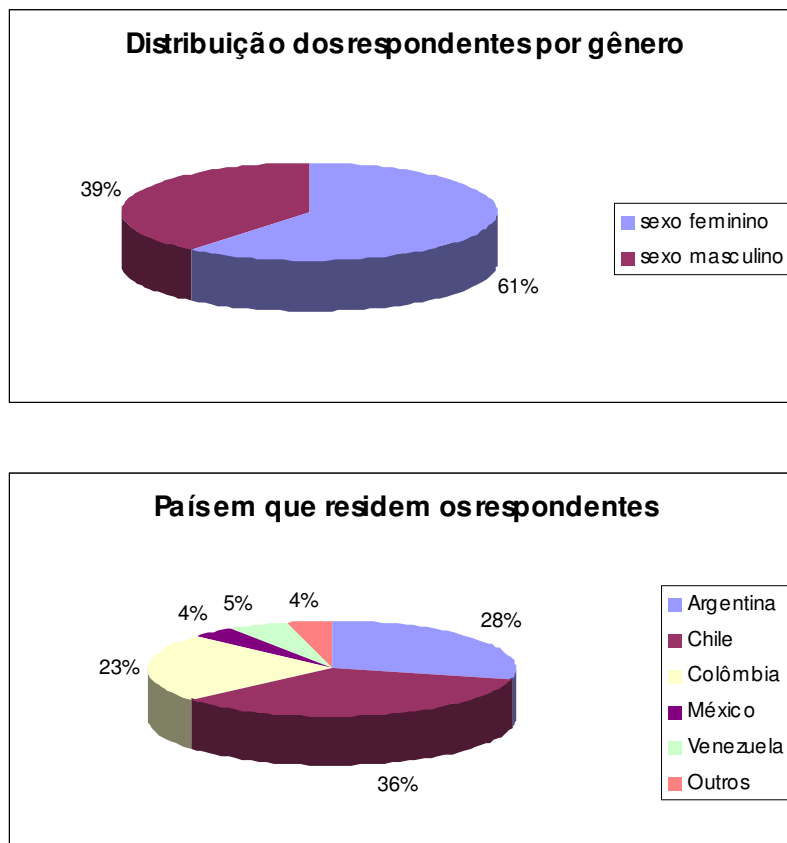


Fig. 2: Dados demográficos de nossos respondentes.

A única condição para participar na pesquisa era ter uma conta no *Facebook*. No entanto, os respondentes não apenas possuem um perfil no *site* como o usam com acentuada frequência: 40,1% disseram acessar suas contas mais de uma vez por dia e 51,9% visitam seus perfis entre uma e três vezes por semana. Além disso, 87,0% dos respondentes afirmaram que o *Facebook* é a rede social que eles mais usam e 9,5% disseram usar o *Facebook* tanto quanto outro *site* de rede social. Apenas 3,4% usam com mais frequência outro *site* de rede social. Dentre as finalidades para as quais os respondentes já usaram ou usam o *Facebook*, as mais apontadas foram as mais pragmáticas dentre a lista de opções disponíveis: manter contato com conhecidos ou pessoas que moram longe de uma maneira barata e conveniente (93,3%); compartilhar fotos e vídeos (77,0%); se divertir com os jogos e aplicativos disponíveis (68,1%). Depois destas, a opção mostrar aos outros fatos sobre minha vida e personalidade foi a mais assinalada (36,2%), lado a lado com a opção conhecer novas pessoas com interesses semelhantes (35,5%). A diferença entre o número de pessoas que usam o *site* com estas duas últimas finalidades não é estaticamente significativa para definir qual dos dois

comportamentos é mais comum ($n = 135$; $t = -1,474$; $Pr = 14,17\%$).¹⁶⁷ As opções aumentar minha popularidade entre meus amigos (17,0%); passar aos outros uma imagem positiva e ser bem aceito socialmente (13,3%) e encontrar um namorado (7,4%) foram as menos assinaladas. Uma possível justificativa para os baixos índices registrados para estas alternativas seria o fato de os usuários sentirem vergonha ou não quererem admitir que já usaram o *site* com estes propósitos. Acquisti e Gross (2006), em pesquisa sobre o comportamento de integrantes da população da universidade americana *Carnegie Mellon* no *Facebook*, perguntaram aos seus respondentes as finalidades para as quais eles usavam o *site* e também as finalidades para as quais eles acreditavam que seus pares usavam o *site*. Ainda que poucos tenham declarado usar o *Facebook* para propostas como mostrar informações sobre si próprios/anunciarem-se; aumentar sua popularidade; encontrar um namorado(a); muitos disseram acreditar que os demais membros usam o *site* com estes objetivos (AQUISTI e GROSS, 2006: 13).

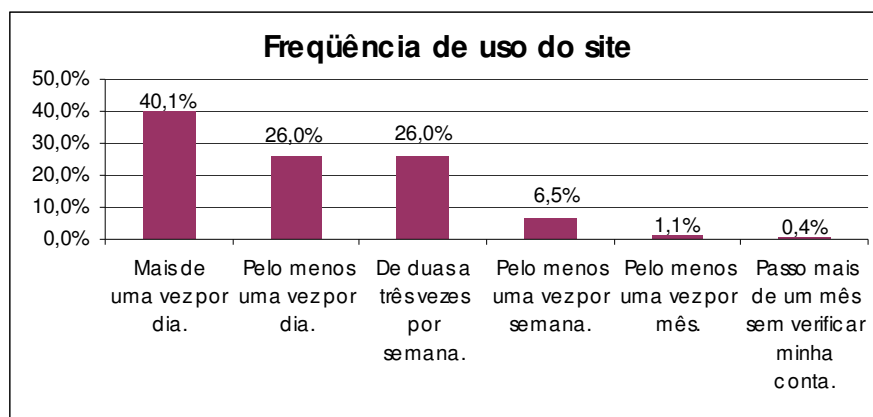


Fig. 3: Frequência com que nossos respondentes acessam suas contas no *Facebook*.

Um dos elementos investigados por meio do questionário foi o nível de preocupação dos usuários em relação à sua privacidade e ao uso das informações pessoais que eles disponibilizam em seus perfis. Perguntamos aos respondentes como eles se sentiam em relação às seguintes situações associadas ao uso da Internet em geral quando usavam o *Facebook*: risco de vírus/*spywares*; prática de crimes cibernéticos; roubo de identidade; ameaças à privacidade; ser perseguido, assediado ou ameaçado por um estranho através da Internet; ter seus dados pessoais coletados e usados para envio de recomendações de produtos ou anúncios personalizados. O que se pode depreender das respostas fornecidas é que, pelo

¹⁶⁷ O n é nossa amostra e indica o número de indivíduos que participaram desta pesquisa. Considere, nas aparições recorrentes da variável n , o mesmo significado.

menos no nível do discurso, os usuários latinos de redes sociais consideram que se expõem a riscos interagindo nestes ambientes, e se sentem, em sua maioria, preocupados em relação a isto. Para cinco dos seis cenários apresentados, a porcentagem daqueles que disseram se preocupar em algum grau foi maior que 75%. A exceção foi a opção riscos de vírus/*spywares*, fator que preocupa 61,4% dos respondentes. Para nossa surpresa, os cenários com os quais o maior número de respondentes se preocupou em algum grau foram ameaças à privacidade e roubo de identidade, empatados com 78,7%, e ter dados pessoais utilizados para *targeting* publicitário, com 78,0%. A diferença entre estes valores segundo um teste-*t* não é estatisticamente significativa, donde podemos afirmar que estes três cenários preocupam em diferentes graus o mesmo número de indivíduos ($n = 127$; $t = 1,717$; $Pr = 8,72\%$).

Diante deste empate, resolvemos considerar a intensidade da preocupação dos indivíduos usando a média das variáveis categóricas obtidas através da *Likert Scale*. Atribuímos pesos de quatro a um para os que marcaram, respectivamente, as alternativas muito preocupado, preocupado, pouco preocupado e isso não me preocupa. Os cenários roubo de identidade ($média = 2,896$; $sd = 1,005$),¹⁶⁸ ameaças à privacidade ($média = 2,769$; $sd = 1,020$) e ter dados pessoais utilizados para *targeting* publicitário ($média = 2,709$; $sd = 1,026$) permaneceram empatados, pois as diferenças encontradas para as respectivas médias não foram estatisticamente significantes segundo um teste-*t*. Roubo de identidade – ameaças à privacidade ($t = 0,991$; $Pr = 32,25\%$); Roubo de identidade – *targeting* publicitário ($t = 1,456$; $Pr = 14,65\%$).¹⁶⁹ Em relação ao cenário ser perseguido por um estranho através da Internet ($média = 2,586$; $sd = 1,005$), temos que os indivíduos se preocupam mais com o roubo de identidade ($t = 2,448$; $Pr = 1,50\%$). A análise comparativa de todos os cenários investigados identificou que ameaças à privacidade e ter dados pessoais utilizados para *targeting* publicitário preocupam tanto os indivíduos quanto ser perseguido por um estranho através da Internet ou o risco de crimes cibernéticos. Apenas o risco de vírus/*spywares* os preocupa menos que estes dois cenários aqui analisados. Assim, vemos que a privacidade e as rotinas da publicidade direcionada são assuntos considerados tão preocupantes por nossos respondentes quanto o roubo de identidade, o *stalking* e crimes cibernéticos. Duas leituras são possíveis: ou aqueles que mais se preocupam o fazem em relação à maior parte dos cenários investigados –

¹⁶⁸ O parâmetro *média* é a média aritmética dos níveis de preocupação de todos os indivíduos que responderam a pesquisa. O parâmetro *sd* é o desvio padrão, que mede o quanto os indivíduos estão distantes da média, para valores superiores e inferiores a ela.

¹⁶⁹ Cada teste de hipótese verifica se dado um valor de média do nível de preocupação, seu desvio padrão e o tamanho da amostra, é possível dizer que não há diferença entre níveis de preocupação encontrados para os dois cenários. Quando a probabilidade é inferior a 5%, rejeitamos esta hipótese e concluímos que um dos cenários traz mais preocupação do que o outro.

o que é pouco provável, visto que este foi o comportamento da maior parte de nossa amostra e que não temos motivos para acreditar que ela seja tendenciosa, no sentido de ter selecionado apenas indivíduos mais preocupados – ou nossos respondentes atribuíram um alto grau de importância à questão da privacidade e do uso de dados individuais para *targeting* publicitário.

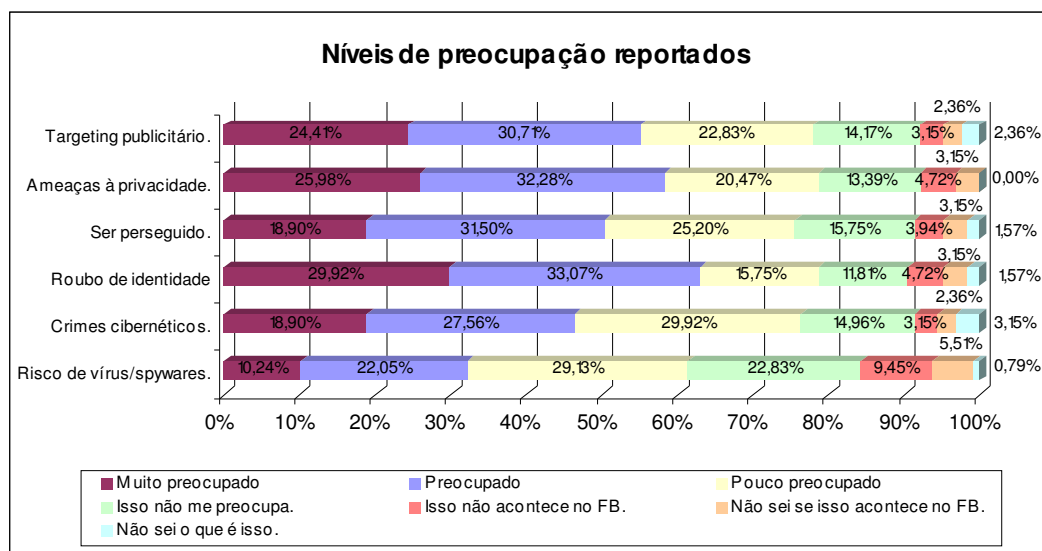


Fig. 4: Preocupação dos usuários com riscos associados de caráter geral quando usam o *Facebook*.

Diante destes resultados, optamos por investigar se os níveis de preocupação reportados por nossos respondentes são compatíveis com suas ações. Avaliamos se os usuários que se disseram muito preocupados e preocupados tomaram com mais frequência alguma atitude para se proteger dos riscos que eles avaliaram ser preocupantes e inerentes ao uso do *Facebook* em relação àqueles que se disseram pouco preocupados, não preocupados ou que declaram desconhecimento sobre o tema. Duas alternativas neste sentido seriam possíveis: deixar de publicar determinado tipo de informação ou usar configurações de privacidade para impedir o acesso de terceiros. Assim, usamos as correlações produto-momento de *Pearson* para avaliar se o grau de preocupação variava com a predisposição para autocensurar a publicação de algum tipo de informação ou para usar configurações de privacidade.

Os resultados encontrados mostram que não é regra geral a existência de correlação entre o tipo de preocupação dos respondentes e suas atitudes em relação à proteção e disponibilização de dados individuais. Na categoria ameaças à privacidade, de 17 modalidades de autocensura e de uso de configuração de privacidade relacionadas, apenas a

predisposição em publicar informações de contato ($Pr = 2,3\%$) variou de acordo com o nível de preocupação dos respondentes, *i.e.*, aqueles que se disseram mais preocupados com ameaças a sua privacidade evitaram mais disponibilizar informações de contato. A predisposição para usar configurações de privacidade mais de uma vez e para restringir o acesso de terceiros ao perfil ou a alguma categoria das informações nele contidas ficaram perto da correlação ($Pr = 9,1\%$ e $Pr = 7,8\%$, respectivamente, sendo que uma porcentagem menor que 5% indicaria que o nível de preocupação e o comportamento estariam correlacionados). Para o cenário de *stalking*, encontramos a existência de correlações com o comportamento de evitar disponibilizar informações que os respondentes não gostariam que os pais, namorados, professores ou alguma autoridade na faculdade/escola ficassem sabendo ($Pr = 1,3\%$) e com evitar disponibilizar informações que possam prejudicar na hora de arrumar um emprego ou entrar na faculdade ($Pr = 3,6\%$). Nenhuma correlação foi encontrada para o cenário do direcionamento de produtos e anúncios publicitários. Não podemos afirmar que o comportamento dos usuários esteja em desacordo com suas declarações visto que, de maneira geral, os mais preocupados evitam com mais frequência disponibilizar informações e usam mais as configurações de privacidade do que os menos preocupados. No entanto, não encontramos, senão em casos isolados, existência de correlação entre os níveis e o tipo de preocupação com o comportamento que visasse proteger o usuário.

Neste sentido, por considerarmos que o tema privacidade pode agrupar preocupações mais amplas e diversas, realizamos uma nova análise para os cenários ser perseguido por um estranho através da Internet e ter dados pessoais utilizados para *targeting* publicitário. Nossa hipótese era a de que o número de pessoas que evitaria disponibilizar informações que envolvessem o lugar e hora onde estariam em um dia determinado seria maior para aqueles que se disseram muito preocupados e preocupados com *stalking* do que entre os que se disseram muito preocupados e preocupados em ter seus dados pessoais utilizados para *targeting* publicitário. Igualmente, presumimos que bloquear o *Beacon* e *Social Ads* e evitar disponibilizar informações que pudessem ser usadas para enviar aos usuários recomendações de produtos e anúncios seriam comportamentos mais comuns entre aqueles que se disseram mais preocupados em ter seus dados usados para *targeting* publicitário. No primeiro caso, aproximadamente a mesma porcentagem de indivíduos entre os que se disseram preocupados e muito preocupados com os dois cenários afirmou evitar disponibilizar informações que incluíssem sua localização ($57,8\%$ entre os mais preocupados com *stalking* e $55,7\%$ entre os mais preocupados com uso de dados pessoais para direcionamento de anúncios, diferença não estatisticamente significativa segundo um teste-*t*). Resultados semelhantes foram encontrados

para a segunda medição realizada. Aqui, o número dos que bloquearam o *Beacon* foi inclusive maior entre os mais preocupados com *stalking* do que entre os mais preocupados com o *targeting* publicitário (20,3% e 17,1%, respectivamente, diferença não estatisticamente significativa segundo um teste-*t*). Ainda, é interessante observar que a porcentagem daqueles que disseram evitar disponibilizar informações que possam ser usadas para lhes direcionar ofertas e anúncios também foi maior entre os mais preocupados com *stalking* (31,2%) do que entre os mais preocupados com o uso de seus dados pessoais para direcionamento de anúncios e com ameaças à privacidade (27,1% e 27,0%, respectivamente).

Desta forma, nossa conclusão é a de que as práticas de autocensura e uso de configurações de privacidade são praticadas em níveis semelhantes entre os indivíduos que se dizem muito preocupados e preocupados. No entanto, estes comportamentos não parecem ser mais comuns ou freqüentes de acordo com os temas que mais preocupam os usuários. Naturalmente, sabemos que determinadas atitudes podem endereçar de uma só vez variadas preocupações. No entanto, em cenários como o do *targeting* publicitário, por exemplo, vemos que os indivíduos não endereçam com mais freqüência suas preocupações com as configurações de privacidade disponíveis nem deixam de disponibilizar informações que possam ser usadas com este fim. Os motivos para tal comportamento não foram investigados, mas podem estar relacionados à falta de conhecimento, ao desejo por receber recomendações ou mesmo a uma avaliação de custo benefício que considere os custos sociais de deixar de disponibilizar determinadas informações. Ressaltamos, por fim, que a porcentagem de indivíduos preocupados e muito preocupados que disseram bloquear o *Beacon* e o *Social Ads* ou deixar de disponibilizar dados que possam ser usados para lhes direcionar anúncios foi baixa para todos os cenários, girando em torno de 15% a 20%, valor que sobe para cerca de 60% a 70% quando os comportamentos são evitar disponibilizar informações que possam ferir a imagem/reputação do respondente ou evitar publicar informações que o respondente não gostaria que seus pais, namorados, familiares ou autoridades soubessem.

Buscamos avaliar também os motivos que contribuem para atenuar as preocupações dos usuários em relação às informações que eles disponibilizam no *Facebook*. Entre todos os respondentes da amostra, os argumentos mais recorrentes foram a autocensura das informações publicadas como forma de proteção dos dados individuais (34,6%) e o uso de configurações de privacidade (29,1%). Em seguida, os motivos mais assinalados como atenuantes da preocupação dos usuários acerca dos dados que disponibilizam no *site* foram o comportamento de rebanho (meus amigos fazem o mesmo) (15,0%), confiança no serviço prestado pelo *Facebook* e no fato de que o *site* não usa ou compartilha as informações

publicadas (15,0%), crença no fato de que não há nenhum tipo de risco associado ao uso do *site* (14,2%), crença na dificuldade de se achar uma informação comprometedora na imensa massa de dados de uma rede social (14,2%) e o julgamento de que compartilhar informações e interagir com os outros pode ser mais útil e trazer mais benefícios do que as possíveis ameaças que o *site* possa representar à privacidade de seus usuários (13,4%). Três dos motivos supracitados, todos com porcentagens muito baixas, estão associados à falta de informação acerca das políticas da empresa, do funcionamento do *site* e dos riscos possivelmente associados ao seu uso.¹⁷⁰ Por outro lado, é importante ressaltar que disponibilizar em sua conta apenas o que possa ser visto por qualquer pessoa foi um comportamento mais recorrente do que o uso das configurações de privacidade. A opção pelo controle empírico, *i.e.*, no ato da postagem e da construção do perfil é mais comum, apesar da ampla variedade de configurações de privacidade disponíveis.

Desta forma, passemos a uma análise da predisposição de nossos respondentes em restringir aos outros o acesso às informações de seus perfis. Investigamos que tipo de informações eles evitam publicar no *site* e o grau de adesão destes usuários às configurações de privacidade disponíveis. Dos respondentes, 67,1% afirmaram já ter usado as configurações de privacidade uma vez ou mais de uma vez, sendo que a porcentagem dos que disseram já ter alterado estes padrões mais de uma vez foi mais que o dobro dos que o fizeram apenas uma vez. Na tabela seguinte, em que avaliamos os objetivos para os quais os usuários já usaram essas configurações, nos chama a atenção o baixo número dos que optaram por bloquear o *Facebook Beacon* (18,1%) ou o *Social Ads* (14,1%). Uma hipótese que justificaria o baixo nível de uso dessas configurações seria o fato de se tratar de funcionalidades mais novas do *site*, sobre a qual nem todos os usuários têm conhecimento. Outra hipótese que levantamos aqui seria a de que tanto os profissionais do *marketing* quanto a própria empresa, embora possam ser audiências indesejadas, são públicos menos visíveis do que aqueles – desejados e indesejados – que os usuários têm em mente ou pelo menos conjecturam quando publicam suas informações nestes *sites*.

As duas opções mais reportadas quando perguntamos aos usuários sobre as informações que eles evitam disponibilizar no *Facebook* mostram a forte presença do imperativo da exposição de si e da censura relacionada ao meio social *offline* do respondente: 64,6% afirmaram evitar disponibilizar informações que possam ferir sua imagem ou

¹⁷⁰ Referimos-nos aqui ao fato de os usuários: a) não saberem que o *Facebook* compartilha informações com terceiros; b) acreditarem que não haja nenhum risco associado ao uso do *site* e c) acreditarem na dificuldade de se encontrar uma informação na massa de dados de uma rede social.

reputação e 62,4% afirmaram evitar publicar informações que eles não gostariam que os pais, namorado, professores, familiares ou autoridades ficassem sabendo. Assim, ainda que ter a própria imagem associada a um anúncio publicitário possa figurar como algo que fira a reputação dos usuários do *site*, o índice de 64,6%, citado acima, nos dá a pista de que a autocensura se relaciona a objetivos predominantemente sociais de gerenciamento da informação. As audiências desconhecidas aparecem com uma porcentagem significativamente menor: 48,8% disseram evitar disponibilizar informações que incluam o lugar e hora em que estarão em um dia particular. Novamente, assuntos relacionados ao *marketing* aparecem em último lugar: apenas 22,8% disseram evitar publicar informações que possam ser usadas para lhes direcionar recomendações de produtos ou anúncios publicitários. É importante ressaltar aqui que, como esta forma de uso das informações pessoais representa um benefício direto para os internautas, ela pode não ter sido associada a nenhuma conotação negativa e sim à vantagem de se receber anúncios coerentes com as próprias intenções e interesses de consumo, fator não avaliado pelo questionário aplicado.

Informações que os usuários evitam disponibilizar através do FB	Valores	Porcentagens
Informações que possam ferir minha imagem ou minha reputação.	82	64,57%
Informações que não gostaria que meus pais, namorado(a), professores(as), familiares ou autoridades na escola/faculdade ficassem sabendo.	78	61,42%
Informações que incluam o lugar/hora em que estarei em um dia em particular.	62	48,82%
Informações que não gostaria que meus amigos soubessem.	60	47,24%
Informações que possam me prejudicar na hora de arrumar um emprego ou entrar na faculdade.	49	38,58%
Informações sobre meus gostos e interesses que possam ser usadas para me direcionar recomendações de produtos ou anúncios publicitários.	29	22,83%
Não há nenhum tipo de informação que eu evite disponibilizar através do FB.	13	10,24%

Tipos de configurações de privacidade utilizados	Valores	Porcentagens
Restringir quem pode ver meu perfil e/ou algum dos tipos de informações nele disponíveis.	74	58,27%
Restringir o número de pessoas que pode buscar pelo meu perfil no FB.	71	55,91%
Restringir quem pode ver minhas informações de contato.	63	49,61%
Restringir as informações que ficam disponíveis em meu anúncio público de busca.	61	48,03%
Restringir quais das minhas atualizações publicadas no News Feed e Mini-Feed.	47	37,01%
Bloquear alguém.	43	33,86%
Não permitir a publicação de históricos Beacon.	23	18,11%
Não aparecer em anúncios sociais mostrados aos meus amigos.	18	14,17%

Fig. 5: Estratégias de autocensura e tipos de configurações de privacidade utilizados.

No que diz respeito à publicação de informações, identificamos níveis significativos de predisposição dos usuários em revelar dados nos campos de data de aniversário e endereço de *e-mail*. Ao contrário, a publicação de informações de contato como telefone residencial e celular foi preterida pela grande maioria dos respondentes. Enquanto 96,3% dos participantes revelam sua data de aniversário e 62,2% publicam seus filmes favoritos, os valores encontrados para as categorias telefone residencial e celular foram, respectivamente, 14,0% e 24,4%. Além disso, identificamos que, uma vez que um usuário se predispõe a revelar uma informação, a tendência é a de que ela seja verdadeira. Perguntados sobre as razões que os motivam a revelar dados incorretos ou precisos no *Facebook*, apenas 5,1% de nossos respondentes admitiram publicar dados falsos. A grande maioria, 80,7%, afirmou que, de maneira geral, as informações que eles publicam no *site* são verdadeiras porque pessoas conhecidas irão usá-las para saber mais sobre eles(as). A segunda condição mais apontada, assinalada por 58,0% dos participantes, foi a de que as informações que eles disponibilizam são verdadeiras porque só é possível compartilhar os próprios interesses com outras pessoas se eles são expressos verdadeiramente. Assim, podemos concluir que o uso do *Facebook* está associado a finalidades que exigem a veracidade ou pelo menos a seleção das informações publicadas: a interação com os outros e a exibição de si.

Consideremos agora a percepção dos usuários avaliados em relação à rede de visibilidade social na qual eles se inserem através da participação no *site*. Dentre nossos respondentes, 61,5% afirmaram que não adicionam ou aceitam pessoas desconhecidas como amigos quando são adicionados porque os amigos podem ver seus perfis, e eles não gostariam que estranhos vissem as informações que eles publicam no FB. Pedimos aos nossos respondentes que apontassem também a principal condição na qual eles se importariam. Aqui, 48,8% disseram não se importar se outros entram em suas páginas. Os principais fatores que os incomodariam no caso de alguém visualizar seus perfis seriam o fato de a pessoa ser desconhecida (26,6%) ou ser alguém de quem o indivíduo avaliado não gosta (14,0%). Desconsiderando os motivos apresentados pelos usuários, no total, 40,7% dos usuários se importam se outros vêem seus perfis e 50,3% não se importam. Dos que se importam, 63,6% declararam já alterado suas configurações de privacidade, percentual que sobe para 88,2% entre os que não se importam. Estes dados nos permitem constatar que as preocupações dos usuários com a visibilidade de seus perfis não se traduz, de maneira geral, em uma maior frequência de uso de configurações de privacidade, como seria esperado. Duas hipóteses são possíveis: a) a de que esta preocupação é endereçada principalmente através da autocensura das informações publicadas; b) a de que apesar de se importar com o fato de outros verem

seus perfis, estes indivíduos não tomam nenhuma atitude para evitar este acesso, seja porque, apesar de se importarem, isso não os preocupa, realmente, ou porque esta preocupação não é suficiente para levá-los a tomar alguma atitude no sentido de impedir o acesso de determinadas audiências a seus perfis.

A hipótese de que as práticas da exibição de si nestas redes estão associadas à emergência de um *voyeurismo* distribuído é verdadeira no universo dos participantes investigados. Perguntados sobre qual a principal situação em que visualizam o perfil de alguém, a mais reportada foi o acesso ao perfil de amigos e conhecidos para saber novidades sobre suas vidas, assinalada por 51,1% dos participantes. Em seguida, o comportamento mais reportado foi a visita a perfis de amigos ou de pessoas desconhecidas para se divertir vendo fotos e sabendo o que eles escrevem sobre eles mesmos, suas experiências de vida, seus gostos e suas relações sociais, declarado por 30,3% dos participantes. É interessante notar que o olhar e a atenção de nossos participantes não estejam voltados apenas aos seus amigos e conhecidos, mas que a navegação aleatória por perfis de desconhecidos também represente uma modalidade de uso do *site* que implique em diversão para aqueles que a executam. O que nos parece é que os perfis constituem um gênero ou narrativa próprio aos ambientes digitais: assim como as pessoas mobilizam sua atenção vendo um programa de TV ou um filme em uma sala de cinema, nas redes sociais seu interesse se volta para a narrativa de si tal como formalizada através das funcionalidades do perfil. Parcelas de vida cotidianas, de indivíduos ordinários, se combinam a fragmentos de mídia na produção de uma modalidade de participação disponível a todos.

Tentamos mensurar também, através do questionário, o nível de conhecimento dos indivíduos acerca dos mecanismos de visibilidade do *Facebook*, das políticas da empresa e de temas relacionados ao trânsito e uso de dados disponibilizados em redes sociais. Perguntamos também sobre a leitura das políticas de privacidade e termos de uso do *site*. Os índices encontrados foram semelhantes: 54,8% e 54,0% afirmaram não ter lido os respectivos documentos, enquanto a mesma porcentagem de pessoas, 26,0%, afirmaram terem lido-os parcialmente. Com relação aos aplicativos, apenas 11,1% disseram se preocupar em permitir que terceiros tenham acesso às informações disponibilizadas em seus perfis. A mesma porcentagem de pessoas disse sempre visitar a página de configurações de privacidade do aplicativo ao adicioná-lo e um número ainda menor, 7,4%, disseram ler cuidadosamente os termos de uso e políticas de privacidade do aplicativo. Entre os respondentes, 20,0% já ouviram falar em portabilidade de dados e 25,1% já ouviram falar em mecanismos de busca de pessoas, como o *Rapleaf.com* e o *Upscoop.com*. Desta forma, resolvemos investigar se o

conhecimento das políticas do *site* e de temas relacionados ao trânsito de dados em redes sociais influenciava o comportamento *online* dos indivíduos. Em outras palavras, associando essas atividades ao fenômeno da vigilância, visamos identificar se a consciência do ato de ser vigiado se traduzia em mudança de comportamento para os indivíduos.

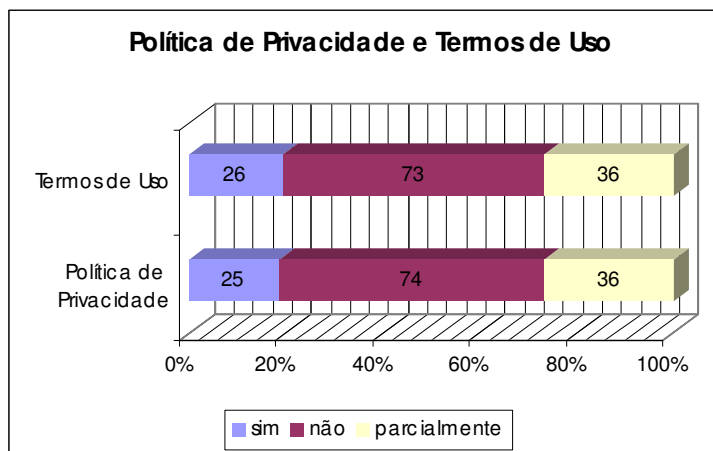


Fig. 6: Percentuais de leitura dos termos de uso e da política de privacidade do *Facebook*.

Para agrupar as variáveis relativas a estes temas construímos dois índices: o de conhecimento das políticas da empresa e o de familiaridade com temas relacionados. Para o primeiro, consideramos as respostas de cada um de nossos participantes a quatro questões, todas com a mesma tríade de respostas possíveis (verdadeiro, falso, não sei). A primeira delas dizia que os aplicativos adicionados podem acessar as informações de um indivíduo através de seus amigos; a segunda que o *Facebook* se reserva o direito de compartilhar as informações de seus usuários com terceiros, sem lhes dizer nem quando nem com quem; a terceira dizia que o *Facebook* coleta informações do perfil de seus usuários e de outras fontes para lhes oferecer uma experiência personalizada no *site*; a quarta dizia que os anúncios que aparecem no *site* estão relacionados aos conteúdos dos perfis em que são exibidos. Para cada resposta certa, um ponto era computado para a construção do referido índice. A maior parte dos usuários (33%) acertou duas questões. Apenas 11% acertaram todas as quatro e 16% não acertaram nenhuma. Por fim, 19% acertaram três e 21% acertaram apenas uma. Assim, podemos concluir que os usuários têm um conhecimento médio sobre as políticas da empresa (63% acertaram quatro, três ou duas questões). Para o caso do índice de familiaridade com temas relacionados perguntamos apenas se os usuários já haviam ouvido falar em portabilidade de dados e em mecanismos de busca de pessoas (respostas dicotômicas, sim e não). Um ponto foi computado a cada vez que o indivíduo respondeu já ter ouvido falar no

tema questionado. Aqui, ao contrário, 67% disseram nunca ter ouvido falar em nenhum dos dois temas. Somente 13% declararam familiaridade com os dois temas e 20% com apenas um deles. Assim, concluímos que o conhecimento médio sobre as políticas da empresa é maior do que a familiaridade com temas relacionados.

Assim, resolvemos correlacionar estes dois índices com a frequência de uso do *site* e com as categorias de informações disponibilizadas, visando investigar se interagir mais no *Facebook* contribui para o conhecimento das políticas da empresa ou para a familiaridade com temas como a portabilidade ou a existência dos mecanismos de buscas de pessoas. Avaliamos também se graus maiores de conhecimento e de familiaridade estariam relacionados a um decréscimo da predisposição dos usuários em revelar informações através de seus perfis. Não consideramos aqui o uso de configurações de privacidade. Encontramos que para os campos data de nascimento e *e-mail*, índices mais altos de conhecimento acerca das políticas da empresa não se traduzem em uma predisposição a não revelar tais informações ($Pr = 17,2\%$ e $Pr = 53,6\%$, respectivamente).¹⁷¹ Para o campo filmes favoritos, encontramos a existência de uma correlação positiva – quem conhece mais as políticas da empresa disponibiliza mais esta informação ($Pr = 3,8\%$). Não possuímos evidências suficientes para justificar o porquê desta relação, mas duas hipóteses prováveis são as de que os usuários tendem a revelar esta informação porque desejam receber anúncios direcionados ou porque, apesar de saberem que os anúncios estão relacionados ao conteúdo de seus perfis e que a empresa compartilha seus dados com terceiros, podem não compreender ou julgar nocivas as implicações de tais atos.

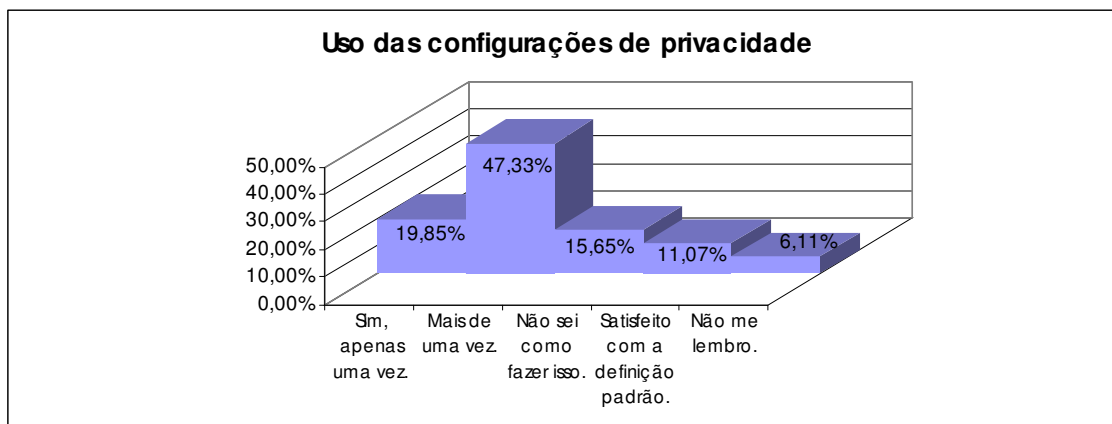


Fig. 7: Percentuais de uso das configurações de privacidade.

¹⁷¹ A probabilidade investigada é a de que não exista correlação entre as duas variáveis. Aceitamos aqui que uma probabilidade inferior a 5% é suficiente para dizer que a hipótese deve ser rejeitada e que há, portanto, uma correlação entre as variáveis.

Para o caso da familiaridade com os temas portabilidade e buscas de pessoas, também não encontramos nenhuma relação entre os índices calculados e um maior grau de autocensura na publicação de informações. Visto que medimos apenas a familiaridade e não o conhecimento dos usuários com tais temas, não podemos afirmar que isto seja um sinal de que eles não se importem, por exemplo, com o uso e disponibilização dos dados de seus perfis por empresas de *people search*. O uso de configurações de privacidade também pode ser uma estratégia para proteger as informações publicadas. De qualquer forma, podemos conjecturar a hipótese de que, por ser silenciosa e invisível e por não incomodar os usuários em suas rotinas de uso do *site*, as modalidades de olhar cujas fontes são a própria empresa ou outras instituições não são vistas como um problema a ser endereçado por estes usuários, mesmo quando eles afirmam conhecer a existência de tais práticas. Não encontramos também nenhuma relação entre uma frequência mais acentuada de uso do *site* e maiores graus de conhecimento das políticas da empresa ou de familiaridade com temas relacionados, fato que pode ser justificado pelo fato de que estas modalidades de olhar são silenciosas e imperceptíveis aos usuários do *site*, que de maneira geral, só virão a saber de tais práticas através da leitura dos termos de uso, da política de privacidade ou de matérias na imprensa.

4.2 Análise de perfis

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 11 redes, 8 latino-americanas e 3 canadenses, das quais recolhemos amostras significativas de perfis para análise. Uma rotina computacional foi desenvolvida para realizar esta tarefa, usando a linguagem de programação *Perl* e *scripts* para o *parsing* das páginas HTML.¹⁷² 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 de maneira automática no *site* retornava usuários integrantes de cada uma dessas redes. Por fim, os perfis buscados eram acessados e salvos juntamente com as informações neles disponibilizadas, com exceção do nome e da foto do participante. Por fim, um banco de dados foi montado para

¹⁷² O *parsing*, neste caso, se refere ao ato de interpretar de forma automática diversas páginas HTML, retirando apenas as informações necessárias ao estudo em questão e armazenando-as organizadamente em um banco de dados.

organizar estas informações: dados como sexo, idade, número de amigos, de fotos e as redes das quais um usuário participava foram armazenados para subsidiar estudos subsequentes. Os demais campos foram convertidos em variáveis binárias: avaliamos apenas o preenchimento ou não preenchimento destas informações nos perfis selecionados. Análises semelhantes foram realizadas no *Facebook* por Jones e Soltren (2005) e Acquisti e Gross (2005), com foco no estudo de universidades americanas. Em nosso caso, como o objetivo é estudar o comportamento do público latino-americano, avaliamos ser necessário considerar de antemão questões relativas à forma como estes membros utilizam o *site*, principalmente no que diz respeito à participação em redes.

As diferenças de uso do *site* entre os públicos envolvidos neste estudo se devem, em grande medida, às condições de surgimento e desenvolvimento do *Facebook*. Focado primeiramente na expansão para outras universidades americanas a partir de Harvard, o *site* só passou a suportar redes de instituições de ensino superior fora dos EUA em outubro de 2005 e somente em setembro de 2006 o *site* abriu a participação a usuários comuns. Desta forma, duas diferenças fundamentais devem ser consideradas. A primeira delas é a de que, nos EUA, no Canadá e no Reino Unido, o *Facebook* possui redes geográficas apenas para cidades e não para países, como ocorre no contexto latino-americano. A outra é a de que, 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. Diferentemente, no contexto latino é comum a existência de redes abertas, que dispensam o cadastro de um *e-mail* institucional. Além disso, devemos considerar que, no contexto norte-americano, originalmente, o uso do *site* começava com a adesão a uma rede de universidade, o que pode estar relacionado ao fato de que o uso destas redes é endêmico em países como o Canadá e os EUA. Assim, para investigar então os padrões de uso dos latinos, usamos em nosso estudo redes de universidades latino-americanas abertas, bem como as redes geográficas dos países correspondentes. Quatro países latino-americanos foram selecionados: Chile, Argentina, Colômbia e México. A Venezuela foi dispensada desta análise, principalmente pela dificuldade de encontrarmos no país uma rede universitária que não exigisse o cadastro de um *e-mail* institucional. Para subsidiar uma comparação com o público norte-americano, usamos o Canadá, não só pelo significativo número de usuários do país no *Facebook* como pela possibilidade de acesso a uma conta de *e-mail* que nos permitisse participar de uma rede universitária – depois de entrarmos 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 23.458 perfis coletados em 11 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, Toronto e *University of British Columbia* (UBC). Para a América Latina, nossa estratégia foi selecionar, dentre as redes universitárias com mais usuários em cada um dos países escolhidos, as maiores que dispensassem um *e-mail* institucional para a participação. No contexto norte-americano, analisamos apenas uma rede de instituição de ensino superior, dada a dificuldade de acesso a uma conta de *e-mail* válida que nos permitisse entrar nas redes fechadas. Buscamos aqui, igualmente, redes com número significativo de usuários. No que diz respeito às redes geográficas, duas foram selecionadas para estudo no Canadá, visando conferir às nossas análises um pouco mais de abrangência. Naturalmente, o mesmo não foi feito para o contexto latino-americano, pois cada um destes países conta apenas com uma única rede regional. As tabelas abaixo mostram a divisão por gênero para os países estudados e para as amostras coletadas. É importante ressaltar que os dados de nossa amostra incluem apenas aqueles que revelaram o gênero em seus perfis. A comparação dos dados demográficos de nossa amostra com os da divisão de gênero para a América do Sul reportada pela O'Reilly Research (LORICA, 2008: *online*) nos dá pistas de que nossa amostra super-representa os indivíduos do sexo masculino e sub-representa os do sexo feminino. Assim, usamos dados atualizados sobre o número de homens e mulheres dos países selecionados, recolhidos através do sistema de direcionamento de anúncios do *Facebook*, para avaliarmos os percentuais de homens e mulheres nos países estudados. Como se pode ver abaixo, tais dados comprovam que nossa amostra não respeita a divisão de gênero dos usuários do *site* em nenhuma das regiões selecionadas. Nossa hipótese para explicar tal fato é a de que as mulheres, de maneira geral, tendem a restringir mais seus perfis do que os homens, já que nossa amostra só considera os usuários cujas contas conseguimos acessar dentre todas as tentativas efetuadas através das buscas que realizamos nas referidas redes. Não possuímos, no entanto, meios de comprovar as razões deste desvio.

País	Total	% MASC	% FEM
Argentina	2.745.020	44,3%	55,7%
Chile	3.902.100	47,1%	52,9%
Colômbia	4.171.480	47,4%	52,6%
México	1.767.020	45,9%	54,1%
Canadá	11.292.220	43,1%	56,9%

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%
Toronto	2776	61,00%	39,00%
Vancouver	2255	61,71%	38,28%
University of British Columbia (UBC)	2338	60,49%	39,50%

Fig. 8: Acima, número de usuários de cada país no *Facebook* e distribuição por sexo segundo o sistema de direcionamento de anúncios do *site*. Abaixo, número de perfis coletados por rede e sua divisão por gênero.

Os gráficos da distribuição por idade para as amostras de perfis coletados estão relacionados em anexo e incluem somente aqueles que revelaram esta informação em seus perfis.¹⁷³ Sua análise nos permite constatar a primeira diferença de uso entre os públicos latino e canadense. 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 (UBC) a frequência de participantes decresce radicalmente a partir dos 27 anos, sendo praticamente inexistente a partir dos 31 anos. Comportamento semelhante é observado para o caso das redes geográficas. Nos países latino-americanos, a participação é mais distribuída entre diferentes faixas etárias. Diferentemente, indivíduos com mais de 31 anos são raros nas redes Vancouver e Toronto. Não acreditamos que os participantes estejam mentindo acerca de suas idades: nosso questionário identificou que os latinos tendem a revelar informações verdadeiras no *Facebook* e estudos semelhantes já afirmaram o mesmo para o contexto norte-americano (ACQUISTI e GROSS, 2005; JONES e SOLTREN, 2005). Não possuímos evidências suficientes para justificar tal fato, mas uma comparação com os dados fornecidos pelo sistema de direcionamento de anúncios do *Facebook* nos permite identificar que o Canadá possui usuários comparativamente mais velhos do que os países latino-americanos. Diferentemente do constatado por nossas análises de perfis, nas quais indivíduos acima dos 31 foram praticamente inexistentes, os dados demográficos coletados apontam que o Canadá é o país que mais possui indivíduos com mais de 36 anos dentre os países selecionados para esta pesquisa (24% dos usuários canadenses do *Facebook* estão nesta faixa etária). Assim, podemos lançar a hipótese de que as pessoas mais velhas no Canadá tendem a bloquear mais seus perfis, revelar menos a idade ou não participar

¹⁷³ Cf. Anexo C, p. 204.

de redes geográficas ou de universidades. Já para o contexto latino americano, há uma proximidade significativa entre a distribuição de idade para os países e para as redes estudadas, tanto geográficas quanto universitárias. Para o caso específico das redes de instituição superior, acreditamos que o fato de as redes latinas serem abertas pode facilitar a entrada de ex-alunos e pessoas interessadas em participar, o que seria mais difícil para o caso da rede UBC.

Nome	Total	Amostra (N)	Disponibilizam perfil	% Disponibilizam
Universidad Catolica Argentina (UCA)	3.193	1303	1052	81%
Argentina	670.229	3020	1795	59%
University of British Columbia (UBC)	37.390	6192	2338	38%
Toronto	1.413.215	8407	2776	33%
Vancouver	863.780	8647	3086	36%
Universidad de Viña Del Mar (UVM)	2.051	1545	1266	82%
Chile	807.673	7923	3844	49%
Universidad Industrial de Santander (UIS)	4.357	3164	2452	77%
Colômbia	1.133.931	3062	1641	54%
Universidad de Guadalajara (UDG)	7.395	2334	2146	92%
México	674.512	5263	2939	56%

Fig. 9: Número total de usuários de cada rede selecionada, seguidos dos números de perfis que tentamos acessar e do número de indivíduos que disponibilizam seus perfis.

Analizamos também o uso de configurações de privacidade para cada uma das redes estudadas 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 aos seus perfis a pessoas de uma rede da qual faziam parte, deixando-o visível apenas aos amigos e/ou a outra rede da qual também participassem. Como descrevemos acima, o *download* dos perfis era feito através do uso de uma rotina computacional, que buscava e tentava acessar perfis randomicamente em cada 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 a leitura dos integrantes da referida rede, usando suas configurações de privacidade. Como mostra a tabela acima, nos dois tipos de redes avaliadas, os canadenses foram os que mais usaram configurações de privacidade para impedir 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 entre o comportamento de latinos e canadenses foi menor.

O percentual dos latinos que disponibilizam seus perfis girou entre 49% e 59%, contra 33% e 36% para as redes Toronto e Vancouver, respectivamente.

Em todos os países latinos estudados, a porcentagem de perfis disponíveis em redes de instituições de ensino superior 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. No entanto, 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 para os dois tipos de rede foi pequena, o que aponta que a predisposição para o uso de configurações de privacidade, para este público, independe do contexto. Duas hipóteses são possíveis. Como a rede UBC é uma rede grande (mais de 37 mil usuários), podemos aproximar o comportamento de seus usuários aos daqueles das redes geográficas. Além disso, considerando que ela exige um *e-mail* da instituição para participação, podemos conjecturar que os canadenses são mais preocupados com as informações que disponibilizam. 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 sobe 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.

Passemos agora à análise da predisposição dos indivíduos em revelar informações nos diferentes países e redes.¹⁷⁴ Antes disso, é importante lembrar que analisamos aqui apenas os perfis daqueles que os disponibilizavam, donde se pode concluir que nossa amostra pode ser considerada levemente tendenciosa. Avaliamos 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,

¹⁷⁴ Cf. Anexo C, p. 204.

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 ou não disponibilizados de acordo com as configurações de privacidade dos usuários. Assim, as informações que os usuários publicam para além desta quantidade mínima necessária 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 das redes geográficas canadenses foram os que revelaram em média mais informações ($m = 6,80$ para a Vancouver e $m = 6,82$ para a Toronto). É importante lembrar aqui que o público canadense foi o que mais usou configurações de privacidade para bloquear o acesso aos seus perfis. Assim, ainda que não possamos constatar tal fato, devemos considerar a possibilidade de que a amostra selecionada seja mais predisposta e/ou menos preocupada em revelar informações através do *Facebook*.

A disponibilização de informações com valor comercial (livros de cabeceira, programas de TV favoritos, músicas favoritas, atividades e interesses) para as redes geográficas analisadas segue a mesma tendência observada acima. O índice criado para calcular a média de publicação destas informações foi menor entre os colombianos ($I_c = 0,93$) e argentinos ($I_c = 1,28$) e maior entre mexicanos ($I_c = 1,65$) e chilenos ($I_c = 1,66$), sendo que a diferença entre os valores do índice para os dois últimos países não é estatisticamente significativa. O maior grau de disponibilização de informações com valor comercial foi para as redes canadenses ($I_c = 2,16$ para a rede Vancouver e $I_c = 2,21$ para a rede Toronto). 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 significativa), a revelação do endereço de *e-mail* apresentou variação significativa. Enquanto no contexto latino-americano a porcentagem dos que publicavam esta informação variou entre 13% e 20%, nas redes Vancouver e Toronto estes valores foram 47% e 48%, respectivamente. 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 de diferentes países em revelar informações não equivale à observada acima, para o caso das redes geográficas. A média total dos dados individuais publicados na rede 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: os usuários da *University of British Columbia* foram os que publicaram, em média, mais informações, dentre todas as redes universitárias observadas ($m = 6,79$). Novamente, o índice de disponibilização de informações com valor comercial (I_c) variou de acordo com a média geral de todas as informações publicadas (ou seja, foi menor entre os integrantes da UCA e maior para os UVM). O maior valor do referido índice foi registrado entre os canadenses da rede UBC. Em relação às informações de contato, como encontramos em nossa análise das redes geográficas, as diferenças entre as porcentagens daqueles que publicaram telefone celular nos diferentes países foi pequena. No entanto, desta vez, o endereço de *e-mail* foi disponibilizado com mais frequência pelos latinos. O maior percentual de publicação desta informação apareceu entre os mexicanos da rede UDG (71%), diferença significativa em comparação com a rede UBC (63%). Novamente, o preenchimento de campos como visão política e religião variaram em desacordo com a tendência prescrita pela média geral de revelação de informações observada para as redes universitárias. O mesmo aconteceu com o status de relacionamento, que desta vez foi publicado com mais frequência pelos integrantes das redes UVM e UIS, que figuraram empatadas com o percentual de disponibilização de 52%.

Comparando agora o comportamento dos usuários latinos e canadenses nas redes geográficas e de instituições de ensino superior, observamos que, 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 os usuários revelam menos informações nas redes de instituições de ensino superior do que na rede geográfica do país

correspondente. No que diz respeito à publicação de informações com valor comercial, com exceção do contexto colombiano, no qual a diferença encontrada não foi significativa ($I_c = 0,92$ para a UIS e $I_c = 0,93$ para a rede Colômbia), os usuários latinos e canadenses do *Facebook* revelam, em média, menos informações com valor comercial em redes de universidades do que em redes geográficas. Além disso, em todos os países latinos analisados, os usuários do *Facebook* que estão em redes geográficas possuem em média mais amigos e publicam mais fotos do que aqueles que estão em redes de universidades. Para o contexto canadense, novamente, o comportamento observado foi semelhante para as redes geográficas e de instituições de ensino superior. O número médio de fotos publicadas e de amigos foi muito próximo para as redes UBC, Vancouver e Toronto (respectivamente 285, 274 e 258 para fotos e 330, 368 e 373 para amigos). A tendência de que os indivíduos publicam mais informações em redes geográficas e menos nas universitárias, observada, salvo raras exceções, para todos os países latinos, só não se repetiu para a categoria das informações de contato. A publicação do telefone celular cresceu ligeiramente nas redes de instituição de ensino superior e a do endereço de *e-mail* em níveis muito significativos, tanto nos países latinos quanto no Canadá, seja porque os usuários se preocupam menos ou porque se torna mais útil disponibilizar esta informação em uma rede de instituição de ensino superior.

Por fim, buscamos a existência de possíveis correlações entre as variáveis sexo, idade, número de fotos, de amigos e o comportamento em relação à disponibilização de informações. Para as variáveis contínuas (idade, número de fotos e amigos), calculamos o coeficiente de correlação entre cada uma delas e o número total de categorias do perfil preenchidas por indivíduo. Investigamos também as relações com o número total de informações comerciais disponibilizadas e a publicação ou não do endereço de *e-mail*. Para cada par de variáveis analisadas, realizamos um teste de hipótese para identificar a probabilidade de não haver correlação. Já para a variável dicotômica sexo, efetuamos um teste de hipótese para verificar a probabilidade de não haver diferença entre o comportamento de homens e mulheres. Como para o contexto anterior, analisamos aqui o total de informações publicadas, o preenchimento dos campos de informação de valor comercial e a disponibilização ou não do endereço de *e-mail*. As conclusões principais estão sumarizadas a seguir.

Em todas as redes estudadas os indivíduos com mais amigos disponibilizaram mais informações (considerando tanto o número total de campos preenchidos no perfil quanto os referentes a informações de valor comercial). A única exceção a este comportamento foi observada na rede da *Universidad Católica Argentina* (UCA), na qual a correlação encontrada não foi estatisticamente significativa para o binário ‘mais amigos - mais informações

publicadas'. No caso da disponibilização do endereço de *e-mail*, encontramos que para as quatro redes latinas universitárias estudadas, quanto menor o número de amigos, maior a predisposição para publicar o endereço de *e-mail*. Diferentemente, a correlação observada para as seis redes geográficas estudadas, latinas e canadenses, foi positiva, ou seja, quanto mais amigos, maior a publicação desta informação. A exceção encontrada foi a rede UBC, na qual a inexistência de correlação se deve ao fato de ser uma rede que requer o *e-mail* no ato do cadastro como condição para a participação.

De maneira semelhante, encontramos que os indivíduos que publicam mais fotos tendem a publicar, igualmente, mais informações em seus perfis, inclusive as de valor comercial. Três exceções a este comportamento foram observadas. Na rede da *Universidad Católica Argentina* (UCA) não podemos afirmar a existência de correlação do número de fotos com nenhuma das duas variáveis analisadas e para a rede geográfica Colômbia não houve correlação entre o número de fotos publicadas e a predisposição para a revelação de informações de valor comercial. O endereço de *e-mail* também foi disponibilizado com mais frequência por aqueles que postavam mais fotos em seus perfis para todas as redes geográficas estudadas. Diferentemente, nas redes universitárias latinas, este comportamento se inverteu: os indivíduos que postavam menos fotos foram os mais predispostos a publicar endereço de *e-mail*. Desta vez, a rede UBC acompanhou a tendência das redes geográficas e apresentou uma correlação positiva com a disponibilização do endereço de *e-mail*.

Correlação menos acentuada foi observada entre a idade dos usuários do *Facebook* e sua predisposição em revelar informações. Para 7 das 11 redes avaliadas, indivíduos mais novos tenderam a publicar mais informações em seus perfis. Para as informações de valor comercial, esta correlação foi observada em apenas 5 das 11 redes estudadas. Cabe destacar que nas redes canadenses a ocorrência desta correlação foi ainda mais rara, o que se deve ao fato das faixas de idade de nossa amostra serem muito próximas neste país, como já relatamos anteriormente. Para a tendência em publicar o endereço de *e-mail*, em 6 das 11 redes avaliadas os indivíduos mais novos revelaram esta informação com mais frequência. Por fim, o estudo das relações entre o gênero dos participantes e seu comportamento nos permitiu identificar que, no contexto canadense, para as três redes estudadas no país, os homens disponibilizam mais informações do que as mulheres. A exceção foi a disponibilização do endereço de *e-mail* da rede UBC, justificada novamente pelo fato da rede exigir um *e-mail* institucional para participação. Diferentemente, no contexto latino, a tendência predominante foi a inexistência de diferença na predisposição em revelar quaisquer informações entre homens e mulheres (este comportamento foi observado em todas as redes da Argentina,

México e Chile).

4.3 Controle e vigilância: hierarquias em xeque?

Apresentados os resultados de nossa pesquisa empírica acerca do comportamento e do grau de consciência dos usuários acerca dos processos de manejo e uso das informações que eles publicam no *Facebook*, retomemos nossas questões fundamentais. O termo vigilância pode ser usado para nos referirmos aos processos que se passam nas redes sociais, especialmente no *Facebook*? Em caso afirmativo, quais dos processos aqui explicitados podem ser assim referenciados? E, sobretudo, quais as características destes processos; *i.e.*, que tipo de vigilância é subsidiada pelo uso dos *sites* de rede social? Lyon (2007: 35) se questiona sobre o porquê da proliferação das tecnologias vigilantes em um mundo no qual as pessoas se dizem cada vez mais preocupadas com sua privacidade. Mesmo diante das evidências recorrentes de que tais dispositivos não são capazes de garantir a segurança das populações e afastar as ameaças do terrorismo e do crime, eles continuam a proliferar. Em nosso caso, diferentemente, estão em foco os benefícios da sociabilidade em rede e não os da segurança, o que naturalmente afasta, à primeira vista, o uso do dispositivo da percepção comum que conservamos a respeito do tema vigilância. Desta forma, nos perguntamos: Há uma avaliação equivocada do funcionamento e das consequências dos processos que ocorrem nas redes sociais por parte dos indivíduos que as usam? Suas atitudes mudariam caso eles soubessem como exatamente são usados os dados que publicam voluntariamente nestes ambientes? Desta forma, a exemplo de Lyon (2007: 35), nos perguntamos sobre o que faz funcionar a vigilância hoje, especialmente no caso das redes sociais.

Descrevemos, no primeiro capítulo, as características da vigilância disciplinar – própria às sociedades modernas – e as características da vigilância contemporânea que ocorre no ciberespaço. Abordemos agora as mutações sofridas por este fenômeno sob a ótica particular da noção de hierarquia. O modelo analisado por Foucault (1977) descrevia a modernidade como momento de passagem das sociedades de espetáculo às de vigilância, instaurando uma dissimetria do olhar que correspondia também a uma lógica de exercício do poder: um vigia, situado no centro da torre, observava todos os vigiados, detendo assim o poder de analisá-los e sancioná-los. Desta forma, Foucault (1977) associa esta particular hierarquia do visível à emergência de uma modalidade de controle social. Desaparece o suplício, entram em cena os minuciosos artifícios disciplinares. Mathiesen (1997, *apud* Lyon, 2007), por sua vez, nos fala sobre a emergência de uma nova hierarquia de visibilidade, por

ele referenciada como sinopticismo, segundo a qual muitos indivíduos se dedicam à observação de alguns poucos. Se o vigia da torre panóptica fosse visível, o ponto de vista do prisioneiro descreveria a forma sinóptica, presente também nos espetáculos de suplício, em que os populares saíam às ruas para observar o sofrimento de um único indivíduo: o condenado.

Esta inversão do modelo panóptico está presente, por exemplo, na cultura de massa e no fenômeno das celebridades. No lugar do poder que investia as populações desviantes, observando-as e visando corrigi-las, teríamos agora o foco de visibilidade voltado a uma elite seleta, não mais a dos reis, mas a dos astros do cinema e da TV, observados de perto pelas massas (BRUNO, 2004: 115). No entanto, como já explicitamos anteriormente, a sociedade contemporânea é marcada por uma nova inversão nas hierarquias da visibilidade, em suma, por um retorno do foco de atenção sobre o indivíduo comum. Agora, longe dos confinamentos disciplinares dentro dos quais o olhar implicava a normatização, eles são movidos pelo desejo de serem vistos, de se constituírem alvo da atenção alheia e se sentirem dignos de notoriedade. Assim, este percurso nos permite perceber a associação da noção de vigilância não apenas a uma dissemetria do olhar, mas a uma conjuntura hierárquica, segundo a qual, originalmente, *i.e.*, de acordo com o modelo panóptico próprio às sociedades disciplinares, aquele que vê exerce poder sobre aqueles que são alvo deste olhar. Neste sentido, como podemos perceber, as inversões próprias aos diferentes momentos que localizamos acima apontam para uma transformação através da qual aqueles que olham não mais exercem sobre aqueles que são vistos um poder que vise a correção ou que implique a sanção. Ainda que o *pop-star* dependa da aprovação constante de seu público e que esta necessidade constitua uma forma de poder; ainda que o indivíduo comum que se exhibe em uma rede social busque a aprovação de seus pares, a hierarquia disciplinar não mais descreve as relações de poder implícitas às dinâmicas do ver e ser visto.

Neste sentido, Albrechtslund (2008) argumenta que a passividade própria aos sujeitos submetidos ao controle disciplinar não se aplica ao fenômeno das redes sociais. E naturalmente, se aqui o olhar do outro é desejado é porque ele não se associa mais à interdição da norma. Assim, o autor sugere uma expansão do campo dos estudos da vigilância para abordar sua ocorrência enquanto uma prática mútua e horizontal. Para ele, ainda que a etimologia da palavra vigilância descreva a atividade de ‘ver sobre’, este fenômeno pode estar associado a relações que se passam em um mesmo nível ou até mesmo àquelas que se dão em favor da pessoa vigiada, seja pela resistência ao olhar vigilante ou através do empoderamento implícito às práticas exibicionistas (ALBRECHTSLUND, 2008). Neste sentido, o autor

propõe o conceito de vigilância participativa para abordar o fenômeno das redes sociais. Enfatizando a noção de compartilhamento da informação no lugar de uma simples troca e defendendo que as práticas de uso destes *sites* implicam o acesso a benefícios imediatos e atuam nas dinâmicas da construção da subjetividade, ele resgata a pró-atividade e a motivação voluntária inerentes à noção de participação para argumentar que, nestes *sites*, a passividade inerente à normatização disciplinar seria substituída pelas tarefas ativas de exibir-se, comunicar-se e buscar informações, o que associa a vigilância a uma perspectiva claramente social (ALBRECHTSLUND, 2008).

Por outro lado, Mark Andrejevic (2008: 212) usa o conceito de vigilância lateral ou *peer-to-peer* para se referir às formas através das quais os indivíduos se engajam no trabalho de monitorar uns aos outros *online*. Apresentando uma condição em que a proliferação das tecnologias vigilantes as tornam acessíveis não apenas às corporações e aos governos, ele descreve o uso destas ferramentas por indivíduos comuns, interessados em monitorar amigos, conhecidos e pessoas próximas. Em primeiro lugar, o autor argumenta que as promessas inclusivas da participação e da interatividade vêm sendo cada vez mais acompanhadas de perto por formas assimétricas de vigilância, colocadas a serviço das grandes corporações e do estado. Em seguida, ele sugere que estas formas de vigilância estão sendo importadas para o contexto das relações interpessoais, subsidiando modalidades de verificação que endereçariam inclusive os riscos criados por estas mesmas tecnologias, como o de mentir sobre a própria identidade em ambientes *online* ou a dúvida acerca do que nossos entes próximos fazem enquanto estão na Internet. Assim, Andrejevic (2008: 213, tradução nossa) se refere a esta vigilância como a atividade através da qual os indivíduos “[...] imitam e amplificam formas *top-down* de vigilância comercial e política”.¹⁷⁵ Associando-a a um contexto de desconfiança e insegurança em relação ao outro, ele afirma que esta modalidade de observação é usada pelos indivíduos para “[...] auto-gerenciamento em nome da eficiência e da segurança” (ANDREJEVIC, 2008: 214, tradução nossa).¹⁷⁶

Outra noção que consideramos importante para a compreensão da vigilância que se passa nos *sites* de rede social é de controle institucional, proposta por Lianos (2003). Para o autor, as instituições são instâncias que se colocam como mediadoras das atividades humanas (LIANOS, 2003: 3). E é através deste processo de interação com campos de atividades institucionais que se exerce predominantemente a regulação do comportamento nas sociedades capitalistas contemporâneas. Assim, o autor diferencia o controle institucional,

¹⁷⁵ Tradução nossa para: “[...] mimics and amplifies top-down forms of commercial and political surveillance”.

¹⁷⁶ Tradução nossa para: “[...] self-management in the name of efficiency and security”.

derivado do gerenciamento planejado e consciente do comportamento humano efetuado pelas instituições e o controle derivado das redes de relações entre indivíduos ou grupos (LIANOS, 2003: 415). Enquanto o último é espontâneo, inerente ao ato social, o primeiro é parte essencial de atividades que não estão relacionadas exclusivamente ou prioritariamente ao desempenho do controle: no exercício de seus atos cotidianos, sujeitos soberanos vinculam-se a diversas instituições com objetivos variados, visando realizar seus desejos ou concretizar seus planos de vida. A função primeira destas instituições é prover esses serviços: elas não são criadas como máquinas de controle, mas exercem tal função através de suas práxis de interação, das formas de uso pré-determinadas que elas propõem aos indivíduos que as acessam e às quais eles devem estar de acordo se visam concretizar suas escolhas. Assim, trata-se de um controle que não é nem intersubjetivo, nem baseado em grupos. “Ao contrário, ele é por definição impessoal em sua origem e atomizado em sua recepção, porque ele é concebido e aplicado por uma instituição enquanto parte da distribuição homogênea de uma certa atividade” (LIANOS, 2003: 416, tradução nossa).¹⁷⁷

Este controle institucional é freqüentemente percebido como benéfico e algumas vezes até libertador tanto quanto constrangedor; ele estabelece um conjunto de condições pré-existent e é freqüentemente parte de um serviço que é oferecido ao público de maneira completa em sua habilidade enquanto ‘usuários’ (LIANOS, 2003: 415, tradução nossa).¹⁷⁸

Resgatadas estas contribuições, sintetizemos, então, a partir de nossas análises prévias, as audiências interessadas em se empenhar em atividades vigilantes através do *Facebook* que identificamos ao longo deste trabalho: a) as audiências institucionais; b) as audiências interessadas; c) as audiências desejadas e d) as audiências inesperadas. Para cada um desses grupos, o ato de vigiar assume contornos particulares. As *audiências desejadas* são basicamente os amigos e conhecidos de um indivíduo, que acessam seu perfil para saber novidades, verificar fatos e saber mais sobre sua vida. Esta modalidade de ver é, em muitos casos, uma forma de amizade, um meio de manter contato com aqueles que não vemos há muito tempo ou dos quais estamos distantes geograficamente. Além disso, consideramos nesta categoria os fenômenos associados à curiosidade em relação ao outro: muitas vezes, usamos os *sites* de rede social para saber mais sobre alguém em que estamos interessados ou

¹⁷⁷ Tradução nossa para: “On the contrary, it is by definition *impersonal* in its origin and *atomised* in its reception, because it is conceived and applied by an institution as part of the homogeneous distribution of a certain activity”.

¹⁷⁸ Tradução nossa para: “This institutional control is often perceived as *beneficial* and sometimes even *liberating* as much as constraining; it establishes a pre-existing set of conditions and is often part of a service offered to the public as a whole in their capacity as ‘users’ ”.

sobre alguém que acabamos de conhecer. Como relata Andrejevic (2008: 229-30), é prática comum buscar por amigos ou conhecidos, sem objetivo específico, só pra ver o que aparece. Muitas outras finalidades podem estar associadas a esta modalidade de vigilância, que identificamos aqui como predominantemente social: ver perfis é uma forma de se relacionar com outros, de se inserir melhor no mundo que nos cerca ou em um meio social novo. Ainda, é importante considerar que ver as trajetórias de vida dos outros é um exercício de alteridade, uma forma de pensar sobre si e sobre as próprias escolhas. Desta forma, esta modalidade de vigilância está associada a práticas de construção da subjetividade e implicam benefícios àqueles que vêem. De maneira semelhante, aqueles que se exibem frequentemente visam esta audiência, para a qual moldam cuidadosamente seus perfis, realizando um trabalho de gerenciamento de sua própria imagem do qual também esperam obter algum tipo de benefício, como a aprovação de seus pares ou o aprimoramento de sua inserção social. Assim, aqui, ser visto implica ser cuidado, significa ter o privilégio de ser alvo da atenção alheia: receber um comentário ou um *feedback* daqueles que o visitaram virtualmente, querendo saber algo sobre você, é sempre uma demonstração de interesse, um sinal de que outros se importam com você de alguma forma. Por fim, consideremos que esta prática é, em geral, recíproca: amigos vêem perfil de amigos, conhecidos o fazem de maneira semelhante, desde que tecnicamente este acesso seja possível.

Já a categoria das *audiências inesperadas* diz respeito a um modo de ver cada vez mais comum nos *sites* de rede social: o direcionamento do foco de visibilidade dos usuários a indivíduos desconhecidos, com objetivos associados ao entretenimento. Denominamos estas audiências inesperadas por falta de um termo que defina melhor sua condição. Por um lado, os indivíduos sabem da possibilidade de que desconhecidos possam acessar nossos perfis com o objetivo de se entreter. Além disso, estas audiências são indesejadas para alguns, desejadas por outros. É possível também que os indivíduos simplesmente não se importem em ter seus perfis vistos por estranhos. Neste sentido, consideramos que os desconhecidos figuram como uma audiência inesperada não porque os usuários de redes sociais não conjecturem esta modalidade de acesso a seus perfis, mas sim porque tal público é frequentemente diverso daquele que os indivíduos visam prioritariamente quando constroem e gerenciam seus perfis. Neste contexto, a prática de ver perfis não está associada a propostas como o crime, a verificação de conformidade ou a coleta de informações em larga escala. A motivação que justifica esta prática é pessoal e está associada à diversão proporcionada pela leitura de perfis, ao prazer de clicar e visualizar aleatoriamente diferentes rostos e momentos, vendo pessoas reais, conhecendo suas atividades, atitudes, preferências, relações, sentimentos e

pensamentos. Há sempre a estranha sensação de se estar tão próximo a alguém que nos é tão distante, tão pouco familiar. Por outro lado, o indivíduo que é visto é tão ordinário quanto aquele que vê, o que pode sugerir um fluxo horizontal de produção de alteridade. Assim, se lançar aos nós da rede nesta busca aleatória por parcelas de vida interessantes constitui uma modalidade de olhar que é, de maneira geral, assimétrica e anônima: se o *site* utilizado não notifica o indivíduo sobre o acesso de outros usuários ao seu perfil, tal prática se torna inclusive transparente.

Se para as duas práticas que descrevemos acima o ato de olhar é movido por um prazer descompromissado, as modalidades de ver associadas aos dois grupos restantes implicam um observar objetivo e organizado. As *audiências interessadas* são as pessoas conhecidas que estão na condição de exercer algum poder de autoridade sobre os indivíduos cujos perfis elas acessam ou aquelas desconhecidas que visam obter alguma informação sobre alguém por interesse próprio. De maneira geral, estas audiências são indesejadas: pais, namorados, professores, familiares, colegas de trabalho, pessoas que os indivíduos não gostariam que vissem alguma informação que ele disponibiliza, relacionada a algum desvio de conduta capaz de gerar repreensões ou sanções. Também é possível que sejam pessoas menos próximas ao indivíduo buscado: aquelas com as quais interagimos apenas *online* e que buscaram por nossos perfis para verificar nossa identidade; pessoas que conhecemos pouco, com as quais estabelecemos pontualmente algum tipo de relação pessoal ou profissional etc. De maneira geral, a finalidade desta forma de busca é predominantemente social (verificar obediência, traição, descobrir se seu colega de trabalho ou namorado mentiu para você, se o candidato com o qual você disputa uma vaga é um forte concorrente etc.): motivações antigas endereçadas de uma forma nova, possibilitada pelas tecnologias digitais. Assim, o mais importante acerca destas audiências é que, para elas, esta modalidade de olhar é uma forma de calcular riscos: responsáveis por sua própria segurança, por sua própria felicidade e sucesso, elas se engajam no trabalho de gerenciar de maneira eficiente sua vida social, alimentando impulsos cada vez mais preditivos, avaliando o futuro para informar suas decisões presentes. Desta forma, esta prática está associada a uma atmosfera marcada pela falta de confiança no outro e pelo uso da verificação no lugar do diálogo (ANDREJEVIC, 2008). Por fim, consideremos que a hierarquia de visibilidade descrita por esta prática é predominantemente assimétrica: o indivíduo buscado não sabe efetivamente quem visitou seu perfil, ainda que a ele esteja facultada a possibilidade de fazer o mesmo.

Já as *audiências institucionais* são os públicos que recorrem aos dados disponíveis nos perfis de usuários de *sites* de rede social visando atender a interesses organizados, que podem

ser os de uma empresa, instituição de ensino, do Estado, de uma grande corporação etc. Incluímos aqui, naturalmente, para o caso do *Facebook*, a própria empresa que fornece o serviço e mantém o funcionamento do *site*. De maneira geral, podemos relacionar neste grupo a polícia, empregadores, escritórios de admissão de universidades, empresas que prestam serviços de busca de pessoas, que vendem bases de dados com perfis para anunciantes etc. Em suma, trata-se de audiências em condição de transformar o acesso individual a perfis para atender a seus interesses em uma prática embutida em processos institucionais organizados ou realizada em larga escala, assistida por métodos computacionais avançados, próprios à vigilância digital.¹⁷⁹ Empregadores ou escritórios de admissão podem criar suas políticas de acesso e uso das informações disponíveis em perfis de seus candidatos, visando gerenciar riscos futuros e realizar as melhores escolhas. O procedimento implícito é o mesmo da perfilação, sendo que aqui o argumento usado para criar o algoritmo que classificará os indivíduos ainda é aplicado manualmente e descrito por regras de conduta mais ou menos formalizadas, o que não impede, naturalmente, que esta prática tenha efeitos sobre as oportunidades disponíveis àqueles que são triados por estes critérios, que subsidiam, em suma, o arranjo do momento presente com base em conjecturas possíveis.

Dentre as possíveis formas de exercício desta modalidade de olhar, cabe destacar os casos em que esta prática se torna tecnicamente organizada, marcadamente aqueles em que a própria empresa que hospeda esses dados ou outras que a eles tenham acesso os utilizem para construir bases de dados poderosas, a partir das quais é possível perfilar os indivíduos segundo variados campos de interesses. Assim, se em todas as demais categorias os indivíduos analisados eram identificados, ou seja, os dados que se visava obter através dos *sites* de rede social visavam pessoas específicas, aqui nem sempre há esta necessidade. Parcelas anônimas de informação disponibilizadas e transações impessoais realizadas serão usadas no processo performativo de retornar recomendações de serviços e produtos. Baseando-se em conjecturas possíveis, estas sugestões constroem campos de atualidade. Afinal, adequada ou inadequada, toda recomendação pode suscitar um interesse imediato: a partir do momento em que vemos um anúncio, a despeito de possuímos ou não algum interesse prévio no produto ou serviço veiculado, estamos sujeitos a nos interessarmos e realizarmos uma compra. Assim, o perfil não é nem falso nem verdadeiro, é efetivo, é da ordem da simulação, e pode produzir um achatamento temporal em que os regimes do provável sufocam as possibilidades presentes, abrindo espaço para mecanismos de orientação

¹⁷⁹ As características da vigilância digital são descritas e analisadas no primeiro capítulo deste trabalho. Cf. p. 32.

da conduta. Por outro lado, um sistema desta natureza produz um regime eficiente, desejado pelas empresas – que maximizam seus investimentos em publicidade direcionando seus esforços de modo a aumentar a possibilidade de que o anúncio leve à compra – e pelos consumidores, que se vêem livres da presença, por vezes incômoda, de anúncios que não se relacionam com seus interesses e que passam a poder contar agora com a ajuda de uma instância inteligente que os ajudam a encontrar as coisas que eles desejam, muitas vezes a preços e condições mais interessantes. Desta forma, estas práticas se associam, em grande medida, à noção de controle institucional tal como proposta por Lianos (2003), visto que os objetivos primordiais que justificam tanto a existência dos *sites* de rede social quanto dos sistemas de recomendação não estão associados inicialmente e diretamente ao controle, o que não significa que tais efeitos não possam aí emergir.

O esforço de enumerar algumas das audiências possíveis em um *site* de rede social, tal como fizemos acima, não visa sistematizar ou categorizar exaustivamente todos os canais de visibilidade e vigilância que emergem nestes ambientes. Ao contrário, esta iniciativa serve aqui para ilustrar o quanto estas práticas estão inter-relacionadas: vemos e somos vistos ao mesmo tempo por públicos diversos, com finalidades diversas, todas elas implícitas a um mesmo *modus operandi*, a uma mesma práxis de uso, a um mesmo ambiente, em toda a sua pluralidade: o das redes sociais. Além disso, todas estas práticas se passam sobre a égide de um único sistema, gerenciado por uma única empresa, com suas políticas e diretrizes próprias. Assim, a esfera social não se desvincula da institucional, apenas pra indicar a clivagem que mais imediatamente se pode depreender da descrição efetuada acima. Acrescentamos, inclusive, que este conflito é frequentemente visível e talvez de maneira ainda mais sensível no *Facebook*, dados os inúmeros esforços da companhia no sentido de promover a monetização de seus serviços. Basta considerar, por exemplo, ferramentas como o *News-Feed*, o *Mini-Feed* e sua relação com o *Beacon* e o *Social Ads*. Concebidas para monitorar o círculo social dos usuários do *site*, elas foram facilmente associadas a um contexto publicitário, a partir da produção de notificações sobre as ações dos indivíduos no *Facebook* ou em *sites* parceiros. Esta relação fica ainda mais problemática quando nos lembramos das informações enviadas por *sites* externos ao *Facebook* através do *Beacon*, fato que prolonga as discussões sobre trânsito e uso dos dados individuais para além do que é meramente publicado. Assim, as mesmas ferramentas de *feeds* que um dia foram temidas pelos usuários por motivos eminentemente sociais adquiriram utilidade com o passar do tempo e ganharam a adesão dos membros do *site*. Simultaneamente, elas adquiriram para a empresa a função de gerar renda a partir de novos serviços oferecidos aos seus anunciantes, e basearam um

mecanismo social de visibilidade que visava, ao mesmo tempo, inserir produtos como recomendações seguras de amigos e subsidiar a coleta expandida de dados do *Facebook* sobre as ações de seus usuários em *sites* parceiros, aumentando o poder e o valor de suas bases de dados. Assim, os objetivos dos anunciantes de vender seus produtos e os dos usuários de redes sociais de potencializar suas conexões sociais acabam associados a rotinas vigilantes no *site*.

Como abordar então a vigilância que ocorre nos *sites* de rede social, diante de tantas ambigüidades? No início do primeiro capítulo circunscrevemos o fenômeno da vigilância associado ao controle, como o monitoramento de indivíduos e populações para propostas específicas (LYON e ZUREIK, 1996: 3). Posteriormente, no início deste capítulo, consideramos as proposições de Albrechtslund (2008) e Andrejevic (2008), acerca da vigilância participativa e da vigilância lateral. Albrechtslund (2008) fala em uma expansão do campo de estudos da vigilância. No entanto, se considerarmos as proposições de Lianos (2003), continuaremos a entender a vigilância como um fenômeno associado ao controle, ou nos termos do autor, ao controle institucional, modalidade diferente daquela própria às sociedades disciplinares. O controle institucional se dá através de dispositivos polivalentes, como se passa no caso das redes sociais. Podemos dizer que elas se referem à potencialização da sociabilidade humana e que implicam práticas de compartilhamento, participação e construção da subjetividade (vigilância participativa); que elas podem servir àqueles que estão em condições de exercer algum poder sobre o indivíduo que disponibiliza seus dados, como no caso dos pais, autoridades, professores (vigilância lateral/repressiva); que elas podem subsidiar a punição dos indivíduos que desrespeitam a lei, servindo a policiais ou escritórios encarregados da segurança em universidades (vigilância punitiva/detectiva); que elas podem subsidiar práticas organizadas em empresas e universidades interessadas em consultar tais dados para julgar candidatos em seus processos de admissão, (vigilância institucional/preditiva); que elas permitem à empresa que presta o serviço coletar dados de seus usuários e oferecer perfis de interesse a seus anunciantes etc. e até mesmo que elas nos oferecem o benefício imediato de receber recomendações de produtos sobre coisas nas quais estamos interessados.

Desta maneira, a exemplo do que propõe Lianos (2003: 415), não nos cabe tentar diferenciar em que medida estas redes se associam a efeitos de controle e em que medida o controle pode estar ausente de determinadas modalidades de uso a elas implícitas. Pois tais efeitos vêm embutidos nas práxis institucionais do *site*, às quais temos que nos submeter para ter acesso às delícias da interatividade e aos benefícios da participação e da ação coletiva. E

justamente por estes benefícios, deixar de participar não é uma alternativa válida – ainda que tecnicamente possível. No entanto, é importante ressaltar que nossa relação com estas instituições se torna cada vez mais desindividualizada: somos abordados tecnicamente enquanto interatores, em um processo através do qual a responsabilidade implícita a nossos atos fica dividida entre indivíduos ou grupos (LIANOS, 2003: 424). Assim, a resistência se dessocializa e o espaço de negociação outrora existente entre os indivíduos e as instituições se dissolve neste limbo atomizante: “[...] entre a instituição e o usuário, não existe nenhuma interação, exceto pelo monitoramento gerencial e o ciclo de *feedback*” (LIANOS, 2003: 416, tradução nossa).¹⁸⁰ Neste ponto, no entanto, uma ressalva se faz importante: sendo uma ferramenta de promoção da sociabilidade, o *Facebook* não pode impedir que seus usuários utilizem o *site* como ferramenta de protesto contra a própria empresa, como relatamos em casos anteriores. Abordar a extensão e a efetividade destes protestos, observados no caso do *Beacon*, por exemplo, pode trazer apontamentos interessantes para as possibilidades de resistência ao contexto aqui delineado.

De qualquer forma, um argumento central nas proposições de Lianos (2003) é o de que a redução deste espaço de negociação entre os indivíduos e as instituições estaria relacionada a um interesse cada vez menor destas instâncias em agirem de maneira a conquistar a confiança de seus usuários. Afinal, ainda que poucos resolvam se posicionar e deixar o serviço, ainda que em muitos casos seja necessário dialogar sobre os posicionamentos da empresa, a lógica é a de que o funcionamento uniforme e orgânico do *site*, que se apresenta da mesma maneira para todos os seus usuários, cuide de impor e efetivar os objetivos da empresa com o mínimo de rejeição e o máximo de eficiência. E no âmbito da interação com estas práxis institucionais, basta o consenso: neste novo contexto, a atividade de internalizar um valor enquanto premissa e estratégia necessária ao exercício do controle, tal como se dava no modelo disciplinar, é substituída pela assimilação empírica do campo normativo implícito e decorrente das práticas cotidianas e práxis procedimentais que comandam nossos processos de interação com as instituições das quais dependemos para o acesso a benefícios imediatos buscados para atender a nossos desejos e escolhas. Assim, somos indivíduos soberanos, optando, escolhendo. Naturalmente, tal fato nos faz lembrar Foucault (1977), e sua argumentação de que os mecanismos de atuação do poder não devem ser concebidos apenas em termos repressivos ou coercitivos. Afinal, não se trata aqui de dominação totalitária ou sujeição absoluta, mas de ações que desejamos tomar em campos

¹⁸⁰ Tradução nossa para: “Between the institution and the user, there exists no interaction, except for a managerial monitoring and feedback cycle”.

institucionais cuja função primeira não é a do controle.

Em primeira instância, isso confirma o truísmo de que toda organização envolve controle. Mas ao mesmo tempo, é importante para tornar claro que na condição pós-industrial *isso não significa que a organização é baseada no controle* [que ela deva ser usada para suportar o posterior exercício do controle] (LIANOS, 2003: 416, grifo do autor, tradução nossa).¹⁸¹

4.4 O argumento panóptico, a normatividade e a participação

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 foucaultiana. 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* planejados 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

¹⁸¹ Tradução nossa para: “In the first instance, this confirms the forgotten truism that all organisation involves control. But at the same time, it is important to clarify that in the postindustrial condition *this does not mean that organisation is built on control*”.

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 à emergência de canais de visibilidade através dos quais alguns poucos observam muitos, 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 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 naturalização progressiva da exposição de si 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 frequentemente 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. Como comprovado pela nossa pesquisa, as pessoas possuem restrições que agenciam prioritariamente através da autocensura das informações que publicam ou do uso de configurações de privacidade. 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. Dessa forma, é interessante retomar a noção de escopofilia, que segundo Christian Metz (1982, *apud*. Lyon, 2007) se refere a um desejo de olhar que diminuiria a liberdade daqueles que dele são alvo de se furtar a esta visibilidade, visto que

nem sempre há consentimento sobre o ser visto.

Desta forma, assim como o panóptico é uma arquitetura que visa permitir ver tudo, no *Facebook*, o senso de proximidade estabelecido pelas redes 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 com 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 quanto à presença do vigilante. Assim como não é possível 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 esta modalidade de acesso. Assim, sabemos que outros olhares e audiências são possíveis, ainda que estas presenças nos sejam atualmente indecíveis. 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 na renúncia a todos os benefícios implícitos ao seu uso. Como resgatamos ao longo desse trabalho, nos casos em que 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. Em primeiro lugar, podemos considerar que o vigiar constante, intimamente relacionado ao medo da sanção passa a se associar, aqui, a um desejo por ver e ser visto, que vigora em uma tensão permanente com a vontade de se furtar aos olhares indesejados. Além

disso, aqui, ao invés de incidir sobre os desviantes, a vigilância se endereça aos circuitos da sociabilidade e da inclusão: ela não visa normatizar as subjetividades perigosas, mas incide sobre indivíduos soberanos, em pleno exercício de suas escolhas e desejos. Trata-se de uma vigilância cujas modalidades plurais de exercício do olhar se dirigem ora a indivíduos específicos, ora a indivíduos anônimos, ora a transações e comunicações impessoais, visando extrair de massas amorfas de dados conjunturas grupais organizadas. Por fim, enquanto temer o olhar vigilante (ou o campo de sanções e punições a ele implícito) estava na base das estratégias de normalização que caracterizavam o modelo disciplinar, diferentemente, hoje, a vigilância não está baseada prioritariamente na premissa da interiorização de valores ou normas. Lianos (2003: 424) propõe que a recepção desta racionalidade implícita aos sistemas sócio-técnicos com os quais interagimos para acessar os serviços que desejamos exerce o efeito de controlar sem realizar esforços no sentido de estruturar as premissas do comportamento dos usuários. Assim, o que se objetiva – frequentemente através do emprego de dispositivos tecnológicos – é promover e garantir o comportamento eficiente, *i.e.*, aquele em acordo com os objetivos institucionais.

Simplemente não faz parte do gerenciamento do ambiente controlado projetar valores em direção àqueles que o usam. A justificativa para o requisitado degrau de conformidade é exclusivamente limitada a operação em acordo com os parâmetros pré-determinados do canal formal de interação que a instituição projeta e monitora [...]. Perspectivas deontológicas e baseadas em valores não são parte de tais contextos de interação (LIANOS, 2003: 423, tradução nossa).¹⁸²

Para o caso do *Facebook*, podemos considerar que a estrutura do *site* e os padrões de uso pré-programados aos quais recorrem os usuários quando usam o serviço seriam canais mediadores do controle institucional. Novamente, consideremos ferramentas como o *News-Feed*, o *Mini-Feed* e o *Beacon*. O funcionamento destes dispositivos funda um campo de interação fechado, com premissas consolidadas: realize a ação “X” em um *site* parceiro e ela será notificada da maneira “Y” nos *feeds* do *Facebook*. No caso do *Beacon*, este padrão de interação inclui, como mostramos anteriormente, o envio de informações sobre o comportamento *online* de um indivíduo em um *site* parceiro a despeito de sua escolha acerca de publicar ou não um histórico desta ação em seu perfil. Estas informações serão usadas para direcionar anúncios de serviços e produtos aos usuários do *site*, exercendo efeitos

¹⁸² Tradução nossa para: “It is simply not part of managing the controlled environment to project values towards those who use it. The justification for the requested degree of conformity is exclusively limited to operating in accordance with the predetermined parameters of the formal channel of interaction that the institution designs and monitors [...]. Deontological and value-based perspectives are not part of such contexts of interaction.”

performativos sobre seu comportamento presente, sem recorrer, de antemão, ou sem buscar internalizar um campo de valores acerca das recomendações enviadas ou do ato de consumir. Como já argumentamos aqui, em um futuro próximo, estes métodos de classificação dos consumidores podem resultar em segmentações detalhadas que pré-estabeleçam as ofertas e condições de compra disponíveis a cada indivíduo. Novamente, os benefícios da personalização aparecem associados às dinâmicas da diferenciação. E assim nos inserimos progressivamente em redes de ambigüidades cada vez mais complexas. Explícitas ou sutis, elas integram de maneira cada vez mais orgânica nossa interação com os dispositivos institucionais.

Por fim, enderecemos a polêmica e necessária premissa da participação. Não há novidade em afirmar que esta atividade caracteriza grande parte de nossas atividades no ciberespaço. O termo pode ser usado para descrever o que fazemos, a todo momento, enquanto interagimos nas redes sociais. No entanto, não acreditamos que ele seja suficiente ou adequado para descrever a vigilância que acontece nestes *sites*. Em primeiro lugar, porque não se pode consentir a assertiva de que a participação seja, por si só, uma atividade que implique dinâmicas produtivas de produção de subjetividade – necessariamente associadas ao empoderamento dos indivíduos. E em segundo lugar, porque não se pode admitir que a participação implique, inexoravelmente, a dissolução de quaisquer hierarquias de poder. Retomemos o argumento apresentado por Albrechtslund (2008), de que o mecanismo disciplinar está associado à passividade enquanto a participação exige o engajamento voluntário. Tal afirmação só seria possível se desconsiderarmos a pró-atividade necessária à tarefa de internalizar um valor, basilar para o funcionamento dos mecanismos de normatização disciplinares. Além disso, considerar que a passividade é necessária ao exercício do poder disciplinar está a um passo de tomar o poder enquanto algo que subjuga e domina, e não enquanto algo que ativamente produz realidades. Neste sentido, é interessante nos lembrarmos da argumentação de Foucault (1977) sobre a lógica do exame, segundo a qual os indivíduos não eram apenas vistos, mas se mostravam ao olho do poder. O panóptico não pode ser tomado como um simples modelo para o vigiar não consentido e unilateral, pois dinâmicas mais complexas estão implícitas ao seu funcionamento.

Assim, para abordar a vigilância que ocorre nos *sites* de rede social, consideramos ser necessário, em primeiro lugar, circunscrever sua especificidade. Para tal, separemos inicialmente características que, a nosso ver, se devem ao fato de estarmos estudando um fenômeno em rede. Afinal, se estamos falando de modalidades de olhar cuja topologia é reversível e cujo exercício é dinâmico, conectivo e distribuído, tais características são

prioritariamente derivadas do fato de que estamos abordando uma estrutura formada por nós relacionados através de *links*. Por isso, é natural que, nas redes sociais, polaridades emergentes possam descrever, a cada momento, novos canais de visibilidade. Assim, podemos descrever estes *sites* como espaços em que o binômio ‘exposição de si - audiências desejadas’ é permanentemente reconfigurado. Se expor, no contexto destes *sites*, é também se expor ao inesperado, se mostrar ao desconhecido. Isto porque, pela estrutura de conectividade generalizada da rede, os *links* virtualmente existentes podem se oferecer constantemente a novos processos de atualização, de acordo com interesses diversos, descrevendo estruturas de exercício do olhar simétricas ou assimétricas, planificadas ou hierárquicas.

Assim, consideramos que a vigilância que ocorre nos *sites* de rede social é menos uma vigilância participativa e mais uma vigilância integralizada, organicamente adaptada aos mecanismos da participação. Ela não se infiltra como um mecanismo dominador ou controlador que visa usurpar, de um ponto exterior, as potencialidades destas redes. Ao contrário, ela está integrada quase que harmonicamente aos mecanismos responsáveis por estas mesmas potencialidades. As funcionalidades vigilantes destas redes são, na verdade, os mesmos mecanismos inerentes ao seu modo operativo usual, e foram criados enquanto ferramentas de conectividade social, enquanto linguagens de dados eficientes e flexíveis, enquanto estruturais cuja finalidade primeira é a de permitir novas formas de se relacionar *online*. Na prática, elas permitem a associação do entretenimento, dos prazeres exibicionistas e “voyerísticos” e mesmo das práticas de empoderamento dos indivíduos e de construção da subjetividade a formas assimétricas e/ou hierárquicas de olhar. Em suma, elas congregam, em um só dispositivo, diversas formas de olhar e vigiar. Desejos e objetivos diversos justificam ver o outro, ver desconhecidos, ver nossos desafetos e também observar grupos anônimos, suas comunicações e transações impessoalizadas. E assim, buscando os benefícios ativos da participação, vamos nos enredando nos circuitos movediços dessas redes que agenciam, a um só tempo, canais de visibilidade dinâmicos e diversos.

CONSIDERAÇÕES FINAIS

O novo sujeito é herdeiro em alguma medida do preconizado por Nietzsche, Foucault, Deleuze; mas de modo algum é o que se esperava gestar na luta contra a disciplina. Ele brotou do útero das lutas contra a disciplina, mas gira oscilante entre a participação na ação coletiva e a vigilância dos monitoramentos informáticos tal um peão desgovernado.
Henrique Antoun¹⁸³

O percurso apresentado no decorrer das páginas deste trabalho sintetizou nossos esforços no sentido de compreender em que medida os fenômenos referentes à publicação, trânsito e uso dos dados individuais disponibilizados através dos *sites* de rede social podem ser considerados sob a égide da vigilância. Simultaneamente, colocamos a noção de vigilância sob investigação, na tentativa de compreender como se articula este fenômeno na contemporaneidade. Visando obter resultados mais profícuos, circunscrevemos nosso objeto de estudo em dois níveis. Por um lado, nos dedicamos a estudar a rede social *Facebook*, de modo a abordarmos as dinâmicas específicas de uso do *site* as políticas da empresa que o mantém. Por outro, nos lançamos ao estudo do público latino-americano e visamos elucidar diferenças comparativas do comportamento referente à revelação de informações em relação ao público norte-americano, ou mais especificamente, canadense. Colocamos em jogo a percepção dos usuários do *site* acerca dos processos relativos a possíveis usos e possíveis audiências interessadas em seus dados pessoais. De maneira semelhante, avaliamos a adesão às configurações de privacidade disponíveis e as práticas de autocensura das informações publicadas, bem como os possíveis riscos associados pelos indivíduos ao uso do *site*.

Nosso esforço empírico não deve ser confundido com um desejo por generalizações conclusivas a qualquer custo. Ao contrário, ele foi movido pela comedida responsabilidade de efetivamente ir a campo e ouvir o que nossos respondentes teriam a dizer, ao invés de nos basearmos em relatos de terceiros ou em observações que excluíssem o contato com o público que constitui nosso objeto de estudo. Naturalmente, um questionário é, sem dúvidas, um meio de aproximação consideravelmente mais mecânico do que entrevistas realizadas face-a-face, complementadas por um estudo das comunidades nos espaços ‘concretos’ correspondentes às redes virtuais estudadas. No entanto, por limitações diversas, circunscrevemos da maneira aqui apresentada as dimensões deste projeto. Esperamos, todavia, que ele possa se colocar

¹⁸³ ANTOUN, Henrique. A web 2.0 e o futuro da sociedade cibercultural. In: XXXI Congresso Brasileiro de Ciências da Comunicação. Natal, RN. Set. 2008. **Anais eletrônicos**, p. 8.

como um estudo prévio que oriente esforços futuros e mobilize parcerias capazes de nos ajudar a driblar algumas de nossas principais dificuldades. Analisar novamente o contexto latino-americano usando redes de universidades que requerem o *e-mail* institucional para participação e conciliar tal estudo com visitas presenciais às comunidades estudadas, parece, a nosso ver, uma meta interessante a ser perseguida, pois poderíamos assim considerar as influências do contexto cultural no comportamento dos usuários do *site* e levantar mais informações acerca de suas posturas e atitudes do que nos permite um pequeno questionário aplicado de maneira impessoal através de um *site* na Internet. Objetivos futuros incluem aumentar o tamanho da amostra de respondentes e endereçar melhor a associação entre autocensura e uso de configurações de privacidade.

Através de nosso questionário, constatamos que os latinos, pelo menos no nível do discurso, se apresentam, em sua maioria, preocupados em relação a possíveis riscos associados ao uso do *Facebook*. No entanto, não encontramos, senão em casos isolados correspondência entre o tipo de preocupação reportado e a presença de comportamento correspondente que visasse proteger o usuário, resguardando suas informações através da autocensura ou do uso de configurações de privacidade. Concluímos que a autocensura endereça mais comumente audiências como os pais, namorados, professores, familiares e autoridades e até mesmo desconhecidos e futuros empregadores do que o *marketing*. Descobrimos que o uso de configurações de privacidade entre os latinos é expressivo. No entanto, de maneira semelhante, comportamentos como bloquear o *Beacon* e o *Social Ads* foram predominantemente incomuns. Também não encontramos relação entre o fato de um indivíduo se preocupar que outros vejam seus perfis e maior probabilidade de uso de configurações de privacidade. Avaliar com mais detalhes em que medida a preocupação destes usuários é suficiente para forçar uma mudança de comportamento se coloca como um campo profícuo para investigações futuras. Identificamos também que os usuários têm um conhecimento mediano das políticas da empresa e baixo em relação a temas relacionados, como portabilidade e busca de pessoas. De maneira geral, maiores graus de conhecimento não desencorajaram a publicação de informações e não estiveram relacionados a maiores taxas de uso do *site*.

Já os dados provenientes da coleta de perfis proporcionaram uma análise mais sólida e conclusiva. Descobrimos que os canadenses se comportam de maneira muito semelhante nos dois tipos de redes avaliadas, enquanto os latinos se expõem mais nas redes geográficas do que nas universitárias. Constatamos que, comparativamente, os canadenses publicam muito mais informações que os latinos, independente do tipo de rede considerada. Em contrapartida,

eles são os que mais usam configurações de privacidade para restringir aos outros indivíduos de uma mesma rede o acesso aos seus perfis. Identificamos também que a predisposição para este comportamento, entre os canadenses, independe do contexto e se dá em níveis semelhantes para redes geográficas e de instituições de ensino superior. Já entre todos os países latinos estudados, o uso de configurações de privacidade com este fim foi mais comum em redes geográficas. Em relação à predisposição para publicar informações, com exceção da Colômbia, os usuários latinos disponibilizaram mais dados em seus perfis nas redes geográficas do que os de redes universitárias. Somente a publicação do endereço de *e-mail* foi avessa a esta tendência. Observamos também que os usuários latinos e canadenses do *Facebook* disponibilizam, em média, menos informações de valor comercial em redes de universidades do que nas redes geográficas. Além disso, constatamos que os indivíduos com mais amigos e mais fotos tendem a publicar mais informações em seus perfis, inclusive as de valor comercial, na maior parte das redes estudadas. Para a variável idade correlações mais fracas foram observadas. Em relação ao gênero dos participantes, identificamos que, especialmente no contexto latino, homens e mulheres tendem a disponibilizar quantidades semelhantes de informação.

Assim, a partir das análises empírica e bibliográfica efetuadas, pudemos localizar diferentes tipos de audiências que ambicionam, com objetivos diversos, os dados individuais publicados no *Facebook*. Afinal, uma vez que interagimos em um ambiente no qual as comunicações, transações e atitudes não se dissociam do registro e no qual os dados que publicamos são efetivamente públicos, a questão nevrálgica se torna menos a possibilidade de acesso e mais a natureza das formas de acesso aos quais estes dados estão sujeitos. Além disso, mostramos como, no caso das redes sociais, os benefícios implícitos ao uso fomentam e possuem como premissa a predisposição em revelar informações. Por um lado, as pessoas desejam ser vistas e por isso exibem fatos sobre suas vidas e personalidades nestas vitrines contemporâneas. Por outro, a participação nessas redes pode nos ajudar na hora de arrumar um emprego, um novo namorado ou mesmo nos apoiar a gerenciar melhor nossa vida social. Assim, é natural que as informações publicadas devam ser verdadeiras, seja porque isso é uma premissa para a interação com os outros ou porque conhecidos as usarão para saber mais sobre nós. Desta forma, tanto o desejo de ser visto quanto o gerenciamento da imagem pessoal e o acesso aos benefícios diretos e indiretos que esta atitude pode trazer estão relacionados à participação dos indivíduos nos *sites* de rede social. Ainda que as motivações conscientes para o uso reportadas em nossa pesquisa sejam predominantemente pragmáticas, devemos considerar que outros motivos estão presentes, já que a importância destes *sites* advém, em

grande medida, do que eles nos permitem construir para além dos limites do espaço virtual em que interagimos.

Assim, as mesmas dinâmicas de exposição que nos abrem a possibilidades deliciosamente inesperadas nos aproximam dos olhares de audiências indesejadas, inesperadas e institucionais. Desta forma, um ambiente originalmente arquitetado para a interação social entre os indivíduos participantes deixa emergir novas polaridades, novas hierarquias do visível que constituem, também, novas hierarquias de poder: em suma, as redes sociais não surgiram como tecnologias vigilantes; ao contrário, a vigilância emergiu integrada aos corpos de informação disponibilizados como um efeito acessório ou colateral do uso e da estrutura deste *sites*. Queremos com isso indicar que não há sentido em separar, de maneira maniqueísta, efeitos maléficos e benéficos destas redes, associados ao controle ou ao empoderamento dos indivíduos. Afinal, a interação nestes *sites* contempla, de uma só vez, todos estes contextos, com suas diversas audiências e modalidades de olhar. Amigos, familiares, criminosos, empresas, conhecidos e desconhecidos participam com objetivos diversos, sempre segundo os protocolos que pré-determinam como se dá a interação nestes ambientes. Afinal, estes *sites* nos apresentam regras que só podemos consentir, pois neles, interagimos o tempo todo com práxis apriorísticas: ainda que possamos flexibilizar determinados padrões de funcionamento através do uso de configurações de privacidade, por exemplo, convivemos constantemente com a impossibilidade de alterar o que a nós não está disponível. Podemos definir as informações usadas para gerar históricos nos *feeds*, mas não podemos mudar o modo de funcionamento do dispositivo; podemos optar por não compartilhar históricos *Beacon* com nossos perfis, mas não podemos impedir que dados sobre nossas ações sejam coletados pelo *site*.

Este jogo entre o que se permite e o que não se permite é controlado pela empresa que oferece o serviço e determina seu modo de funcionamento. Como pudemos observar, enquanto os controles de configurações de privacidade são extremamente refinados no *Facebook*, eles não oferecem, por exemplo, opções que nos permitam delimitar o campo de visibilidade e as formas de usos da própria companhia acerca dos dados disponibilizados. Neste sentido, a restrição ao acesso de determinadas audiências funciona como um propulsor para a disponibilização de mais informações, que por sua vez, estarão amplamente disponíveis a uma audiência da qual não podemos nos furtar. Assim, os mesmos mecanismos construídos para promover e possibilitar as práticas de interação no *site* acabam por favorecer atividades vigilantes. Esta premissa é verdadeira também quando abordamos aspectos mais técnicos do funcionamento do sistema. Sabemos, por exemplo, que os dados publicados devem ser

armazenados de modo eficiente para permitir o bom funcionamento do *site*. Ao mesmo tempo, estas técnicas facilitam a implementação de outras, que subsidiam, por exemplo, a perfilação dos indivíduos para a construção dos sistemas de direcionamento de anúncios oferecidos pela empresa aos seus anunciantes. Assim, temos que não apenas os campos de visibilidade definidos pelas diversas audiências do *site* são dinâmicos e reversíveis como também o são as linguagens que o operam e o conferem existência. E esta rede de conexões instáveis oscila de acordo com as intempéries de interesses conflitantes, sejam eles os das diversas audiências, os dos usuários ou da empresa que oferece o serviço.

Naturalmente, não é possível usar *sites* de rede social sem se envolver nos circuitos de mediação institucional delineados pelas companhias responsáveis pela manutenção destes serviços. No entanto, outros usos dos dados individuais ali disponibilizados podem gerar novos acoplamentos e conexões entre esta forma de sociabilidade e contextos institucionais diversos, amplificando e dissolvendo os contornos do campo de possíveis associações entre os *sites* de rede social e a prática de atividades vigilantes. No que diz respeito ao *Facebook*, nosso foco nas práticas através das quais a empresa vem perseguindo ferozmente um modelo adequado para gerar lucros satisfatórios, condizentes com o amplo sucesso do empreendimento em diversos países e culturas ao redor do mundo, nos permitiu observar um percurso interessante. Sabemos que o *Facebook* surgiu como mais um dos empreendimentos livres da rede, baseado na lógica do faça você mesmo, gestado por indivíduos comuns de maneira independente. Mas seu astronômico crescimento originou rapidamente uma empresa organizada, com o objetivo de gerar renda e se manter, como qualquer outra, inclusive para sustentar o serviço oferecido gratuitamente aos seus usuários. Não faltam evidências de que este caminho será perseguido de maneira generalizada pela maior parte dos *sites* semelhantes na Internet. Assim, é importante afirmar que, enquanto a monetização das redes sociais for centrada no uso unilateral das bases de dados acumuladas a partir das informações pessoais cedidas voluntariamente pelos participantes, ele estará claramente e inevitavelmente associado a um contexto de vigilância institucional.

Por fim, ressaltemos que nosso objetivo não foi adotar aqui uma visão apocalíptica acerca das novas tecnologias, e muito menos nostálgica, atribuindo a este novo modo de interação um subtexto sombrio povoado por forças demoníacas e totalitárias. Continuamos acreditando que os *sites* de rede social são parte significativa das estratégias comunicativas contemporâneas, e que eles desempenham sim papéis importantes na vida de milhões de indivíduos ao redor do mundo. Não queremos aqui diminuir sua significância nem sugerir o fim da festa, a não participação, a recusa aos prazeres e benefícios que eles encerram. De

maneira semelhante, não queremos nos colocar a lamentar ingenuamente as perversidades de um mundo outrora perfeito ou amistoso. Muito menos retomar as premissas de que as redes, dentre elas a Internet e os *sites* de rede social, constituem em si, estruturas livres e libertárias, isentas de formas de controle e nas quais a participação implica, necessariamente, a realização de ideais democráticos e de empoderamento dos indivíduos. À maneira de Deleuze e Guatarri (1995: 32), escrevamos a *n-1* e subtraímos o *uno* da multiplicidade. Seria errôneo tomar essas redes como estruturas previamente orientadas a um ponto exterior, ao qual todas as ações se endereçariam. Cabe antes considerar que elas se constituem como redes de conexões heterogêneas e dinâmicas, que conectam pontos diversos, encadeando devires e fazendo circular intensidades. É como considerar a concepção nietzschiana segundo a qual a essência não é, senão, a força que mais afinidade guarda em relação a um determinado objeto. Assim, não se trata de ontologia, de determinar os fluxos de afetação que possibilitarão os efeitos emergentes observados. Justamente por isso, não podemos afirmar que as redes estejam imunes a novas formas de controle.

Talvez não exista lição maior sobre as redes do que a lição sobre o controle: redes, por sua mera existência, não são libertadoras; elas exercitam novas formas de controle que operam em um nível anônimo e não-humano, que dizer, material (GALLOWAY e THACKER, 2007: 5, tradução nossa).¹⁸⁴

Por fim, consideremos também que as formas de controle contemporâneas estão intimamente associadas aos circuitos do desejo, da realização e da participação. Por isso, não há sentido em dizer que os *sites* de rede social sejam máquinas totalitárias de controle. Diferentemente, os procuramos porque eles representam uma forma interessantíssima e conveniente de diversão e potencialização de nossas conexões sociais. No entanto, neles, à medida que somos abordados enquanto interatores e nos deparamos com os cerceamentos institucionais (LIANOS, 2003), acabamos por consentir as regras do jogo, justamente para que a festa possa continuar. Assim, sutilmente, agem os novos mecanismos de orientação da conduta, presentes também nestes *sites*, organicamente integrados às dinâmicas e benefícios da participação. Eles se baseiam no uso dos dados individuais neles disponibilizados, seja pela empresa que oferece o serviço ou por outras empresas e contextos institucionais, nos quais também experimentaremos novos cerceamentos, nos quais as rotinas da personalização e as políticas de diferenciação e classificação terão impactos sobre as oportunidades que

¹⁸⁴ Tradução nossa para: “Perhaps there is no greater lesson about networks than the lesson about control: networks, by their mere existence, are not liberating; they exercise novel forms of control that operate at a level that is anonymous and non-human, which is to say material”.

efetivamente nos estarão disponíveis. Restam-nos assim o benefício da dúvida, o conforto da ignorância ou a luta por maior transparência nas práticas institucionais acerca dos dados individuais que hoje trafegam livremente pelo ciberespaço. Seja qual for a direção a ser tomada pelas companhias que mantêm os *sites* de rede social nas próximas décadas, seja qual forem os posicionamentos adotados pelos usuários no decorrer dos próximos anos, interesses desafiadores e conflitantes já estão a postos, exigindo, minimamente, a negociação e o diálogo sincero e compromissado.

REFERÊNCIAS BIBLIOGRÁFICAS

- ACQUISTI, Alessandro; GROSS, Ralph. Information Revelation and Privacy in Online Social Networks. In: Workshop on Privacy on Electronic Networks (WPES), 2005, Alexandria. **Proceedings...** Alexandria: ACM, 2005. Disponível em: <<http://portal.acm.org/results.cfm?coll=GUIDE&CFID=16206531&CFTOKEN=76266819&query=Gross%20Acquisti&dl=GUIDE&dimval=4294832877>>. Acesso em: 29 ago. 2008.
- _____. Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. In: Workshop on Privacy Enhancing Technologies (PET), 6., 2006, Cambridge. **Proceedings...** Cambridge: Springer, 2006. Disponível em: <<http://www.heinz.cmu.edu/~acquisti/papers/acquisti-gross-facebook-privacy-PET-final.pdf>>. Acesso em: 22 ago. 2008.
- ADAMIC, Lada A.; BUYUKKOKTEN, Orkut; ADAR, Eytan. A social network caught in the web. **First Monday**, vol. 8, n. 6, jun. 2003. Disponível em: <http://outreach.lib.uic.edu/www/issues/issue8_6/adamic/>. Acesso em: 15 maio 2008.
- ALBRECHTSLUND, Anders. Online Social Networking as Participatory Surveillance. **First Monday**, v. 13, n. 3, mar. 2008. Disponível em: <<http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2142/1949>>. Acesso em: 10 abr. 2008.
- ANDREJEVIC, Mark. **iSpy**: surveillance and power in the interactive era. Lawrence: University Press of Kansas, 2007.
- ANTOUN, Henrique. De uma teia à outra: a explosão do comum e o surgimento da vigilância participativa. In: _____. (org.). **Web 2.0**: participação e vigilância na era da comunicação distribuída. Rio de Janeiro: Mauad X, 2008. p. 11-28.
- _____. A web 2.0 e o futuro da sociedade cibercultural. In: Congresso Brasileiro de Ciências da Comunicação, 31., 2008, Natal. **Anais eletrônicos**. São Paulo: Intercom, 2008. Disponível em: <<http://www.intercom.org.br/papers/nacionais/2008/resumos/R3-0874-1.pdf>>. Acesso em: 14 dez. 2008.
- ARNS, Inke. Code as performative speech act. **Artnodes**, Barcelona, n. 4, jul. 2005. ISSN 1695-5951. Disponível em: <<http://www.uoc.edu/artnodes/espai/eng/art/arns0505.pdf>>. Acesso em: 26 mar. 2006.
- ARRINGTON, Michael. Facebook Launches Facebook Platform; They are the Anti-MySpace. **TechCrunch**, 24 maio 2007. Disponível em: <<http://www.techcrunch.com/2007/05/24/facebook-launches-facebook-platform-they-are-the-anti-myspace/>>. Acesso em: 14 dez. 2008.
- _____. Facebook Now Nearly Twice The Size Of MySpace Worldwide. **TechCrunch**, 22 jan. 2009. Disponível em: <<http://www.techcrunch.com/2009/01/22/facebook-now-nearly-twice-the-size-of-myspace-worldwide/>>. Acesso em: 2 fev. 2009.
- BARABÁSI, Albert-László. **Linked**. how everything is connected to everything else and what it means for business, science, and everyday life. Cambridge: Plume, 2003.
- BECK, Ulrich. **Risk Society**: towards a new modernity. London: Sage Publications, 1992.
- BECKMAN, Rachel. Facebook Ads Target You Where It Hurts. **The Washington Post**, 3 set. 2008. Disponível em: <http://www.facebook.com/ext/share.php?sid=47190433792&h=A_LXI&u=-0u0i>. Acesso em: 10 dez. 2008.

BERNOFF, Josh; LI, Charlene. **Groundswell**: winning in a world transformed by social technologies. Boston: Harvard Business Press, 2008.

BERTEAU, Stefan. Facebook's Misrepresentation of Beacon's Threat to Privacy: Tracking users who opt out or are not logged in. **CA**, 29 nov. 2007. Disponível em: <<http://community.ca.com/blogs/securityadvisor/archive/2007/11/29/facebook-s-misrepresentation-of-beacon-s-threat-to-privacy-tracking-users-who-opt-out-or-are-not-logged-in.aspx>>. Acesso em: 29 nov. 2008.

BIZANNES, Elias. Vision & Mission. **The DataPortability Project**, 19 mar. 2009. Disponível em: <<http://wiki.dataportability.org/pages/viewpage.action?pageId=3440714>>. Acesso em: 5 nov. 2008.

BOGARD, William. **The simulation of surveillance**: hypercontrol in telematic societies. Cambridge: Cambridge University Press, 1996.

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

BOWKER, Geoffrey C.; STAR, Susan Leigh. **Sorting things out**: classification and its consequences. Cambridge: MIT Press, 1999.

BOYD, Danah. Friends, friendsters, and top 8: Writing community into being on social network. **First Monday**, vol. 11, n. 12, dez. 2006. Disponível em: <http://firstmonday.org/issues/issue11_12/boyd/index.html>. Acesso em: 21 nov. 2008.

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

_____. Social Network Sites: Public, Private, or What? **Knowledge Tree**, 13 maio 2007b. Disponível em: <<http://www.danah.org/papers/KnowledgeTree.pdf>>. Acesso em: 17 out. 2008.

BOYD, Danah; ELLISON, Nicole. B. Social network sites: Definition, history, and scholarship. **Journal of Computer-Mediated Communication**, vol 13, n. 1, out. 2007. Disponível em: <<http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html>>. Acesso em: 21 nov. 2008.

BOYD, Danah; DONATH, Judith. Public displays of connection. **BT Technology Journal**, vol. 22, n. 4, p. 71-82, out. 2004.

BRUNO, Fernanda. Máquinas de ver, modos de ser. **Revista Famecos**, n. 24, p. 110-24, jul. 2004. Disponível em: <<http://www.pucrs.br/famecos/pos/revfamecos/24/Fernanda.pdf>>. Acesso em: 22 set. 2008.

_____. Quem está olhando? Variações do público e do privado em weblogs, fotologs e reality shows. **Contemporânea**, vol. 3, n. 2, p. 53-70, jul./dez. 2005. Disponível em: <http://www.contemporanea.poscom.ufba.br/v3n2_pdf_dez05/bruno-olhando-n3v2.pdf>. Acesso em: 13 set. 2008.

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

_____. Monitoramento, classificação e controle nos dispositivos de vigilância digital. In: ANTOUN, Henrique (org.). **Web 2.0**: participação e vigilância na era da comunicação distribuída.

- Rio de Janeiro: Mauad X, 2008. p. 167-82.
- CAPLAN, Jane; TORPEY, John (eds.). Introduction. In: CAPLAN, Jane; TORPEY, John (eds.). **Documenting Individual Identity: The Development of State Practice in The Modern World**. Princeton: Princeton University Press, 2001. p. 1-13.
- CAREERBUILDER. One-in-Five Employers Use Social Networking Sites to Research Job Candidates, CareerBuilder.com Survey Finds. **Carrerbuilder.com**, 10 set. 2008. Disponível em: <<http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?id=pr459&sd=9%2f10%2f2008&ed=12%2f31%2f2008>>. Acesso em: 16 dez. 2008.
- CASSIDY, John. Me media. **The New Yorker**, 15 maio 2006. Disponível em: <http://www.newyorker.com/archive/2006/05/15/060515fa_fact_cassidy?currentPage=1>. Acesso em: 5 nov. 2008.
- ÇENTIMENTEL, U., FRANKLIN, M. J. and GILES, C. L. **Self-adaptative User Profiles for Large-Scale Data Delivery**. In: International Conference on Data Engineering (ICDE), 16., 2000, San Diego. **Proceedings...** San Diego: IEEE Computer Society Press, 2000. p. 622-633.
- COMSCORE. Microsoft Ranks as Top U.S. Online Display Advertiser in June, According to comScore Ad Metrix. **comScore**, 26 ago. 2008. Disponível em: <<http://www.comscore.com/press/release.asp?press=2415>>. Acesso em: 20 dez. 2008.
- _____. Global Internet Audience Surpasses 1 billion Visitors, According to comScore. **comScore**, 23 jan. 2009. Disponível em: <<http://www.comscore.com/press/release.asp?press=2698>>. Acesso em: 2 fev. 2009.
- CRAMER, Florian. Concepts, notations, software, art. In: **Readme 1.2**, mar. 2002. Disponível em: <http://userpage.fuberlin.de/~cantsin/homepage/writings/software_art/concept_notations/concepts_notations_software_art.html>. Acesso em: 23 abr. 2006.
- DEGENNE, Alain e FORSÉ, Michel. **Introducing Social Networks**. London: Sage, 1999.
- DELEUZE, Gilles. **Conversações**. Rio de Janeiro: Ed. 34, 1992.
- DELEUZE, Gilles; GUATTARI, Félix. **Mil platôs: capitalismo e esquizofrenia**. vol. 1. São Paulo: Ed. 34, 1995.
- DOUGLAS, Mary. **Risk and Blame: essays in cultural theory**. London: Routledge, 1992.
- DWYER, Catherine. Digital relationships in the 'MySpace' generation: results from a qualitative study. In: Hawaii International Conference on System Sciences (HICSS), 40., 2007. Waikoloa. **Proceedings...** Waikoloa: IEEE Computer Society Press, 2007. Disponível em: <<http://csdl2.computer.org/comp/proceedings/hicss/2007/2755/00/27550019c.pdf>>. Acesso em: 28 set. 2008.
- ELKINS, Sarah. A Social Network's Faux Pas? **Newsweek**, 9 nov. 2007. Disponível em: <<http://www.newsweek.com/id/69275/page/1>>. Acesso em: 21 set. 2008.
- E-MARKETER. Behind the Numbers: MySpace and Facebook. **E-marketer**, 19 nov. 2008. Disponível em: <<http://www.emarketer.com/Article.aspx?id=1006751>>. Acesso em: 5 dez. 2008.
- FACEBOOK. Facebook Unveils Facebook Ads. **Facebook**, nov. 2007. Disponível em: <<http://www.facebook.com/press/releases.php?p=9176>>. Acesso em: 18 nov. 2008.

- _____. **Platform Applications Terms of Use**. Disponível em: http://developers.facebook.com/user_terms.php. Acesso em: 12 dez. 2008.
- FLIXSTER. **Terms of service**. Disponível em: <http://www.flixster.com/misc/terms>. Acesso em: 12 dez. 2008.
- FAYYAD, Usama; PIATETSKY-SHAPIO, Gregory e SMYTH, Padhraic. From Data Mining to Knowledge Discover in Databases. In: **American Association for Artificial Intelligence**, 1996. Disponível em: <http://www.daedalus.es/fileadmin/daedalus/doc/MineriaDeDatos/fayyad96.pdf>. Acesso em: 22 dez. 2008.
- FOUCAULT, Michel. **Vigiar e punir: nascimento da prisão**. Petrópolis: Vozes, 1977.
- _____. **História da sexualidade: a vontade de saber**. vol. 1. Rio de Janeiro: Edições Graal, 1988.
- GANDY, Oscar. Coming to Terms with the Panoptic Sort. In: LYON, David; ZUREIK, Elia (eds.), **Computers, surveillance, and privacy**. Minneapolis: University of Minnesota Press, 1996. p. 132-155.
- GALLOWAY, Alexander R. **Protocol: how control exists after decentralization**. Cambridge: MIT Press, 2004.
- GALLOWAY, Alexander R.; THACKER, Eugene. **The Exploit: a theory of networks**. Minneapolis: University of Minnesota Press, 2007.
- GARTON, Laura; HARTHORNTHTWAITE, Caroline; WELLMAN, Barry. Studying Online Social Networks. **Journal of Computer Mediated Communication**, vol. 3, n. 1, jun. 1997. Disponível em: <http://www.ascusc.org/jcmc/vol3/issue1/garton.html>. Acesso em: 29 out. 2008.
- GOFFMAN, Erving. **The Presentation of Self in Everyday Life**. Nova Iorque: Anchor Books, 1959.
- 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 out. 2008.
- GRASMAYER, Bas. Facebook's Social Ads & Privacy. **Bas to Bulgaria**, 12 nov. 2007. Disponível em: <http://baslife.wordpress.com/2007/11/12/facebooks-social-ads-privacy/>. Acesso em: 10 dez. 2008.
- GROEBNER, Valentin. Describing the Person, Reading the Signs in Late Medieval and Renaissance Europe: Identity Papers, Vested Figures, and the Limits of Identification, 1400-1600. In: CAPLAN, Jane; TORPEY, John (eds.). **Documenting Individual Identity: The Development of State Practice in the Modern World**. Princeton: Princeton University Press, 2001. p.15-27.
- HACKING, Ian. **The taming of chance**. Cambridge University Press, 1990.
- HAGGERTY, Kevin D.; ERICSON, Richard V. The surveillant assemblage. **British Journal of Sociology**, vol. 51, n. 4, p. 605-622, dez. 2000. Disponível em: <http://www.uofaweb.ualberta.ca/sociology/pdfs/survassemb.pdf>. Acesso em: 23 jun. 2008.
- HANSELL, Saul. Facebook's next privacy problem. **Bits Blog**, 7 nov. 2007. Disponível em: <http://bits.blogs.nytimes.com/2007/11/07/facebooks-next-privacy-problem/>. Acesso em: 17 nov. 2008.

- HAVENSTEIN, Heather. Beware Job Seekers: Facebook, MySpace Could Harm Your Job Search. **Computerworld**, 12 set. 2008. Disponível em: <http://www.cio.com/article/449094/Beware_Job_Seekers_Facebook_MySpace_Could_Harm_Your_Job_Search>. Acesso em: 16 dez. 2008.
- HAYMAN, Karen. The Move to Make Social Data Portable. **Computer**, vol. 41, n. 4, p. 13-15, abr. 2008. Disponível em: <<http://www2.computer.org/portal/web/csdl/doi/10.1109/MC.2008.136>>. Acesso em: 15 out. 2008.
- HARDT, Michael; NEGRI, Antonio. **Império**. Rio de Janeiro: Record, 2000.
- HECHINGER, John. College Applicants, Beware: Your Facebook Page Is Showing. **The Wall Street Journal**, 18 set. 2008. Disponível em: <http://online.wsj.com/article/SB122170459104151023.html?mod=googlenews_wsj>. Acesso em: 16 dez. 2008.
- HODGKINSON, Tom. With friends like these. **The Guardian**, 14 jan. 2008. Disponível em: <<http://www.guardian.co.uk/technology/2008/jan/14/facebook>>. Acesso em : 12 out. 2008.
- JAGATIC, Tom N.; JOHNSON, Nathaniel A.; JAKOBSSON, Markus; MENCZER, Filippo. Social phishing. **Communications of the ACM**, vol. 50, n. 10, p. 94-100, out. 2007.
- JENSEN, David; NEVILLE, Jennifer. Data mining in social networks. In: National Academy of Sciences Symposium on Dynamic Social Network Analysis, 2002. **Proceedings...** Disponível em: <<http://www.cs.purdue.edu/homes/neville/papers/jensen-neville-nas2002.pdf>>. Acesso em: 13 nov. 2008.
- JONES, Harvey; SOLTREN, José Hiram. **Facebook: threats to privacy**. Cambridge: 2005. Disponível em: <<http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall05-papers/facebook.pdf>>. Acesso em: 18 ago. 2008.
- JONES, Steve; MILLERMAIER, Sarah; GOYA-MARTINEZ, Mariana; SCHULER, Jessica. Whose space is MySpace? A content analysis of MySpace profiles. **First Monday**, vol. 13, n. 9, set. 2008. Disponível em: <<http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/rt/prINTERfriendly/2202/2024>>. Acesso em: 3 out. 2008.
- KALTON, Graham. **Introduction to Survey Sampling**. Sage University Paper Series on Quantitative Applications in the Social Sciences, n. 07-035. Beverly Hills: Sage, 1983.
- KAPLAN. At top schools, one in ten college admissions officers visits applicants' social networking sites. **Kaplan.com**. Disponível em: <http://www.kaplan.com/aboutkaplan/pressreleases/archive/2008/KaplanCAOSurveyResults.htm?wbc_purpose=Basic&WBCMODE=PresentationUnpublished>. Acesso em: 16 dez. 2008.
- KNOKE, David; YANG, Song. **Social Network Analysis**. Thousand Oaks: Sage Publications, 2008.
- KOSELLECK, Reinhart. **Futuro Passado: contribuição à semântica dos tempos históricos**. Rio de Janeiro: Editora da Pontifícia Universidade Católica do Rio de Janeiro, 2006.
- LACY, Sarah. Facebook Learns from Its Fumble. **BusinessWeek**, 8 set. 2006. Disponível em: <http://www.businessweek.com/technology/content/sep2006/tc20060908_536553.htm?chan=top+news_top+news+index_technology>. Acesso em: 23 nov. 2008.
- LAPPONI, Juan Carlos. **Estatística usando Excel**. Rio de Janeiro Elsevier, 2005.

- LEMOS, André. Cidade-Ciborgue: A cidade na cibercultura. In: _____ (org.). **Cibercidade II. Ciberurbe: A cidade na sociedade da informação**. Rio de Janeiro: E-papers, 2005.
- LEONARD, Andrew. You are who you know. **Salon.com**, 15 jun. 2004. Disponível em: <http://www.salon.com/tech/feature/2004/06/16/social_software_two/print.html>. Acesso em: 19 ago. 2008.
- LESSIG, Lawrence. **Code and other laws of cyberspace**: version 2.0. Basic Books, 2006.
- LEVINE, Rick; LOCKE, Christopher; SEARLS, Doc; WEINBERGER, David. **The Cluetrain Manifesto: the end of business as usual**. Cambridge: Perseus, 2000.
- LIANOS, Michalis. **Le nouveau contrôle social**: toile institutionnelle, normative et lien social. Paris: L'Harmattan, 2001.
- LIANOS, Michalis. Social Control after Foucault. **Surveillance & Society**, v. 1, n. 3, p. 412-30, 2003. Disponível em: <[http://www.surveillance-and-society.org/articles1\(3\)/AfterFoucault.pdf](http://www.surveillance-and-society.org/articles1(3)/AfterFoucault.pdf)>. Acesso em: 11 ago. 2008.
- LIMA, Carlos Eduardo. Buzz Marketing: é possível controlar? **iMasters**, 20 ago. 2008. Disponível em: <http://imasters.uol.com.br/artigo/9669/webmarketing/buzz_marketing_e_possivel_controlar/>. Acesso em: 13 nov. 2008.
- LINDEN, Greg.; SMITH, Brent.; YORK, Jeremy. Amazon. com recommendations: item-to-item collaborative filtering. **IEEE Internet Computing**, v. 7, p. 76-80, jan./fev. 2003.
- LIU, Hugo; MAES, Pattie; DAVENPORT, Gloria. **Unraveling the Taste Fabric of Social Networks**. Boston: The Media Laboratory, Massachusetts Institute of Technology, 2005. Disponível em: <<http://web.media.mit.edu/~hugo/publications/drafts/IJSWIS2006-tastefabrics.pdf>>. Acesso em: 20 out. 2007.
- LORICA, Ben. Facebook Growth Regions and Gender Split. **O'Reilly Radar**, 4 dez. 2008. Disponível em: <<http://radar.oreilly.com/2008/12/facebook-growth-regions-and-ge.html>>. Acesso em: 22 dez. 2008.
- LYON, David; ZUREIK, Elia. Surveillance, Privacy, and the New Technology. In: LYON, David; ZUREIK, Elia (eds.), **Computers, surveillance, and privacy**. Minneapolis: University of Minnesota Press, 1996. p. 1-21.
- LYON, David. Globalizing Surveillance: comparative and sociological perspectives. **International Sociology**, vol. 19; n. 2, p. 135-149, jun. 2004.
- _____. 9/11, Synopticon, and Scopophilia: Watching and Being Watched. In: HAGGERTY, Kevin D.; ERICSON, Richard V. (eds.). **The new politics of surveillance and visibility**. Toronto: University of Toronto Press, 2006. p. 36-54.
- MACCARTH, Caroline. ComScore: Facebook is beating MySpace worldwide. **Cnet News**, 20 jun. 2008. Disponível em: <http://news.cnet.com/8301-13577_3-9973826-36.html>. Acesso em: 22 jan. 2008.
- MCCARTHY, Megan. Facebook Ads Make you the Star – And You May Not Know It. **Wired Blog Network**, 2 jan. 2008. Disponível em: <<http://blog.wired.com/business/2008/01/facebook-ads-ma.html>>. Acesso em: 23 nov. 2008.

MCGEVERAN, William. Facebook Inserting Users Into Ads. **Info/Law**, 8 nov. 2007a. Disponível em: <<http://blogs.law.harvard.edu/infolaw/2007/11/08/facebook-social-ads/>>. Acesso em: 17 nov. 2008.

MCGEVERAN, William. More Thoughts on Facebook's "Social Ads". **Info/Law**, 9 nov. 2007b. Disponível em: <<http://blogs.law.harvard.edu/infolaw/2007/11/09/more-thoughts-on-facebooks-social-ads/>>. Acesso em: 17 nov. 2008.

MANOVICH, Lev. **Language of New Media**. Cambridge: MIT Press, 2001.

_____. O excesso de dados e o belo. **Enciclopédia Itaú Cultural Arte e Tecnologia**, 4 jun. 2007. Disponível em: <http://www.cibercultura.org.br/tikiwiki/tiki-read_article.php?articleId=18&highlight=%22manovich%22> Acesso em: 18 jun. 2007.

MARX, Gary T. What's new about the "new surveillance"? Classifying for change and continuity. **Surveillance & Society**, v. 1, n. 1, p. 9-29, 2002. Disponível em: <<http://www.surveillance-and-society.org/articles1/whatsnew.pdf>>. Acesso em: 10 jul. 2008.

MEYER, Eric A. **XFN and FOAF**. Disponível em: <<http://www.gmpg.org/xfn/and/foaf>>. Acesso em: 3 dez. 2008.

MEYROWITZ, Joshua. **No sense of place: The Impact of Electronic Media on Social Behavior**. New York: Oxford University Press, 1985.

MORIN, Dave. Announcing Facebook Connect. **Facebook Developers Blog**, 9 maio 2008. Disponível em: <<http://developers.facebook.com/news.php?blog=1&story=108>>. Acesso em: 12 dez. 2008.

MURRAY, Jannet H. **Hamlet no holodeck: o futuro da narrativa no ciberespaço**. São Paulo: Itaú Cultural: Unesp, 2003.

NAONE, Erica. Who owns your friends? **Technology Review**, jul./ago. 2008a. Disponível em: <<http://www.technologyreview.com/communications/20920/page4/>>. Acesso em: 2 set. 2008.

NATIONAL STATISTICS (Reino Unido). **National Statistics Code of Practice: protocol on data matching**. Londres, 2004. 22 p. ISBN 0 11 703258 1.

NEWMAN, M. E. J. The structure and function of complex networks. **Siam Review**, vol. 45, n. 2, p. 167-256, mar. 2003. Disponível em: <<http://www.siam.org/journals/sirev/45-2/42480.html>>. Acesso em: 4 abr. 2007.

OBASANJO, Dare. Google OpenSocial: Technical Overview and Critique. **Dare Obasanjo aka Carnage4Life**, 3 nov. 2007. Disponível em: <<http://www.25hoursaday.com/weblog/2007/11/03/GoogleOpenSocialTechnicalOverviewAndCritique.aspx>>. Acesso em: 15 dez. 2008.

OLSEN, Stefanie. At Rapleaf, your personals are public. **ZDNet**, 31 ago. 2007. Disponível em: <http://news.zdnet.com/2100-9588_22-162371.html>. Acesso em: 22 set. 2008.

O'REILLY, Tim. **What is Web 2.0?**. Disponível em: <<http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html>>. 2005. Acesso em: 9 jan. 2008.

OWYANG, Jeremiah. What Facebook's New 'Engagement Advertising' Means to Brands. **Web Strategy**, ago. 2008. Disponível em: <<http://www.web-strategist.com/blog/2008/08/21/facebooks->

- engagement-ads/>. Acesso em: 12 dez. 2008.
- PARR, Ben. Social Media and Privacy: Where Are We Two Years After Facebook News Feed? **Mashable**, 8 set. 2008. Disponível em : <<http://mashable.com/2008/09/08/social-media-privacy-news-feed/>>. Acesso em: 11 nov. 2008.
- PEREZ, Juan Carlos. Facebook Admits Ad Service Tracks Logged-Off Users. **PCWorld**, 3 dez. 2007. Disponível em: <http://www.pcworld.com/businesscenter/article/140225/facebook_admits_ad_service_tracks_loggedoff_users.html>. Acesso em: 24 nov. 2008.
- PERRY, Katie. Officials at institutions nationwide using Facebook site. **TheObserver**, 29 mar. 2006. Disponível em: <http://media.www.ndsmcobserver.com/media/storage/paper660/news/2006/03/29/News/Officials_At.Institutions.Nationwide.Using.Facebook.Site-1763490.shtml>. Acesso em: 19 dez. 2008.
- PICK, Michael. **Attention Profiling: APML Beginner's Guide**. Disponível em: <http://www.masternewmedia.org/online_marketing/attention-profiling-apml/apml-beginners-guide-attention-profile-20071113.htm>. Acesso em: 15 out. 2008.
- POSTER, Mark. **The mode of information: poststructuralism and social context**. The University of Chicago Press, 1990.
- _____. Databases as Discourse; or, Electronic Interpellations. In: LYON, David; ZUREIK, Elia (eds.). **Computers, surveillance, and privacy**. Minneapolis: University of Minnesota Press, 1996. p. 175-192.
- POWERS, Shelley. Terms. **Burningbird**, 2 nov. 2007. Disponível em: <<http://burningbird.net/technology/terms/>>. Acesso em: 15 dez. 2008.
- PRIMO, Alex. Interação mútua e reativa: uma proposta de estudo. **Revista da Famecos**, n. 12, p. 81-92, jun. 2000.
- _____. O aspecto relacional das interações na web 2.0. In: ANTOUN, Henrique (org.). **Web 2.0: participação e vigilância na era da comunicação distribuída**. Rio de Janeiro: Mauad X, 2008. p. 101-22.
- RECUERO, Raquel. Um estudo do Capital Social gerado a partir de Redes Sociais no Orkut e nos Weblogs. **Revista Famecos**, n. 28, p. 88-106, dez. 2005. Disponível em: <<http://www.pucrs.br/famecos/pos/revfamecos/28/raquelrecuero.pdf>>. Acesso em: 10 nov. 2008.
- REID, Michael D. 'Dexter' murder case raises alarms over pop-culture violence. **National Post**, 6 nov. 2008. Disponível em: <<http://www.nationalpost.com/related/topics/story.html?id=938094>>. Acesso em: 16 dez. 2008.
- RHEINGOLD, Howard. **The Virtual Community: homesteading on the electronic frontier**. Nova Iorque: Harper Collins, 1993.
- RÖHLE, Theo. Desperately seeking the consumer: Personalized search engines and the commercial exploitation of use data. **First Monday**, vol. 12, n. 9, set. 2007. Disponível em: <<http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2008/1883>>. Acesso em: 2 maio 2008.
- SCHIFFMAN, Betsy. MoveOn Declares War on Facebook. **Wired Blog Network**, 21 nov. 2007. Disponível em: <<http://blog.wired.com/business/2007/11/moveon-declares.html>>. Acesso em: 23

nov. 2008.

SIBILIA, Paula. Em busca da aura perdida: espetacularizar a intimidade para ser alguém. In: ANTOUN, Henrique (org.). **Web 2.0: participação e vigilância na era da comunicação distribuída**. Rio de Janeiro: Mauad X, 2008. p. 241-60.

SMITH, Ken. NCSU Students Face Underage Drinking Charges Due To Online Photos. **WRAL.com**, 30 out. 2005. Disponível em: <<http://web.archive.org/web/20051031084848/http://www.wral.com/news/5204275/detail.html>>. Acesso em: 19 dez. 2008.

SOLOVE, Daniel. The New Facebook Ads – Starring You: Another Privacy Debacle? **Concurring Opinions**, 8 nov. 2007. Disponível em: <http://www.concurringopinions.com/archives/2007/11/the_new_faceboo.html>. Acesso em: 17 nov. 2008.

STONE, Brad; STORY, Louise. Facebook Retreats on Online Tracking. **The New York Times**, 30 nov. 2007. Disponível em: <<http://www.nytimes.com/2007/11/30/technology/30face.html?ex=1354165200&en=f448f8a210da7bdf&ei=5124&partner=permalink&expprod=permalink>>. Acesso em: 22 nov. 2008.

STORY, Louise. The Evolution of Facebook's Beacon. **Bits Blog**, 29 nov. 2007. Disponível em: <<http://bits.blogs.nytimes.com/2007/11/29/the-evolution-of-facebooks-beacon/>>. Acesso em: 22 nov. 2008.

STRATER, Katherine; RICHTER, Heather. Examining Privacy and Disclosure in a Social Networking Community. In: Symposium on Usable Privacy and Security, 3., jul. 2007, Pittsburgh. **Proceedings...** Pittsburgh: ACM, 2007. Disponível em: <http://portal.acm.org/ft_gateway.cfm?id=1280706&type=pdf&coll=GUIDE&dl=GUIDE&CFID=15833498&CFTOKEN=79391213>. Acesso em: 11 set. 2008.

STUTZMAN, F. An evaluation of identity-sharing behavior in social network communities. **International Digital and Media Arts Journal**, vol. 3, n. 1. Disponível em: <http://www.ibiblio.org/fred/pubs/stutzman_pub4.pdf>. Acesso em: 12 out. 2008.

STYLEFEEDER. **Terms of Service**. Disponível em: <<http://www.stylefeeder.com/info/terms-of-service.html>>. Acesso em: 13 dez. 2008.

TAPSCOTT, Don; WILLIAMS, Anthony D. **Wikinomics: como a colaboração em massa pode mudar o seu negócio**. Rio de Janeiro: Editora Nova Fronteira, 2007.

TECHRADAR. Facebook, MySpace Statistics. **TechRadar**, 11 jan. 2008. Disponível em: <<http://techradar1.wordpress.com/2008/01/11/facebookmyspace-statistics/>>. Acesso em: 22 jan. 2008.

THOMPSON, Clive. Brave New World of Digital Intimacy. **The New York Times Magazine**, 5 set. 2008. Disponível em: <http://www.nytimes.com/2008/09/07/magazine/07awareness-t.html?_r=1>. Acesso em: 13 nov. 2008.

TUROW, Joseph. **Cracking the consumer code: Anxiety and Surveillance in the Digital Age**. In: HAGGERTY, Kevin D.; ERICSON, Richard V. (eds.). **The new politics of surveillance and visibility**. Toronto: University of Toronto Press, 2006. p. 279-307.

_____. Audience Construction and Culture Production: Marketing Surveillance in the Digital Age. In: The ANNALS of the American Academy of Political and Social Science. **Proceedings...**

vol. 597, n 1, p. 103-21, jan. 2005. Disponível em:
<<http://ann.sagepub.com/cgi/reprint/597/1/103>>. Acesso em: 18 nov. 2008.

URSTADT, Bryant. Part I: The Business of Social Networks. Can social-networking sites make money? **Technology Review**, jul./ago. 2008b. Disponível em:
<<http://www.technologyreview.com/Biztech/20978/?a=f>>. Acesso em: 2 set. 2008.

_____. Part II: The Business of Social Networks. Can social-networking sites make money? **Technology Review**, jul./ago. 2008a. Disponível em:
<<http://www.technologyreview.com/business/20979/?a=f>>. Acesso em: 2 nov. 2008.

VASCELLARO, Jessica. Facebook Tries to Woo Marketers. **The Wall Street Journal**, 11 nov. 2008. Disponível em: <<http://online.wsj.com/article/SB122637098500816351.html>>. Acesso em: 21 nov. 2008.

VORA, Ami. Opening up Facebook Platform Architecture. **Facebook Developers Blog**, 13 dez. 2007. Disponível em: <<http://developers.facebook.com/news.php?blog=1&story=60>>. Acesso em: 10 dez. 2008.

WASSERMAN, Stanley e FAUST, Katherine. **Social Network Analysis. Methods and Applications**. Cambridge: Cambridge University Press, 1994.

WIKIPEDIA. Bulletin Board System. Disponível em:
<http://en.wikipedia.org/wiki/Bulletin_board_systems>. Acesso em: 2 nov. 2008.

ZUCKERBERG, Mark. An Open Letter from Mark Zuckerberg: **The Facebook Blog**, 8 set. 2006. Disponível em: <<http://blog.facebook.com/blog.php?post=2208562130>>. Acesso em: 2 dez. 2008.

_____. Thoughts on Beacon. **The Facebook Blog**, 5 dez. 2007. Disponível em:
<<http://blog.facebook.com/blog.php?post=7584397130>>. Acesso em: 2 dez. 2008.

ANEXO A:
DADOS DEMOGRÁFICOS DO FACEBOOK

Top 15 Worldwide Properties Ranked by Total Worldwide Unique Visitors (000)* Age 15+, Home & Work Locations, December 2008 (Source: comScore World Metrix)		
Property	Total Unique Visitors (000)	% Reach of Total Worldwide Internet Audience
<i>Total Worldwide Internet Audience</i>	1,007,730	100.0%
Google Sites	775,980	77.0%
Microsoft Sites	646,915	64.2%
Yahoo! Sites	562,571	55.8%
AOL LLC	273,020	27.1%
Wikimedia Foundation Sites	272,998	27.1%
eBay	240,947	23.9%
Facebook.COM	221,791	22.0%
Amazon Sites	187,354	18.6%
CBS Corporation	178,844	17.7%
Fox Interactive Media	172,841	17.2%
Ask Network	164,513	16.3%
Apple Inc.	161,500	16.0%
Tencent Inc.	158,617	15.7%
Baidu.com Inc.	152,447	15.1%
Adobe Sites	123,623	12.3%

Fig. 1: *Sites* mais acessados da Internet no mês de dezembro de 2008, de acordo com a *comScore*.
Fonte: COMSCORE, 2009: *online*.

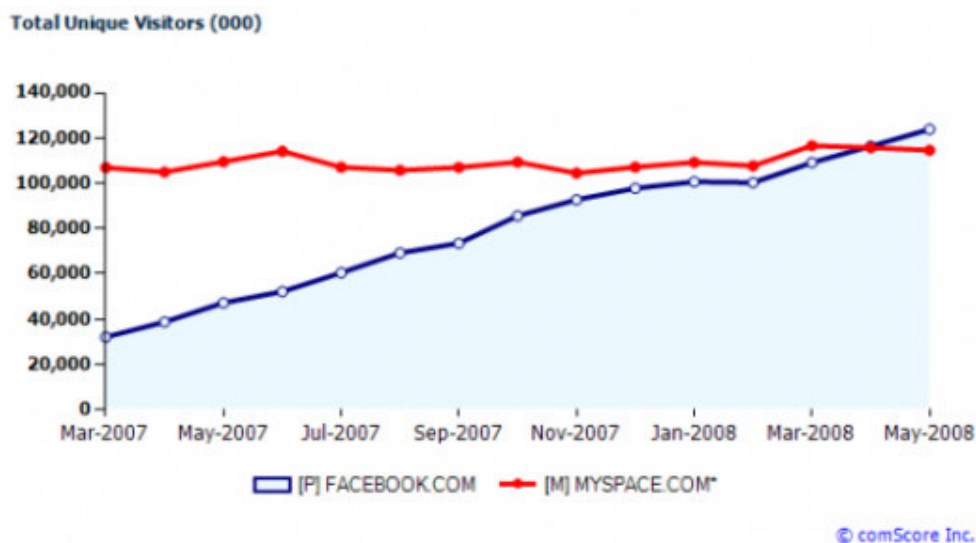


Fig. 2: Número de visitantes únicos do *Facebook* e do *MySpace* entre março de 2007 e maio de 2008, de acordo com a *comScore*. Fonte: MCCARTHY, 2008 (*online*).

	País	Usuários
01	Estados Unidos	33.718.780
02	Reino Unido	13.019.360
03	Canadá	10.065.720
04	Turquia	4.926.180
05	Austrália	3.727.340
06	França	3.600.800
07	Chile	3.410.140
08	Colômbia	3.349.740
09	Venezuela	1.572.740
10	Suécia	1.391.400
11	Noruega	1.341.660
12	México	1.265.820
13	Dinamarca	1.240.180
14	Itália	1.233.980
15	Espanha	1.192.720
16	Hong Kong	1.162.680
17	África do Sul	1.053.600
18	Argentina	1.051.580
19	Bélgica	899.200
20	Alemanha	876.720
21	Egito	851.040
22	Índia	835.020
23	Suíça	701.440
24	Finlândia	688.760
25	Israel	672.260
26	Grécia	668.160
27	Malásia	626.680
28	Cingapura	557.480
29	Porto Rico	473.560
30	Nova Zelândia	447.420
31	Emirados Árabes Unidos	416.640
32	Líbano	385.100
33	Indonésia	350.520
34	Irlanda	323.160
35	Croácia	314.680
36	Paquistão	305.240
37	Holanda	297.520
38	Sérvia	289.040
39	Arábia Saudita	275.820
40	Filipinas	248.460
41	Marrocos	233.220
42	Panamá	224.480
43	Peru	218.940
44	Jordânia	217.260
45	China	207.960
46	Japão	178.960
47	Brasil	167.220
48	Bolívia	159.480
49	Áustria	157.800
50	Nigéria	152.460

51	Bangladesh	141.460
52	Polônia	123.520
53	Tailândia	117.820
54	Quênia	114.580
55	Trindade e Tobago	112.420
56	Equador	110.240
57	Uruguai	100.120
58	Coréia do Sul	99.960
59	Rússia	99.580
60	Bósnia e Herzegovina	98.780
61	República Dominicana	95.020
62	Kuwait	94.500
63	Eslovênia	91.600
64	Formosa	90.760
65	Guatemala	86.500
66	República Tcheca	84.600
67	Tunísia	83.340
68	Bulgária	82.640
69	Chipre	77.720
70	Hungria	67.960
71	Portugal	65.120
72	Islândia	62.480
73	Costa Rica	60.700
74	Catar	57.040
75	Palestina	56.620
76	El Salvador	55.300
77	Eslováquia	52.520
78	Luxemburgo	52.260
79	Jamaica	51.240
80	Honduras	45.520
81	Reino de Bahrain	44.180
82	Ilhas Maurício	43.700
83	Gana	39.060
84	Malta	37.020
85	Lituânia	31.920
86	Maldivas	31.200
87	Bahamas	31.140
88	Ucrânia	30.460
89	Vietnã	28.000
90	Nicarágua	26.460
91	Paraguai	12.280
92	Sri Lanka	11.240
93	Romênia	10.840
* Dados coletados em 29/09/08.		

Fig. 3: Levantamento preliminar do número de usuários do *Facebook* por país realizado em setembro de 2008 com o objetivo de definir o público alvo deste estudo.

	País	Usuários
01	Estados Unidos	47.457.600
02	Reino Unido	15.366.840
03	Canadá	9.863.120
04	Turquia	7.664.320
05	Itália	7.229.600
06	França	6.741.880
07	Austrália	4.629.900
08	Espanha	3.475.060
09	Colômbia	3.462.280
10	Chile	3.353.360
11	Argentina	2.623.500
12	Venezuela	1.862.700
13	Suécia	1.818.580
14	Indonésia	1.744.740
15	Bélgica	1.718.240
16	Dinamarca	1.645.240
17	México	1.589.120
18	Noruega	1.561.880
19	Alemanha	1.509.740
20	Hong Kong	1.463.380
21	Grécia	1.217.720
22	Suíça	1.191.400
23	Índia	1.185.600
24	África do Sul	1.080.960
25	Finlândia	1.000.440
26	Malásia	966.380
27	Egito	964.260
28	Cingapura	851.700
29	Israel	807.860
30	Filipinas	733.380
31	Sérvia	625.520
32	Nova Zelândia	621.620
33	Porto Rico	575.560
34	Irlanda	510.580
35	Emirados Árabes Unidos	495.020
36	Croácia	459.800
37	Holanda	437.380
38	Paquistão	422.720
39	Líbano	380.740
40	Áustria	359.980
41	Marrocos	345.540
42	República Tcheca	323.420
43	Tunísia	318.920
44	Peru	316.800
45	Arábia Saudita	308.380
46	China	254.280
47	Jordânia	253.440
48	Brasil	241.020
49	Eslováquia	240.520

50	Nigéria	237.520
51	Bósnia e Herzegovina	232.680
52	Eslovênia	229.960
53	Japão	228.620
54	Bangladesh	224.800
55	Polônia	216.120
56	Tailândia	214.160
57	Bulgária	204.040
58	Uruguai	202.580
59	Quênia	177.820
60	Panamá	174.000
61	Sri Lanka	161.940
62	Bolívia	154.120
63	Formosa	139.960
64	Islândia	133.840
65	Trinidad e Tobago	132.820
66	Equador	126.520
67	Rússia	124.880
68	Macedônia	121.960
69	República Dominicana	120.060
70	Coréia do Sul	118.400
71	Hungria	115.040
72	Portugal	112.080
73	Kuwait	110.160
74	Chipre	107.960
75	Guatemala	95.300
76	Costa Rica	87.460
77	Catar	78.680
78	Luxemburgo	78.480
79	Romênia	77.460
80	Gana	69.960
81	Jamaica	68.960
82	Palestina	66.520
83	El Salvador	66.360
84	Lituânia	58.380
85	Ilhas Maurício	57.220
86	Honduras	52.820
87	Malta	51.260
88	Reino de Bahrain	50.720
89	Vietnã	47.780
90	Ucrânia	43.800
91	Bahamas	40.560
92	Maldivas	33.600
93	Nicarágua	31.780
94	Omã	26.060
95	Paraguai	23.040
* Dados coletados em 26/02/08.		

Fig. 4: Levantamento preliminar do número de usuários do *Facebook* por país realizado em setembro de 2008 com o objetivo de definir o público alvo deste estudo.

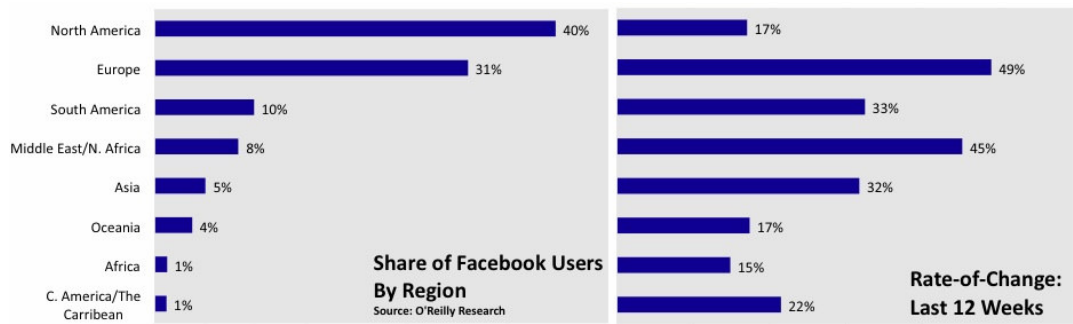


Fig. 5: Distribuição dos usuários do Facebook por região. Fonte: O'Reilly Research.

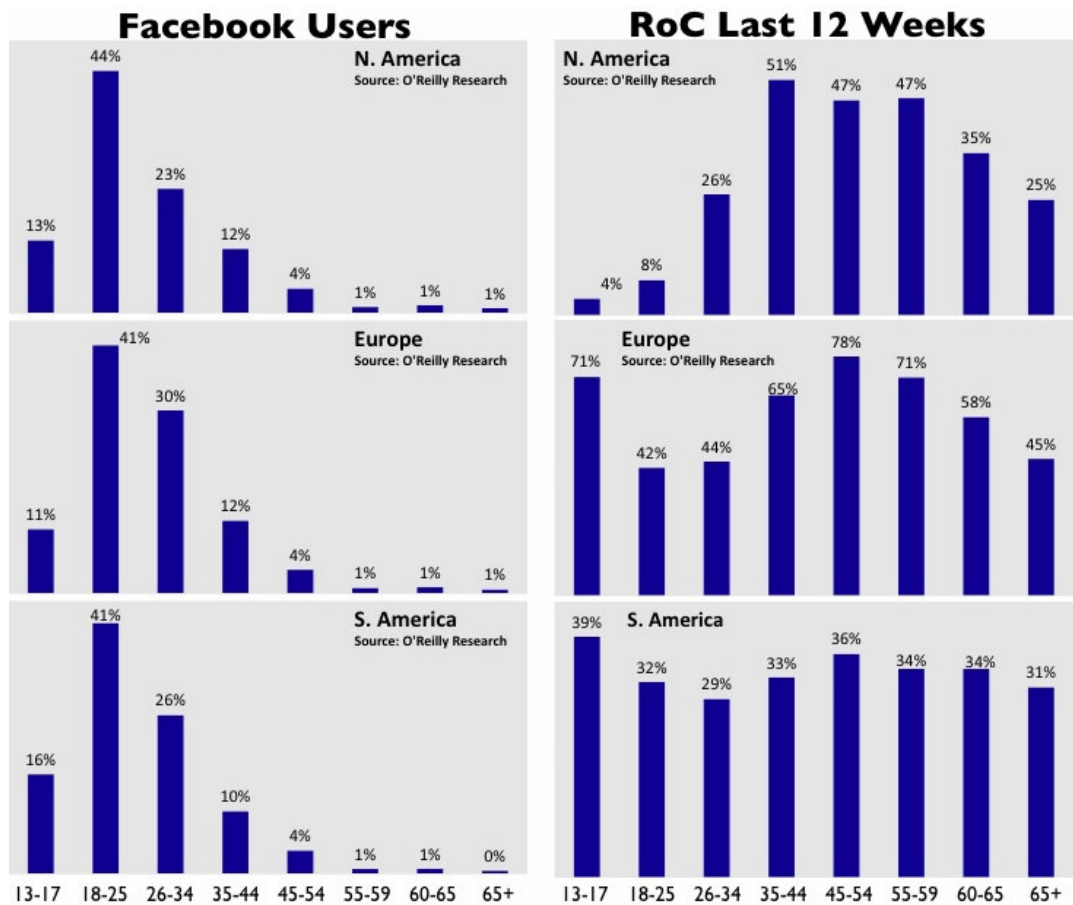


Fig. 6: Distribuição de idade dos usuários do Facebook por região. Fonte: O'Reilly Research.

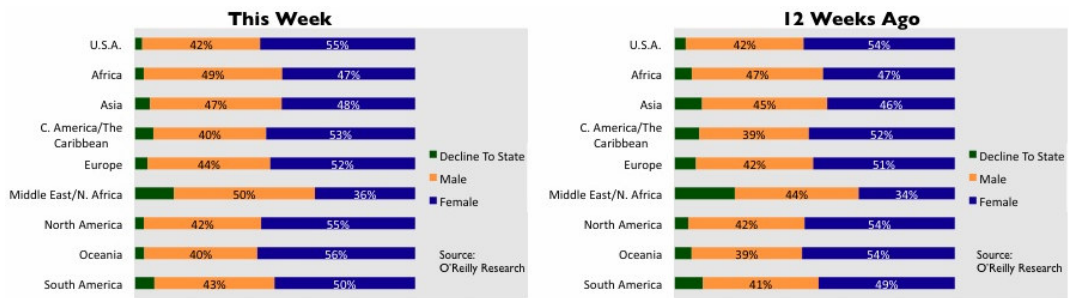


Fig. 7: Distribuição dos usuários do Facebook por gênero em diferentes regiões. Fonte: O'Reilly Research.

ANEXO B:
QUESTIONÁRIOS APLICADOS

Questionário I

S U R V E Y

Por favor, responda as questões seguintes fornecendo apenas informações verdadeiras.

Não se identifique em nenhum dos campos deste formulário.

Ao preenchê-lo, você concorda com a utilização destas informações para fins científicos. Em contrapartida, nos comprometemos a preservar sua identidade e não associá-la às informações por você fornecidas.

Você só deve responder a esta pesquisa se você tem um perfil pessoal no Facebook (FB):
(www.facebook.com).

Por favor, selecione corretamente os seus dados demográficos:

Sexo: () Masculino. () Feminino. **Idade:** _____. **Nacionalidade:** _____.

País em reside atualmente: _____.

Em que tipos de rede você entrou no Facebook?

() Ensino médio () Ensino superior () Local de trabalho () Região () Nenhuma

Se você participa de uma rede de instituição de Ensino Superior, diga-nos seu status:

() Aluno de graduação () Discente de pós-graduação () Ex-discente () Corpo docente () Equipe de funcionários

1. Com que frequência você acessa a sua conta no Facebook?

- a) mais de uma vez por dia.
- b) pelo menos uma vez por dia.
- c) de duas a três vezes por semana.
- d) pelo menos uma vez por semana.
- e) pelo menos uma vez por mês.
- f) passo mais de um mês sem verificar minha conta.

2. O Facebook é a rede social que você usa com mais frequência?

- a) Sim.
- b) Não, eu uso com mais frequência outra rede social (Orkut, LinkedIn, MySpace, etc.)
- c) Eu uso o Facebook tanto quanto eu uso outro site de rede social.

3. Abaixo, você tem uma lista de possíveis riscos associados ao uso da internet em geral.

Como você se sente em relação a cada um deles quando você usa o Facebook?

Risco de vírus/spywares.

() Muito preocupado. () Preocupado. () Pouco preocupado. () Isso não me preocupa. () Isso não acontece no FB. () Não sei se isso acontece no FB. () Não sei o que é isso.

Prática de crimes cibernéticos.

() Muito preocupado. () Preocupado. () Pouco preocupado. () Isso não me preocupa. () Isso não acontece no FB. () Não sei se isso acontece no FB. () Não sei o que é isso.

Roubo de identidade.

() Muito preocupado. () Preocupado. () Pouco preocupado. () Isso não me preocupa. () Isso não acontece no FB. () Não sei se isso acontece no FB. () Não sei o que é isso.

Ser perseguido, assediado ou ameaçado por um estranho através da Internet.

() Muito preocupado. () Preocupado. () Pouco preocupado. () Isso não me preocupa. () Isso não acontece no FB. () Não sei se isso acontece no FB. () Não sei o que é isso.

Ameaças à privacidade.

() Muito preocupado. () Preocupado. () Pouco preocupado. () Isso não me preocupa. () Isso não acontece no FB. () Não sei se isso acontece no FB. () Não sei o que é isso.

Ter meus dados pessoais coletados e usados para envio de recomendações de produtos ou anúncios personalizados.

() Muito preocupado. () Preocupado. () Pouco preocupado. () Isso não me preocupa. () Isso não acontece no FB. () Não sei se isso acontece no FB. () Não sei o que é isso.

4. Algumas vezes, você busca por alguém no FB mas não pode acessar seu perfil. Você sabe quem pode buscar e quem pode acessar o seu perfil no Facebook?

- a) Seu perfil pode ser buscado e acessado apenas pelos seus amigos.
- b) Seu perfil pode ser buscado por qualquer pessoa que use o site e acessado só pelas pessoas que participam da(s) mesma(s) rede(s) que você.
- c) Seu perfil pode ser buscado por qualquer pessoa dentro ou fora do FB (inclusive através do Google) e acessado apenas pelos seus amigos e por qualquer pessoa que faça parte das mesmas redes que você.
- e) Eu não sei quem pode buscar e quem pode acessar o meu perfil no FB.

5. Você estima que o seu perfil possa ser visualizado por:

- a) Dezenas de pessoas.
- b) Centenas de pessoas.
- c) Milhares de pessoas.
- d) Milhões de pessoas.
- e) Não sei.

6. Você já alterou as configurações de privacidade de sua conta no FB?

- a) Sim, apenas uma vez.
- b) Sim, mais de uma vez.
- c) Não, porque não sei como fazer isso.
- d) Não, porque estou satisfeito com as configurações de privacidade que o FB definiu para mim como padrão.
- e) Eu não me lembro se já alterei minhas configurações de privacidade.

7. Para quais destas finalidades você já usou as configurações de privacidade do Facebook? Marque todas as alternativas que se aplicam a você.

Atenção: se você nunca usou as configurações de privacidade do FB, vá para a questão 9; se você já alterou as suas configurações de privacidade mais de uma vez, responda considerando a última vez que você as modificou.

- () restringir o número de pessoas que pode buscar pelo meu perfil no FB.
- () restringir as informações que ficam disponíveis em meu anúncio público de busca (para as pessoas que não são meus amigos e que não podem acessar minha página).
- () restringir quem pode ver meu perfil e/ou algum dos tipos de informações nele disponíveis.
- () restringir quem pode ver minhas informações de contato.

- ☐ restringir quais das minha atualizações e atividades recentes no site irão gerar os históricos que são publicados em meu mural e na página de meus amigos (News Feed e Mini-Feed).
- ☐ não permitir que históricos sobre minhas atividades recentes em sites afiliados Beacon sejam publicados em meu perfil ou entregues aos meus amigos.
- ☐ não aparecer em anúncios sociais mostrados aos meu amigos.
- ☐ bloquear alguém.

8. Você já usou alguma das configurações de privacidade listadas acima no sentido de disponibilizar mais informações ou permitir que mais pessoas tenham acesso às informações em questão?

- ☐ Sim ☐ Não

9. Existe algum tipo de informação que você evita disponibilizar através do FB? Marque todas as alternativas que se aplicam a você.

- ☐ Evito disponibilizar informações que não gostaria que meus pais, namorado(a), professores(as), familiares ou autoridades na escola/faculdade ficassem sabendo.
- ☐ Evito disponibilizar informações que possam me prejudicar na hora de arrumar um emprego ou entrar na faculdade.
- ☐ Evito disponibilizar informações que possam ferir minha imagem ou minha reputação.
- ☐ Evito disponibilizar informações que incluam o lugar/hora em que estarei em um dia em particular.
- ☐ Evito disponibilizar informações que não gostaria que meus amigos soubessem.
- ☐ Evito disponibilizar informações sobre meus gostos e interesses que possam ser usadas para me direcionar recomendações de produtos ou anúncios publicitários.
- ☐ Não há nenhum tipo de informação que eu evite disponibilizar através do FB.

10. Marque as alternativas que descrevem suas atitudes em relação às informações que você disponibiliza através do Facebook.

- ☐ Eu não me preocupo com as informações que eu disponibilizo através do FB porque acredito que não exista nenhum risco associado ao uso do site.
- ☐ Eu uso as configurações de privacidade e isso faz com que eu me sinta menos preocupado em relação às informações que disponibilizo através do FB.
- ☐ Eu não uso as configurações de privacidade porque elas podem ser burladas facilmente.
- ☐ Eu protejo as informações que eu publico através do FB colocando em minha página apenas o que possa ser visto por qualquer pessoa.
- ☐ Eu me sinto menos preocupado em relação às informações que disponibilizo porque estou interagindo com a comunidade da minha escola/universidade.
- ☐ Eu me sinto menos preocupado em relação às informações que disponibilizo porque estou interagindo com a comunidade do meu estado/país.
- ☐ Eu acredito que o que você publica em um website não pode ter sérias consequências em sua vida real e isso faz com que eu me sinta menos preocupado em relação às informações que publico no FB.
- ☐ Eu acho que dificilmente alguém irá encontrar uma informação inadequada ou comprometedor sobre mim na imensa massa de dados de um site como o FB e isso faz com que eu me sinta menos preocupado em relação às informações que disponibilizo no site.
- ☐ Eu não penso muito nos riscos de publicar uma informação quando se trata de algo realmente importante para mim, porque isso não poderia deixar de fazer parte de meu perfil no FB.
- ☐ Eu acho que compartilhar informações e interagir com os outros pode ser mais útil e trazer mais benefícios do que as possíveis ameaças que eu possa sofrer em relação a minha

privacidade. Então, isso faz com que eu me sinta menos preocupado em relação às informações que disponibilizo através do FB.

() Eu me sinto menos preocupado em disponibilizar uma informação quando meus amigos fazem o mesmo.

() Eu confio no FB e acredito que o site não usará as informações que publico nem as compartilhará com terceiros. Então, isso faz com que eu me sinta menos preocupado em relação às informações que disponibilizo através do FB.

() Nenhuma das alternativas acima.

Questionário II

S U R V E Y

Por favor, responda as questões seguintes fornecendo apenas informações verdadeiras.
Não se identifique em nenhum dos campos deste formulário.

Ao preenchê-lo, você concorda com a utilização destas informações para fins científicos. Em contrapartida, nos comprometemos a preservar sua identidade e não associá-la às informações por você fornecidas.

Você só deve responder a esta pesquisa se você tem um perfil pessoal no Facebook (FB): (www.facebook.com).

Por favor, selecione corretamente os seus dados demográficos:

Sexo: () Masculino. () Feminino. **Idade:** _____. **Nacionalidade:** _____.

País em reside atualmente: _____.

Em que tipos de rede você entrou no Facebook?

() Ensino médio () Ensino superior () Local de trabalho () Região () Nenhuma

Se você participa de uma rede de instituição de Ensino Superior, diga-nos seu status:

() Aluno de graduação () Discente de pós-graduação () Ex-discente () Corpo docente ()

Equipe de funcionários

1. Com que frequência você acessa a sua conta no Facebook?

- a) mais de uma vez por dia.
- b) pelo menos uma vez por dia.
- c) de duas a três vezes por semana.
- d) pelo menos uma vez por semana.
- e) pelo menos uma vez por mês.
- f) passo mais de um mês sem verificar minha conta.

2. O Facebook é a rede social que você usa com mais frequência?

- a) Sim.
- b) Não, eu uso com mais frequência outra rede social (Orkut, LinkedIn, MySpace, etc.)
- c) Eu uso o Facebook tanto quanto eu uso outro site de rede social.

3. Quais dessas informações você publica em seu perfil e com que grau de precisão?

Data de nascimento

() Publico e a informação é verdadeira. () Publico e a informação é propositalmente incorreta. () Não publico.

Endereço de e-mail

() Publico e a informação é verdadeira. () Publico e a informação é propositalmente incorreta. () Não publico.

Telefone residencial

() Publico e a informação é verdadeira. () Publico e a informação é propositalmente incorreta. () Não publico.

Telefone celular

() Publico e a informação é verdadeira. () Publico e a informação é propositalmente

incorreta. () Não publico.

Filmes favoritos

() Publico e a informação é verdadeira. () Publico e a informação é propositalmente incorreta. () Não publico.

Nome

() Publico e a informação é verdadeira. () Publico e a informação é propositalmente incorreta. () Não publico.

Foto

() Publico uma foto minha (em que apareço sozinho(a) ou com outros) e é possível me identificar através dela. () Publico outro tipo de foto. () Não uso foto em meu perfil.

4. Marque todas as alternativas que se aplicam a você. Em geral, as informações que você coloca no FB:

- () são verdadeiras porque as pessoas que você conhece irão usá-las para saber mais sobre você.
- () são verdadeiras porque você só pode compartilhar seus interesses com outras pessoas se os expressa verdadeiramente.
- () são verdadeiras porque todo mundo também coloca informações verdadeiras em suas páginas.
- () são imprecisas porque você quer proteger sua privacidade.
- () são imprecisas porque você quer parecer mais legal e ser bem aceito socialmente.
- () nenhuma das alternativas acima.

5. Marque todas as opções que descrevem com que finalidades você usa ou já usou o Facebook.

- () Para manter contato com pessoas que conheço, antigos amigos, pessoas que não vejo com frequência e/ou pessoas que vivem em outra cidade/país de uma maneira barata e conveniente.
- () Para conhecer novas pessoas com interesses semelhantes.
- () Para me expressar na internet com liberdade.
- () Para compartilhar fotos e vídeos.
- () Para aumentar minha popularidade entre meus amigos.
- () Para fazer contatos profissionais.
- () Para encontrar um namorado(a).
- () Para me divertir com os jogos e aplicativos disponíveis.
- () Para mostrar aos outros fatos sobre minha vida e minha personalidade.
- () Para passar aos outros uma imagem positiva e ser bem aceito socialmente.

6. Marque, na relação dos seguintes tipos de amigos listados abaixo, aqueles que você adiciona, aceita e recusa quando é adicionado.

Amigo que você adiciona	Amigos que você aceita quando é adicionado	Amigos que você recusa quando é adicionado
() Amigos próximos	() Amigos próximos	() Amigos próximos
() Pessoas conhecidas	() Pessoas conhecidas	() Pessoas conhecidas
() Pessoas das quais não gosto muito	() Pessoas das quais não gosto muito	() Pessoas das quais não gosto muito
() Pessoas que encontrei apenas uma vez na vida	() Pessoas que encontrei apenas uma vez na vida	() Pessoas que encontrei apenas uma vez na vida
() Desconhecidos	() Desconhecidos	() Desconhecidos

7. Marque as alternativas que descrevem seu comportamento em relação aos amigos no Facebook.

- ☐ () Eu aceito pessoas desconhecidas como amigos ou as adiciono para aumentar meu número de amigos.
- ☐ () Eu não adiciono pessoas desconhecidas ou as aceito como amigos quando sou adicionado porque os amigos podem ver meu perfil, e eu não gostaria que estranhos vissem as informações que publico no meu FB.
- ☐ () Nenhuma das alternativas acima.

8. Você leu a política de privacidade do Facebook antes de se cadastrar no site?

- ☐ () Sim. ☐ () Não. ☐ () Li parcialmente.

9. Você leu os termos de uso do Facebook antes de se cadastrar no site?

- ☐ () Sim. ☐ () Não. ☐ () Li parcialmente.

10. Você já alterou as configurações de privacidade de sua conta no FB?

- a) Sim, apenas uma vez.
- b) Sim, mais de uma vez.
- c) Não, porque não sei como fazer isso.
- d) Não, porque estou satisfeito com as configurações de privacidade que o FB definiu para mim como padrão.
- e) Eu não me lembro se já alterei minhas configurações de privacidade.

11. Em quais dessas situações você lê o perfil de alguém? Marque abaixo as alternativas que se aplicam a você.

- ☐ () Eu costumo visitar o perfil de meus amigos para saber novidades sobre suas vidas.
- ☐ () Eu já usei o FB para checar se uma informação que me disseram sobre alguém era verdadeira.
- ☐ () Eu já usei o FB para saber informações sobre um conhecido, um novo colega de classe ou sobre alguém em que estava interessado(a).
- ☐ () Eu às vezes visito perfis de amigos ou de pessoas que não conheço para me divertir vendo fotos e sabendo o que eles escrevem sobre eles mesmos, suas experiências de vida, seus gostos e suas relações sociais.
- ☐ () Eu já procurei informações sobre um ex-namorado ou alguém de quem não gosto.
- ☐ () Nenhuma das alternativas acima.

12. Você se importaria se soubesse que alguém visitou o seu perfil no FB?

- ☐ () Sim, se fosse alguém que não conheço.
- ☐ () Sim, se fosse uma pessoa de quem eu não gosto.
- ☐ () Não, eu não me preocupo se outras pessoas vêem meu perfil.
- ☐ () Eu ficaria desapontado se as pessoas não vissem meu perfil.
- ☐ () Nenhuma das alternativas acima.

13. Que aplicativos você utiliza no Facebook?

14. Marque todas as alternativas que se aplicam a você. Quando você adiciona um novo aplicativo ao seu perfil no Facebook, você:

- ☐ O adiciona porque algum amigo também faz uso dele e ele parece ser legal.
- ☐ O adiciona porque ele é divertido ou útil.
- ☐ Se preocupa em permitir que terceiros tenham acesso às informações que você disponibiliza em seu perfil.
- ☐ Lê cuidadosamente os termos de uso e a política de privacidade do aplicativo.
- ☐ Sempre visita a página do aplicativo para definir suas configurações de privacidade.
- ☐ Nenhuma das alternativas acima.

15. Você já ouviu falar em:

Portabilidade de dados

☐ Sim ☐ Não

Mecanismos de busca de pessoas (Rapleaf.com; Upscoop.com; etc.)

☐ Sim ☐ Não

16. Marque se as alternativas abaixo são verdadeiras ou falsas.

Quando um amigo seu adiciona um aplicativo, o aplicativo também terá acesso a todas as informações que este seu amigo pode ver sobre você, a não ser que você limite este acesso através das suas configurações de privacidade.

☐ verdadeiro ☐ falso ☐ não sei

Os anúncios mostrados a você no FB estão relacionados ao conteúdo do seu perfil.

☐ verdadeiro ☐ falso ☐ não sei

O Facebook pode compartilhar as informações do seu perfil com terceiros. Nesses casos, o FB não o identifica pessoalmente a estas partes e não lhe informa nem que tipo de informação é compartilhada nem com quem.

☐ verdadeiro ☐ falso ☐ não sei

O Facebook coleta a informação que você coloca em seu perfil e informações de outras fontes (jornais, blogs, etc.) para lhe oferecer uma experiência personalizada no site.

☐ verdadeiro ☐ falso ☐ não sei

ANEXO C: ANÁLISE DE PERFIS

Nome	Desvio Padrão Corrigido
Universidad Catolica Argentina	2,5%
Argentina	2,3%
UBC	2,0%
Vancouver	1,8%
Toronto	1,9%
UVM	1,7%
Chile	1,6%
UIS	1,3%
Colômbia	2,4%
UDG	1,8%
México	1,8%

Fig. 1: Desvios-padrão para cada uma das redes estudadas. Cálculos elaborados com a metodologia disponível em KALTON, 1983.

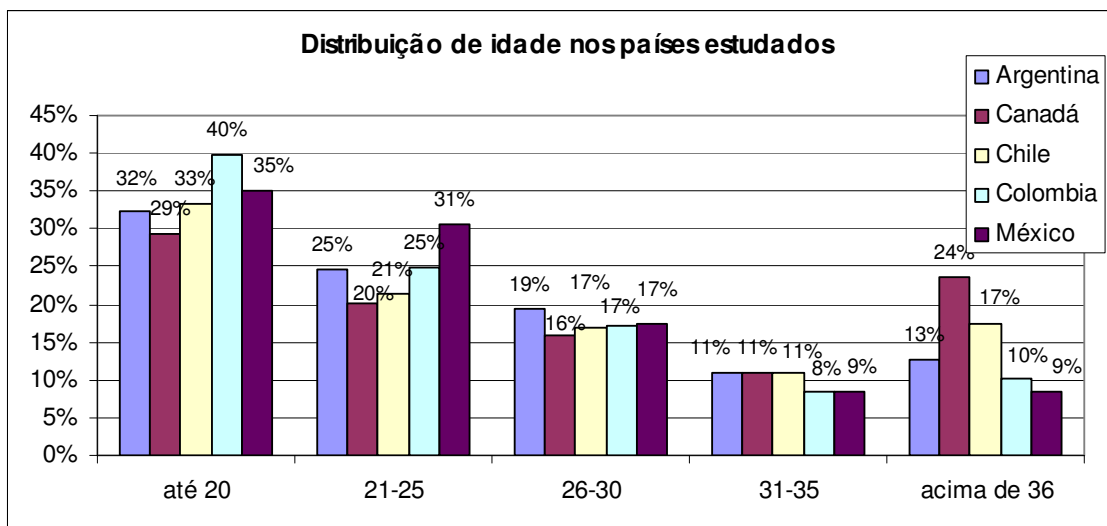


Fig. 2: Distribuição de idade nos países estudados, com base nos dados fornecidos pelo sistema de direcionamento de anúncios do Facebook. Coleta realizada em 23/02/09.

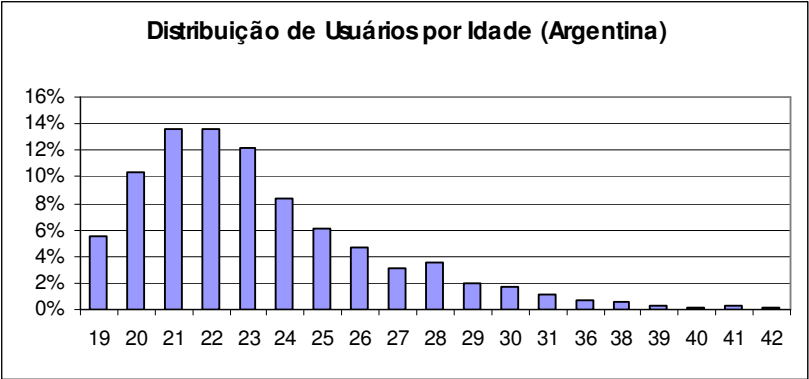


Fig. 3: Distribuição de idade na rede Argentina (considerando apenas os que declararam esta informação).

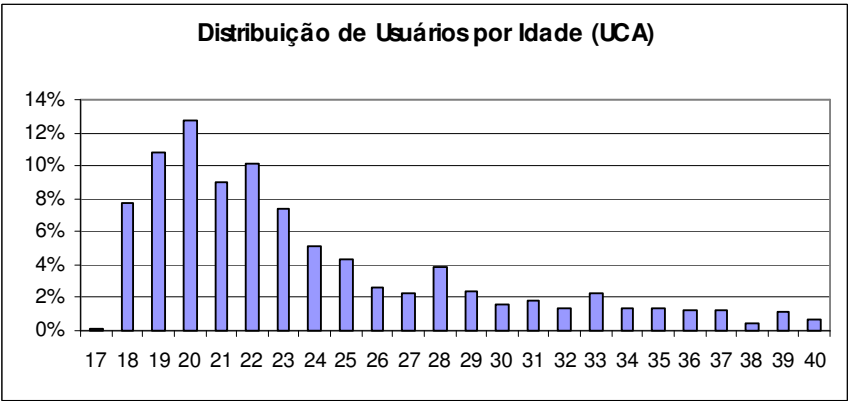


Fig. 4: Distribuição de idade na rede UCA (considerando apenas os que declararam esta informação).

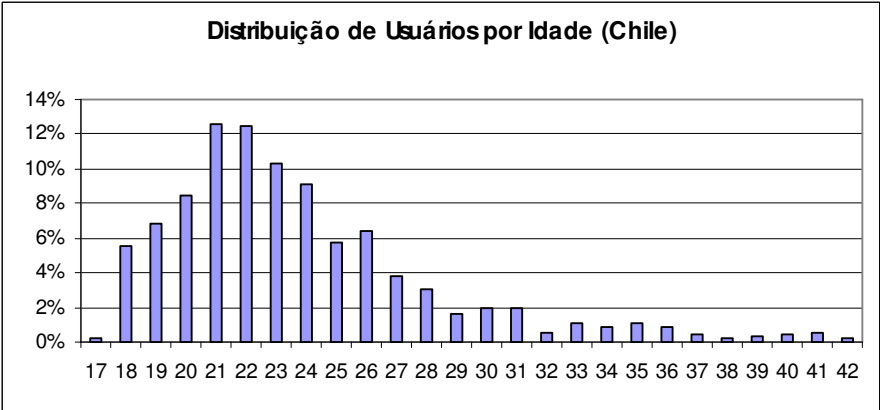


Fig. 5: Distribuição de idade na rede Chile (considerando apenas os que declararam esta informação).

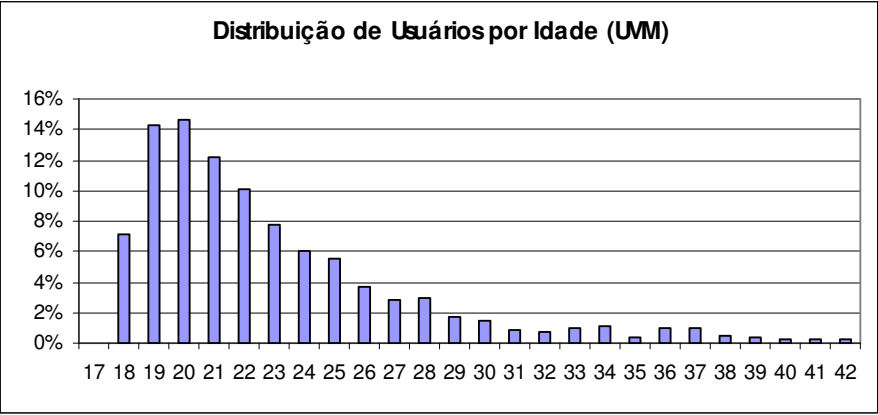


Fig. 6: Distribuição de idade na rede UVM (considerando apenas os que declararam esta informação).

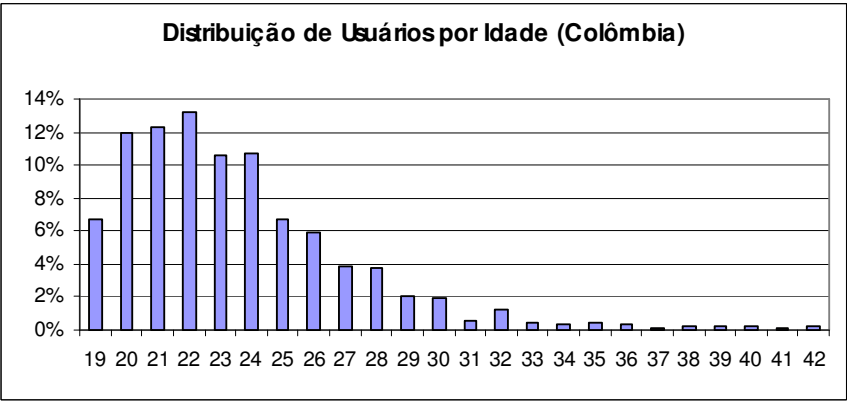


Fig. 7: Distribuição de idade na rede Colômbia (considerando apenas os que declararam esta informação).

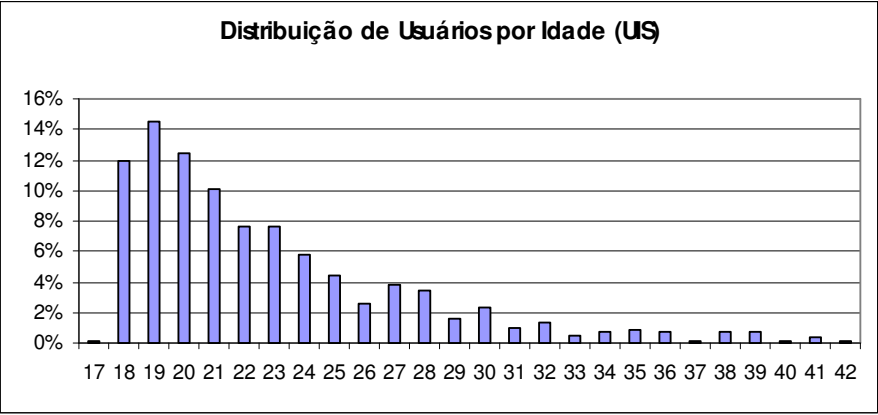


Fig. 8: Distribuição de idade na rede UIS (considerando apenas os que declararam esta informação).

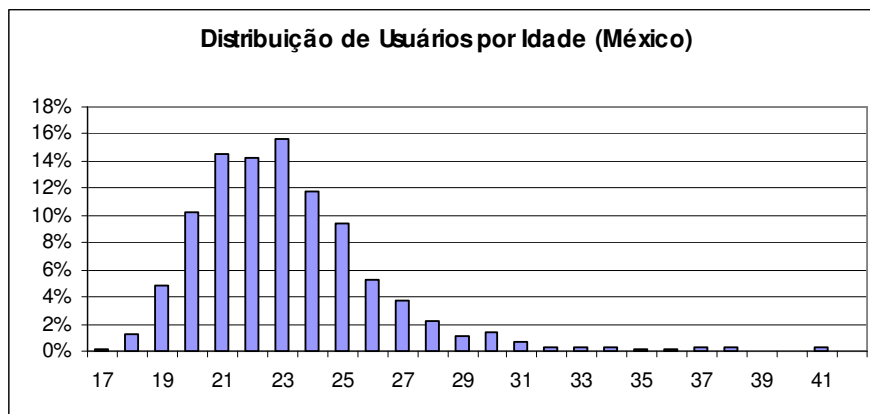


Fig. 9: Distribuição de idade na rede México (considerando apenas os que declararam esta informação).

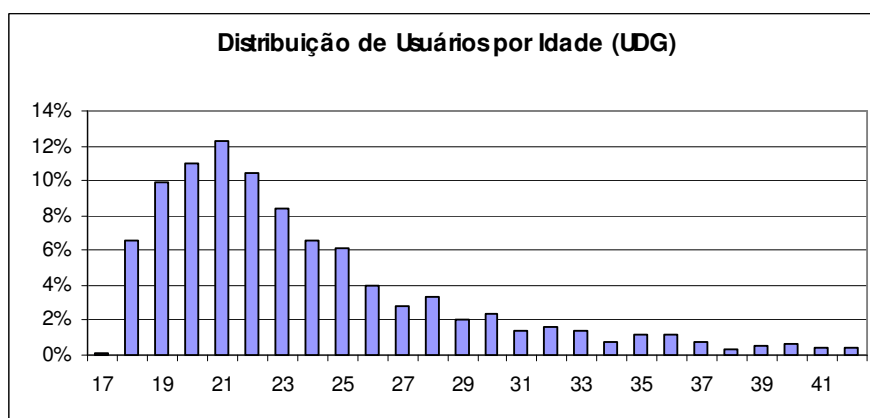


Fig. 10: Distribuição de idade na rede UDG (considerando apenas os que declararam esta informação).

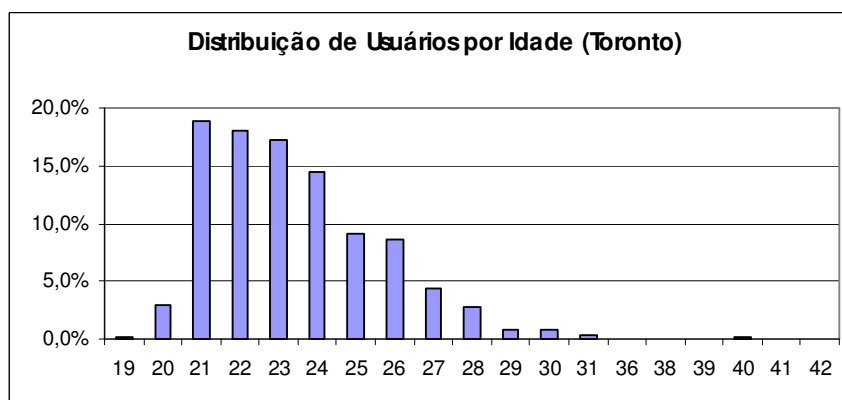


Fig. 11: Distribuição de idade na rede Toronto (considerando apenas os que declararam esta informação).

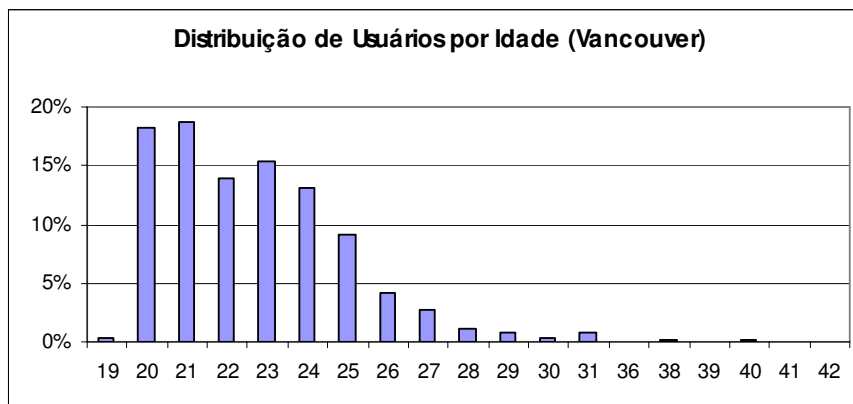


Fig. 12: Distribuição de idade na rede Vancouver (apenas os que declararam esta informação).

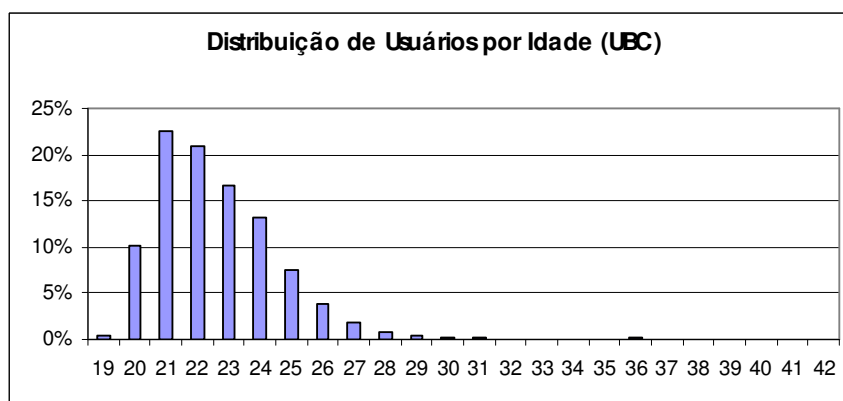


Fig. 13: Distribuição de idade na rede UBC (considerando apenas os que declararam esta informação).

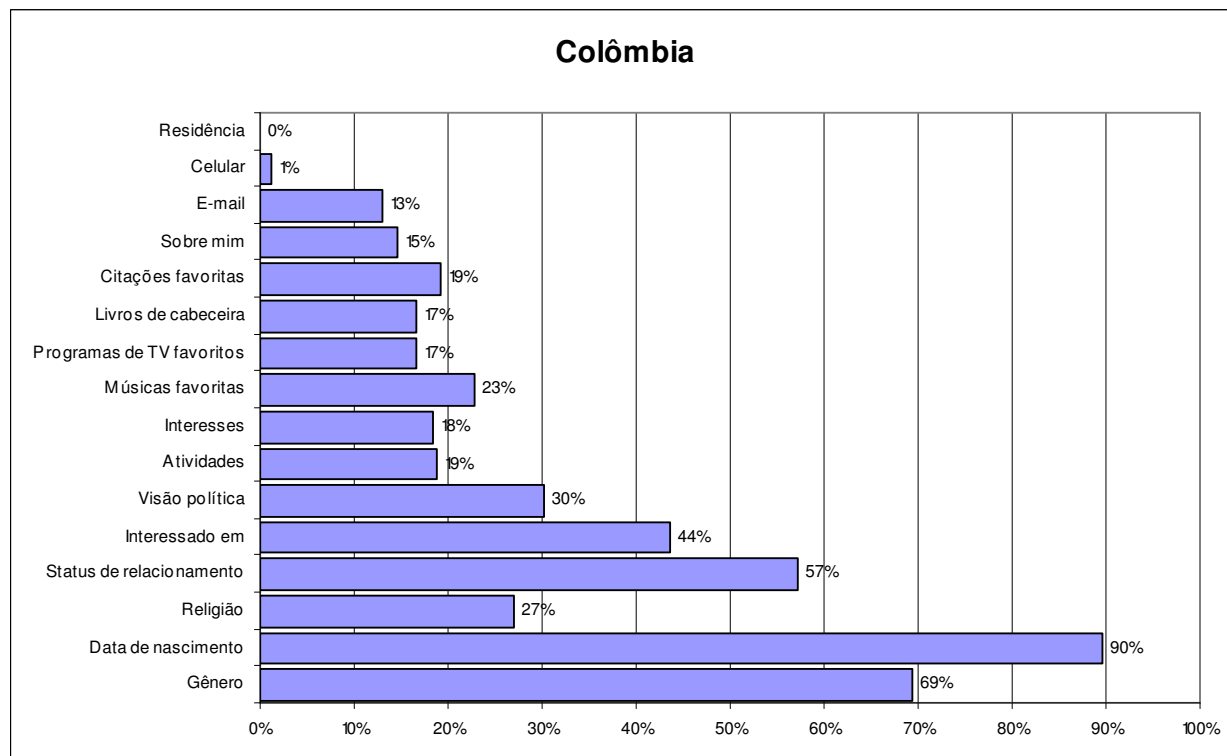


Fig. 14: Informações disponibilizadas na rede Colômbia.

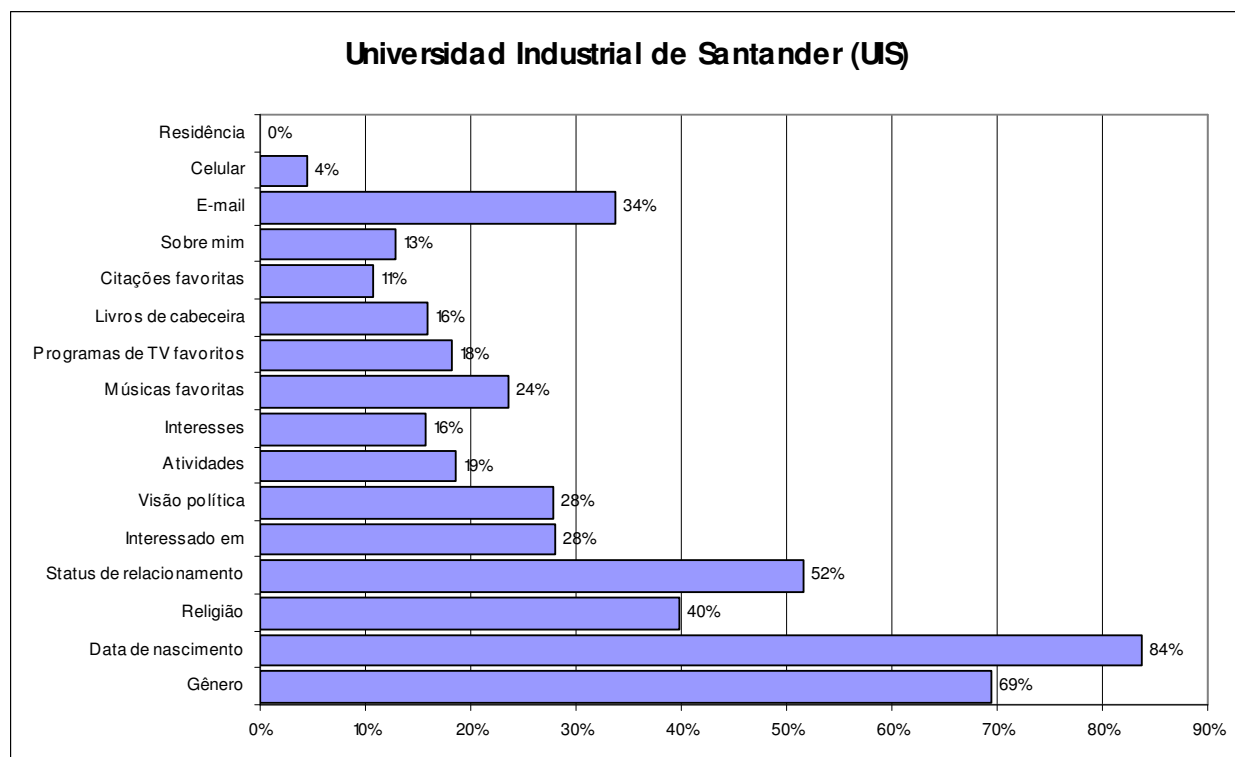


Fig. 15: Informações disponibilizadas na rede UIS.

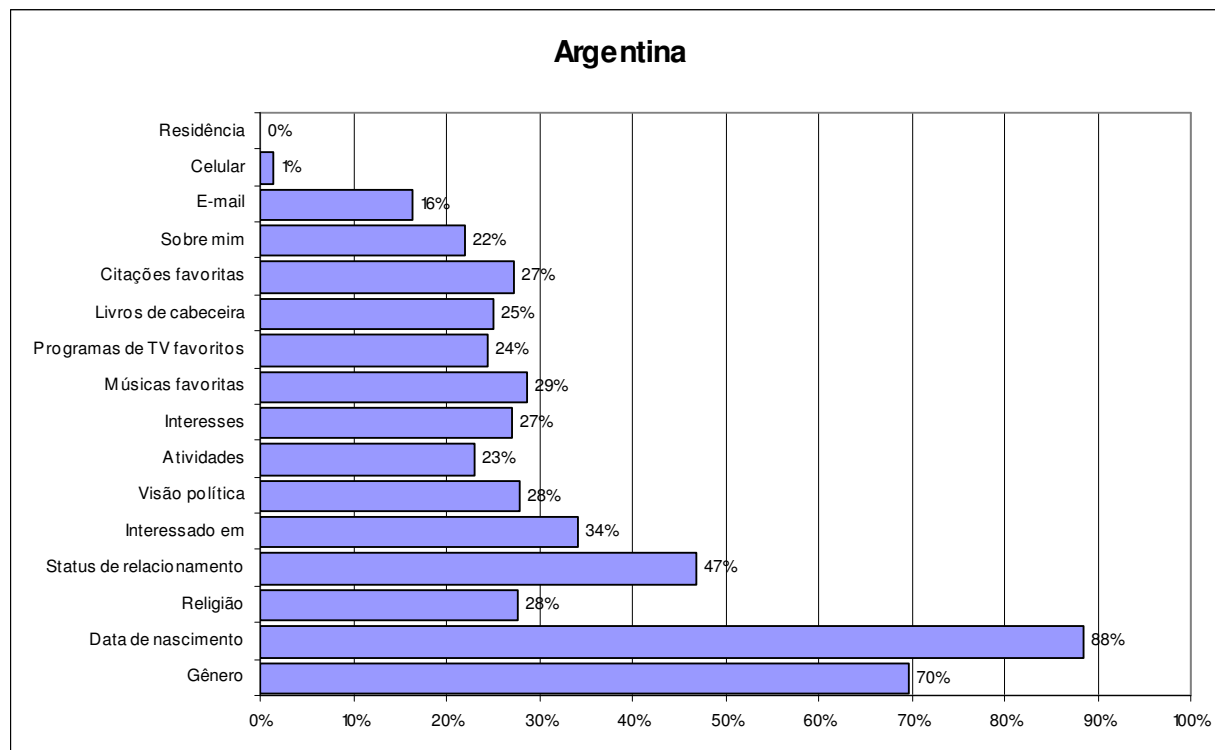


Fig. 16: Informações disponibilizadas na rede Argentina.

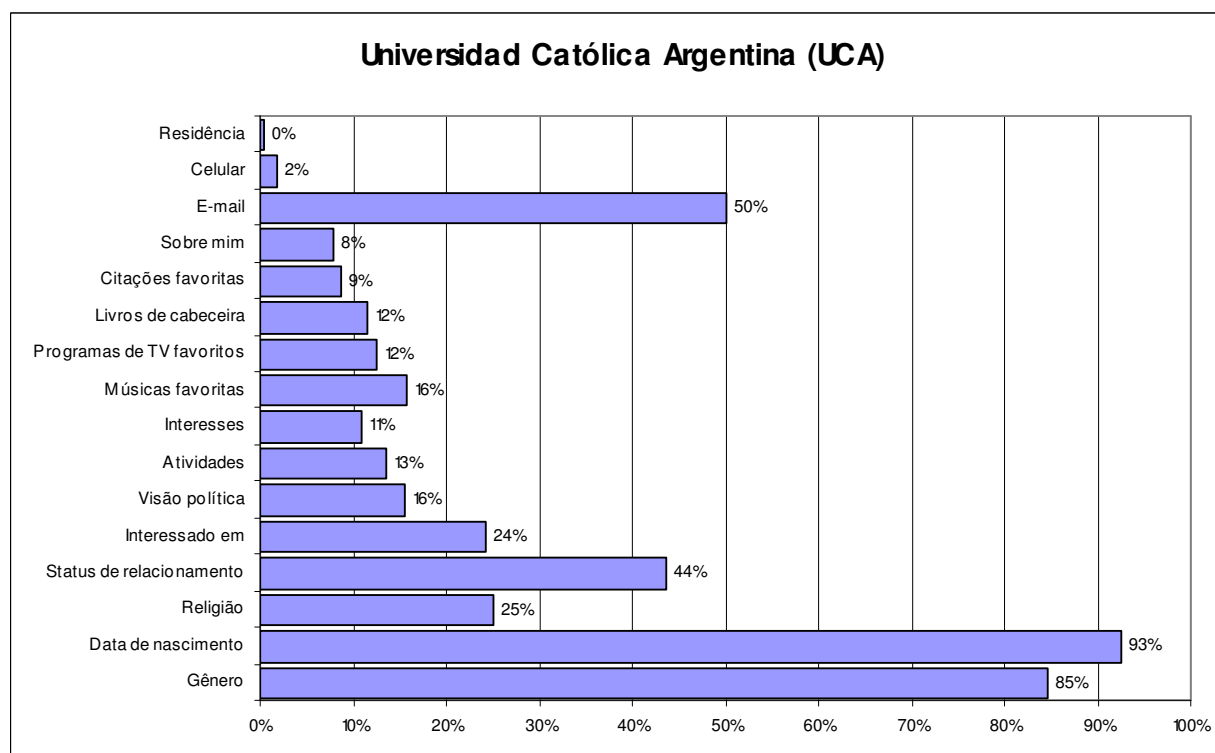


Fig. 17: Informações disponibilizadas na rede UCA.

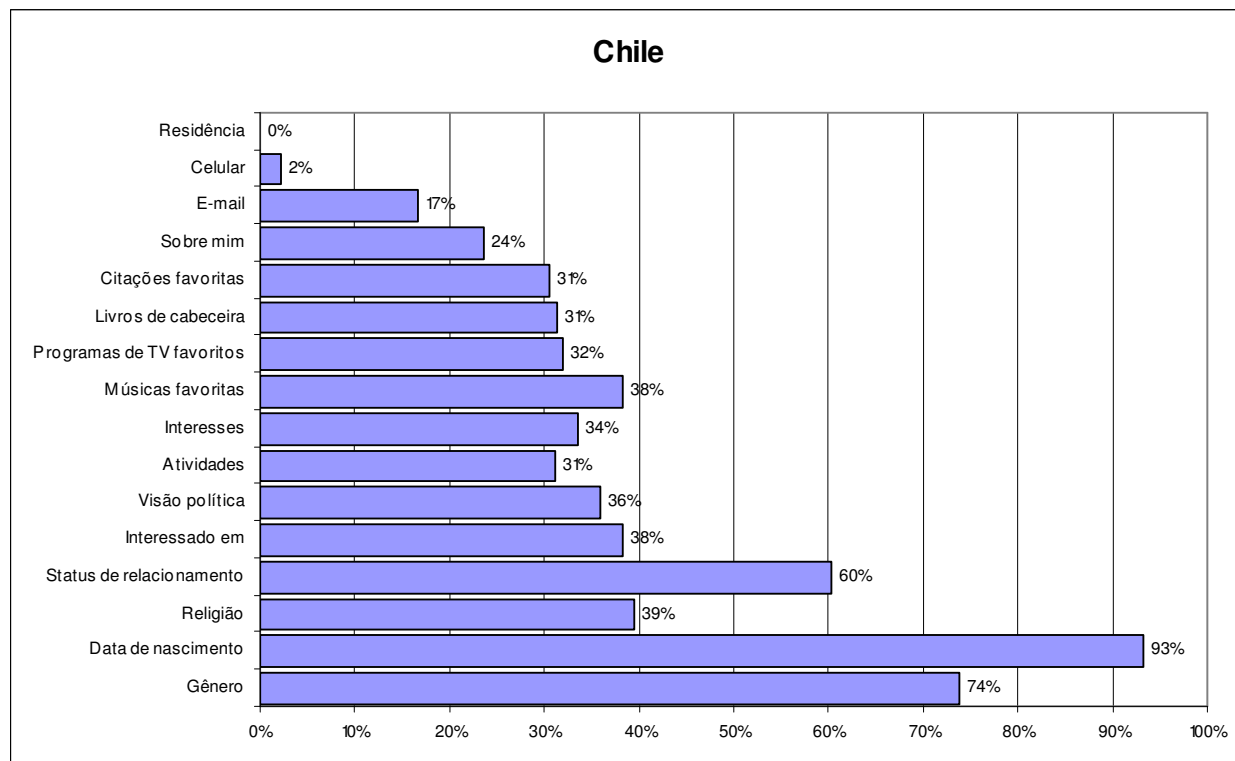


Fig. 18: Informações disponibilizadas na rede Chile.

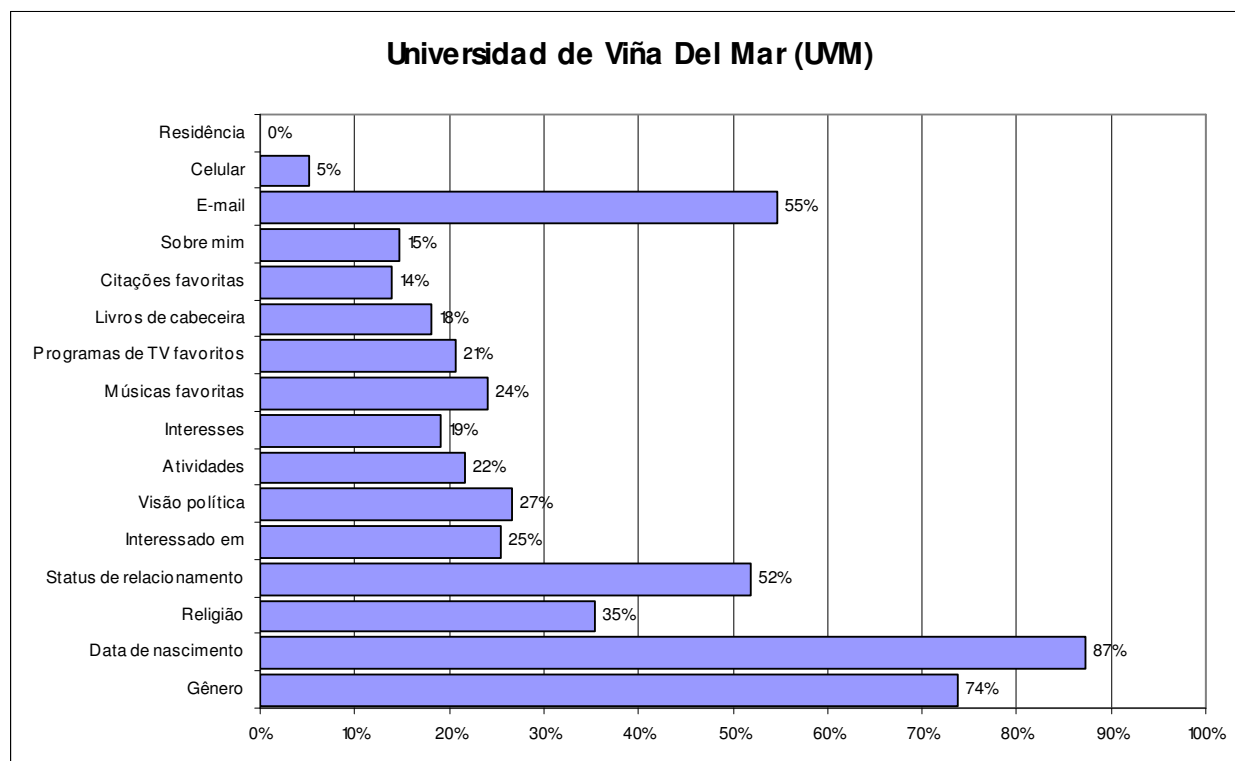


Fig. 19: Informações disponibilizadas na rede UVM.

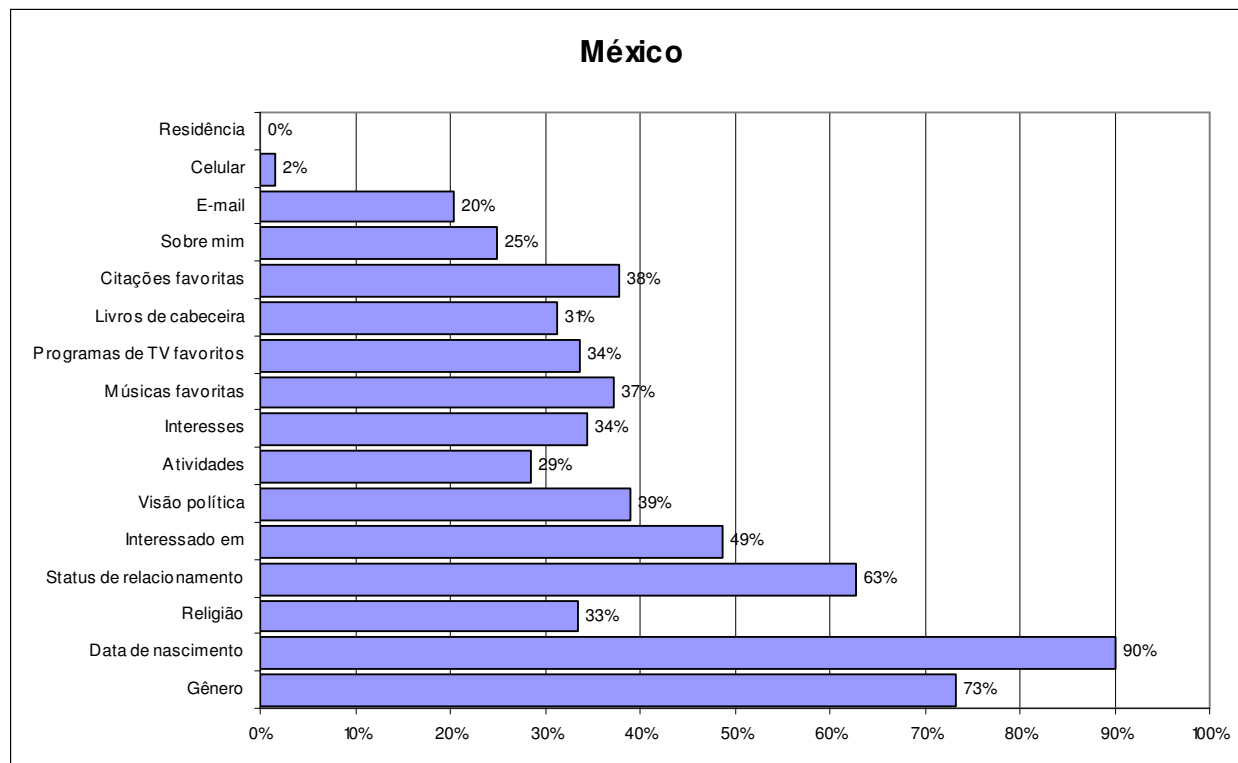


Fig. 20: Informações disponibilizadas na rede México.

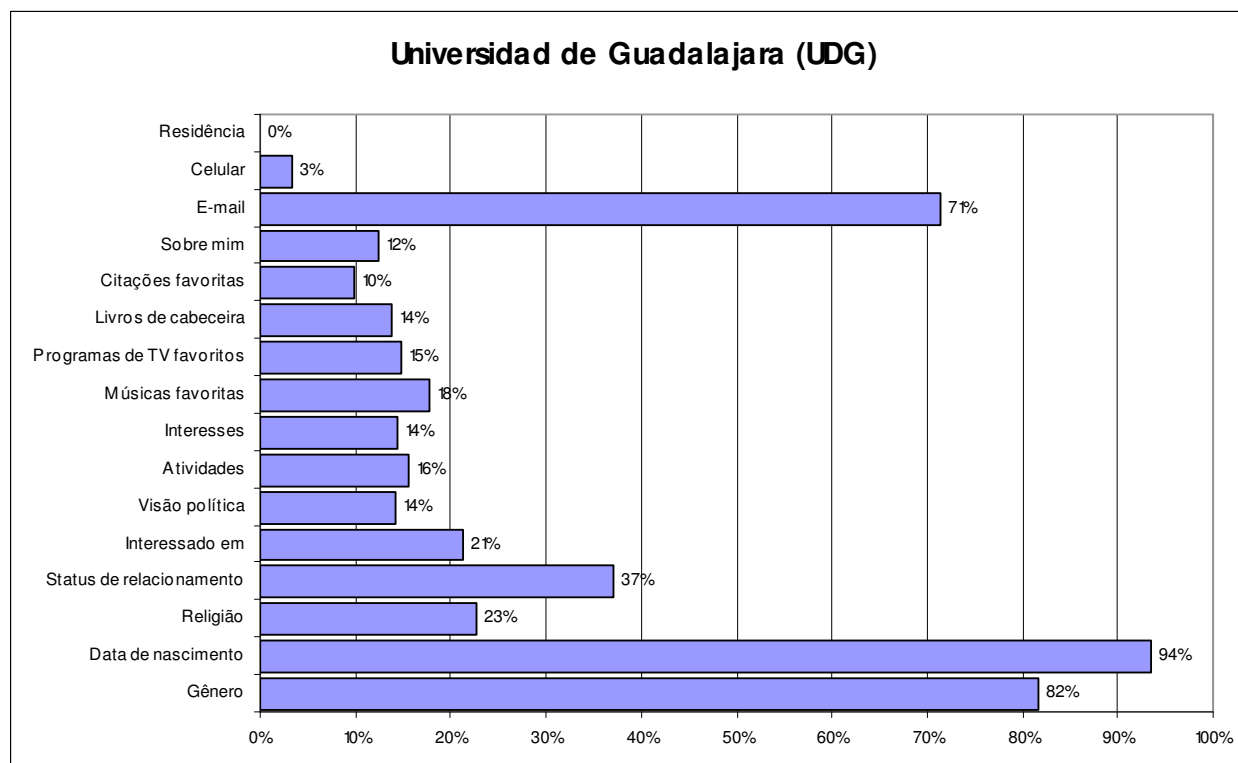


Fig. 21: Informações disponibilizadas na rede UDG.

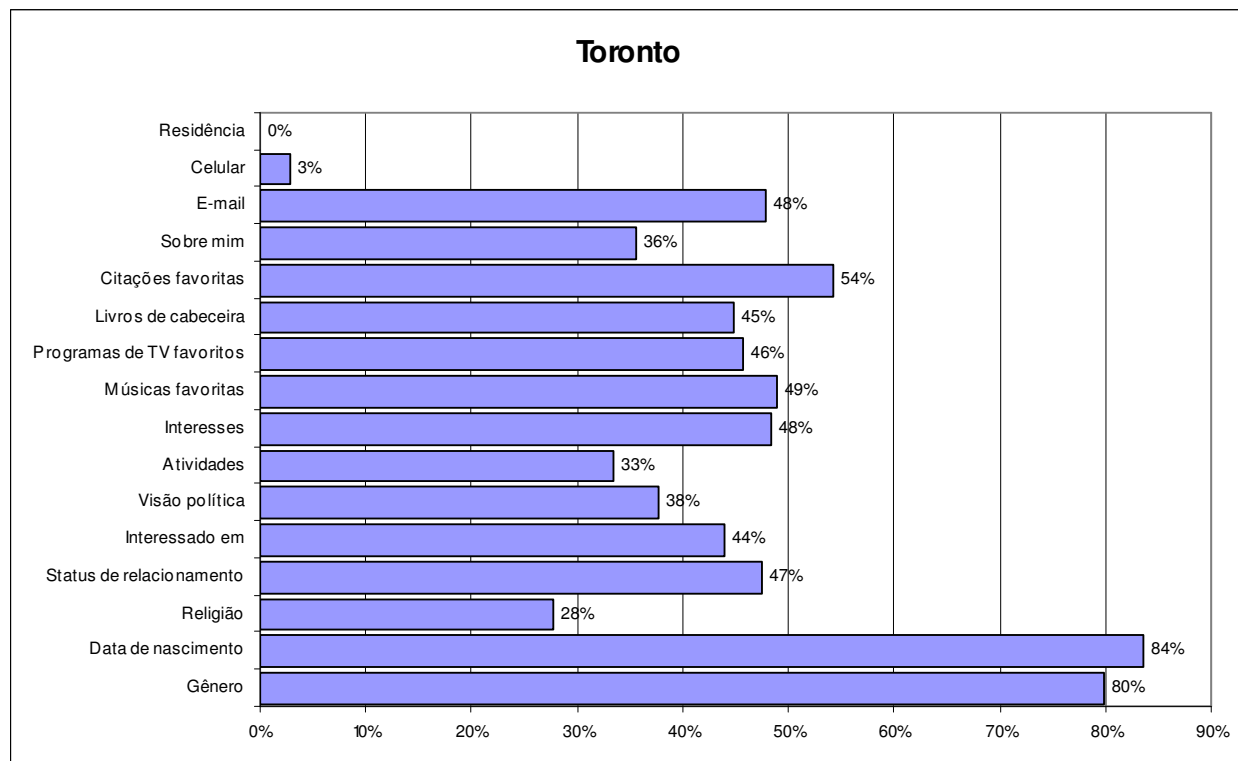


Fig. 22: Informações disponibilizadas na rede Toronto.

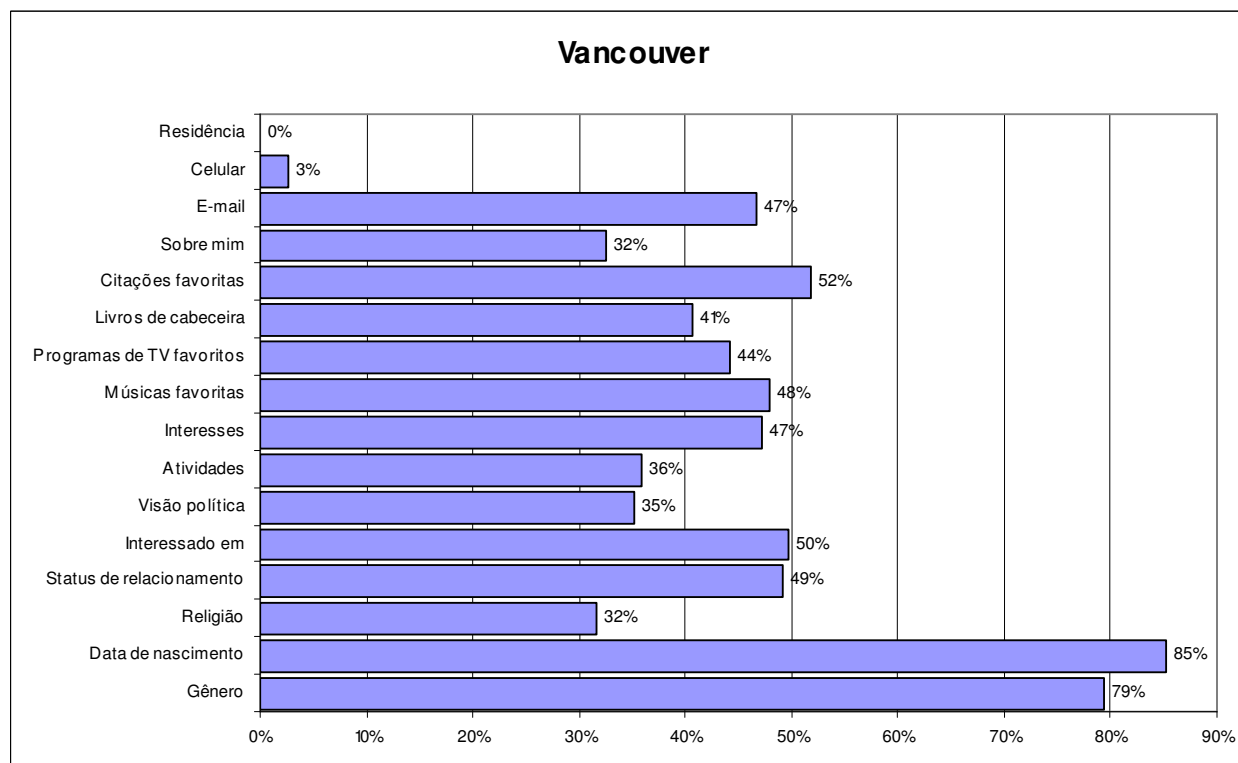


Fig. 23: Informações disponibilizadas na rede Vancouver.

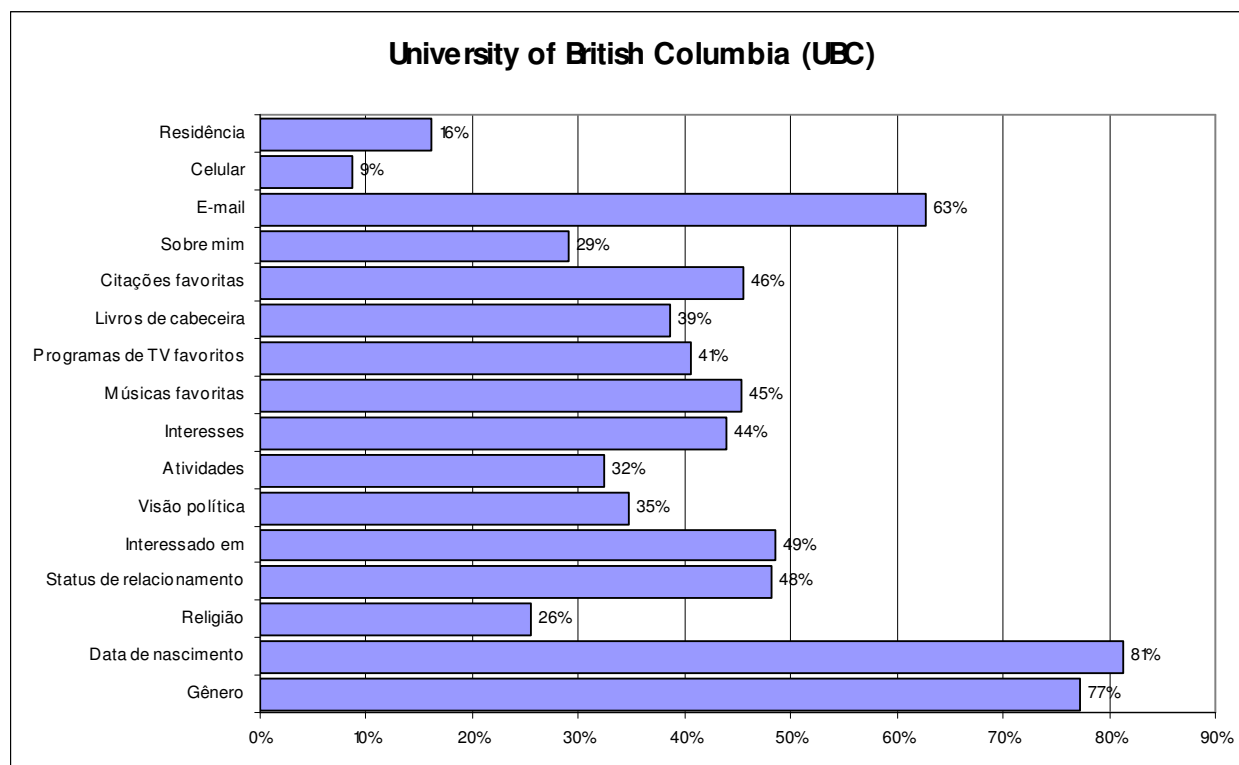


Fig. 24: Informações disponibilizadas na rede UBC.