

De que vigilância estamos falando?

André Lemos¹

Agora, no momento em que começo a escrever este relato crítico do texto de Fernanda Bruno, “Mapas de crime. Vigilância distribuída e participação na cibercultura”, vejo uma notícia informando que uma universidade japonesa distribui *iPhones*, de graça, com o intuito de vigiar, nominalmente, os alunos e os professores. O sistema sabe, por GPS, o posicionamento de cada um e informa se eles estão ou não em sala de aula. De acordo com a matéria da Reuters, “Universidade japonesa usa *iPhone* para checar frequência”²,

“... assim que os alunos entrarem na sala de aula, em vez de escreverem o nome em uma folha, eles simplesmente digitam um número de identificação e um número de classe específico em uma aplicação criada para o iPhone. Para evitar que os estudantes façam isso em casa ou fora da sala de aula, o aplicativo utiliza dados de localização por satélite e verifica por qual roteador o aluno fez o registro no aparelho.”

Imediatamente me vem à memória outras formas de vigilância com as mídias locativas como, por exemplo, o trabalho do grupo londrino LOCA, “*Set to Discoverable*”³, apresentado no ISAE 2006. Nesta intervenção urbana, os artistas monitoram, controlam e vigiam os passantes da rua através de um rastreamento dos dispositivos móveis com redes *bluetooth* abertas. Sensores detectam as redes abertas de cada usuário e enviam mensagens individuais do tipo: “*por que você saiu do banco da praça*”, “*you já passou por aqui antes*”, etc. Como afirmam os artistas:

“Loca is an exercise in everyday surveillance, tracking digital bodies in physical space. It examines what happens when it is easy for everyone to track everyone, when surveillance can be affected by consumer level technology within peer-to-peer networks without being routed through a central point. The Loca project walks the knife-edge of locative media, itself involving surveillance. But it does not create a new surveillance potential, it only reveals what was already there.”

Outro exemplo é o sistema de redes sociais móveis do Google, o “Google Latitude”, onde pessoas podem rastrear amigos e conhecidos próximos, através de um celular equipado com um GPS, afim de realizar encontros “reais” nos espaços das cidades. O sistema, como mostrei no “Carnet de Notes”⁴, tem servido às empresas para vigiar nominalmente os seus funcionários. Escrevia na ocasião:

“(...) o Google Latitude é um interessante instrumento para criação de redes sociais móveis, mas pode também servir como instrumento de vigilância. (...) Matéria da [PC](#)

1 Professor Associado da Faculdade de Comunicação da UFBA – <http://andrelemos.info>

2 <http://br.tecnologia.yahoo.com/article/28052009/5/noticias-tecnologia-universidade-japonesa-iphone-quecar.html>

3 <http://www.loca-lab.org/settodiscoverable/>

4 http://www.andrelemos.info/2009/02/google-latitude_07.html

World, (...) mostra como as empresas podem usá-lo para espionar funcionários. (...) 'It's easy to think of business uses for Latitude, such as tracking service people as they move from call-to-call. (...) The downside of Latitude is the amount of extremely personal information, such as the details of all a person's travels that is sent to Google (...).' A organização Privacy International, baseada em Londres, afirma em relatório que esse tipo de vigilância já está sendo usado por empresas (...) 'without the knowledge or consent of their users'."

Recentemente, em artigo apresentado no "I Simpósio Internacional sobre Vigilância na América Latina" (Lemos, 2009), afirmava que as novas formas de vigilância com as mídias locativas são sutis, invisíveis, utilizando novos dispositivos móveis, redes sem fio e sensores espalhados pelo espaço urbano. As mídias locativas (este conjunto de tecnologias, redes e sensores sensíveis ao contexto local), ampliam as formas mais tradicionais de ameaça à privacidade e ao anonimato, como os sistemas de escuta ou as câmeras de vigilância. Podemos ainda pensar na vigilância eletrônica com *hackings*, roubo de senhas, clonagem de identidades, etc. Os sistemas eletrônicos ampliam e possibilitam novas ações de vigilância. Em um mundo cada vez mais interligado por redes telemáticas e bancos de dados, estes sistemas propõem instrumentos de controle, de monitoramento e de vigilância cada vez mais performáticos e distribuídos. É necessário, no entanto, diferenciar estas ações a fim de evitar um visão generalizante.

"Controle, monitoramento e vigilância informacionais, palavras que em muitos momentos podem parecer sinônimas, devem ser diferenciadas aqui para um melhor entendimento do problema. Compreendemos controle como fiscalização de atividades, como ações normalmente associadas a governo e ao domínio de pessoas, ações, processos. Monitoramento pode ser entendido como forma de observação para acumular informações visando projeções ou construção de cenários e históricos, ou seja, como uma ação de acompanhamento e de avaliação de dados. Já vigilância pode ser definida como um ato com vistas a evitar algo, como uma observação com fins de prevenção, como um comportamento atencioso, cauteloso ou zeloso. (...) Vamos definir vigilância (...) de acordo com Gow. Para o autor, vigilância *'implies something quite specific as the intentional observation of someone's actions or the intentional gathering of personal information in order to observe actions taken in the past or future'* (GOW, 2005, p. 8)." (Lemos, 2009)

De acordo com esta definição, ações de vigilância pressupõem monitoramento e controle, mas nem toda forma de controle e/ou monitoramento podem ser chamadas de vigilantes. Os exemplos no começo deste relato remetem a ações nominais com vistas a evitar ou causar algo. São assim, ações de vigilância. Poderíamos dizer que toda forma de vigilância exigiria dois elementos: uma intencionalidade, com vistas a evitar/causar algo, e uma identificação nominal de indivíduos ou grupos. Me parece difícil compreender vigilância sem identificação do vigiado (anônima) e sem intenção preventiva (evitar algo). Me parece exagerado dizer, por exemplo, que o sistema de controle e monitoramento das minhas ligações telefônicas pela operadora do meu telefone celular, está me

vigiando. Aqui há identificação mas não intenção. No entanto, ele pode, certamente, ser usado para isto. A polícia federal pode pedir a quebra do sigilo telefônico e vigiar meus contatos telefônicos. O mesmo pode ser dito do controle e do monitoramento feito dos usuários nos transportes públicos. Isso faz parte da rotina administrativa das empresas. Mais uma vez, o sistema, no entanto, pode acolher ações de vigilância (algum suspeito pode ser vigiado pelos sistemas de seguranças das empresas e/ou da polícia). Notem, neste caso, a recente implementação do cartão “Navigo”, na França, que vai substituir a analógica “*Carte Orange*”. Com a “*Carta Orange*” há um controle e monitoramento dos usuários (a RATP sabe quantos usam o serviço) mas não vigilância. Entretanto, com o cartão “Navigo”, há uma **possibilidade** mais explícita de vigilância, já que o cartão tem um registro nominal do usuário (havendo aqui intenção e identificação). Escrevia no Carnet de Notes:

“(…) Este novo cartão digital permitirá à empresa saber quando, onde e por que transporte uma pessoa se desloca pelo país. Segundo o blog [BugBrother](#), o Navigo tem foto, nome, sobrenome, endereço e um chip RFID que associa a um número único os trajetos do cidadão na rede de transporte. (...) Matéria do [Le Monde](#) informa que a [CNIL](#), "Commission Nationale de l'Informatique et des Libertés", considera o novo cartão uma real ameaça ao anonimato e à vida privada. A CNIL afirma que "*l'exercice du droit des usagers à se déplacer anonymement n'est pas garanti?*" (...)”⁵

O artigo de Fernanda Bruno aponta para importantes questões relativas às formas de controle, monitoramento e vigilância e mostra como estas são práticas correntes e em expansão na cibercultura. Não há dúvidas em relação a isto. O ponto que quero problematizar é se não haveria uma excessiva ênfase em identificar alguns procedimentos (que estariam na minha opinião mais para ações de controle e monitoramento) como ações distribuídas de vigilância. Como mostrei rapidamente nos exemplos acima, me parece que em redes sociais, mapas colaborativos, dispositivos móveis, redes sem fio, e nos diversos e inúmeros bancos de dados que compõem a sociedade da informação, há efetivamente controle, monitoramento e possibilidade reais de vigilância. A minha questão é se podemos generalizar para TODAS estas ações e sistemas o adjetivo de vigilantes (uma “vigilância imanente” como afirma a autora). Não me parece que, ao usar o “Facebook” eu esteja sendo vigiado (as informações são protegidas e não há intencionalidade). Mas o “Facebook” pode ser usado para vigiar (se houver quebra da proteção dos meus dados pessoais e uma intenção com vistas a evitar ou causar algo).

Bruno está correta ao afirmar que a vigilância pode ser definida como “*a atividade de observação sistemática e focalizada de indivíduos, populações ou informações relativos a eles, tendo em vista extrair conhecimento e intervir sobre os mesmos, de modo a governar suas condutas ou subjetividades.*” Mas não diferencia vigilância, controle e monitoramento. Tudo é vigilância. Segundo a autora, teríamos hoje, com os sistemas participativos e redes sociais uma perigosa ampliação das formas de observação dos indivíduos, consolidando o que ela chama de “vigilância distribuída”. Esta pode ser definida como:

5 <http://www.andrelemos.info/2009/01/mobilidade-e-anonimato.html>

“(...) uma vigilância que tende a se tornar ubíqua e incorporada a diversos dispositivos, serviços e ambientes que usamos cotidianamente, mas que se exerce de modo descentralizado, não hierárquico e com uma diversidade de propósitos, funções e significações nos mais diferentes setores (...)”.

A autora questiona a posição de que as ações de vigilância seriam realizadas com o objetivo de observar um indivíduo, nominalmente, com vistas a evitar algo, como defini mais acima. Contrariamente ao que afirmo, ela tenta demonstrar que estas ações “*não mais se restringem nem se justificam por grupos suspeitos ou supostamente perigosos, mas que podem ser todos e qualquer um – consumidores, transeuntes, internautas, criminosos, participantes de reality shows etc.*”. Mais ainda:

“Pelas características mencionadas, nota-se logo que a vigilância distribuída não se confunde com uma vigilância hiper-panóptica, a qual supõe sistemas centralizados, hierarquizados, dirigidos a grupos ou indivíduos previamente delimitados cujas identidades supostamente portam uma periculosidade que demanda vigilância e se inscreve num projeto de normalização. Ainda que aspectos desses sistemas persistam hoje, a vigilância contemporânea se complexificou em relação aos modelos modernos, ganhando novos sentidos, modos de atuação, efeitos.”

Assim, os sistemas sociais estariam todos imersos neste regime de vigilância (vejam no meu destaque abaixo que vigilância equivale a monitoramento, sem diferenciação):

“Não há, por exemplo, redes sociais (Myspace, Facebook, Orkut) com suas práticas de sociabilidade isentas de qualquer forma de **vigilância ou monitoramento**, e um aparato de vigilância adicional que se apropriaria delas. Ao contrário, os sistemas de **vigilância e monitoramento** são imanentes a tais redes e são parte integrante tanto da eficiência do sistema, que monitora, arquiva e analisa os dados disponibilizados pelos usuários de modo a otimizar seus serviços, quanto das relações sociais que aí se travam, as quais encontram um de seus motores na vigilância mútua e consentida, com pitadas de voyeurismo e exibicionismo.”

É interessante a ampliação do conceito aqui proposto e parece mesmo instigante pensar formas de vigilância distribuídas e ampliadas. Mas uma ampliação deste porte não enfraqueceria a carga semântica do conceito? Não seria excessivo colocar, sem distinção, controle, monitoramento e vigilância e ampliar esta última para toda e qualquer forma de captação de informação? Me parece, e insisto mais uma vez, que há formas de controle e de monitoramento nas redes sociais, mas que não podemos colocá-las como imaneamente vigilantes. Mais uma vez, para haver vigilância é preciso um acompanhamento sistemático, personalizado, nominal, intencional, com vistas a evitar ou causar algo a quem se vigia. Continuo, reconheço, preso à uma definição mais tradicional, policial e/ou jurídica de vigilância. Reconheço também os novos tempos e os novos dispositivos, mas não estou convencido de que controle, monitoramento e vigilância sejam a mesma coisa, ou que sistemas (as redes sociais) que colhem dados não nominais e cruzam com bancos de dados de outros sistemas com dados também não

nominais estariam sendo constituídos sobre uma base imanentemente vigilante. Ao me ver, estes sistemas monitoram e controlam e isso é perigoso justamente por poder acarretar, **a posteriori**, forma de vigilância individual ou grupal. Reconheço a pró-atividade dos perfis, mostrada pela autora em outros textos, e como esse controle e vigilância podem me afetar no cotidiano, mas mesmo assim, me parece um pouco desproporcional colocar as trocas de dados, e mesmo o voyeurismo e o exibicionismo como ações iminentemente de vigilância. Como a autora diferencia controle, monitoramento e vigilância? A vigilância distribuída seria qualquer forma de captação de informação em redes telemáticas?

No análise específica sobre os mapas de crime, a ação me parece efetivamente próxima de um olhar vigilante. Aqui os participantes estão desempenhando ações, colaborativas e anotativas – os mapas - com vistas a denunciar algo (há intenção – evitar o crime e é nominal – assalto na Rua X, assassinato na Rua Y). Este é um olhar atento e vigilante com o intuito (ilusório) de denunciar e impedir que algo aconteça no futuro, aumentando o sentimento de insegurança. Veja que, no meu entendimento, esta ação é bem diferente do controle e do monitoramento exercido sobre os usuários pelos sistemas de redes sociais mediadas por computadores. No caso dos mapas de crime, a autora afirma acertadamente que

“(...) a produção de conteúdo está associada ao posicionamento do produtor-usuário como vigilante. Os mapas de crime se inserem precisamente nesses casos, cruzando a vigilância e a comunicação distribuídas. Problematizarei, nesse contexto, o modo como os indivíduos são mobilizados a adotarem, como parte do seu espírito e prática cidadãos, um olhar e uma atenção vigilantes sobre o outro, a cidade, o mundo”.

E, mais adiante, que *“a vigilância figura aí como uma atividade ou estado atencional que deve ser ‘partilhada’ por todos de forma descentralizada.”* Neste ponto estamos de acordo. Os mapas de crimes propõem uma falsa segurança, colocam todos como vigias e vigiados, próximos, como afirma Bruno, dos jornalismo cidadão e da falsa panacéia da participação. Ela afirma: *“É preciso, ainda, desconfiar do sonho da transparência bottom-up embutida na idéia do ‘panóptico participativo’”*

O texto é muito bem escrito, apresenta bons argumentos e referências e trata de um problema da atualidade, chamando a atenção para regimes de visibilidade, de construção de subjetividade e para os perigos da expansão dos bancos de dados, dos regimes de controle, monitoramento e de vigilância da fase atual da cibercultura. Entretanto, a pergunta permanece: de que vigilância estamos falando?

REFERÊNCIAS

- GOW, G. **Privacy and Ubiquitous Network Societies**. Background Paper, ITU, march 2005
- LEMONS, A. **Mídia Locativa e Vigilância. Sujeito Inseguro, Bolhas Digitais, Paredes Virtuais e Territórios Informacionais**. Texto apresentado no I Seminário Internacional sobre Vigilância na América Latina, PUC-PR, março de 2009, no prelo.