Publicado in in Bruno, F., Kanashiro, M., Firmino, R., Vigilância e visibilidade - Espaço, tecnologia e identificação., Porto Alegre, Editora Sulina, 2010., 296 páginas., ISBN: 978-85-205-0553-3.

MÍDIAS LOCATIVAS E VIGILÂNCIA.

Sujeito inseguro, bolhas digitais, paredes virtuais e territórios informacionais.

André Lemos

PRIVACIDADE E ANONIMATO EM MEIO ÀS MÍDIAS LOCATIVAS

> "Não há necessidade de ficção científica para conceber um mecanismo de controle que forneça a cada instante a posição de um elemento em meio aberto, animal numa reserva, homem numa empresa (coleira eletrônica). (...)o que conta não é a barreira, mas o computador que localiza a posição de cada um, lícita ou ilícita, e opera uma modulação universal"(Deleuze, 1992, p. 226)

Entramos na era da mobilidade informacional. Serviços e tecnologias baseados em localização estão em expansão com a disseminação de dispositivos móveis (telefones celulares, *smartphones*, GPS), redes telemáticas sem fio (*Wi-Fi*, *Wi-Max*, *Bluetooth*, GPS) e sensores (RFID principalmente) possibilitando aliar, pela primeira vez, localização, vigilância e mobilidades física e informacional (capacidade de consumir, produzir e distribuir informação)[1].

Podemos definir as mídias locativas como a conjunção de LBS e LBT[2], como dispositivos, sensores e redes digitais (e os serviços a eles associados) que reagem ao contexto local (Kellerman, 2006; Benford, 2005, 2006; Pope, 2005). O termo é uma expressão criada por artistas para se diferenciarem de projetos comerciais e mostrar ambiguidades de questões atuais como mobilidade, localização, espaço público, vigilância. A expressão foi proposta, em 2003, por Karlis Kalnins em evento homônimo em Karosta, Latvia[3] e vários autores têm aderido a essa terminologia. Um dos pioneiros foi Russel (1999) propondo um manifesto em que dizia que, de agora em diante, o ciberespaço estaria "pingando" nas coisas: "the internet has already started leaking into the real world*"*.

A mobilidade por redes ubíquas implica maior liberdade informacional pelo espaço urbano mas, também, uma maior exposição a formas (sutis e invisíveis) de controle, monitoramento e vigilância. Segundo Gow (2005), *"*the essential qualities of the ubiquitous network society vision are invisibility and pervasiveness*"*. Invisibilidade e penetração em todas as coisas têm sido o tema dos debates

---

1 *Wi-Fi* é sigla para redes sem fio de acesso a internet. *Wi-Max* é uma rede *Wi-Fi* de longo alcance. *Bluetooth* é um *chip* que permite a conexão de curto alcance entre dispositivos. GPS significa Global Positioning System, sistema de posicionamento global por satélite. RFID, *Radio Frequence Identification* e *Tags* são etiquetas de rádio freqüência. Doravante, serão mencionadas apenas essas siglas.

2 LBS e LBT são siglas em inglês, respectivamente para Location-based service e Location-based technologies. Doravante, serão mencionadas apenas essas siglas.

3 Ver http://locative.x-i.net/intro.html (acesso em 8 de julho de 2009).

contemporâneos sobre as mídias locativas e a "internet das coisas". Emergem aqui sérias ameaças à privacidade e ao anonimato.

Controle, monitoramento e vigilância informacionais, que em muitos momentos podem parecer sinônimos, devem ser diferenciados aqui para um melhor entendimento do problema. Compreendemos controle como fiscalização de atividades, como ações normalmente associadas ao 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 de históricos, ou seja, como uma ação de acompanhamento e 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. Interessante notar que a palavra tem sentidos diferentes em francês e inglês, mas não encontramos a distinção em português. Em inglês e francês há duas palavras, com as mesmas grafias e os mesmos sentidos: "*vigilant*" - para alguém que se dedica a uma atenção cuidadosa e "*surveillance*" - para atos ligados à ação policial ou judicial com fins de proteção ao crime. Em português, vigilância/vigilante tem os dois sentidos. Vamos definir vigilância como ações que implicam as dimensões de controle e de monitoramento 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).

Vigiando (controlando e monitorando) as mídias locativas ameaçam a vida privada e o anonimato. A privacidade pode ser definida como o controle e a posse de informações pessoais, bem como o uso que se faz posteriormente delas. Anonimato, por sua vez, implica a ausência de informação sobre um indivíduo e também o controle sobre a coleta de informações pessoais (Gow, 2005). A privacidade é um pilar das sociedades democráticas já que:

> "empowers people to control information about themselves; protects people against unwanted nuisances, or the right to be left alone; (...) is related to dignity in the reciprocal obligations of disclosure between parties; (...) is also a regulating agent in the sense that it can be used to balance and check the power of those capable of collecting data" (Lessig; Gow, 2005, p. 7).

Embora correlatos, privacidade e anonimato sofrem impactos diferenciados pela ação das tecnologias locativas. Estas podem coletar dados pessoais e difundir outros já gerados sem o consentimento ou mesmo o conhecimento do usuário em ações de fiscalização (controle), acompanhamento e avaliação (monitoramento) e prevenção e zelo (vigilância). Indivíduos podem perder o controle sobre a geração de dados e a circulação dos existentes. Eles são, então, constrangidos respectivamente em seu anonimato ou privacidade. Como mostra Gow:

> "There is an urgent need for sophisticated mobile marketing techniques based on detailed knowledge of customer profiles, history, needs, and preferences. Information existing in customer databases developed by retailers like Amazon.com, for example, can be used in parallel with location-based information'"(Gow, 2005, p. 12).

As mídias locativas podem ser, efetivamente, ferramentas de invasão da privacidade e de violação do anonimato para fins comerciais, militares, políticos ou policiais. O novo regime "invisível" dos bancos de dados, de localização e cruzamento de informações, de monitoramento de perfis de consumo e dos movimentos pelo espaço urbano crescem na mesma medida que a liberdade de locomoção e de acesso/distribuição de informação. Não é por acaso que esses serviços e tecnologias surgem de pesquisas militares, prolongando a vigilância estatal, policial, comercial e industrial desde o século XVIII. Empresas e governos têm utilizado essas tecnologias para a coleta de dados pessoais, nem sempre realizada com o conhecimento ou o consentimento do cidadão. Para uma ação efetiva que proteja os indivíduos de sistemas de vigilância (estatais, militares, comerciais) que possam violar seus direitos, é necessário o reconhecimento dos novos territórios informacionais.

Como venho insistindo em outros trabalhos, a intersecção cada vez mais evidente do espaço físico com o eletrônico cria zonas de controle informacional que chamo de "território informacional". O território informacional pode ser pensado como uma nova heterotopia (Foucault, 1984) criando funções informacionais (digital/telemática) no espaço físico, a partir de bancos de dados e dispositivos eletrônicos. Esse território informacional é percebido por autores como "território digital ou bolha" (Beslay; Hakala, 2005), "espaço intersticial" (Santaella, 2008), "realidade híbrida, aumentada ou *cellspace"* (Manovich, 2005), "*virtual wall*" (Kapadia, 2007). Em todas essas concepções, o que está em jogo é o controle (territorialização) informacional e, consequentemente, uma nova função dos espaços (públicos e privados). Emerge aqui o lugar de onde a privacidade e o anonimato podem ser violados, mas também protegidos. Para compreender a ontologia e os novos sentidos dos lugares, proponho o conceito de território informacional que enfatiza o controle de fronteiras.

Compreender os novos territórios é fundamental para visualizar os impactos das mídias locativas sobre a privacidade e o anonimato ameaçados por novas formas de controle, monitoramento e vigilância. Para tanto, em primeiro lugar vou tomar o ideia de "sujeito inseguro", proposta por Mireille Rosello (Rosello, 2008), como um estrutura maior do regime de vigilância contemporâneo. Em seguida, explico os conceitos de "território digital ou bolha" e de "muro ou parede virtual" para explicitar a nova fronteira dos territórios informacionais. Entre uma coisa e outra, darei alguns exemplo concretos de vigilância e também de *sousveillance*[4].

[4] Termo proposto por Steve Mann (2003) em língua francesa, *sousveillance* designa atividades de contra-vigilância ou de

SUJEITO INSEGURO.

Mireille Rosello, professora da Universidade de Amsterdã, proferiu uma palestra sobre o tema "a cultura da insegurança" (Rosello, 2008) no colóquio "Insécurité linguistique et rencontres barbares", do Cérium na Université de Montréal, do qual participei em 2008. O objetivo era explorar a questão das câmeras de vigilância e das transformações que elas aportam à relação do sujeito com o espaço público e a cultura em geral. A palestra se desenvolveu para sustentar a tese da existência, na contemporaneidade, de um sujeito inseguro (*sujet insécure)*.

Na primeira parte, Rosello discutiu a noção de "cultura da insegurança", colocando o acento sobre a ideia de cultura, ou seja, sobre a dimensão social, comunicacional e política onde estamos imersos. Para ela, seria hoje impossível nos situarmos fora dela e temos que levar em conta este fato. No entanto, o sentimento de medo coletivo não é novo. A Idade Média gerou mitos e narrativas aterrorizantes. A diferença é que hoje a cultura do medo, sob o nome genérico de uma cultura da insegurança, ganha contornos planetários. Para Rosello, o "modo" da insegurança passa a ser uma ontologia, uma forma de ser, de conhecer e de ler a contemporaneidade. A questão, para Rosello, é que devemos aceitar fazer parte dessa cultura para transformá-la. Essa é a primeira constatação e o pano de fundo para a compreensão do problema da vigilância hoje.

Analisando as atuais e onipresentes câmeras de vigilância no espaço público, Rosello mostra que elas fazem parte do discurso sobre a segurança e, ao mesmo tempo, criam uma cultura da insegurança. Não há como escapar, e mesmo sistemas de desvio e apropriações desses dispositivos (como veremos adiante com experiências artísticas sob a rubrica de "*sousveillance*") estão enquadrados na mesma dinâmica cultural. As câmeras e demais dispositivos de vigilância, públicos e privados, fazem parte da forma de viver nas sociedades avançadas. É nesse contexto que se expandem as tecnologias, serviços e usos das mídias locativas. A própria ênfase atual em tudo localizar e indexar com coordenadas (latitude, longitude) e etiquetas - como vemos hoje com telefones celulares, GPS automotivos, *geotagging*[5] em fotos e vídeos, etc - parece mostrar a cultura do medo e da insegurança: medo da deriva e da desorientação transformada em uma ação racionalizante de tudo indexar, etiquetar, localizar e reconhecer no espaço.

Rosello desenvolve três postulados que, segunda ela, estão presentes nos debates atuais sobre vigilância e invasão da privacidade. O primeiro postulado afirma que "há razões para ter medo". O segundo postulado constata que "o cidadão está preso entre dois medos: o medo de quem é vigiado*"*

vigilância invertida efetuadas por artistas ou indivíduos ordinários, que se exercem de "baixo para cima", diferentemente da vigilância organizacional, que implica uma observação de "cima para baixo".

[5] Geotagging é um processo de identificação geográfico de dados sobre fotografias, vídeos, e *websites*, dentre outros.

(sendo essa uma perspectiva que ela chama de direita) e o *"*medo de quem nos vigiam*"* (perspectiva que ela aponta como sendo de esquerda). O terceiro postulado reconhece que "o sentimento de insegurança é indesejável". Segundo Rosello, isso leva à criação de uma subjetividade vulnerável que se estabelece por dicotomias e oposições simplórias. O sujeito quer reagir às câmeras na luta entre, por um lado, o direito à privacidade e à liberdade individual e, por outro, a segurança social e o controle visível do movimento do outro sempre ameaçador. O debate, sendo colocado sempre nesse tom, nos deixa presos a ideologias sem conseguirmos avançar na análise do problema.

Poucos são os que afirmam um princípio para além da dicotomia entre esquerda e direita. Muitos dos que são contra as câmeras de vigilância atuais, o são em nome de sua ineficácia no combate ao crime. A perspectiva de esquerda, conforme nomeou Rosello, afirma que elas ameaçam a privacidade e o anonimato, não resolvendo os problemas da criminalidade. Da mesma forma, o discurso de direita afirma que devemos, na vida em sociedade, abrir mão de alguma privacidade para termos mais segurança. No entanto, atropelos e atentados contra o direito dos cidadãos têm sido muito maiores do que a efetividade de uma diminuição da criminalidade. No Brasil, por exemplo, a adoção tem sido crescente e o discurso da segurança pela vigilância está presente em todos os lugares (polícia, academia, mídia). O crescimento da adoção de câmeras de vigilância é gigantesco. Dados da Abese (Associação Brasileiras das Empresas de Sistemas Eletrônicos), mostram que o total de um milhão de câmeras de vigilância estão espalhadas pelo país, 80% no Estado de São Paulo. A taxa de crescimento da adoção de câmeras de segurança por IP (Internet Protocol) é de 40% ao ano. Nem parece haver distinção entre direita e esquerda aqui. No entanto, há muita polêmica e controvérsia. Efetivamente, não há muitos avanços em situar o debate nessa polarização ideológica.

Para resolver esse problema, Rosello vai renunciar a esses argumentos e propor um outro ângulo de análise. Para ela, e esse me parece o ponto forte de sua argumentação, a solução é reconhecer não somente as ideologias, mas a materialidade do objeto, a câmera (e podemos dizer os sensores, as redes sem fio, os dispositivos de localização) e sua relação com o espaço, a fenomenologia do dispositivo. Baseada em pesquisas sobre as CCTV (Closed-circuit television), Rosello mostra que elas apresentam dados em que os usuários demonstram que a simples instalação de uma câmera cria medo, vulnerabilidade e insegurança, independente ou não da resolução do problema da criminalidade. A câmera estimula, por um lado, uma reação positiva, produzindo a ideia de que há um problema de segurança no lugar e que ela vai resolver. Por outro, ela cria uma sensação de medo e de insegurança temporal, no passado, no presente e no futuro: em relação ao presente, porque a simples introdução do dispositivo traz a ideia de que "algo acontece aqui"; em relação ao passado, pois "algo poderia ter acontecido"; e em relação ao futuro pois "algo pode acontecer". A materialidade do dispositivo altera a relação com o espaço/lugar produzindo um sentimento de insegurança. E pouco importa se essa

insegurança será ou não resolvida. O medo se dá no presente (“a câmera está aí para proteger de algo”), na atualização do passado (“deveria ter tido medo antes”) e no futuro (problemas acontecerão, ou serão inibidos). O interessante nesse ângulo de análise é que ele sai da polarização resolver - não resolver e entra nos princípios fenomenológico (o dispositivo), topológico (o lugar) e genealógico (o medo e a insegurança) instaurados pela existência das câmeras. De uma forma ou de outra, a angústia é gerada, aumentando o medo e a paranoia. Aí está a essência do “sujeito inseguro” moderno. A presença da câmera não cria tanto o medo de ser vigiado, segundo pesquisas citadas por Rosello, mas a sensação de que temos que sentir medo, já que a câmera está aqui.

Rosello propõe ver e aceitar a câmera como um "cidadão incivilizado". Baseada na literatura sobre formas de incivilidade na sociedade (maneiras de ocupar o espaço fora das normas, violência verbal, desrespeito ao outro, falta de educação no dia a dia, etc.), Rosello mostra que essas sempre foram combatidas por serem elementos geradores de mais violência. As câmeras, ou outro dispositivo de vigilância, devem ser vistas como algo que incomoda, que instaura relações de incivilidade violando o respeito ao outro. Pode-se então diagnosticar o princípio de sua violência, já que elas instituem olhares intrusivos e a produção de uma sensação de medo proveniente da observação e da vigilância permanente. Um medo, como vimos, atual, passado e futuro, ao mesmo tempo. Invadindo o presente, evocando um passado assustador e produzindo uma catástrofe futura, as câmeras são, para Rosello, “incivis” e assim devem ser reconhecidas. E elas produzem violência sem resolver nada, já que apenas filmam. As câmeras são, consequentemente, formas de "pré-mediação" social vulgar, não civilizada, bárbara.

Voltemos então aos postulados. Pode-se afirmar que vivemos em uma cultura da insegurança e não podemos fugir dela. A insegurança é um sentimento indesejável e temos que fazer de tudo para diminui-lo. Retomando o terceiro postulado (o sentimento de insegurança é indesejável), Rosello afirma que a insegurança é fruto de um contexto cultual específico e que os eventos de 11/9 só serviram como desculpa pra tentar resolver o problema pelo viés tecnocrático ou ideológico, instituindo diferenças, estigmas, aumentando o medo do "outro". Não apenas por câmeras, a vigilância/violência/incivilidade se dá agora por satélites, telefones celulares, monitoramento de perfis na internet, etiquetas de radiofrequência, tornando-se mais difusa, performática (bancos de dados eletrônicos) e invisível. Os sujeitos incivilizados cresceram e ganharam novas formas e propriedades mais performáticas, já que agora são dotados de memória em bancos de dados, mobilidade em redes telemáticas e fácil localização. Nesse regime global da insegurança, há alguns (o “outro”) que devem ser vigiados e outros não. Para Rosello, é fundamental que todos nós possamos nos colocar no lugar desse "outro" e aceitar o regime de insegurança. Não de forma passiva, mas de forma compreensiva, dialógica e social. Desenvolvendo aqui uma perspectiva que ela mesma chama de mais “otimista”, a

autora vai afirmar que a miséria não é tanto o excesso de olhar, mas a sua falta. Se tenho medo, como humano, posso me colocar no lugar desse outro que me assusta. O problema não seria tanto eliminar o outro (não ver) mas nos ocuparmos dele, reconhecermos sua vulnerabilidade que também é a nossa. Assim, para Rosello, aceitar a vulnerabilidade pode produzir sociabilidade e "compaixão". O sujeito deve encarar as câmeras (e os demais dispositivos) como um outro que o olha, mas que também precisa de ajuda. Não se trata tanto de evitar o olhar mas de reforçá-lo para pode ver, não tanto as diferenças, mas o que nos torna semelhantes. A insegurança e a vulnerabilidade podem ser formas de aproximação ao outro, formas de reforço social.

Para concluir, Rosello reivindica o reconhecimento desse "sujeito inseguro", sujeito vulnerável e que se aceita fundado na e pela insegurança - já que a segurança total e completa é uma ilusão. Esse "sujeito inseguro" deve ter a capacidade de aceitar a relação de vulnerabilidade e de insegurança e não ficar preso a dicotomias que fazem da primeira um aspecto individual e da segunda um fato social. O "sujeito inseguro" sabe da ilusão de segurança das câmeras de vigilância, sabe que elas geram medo e intolerância e que, ao invés de resolver o problema, elas só o agravam, produzindo mais sentimento de insegurança. Esse "cidadão inseguro" estaria melhor adaptado para se locomover no regime de visibilidade e de vigilância locativa difusa atual e poderia, com mais clareza, denunciar as tentativas perversas de resolução dessa "insegurança universal" da qual eles são vítimas.

É nesse contexto que devemos perceber não apenas as câmeras de vigilância, mas os demais dispositivos portáteis, móveis e em rede (redes *Wi-Fi*, *Bluetooth*, telefones celulares, GPS; sensores e etiquetas de radiofrequência) que ampliam sobremaneira as formas de controle, monitoramento e vigilância. Os exemplos em relação às câmeras de vigilância são importantes para situar o debate e mostrar a emergência de uma cultura da insegurança. O caráter locativo existe apenas nas novas câmeras IP que utilizam redes sem fio digitais para a comunicação a sistemas de controle, monitoramento e vigilância móvel (carros de polícia, por exemplo) aliados à localização com GPS. A disseminação de câmeras em telefones celulares leva essa cultura de insegurança (do testemunho de acontecimentos, do voyeurismo, da invasão da privacidade e do anonimato) a uma fase ainda mais aguda, colocando a potência da vigilância nas mãos de qualquer indivíduo.

Vejamos rapidamente a relação das mídias locativas com a sociedade da insegurança ou do controle para depois examinarmos as noções de "bolha digital" e "parede virtual", bordas do "território informacional" que, uma vez reconhecidas, podem proteger a privacidade e o anonimato dos "sujeitos inseguros".

Mídia Locativa e Sociedade de Controle. Alguns Exemplos.

A sociedade de controle está em toda parte. Para além do *panopticon* que vigia o confinado, as atuais câmeras de vigilância, cartões com *chips*, perfis na internet, GPS e sensores, controlam o sujeito "inseguro" em sua mobilidade cada vez maior. Mobilidade é mesmo a palavra-chave para pensar as massas (império?), o uso da informação (vivendo sem fronteiras?) e as possibilidades de localização e reconhecimentos de coisas no espaço. Mais movimento significa também maior possibilidade de controle, vigilância e monitoramento de pessoas, informações e objetos. As mídias locativas, onde localização e mobilidade significam possibilidades de produção de sentido no espaço e nos lugares, são também instrumentos de controle, monitoramento e vigilância de lugares, espaços e indivíduos, agora enredados em bancos de dados moduláveis, sensores ubíquos e onipresentes, redes sem fio fluidas e inteligentes, dispositivos de localização "atentos às coisas". Não esqueçamos que essas tecnologias têm origem militar. Toda mídia locativa, por seu caráter intrínseco associando mobilidade e localização, pode ser usada para monitorar movimentos, vigiar pessoas e controlar ações no dia a dia.

A ideia da sociedade de controle de Deleuze (1992) parte da constatação da superação da vigilância panóptica de Foucault (1987) e da sociedade disciplinar do confinamento. Na realidade, os dois regimes convivem hoje, havendo, entretanto, uma inflexão em direção a uma vigilância mais sutil e invisível, mais modular. Para Deleuze, a sociedade do controle era o que Foucault anunciava como o nosso futuro próximo, o que em termos práticos de vigilância significa que as tecnologias não são mais visíveis e imóveis, mas ubíquas, pervasivas (*pervasive)*, "nas coisas", difusas, não exigindo do sujeito o confinamento, mas pedindo exatamente o contrário, a mobilidade permitindo um controle dinâmico.

A nova vigilância da sociedade de controle está em todos os lugares e, ao mesmo tempo, em lugar nenhum. Diferente dos "internatos", os atuais meios de vigilância não se dão mais em espaços fechados, mas nos "controlatos" dos perfis da internet, nos bancos de dados em redes sociais interconectadas, nos deslocamentos com o telefone celular monitorando o "*roaming*" do usuário, na localização por GPS, nos rastros deixados pelo uso de cartões eletrônicos, nos *smartcards* dos transportes públicos, nos sinais emitidos e captados por redes *bluetooth,* nas etiquetas de radiofrequência que acompanham produtos e compradores... Certamente tudo está menos visível e mais difuso, tornando essa invisibilidade vigilante mais performativa e o controle dos movimentos mais efetivo. Não se trata mais de fechar e imobilizar para vigiar, mas de deixar fluir o movimento, monitorando, controlando e vigiando pessoas, objetos e informação para prever consequências e exercer o domínio sob as "modulações". Como diz Deleuze (1992), *"*o homem do controle é antes ondulatório, funcionando em órbita, num feixe contínuo*"*.

Bancos de dados, dispositivos portáteis eletrônicos, redes de satélite e sem fio para acesso à internet ou celulares, redes sociais móveis por GPS e triangulação de *Wi-Fi* e torres de celulares, bem como sensores fazem muito bem o serviço. Essas mídias com funções locativas são instrumentos de

produção do medo e de insegurança da qual fala Rosello. O "sujeito inseguro" deve efetivamente reconhecê-las para poder encarar com responsabilidade os novos instrumentos da cultura da insegurança. Antes de falarmos de bolhas, paredes e territórios informacionais, vejamos alguns exemplos concretos dessa ameaça.

Câmeras de vigilância

O artista francês Renaud Auguste-Dormeuil, interessado nos processos de vigilância e de militarização, ao chegar em Montreal recebe no aeroporto um guia da cidade onde são propostos cinco percursos turísticos. Esses percursos visam mostrar uma Montreal bela, dinâmica, multicultural. O lugar é assim investido dos "mitos e sonhos", um lugar idealizado pelas instituições. Para Renaud, o papel do artista é "injetar realidade" no sonhos produzidos por aqueles que controlam o espaço. Ao receber o guia, Renaud fez os mesmo percursos anotando todas as câmeras de vigilância (com endereços precisos e nome dos proprietários), produzindo um mapeamento das mesmas. Em seguida, colocou uma "errata" no guia gratuitamente distribuído e os empilhou. Um outro projeto interessante é "Mabuse", onde o artista cria um percurso turístico em micro-ônibus para que os turistas possam ver as câmeras de vigilância da cidade (as mais importantes vistas e filmadas no mundo: obelisco da Place de la Concorde; Hotel Ritz que pegaram as últimas imagens de Dodi e Diana, etc).

Nesse mesmo espírito de "*sousveillance*", o projeto "iSee" mapeia as CCTV de uma cidade (Londres) e propõe um mapa interativo de percursos alternativos. Ao escolher um endereço, o sistema indica as ruas por onde o transeunte deve passar para não ser visto pelas câmeras. O objetivo é produzir anonimato nos percursos. Como explica o *site* do projeto: *"*iSee enables users to avoid CCTV surveillance cameras. Some UK-based artists working on ideas of counter-surveillance for the broad public have discovered that in fact most people are totally comfortable with the idea of surveillance in public space.*"*

Outro projeto interessante é o "Life. A user's manual" da canadense Michelle Teran. O projeto detecta vídeos de CCTV que usam redes *Wi-Fi* e os expõem na rua. A artista desenvolveu um dispositivo que intercepta essas imagens e, invertendo a lógica, as expõem para os passantes no espaço público. Há aqui uma referência explícita à obra "Vida, modo de uso" de Georges Perec. O que é interno, privado e vigiado por poucos vira externo e visível para muitos. Como explica o *site* da artista:

> "A tiny fraction of the radio spectrum has been allocated for public use. Taking advantage of this unlicensed part of the spectrum, the result has been an increase in use of wireless devices that are transmitting on this narrow band. Private use of wireless internet, cordless phones, bluetooth and wireless surveillance cameras has turned the average consumer into 'micro-broadcasters' who transmit their personal narratives through the airwaves. The culmination of these autonomous and synchronous acts

> contributes to an invisible, ad-hoc network of media overlaid within the socially codified spaces of urban environments, the café, the home, the apartment building, the office, the store, the bar, the hallway, the entrance, the parking lot and the street. 'Life: a user's manual' focuses on the use of wireless surveillance cameras within public and private places that transmit on the 2.4 Ghz frequency band. Easily intercepted using a consumer model video scanner, the captured, live images create a sequence of readings and views of the city and its inhabitants which are observed while walking through the streets."(http://www.ubermatic.org/life/)

Multissenhas bancárias

Para Deleuze, uma das características da sociedade de controle não é a assinatura que indica o indivíduo e sua posição na massa, mas a senha, a linguagem numérica que garante o acesso à informação:

> "nas sociedades de controle, ao contrário, o essencial não é mais uma assinatura e nem um número, mas uma cifra: a cifra é uma senha (...). A linguagem numérica do controle é feita de cifras, que marcam o acesso à informação, ou a rejeição (...). Os indivíduos tornaram-se 'dividuais', divisíveis, e as massas tornaram-se amostras, dados, mercados ou 'bancos'" (Deleuze, 1992).

Um exemplo desse controle de cifras são as multissenhas de instituições bancárias. Passando da moldagem (sociedade disciplinar) à modulação (sociedade de controle), estas obrigam o uso de senhas de acesso (para aferir maior controle sobre a assinatura e o número de identificação do cliente) como também, mais recentemente, senhas de acesso moduláveis (em alguns casos, um pequeno dispositivo em forma de chaveiro) produzindo uma combinação a cada uso (hipermodulação e hipermobilidade) para melhor controle e segurança do banco e do usuário. O uso de multissenhas é obrigatório, apontando para um controle que cresce e expande-se através de uma maior mobilidade física do usuário e uma maior mobilidade informacional (uma senha "móvel"). Essa modulação é uma estratégia dos bancos para aumentar a responsabilidade do usuário em relação ao roubo de senhas. Vemos a "cifra" dos "dividuais" onde aparentemente o usuário controla melhor sua conta mas, na realidade, é o sistema que controla o correntista, dando ao mesmo tempo a impressão de uma maior mobilidade e liberdade.

Life-Loggs

Outro exemplo de vigilância, aliando mobilidade e liberdade, são os *life-loggs.* Podemos defini-los como informações pessoais geradas e estocadas diariamente por dados gerados em redes telemáticas como um histórico eletrônico da vida de um indivíduo. Martin Dodge e Rob Kitchin (2007) mostram que a vigilância de dados pessoais cresce com as redes sociais e os perfis na internet (Bruno, 2008), sendo efetivamente instrumentos de vigilância. Cada ação, movimento, conversação ou produção de conteúdo (textos, fotos, vídeos) é acumulado em bancos de dados eletrônicos

disseminados pelo planeta, representando uma ameaça à privacidade e ao anonimato. Notemos aqui que muito desses dados são gerados a partir da livre iniciativa dos usuários, colocando em tensão a produção livre, a mobilidade e a ameaça à privacidade e ao anonimato. Indivíduos, em suas ações quotidianas no ciberespaço, participam de *blogs*, *microblogs*, *softwares* sociais, fóruns, sistemas de publicação de fotos e vídeos, uso de mapas digitais e outras ferramentas da *web 2.0*. Essas informações são captadas de forma automática gerando uma memória da vida do indivíduo. Trata-se de reconhecer não tanto o "*data*", que representa aquilo que é dado (fornecido), mas sim o "*capta"*, a informação digital retirada, captada pelos diversos sistemas eletrônicos disponíveis gratuitamente na internet. Na palavra dos autores:

> "As such, the present ability to capture and store vast amounts of information is inspiring a vision of pervasive computing that generates ubiquitous information of the present, which is kept to become a continuous record of the past. Such information constitutes capta (Dodge and Kitchin, 2005). Capta (derived from the Latin capere, meaning `to take') are units of data that have been selected and harvested from the sum of all potential data (derived from the Latin dare, meaning `to give') (Jensen, cited in Becker, 1952). To date, recording regimes have generated capta from an `exterior' position, generally through one dimension and held by an organization which is external to an individual and which they do not control (eg, they constitute surveillance). A life-log will generate capta from an `interior' (or first-person) perspective, from which the individual watches themselves through intimate technologies (ie, technologies in service to the individual ö eg, phones, car, wearable computing), with the capta pooled into a unified, multimedia archive which they control [eg, it constitutes sousveillance - sousveillance being the internal counter to external surveillance (Mann, 2003)" (Dodge; Kitchin, 2007, p. 432).

Cada vez mais *captas* são integrados em sistemas agregadores de informação, configurando-se como verdadeiros bancos de dados sobre a vida das pessoas. O mais problemático é que os *life-loggs* nunca esquecem os traços captados nas mais diversas ações, eventos, conversas ou outras expressões da vida quotidiana na rede. Todos esses movimentos pelo ciberespaço e com dispositivos, redes e sensores portáteis geram *datas* e *captas.* Para escapar a esses sistemas os autores propõem uma ética do esquecimento como forma de proteção à privacidade e inibição de formas de controle e vigilância. Para evitar que *datas* e *captas* criem uma memória absoluta, sem esquecimento, fazendo com que tudo, absolutamente todos os passos sejam lembrados, os autores sugerem que, como na vida fora da rede, o esquecimento seja uma forma de sobrevivência, que um apagamento da memória eletrônica seja projetado no interior dos sistemas. Não se trata tanto aqui de construção de "bolhas" e "paredes" virtuais que protejam as fronteiras dos territórios informacionais, mas do apagamento (esquecimento) de *data* e *capta.* Na palavra dos autores:

> "To counter the potentially pernicious effects of pervasive computing we have

> suggested the development of an ethics of forgetting that is materialized through the `loss of memory' in a life-log. While building fallibility into the system seemingly undermines life-logging, it seems to us the only way to ensure that humans can forget, can rework their past, can achieve a progressive politics based upon debate and negotiation, and can ensure that totalitarian disciplining does not occur."(2007, p. 431).

Redes sociais móveis

A gigante Google acaba de lançar o sistema Google Latitude para localização de pessoas. O sistema encontra usuários e mostra a sua localização em mapa na tela dos *smartphones.* Esse tipo de localização, conhecida como "*mobile social networking*", ou redes sociais móveis, serve para que o usuário saiba onde estão os amigos e possa eventualmente encontrá-los no espaço urbano. O sistema permite ajustar níveis de privacidade (quem você quer que te veja) e níveis de anonimato (graus de precisão da sua localização). O Google também não mantém um *log* de suas localizações. Vemos aqui "bolhas", "paredes" e "territórios" informacionais, como mostraremos adiante. Mesmo assim, possibilidades de controle, monitoramento e vigilância vão surgir. Recente matéria da PC World, "Spy on your workers with Google Latitude" de David Coursey (2009), 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. Delivery vehicles might also be tracked, and the service could also be used to make certain the closest resource is always sent to a customer's request. (...) 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. I know people who simply don't trust Google to not become evil, if the company hasn't already. They wonder why the company offers so many free applications unless it has some way to monetize them that isn't obvious to the user."

A organização Privacy International, baseada em Londres, afirma que esse tipo de vigilância já está sendo usado por empresas com dispositivos móveis *"*without the knowledge or consent of their users*"*. Assim como o Google Latitude oferece possibilidades de criar privacidade e anonimato, como vimos acima, a Privacy International adverte que o mesmo sistema pode ser usado para que usuários não saibam que estão sendo seguidos. Segundo a organização: *"*The only means of minimizing this threat might be a regular message sent to a phone advising that it has been Latitude-enabled. (...) However, according to Google, this function is available only in certain circumstances" and may only apply to "certain unspecified phone types."

RFID

Exemplos de violação da privacidade podem ser encontrados em experiências com o uso das etiquetas de radiofrequência, RFID, comumente chamadas de *spychips*. Albrecht e McIntyre (2006) oferecem

inúmeros casos de uso de RFID com violação de privacidade, com fins policiais, políticos ou comerciais. Essas microetiquetas estão disseminando-se em todos os lugares (roupas, placas de carros, produtos, passaportes) e têm como objetivo melhorar a eficiência e segurança de empresas e governos já que servem para monitorar produtos e pessoas, aliando mobilidade física e informacional. Segundo as autoras:

> "in a future world laced with RFID spychips, cards in your wallet could 'squeal' on you as you enter malls, retail outlets, and grocery stores, announcing your presence and value to businesses. Reader devices hidden in the doors, walls, displays, and floors could frisk the RFID chips in your clothes and other items on your person to determine your age, sex, and preferences. Since spychip information travels through clothing, they could even get a peek at the color and size of your underwear" (Albrecht; McIntyre, 2006, p. 3)

Várias empresas colocam, sem avisar o consumidor, etiquetas RFID em seus produtos com o objetivo de vigiar os atos de compra e monitorar os usuários até suas casas. Substituindo os atuais códigos de barra (estáticos), cada produto terá em breve uma etiqueta RFID. Por exemplo, ao comprar um produto com o seu cartão de crédito, por exemplo, você estará associando seu número de cartão ao produto e a etiqueta colada nele (digamos, um sapato que só você usa ou um cartão de fidelidade da loja, que só você tem). Ao passar por qualquer leitor com esse produto (em postes, no chão, em semáforos, em lojas, etc) você será identificado e seus movimentos podem ser vigiados para os mais diversos fins: marketing, publicidade focada, polícia, etc. No Brasil, desde 2007, o governo vem implementando essas etiquetas nas placas dos carros. O discurso é que o sistema trará mais segurança, uma melhoria do trânsito e um melhor controle de pagamento de impostos. Mas, com certeza, ele será uma ameaça à privacidade e ao anonimato já que, ao passar por um leitor (digamos um semáforo), seu carro (você) será identificado e monitorado (podendo, no cruzamento de bancos de dados, receber publicidade focada, alimentar o seu perfil para usos futuros, ser parado pela polícia por não ter pago o imposto, etc).

Um outro exemplo vem da França com o cartão Navigo do sistema de transportes RATP, ameaçando o anonimato dos usuários do sistema de transporte. A RATP pretende mudar a analógica *carte orange* (um comprovante de pagamento de uma mensalidade para usar metro e ônibus) para o Navigo (uma *contactless transit card*). Esse novo cartão digital permitirá a empresa saber quando, onde e por que transporte uma pessoa se desloca no país. O Navigo tem foto, nome, sobrenome, endereço e uma RFID que associa a um número único os trajetos do cidadão na rede de transporte. A CNIL, (Commission Nationale de l'Informatique et des Libertés*)*, considera o novo cartão uma real ameaça ao anonimato e à vida privada. Vemos aqui mais um exemplo das tensões entre a nova cultura da

mobilidade e a sociedade do controle com ameaças concretas. Com o Navigo, e toda a cadeia de leitores e etiquetas RFID, incluindo celulares, o usuário move-se mais facilmente, mas, ao mesmo tempo, deixa marcas de todos os seus passos.

Mas há usos alternativos para as RFID, para além do corporativo, policial ou político e alguns artistas têm desenvolvido interessantes projetos de contra-vigilância. No plano comercial, temos Tikitag da Alcatel-Lucent de 2008 e o Nokia 3220 da Nokia, de 2005. Ambos propõem etiquetas RFID para que o usuários possam agenciar o sistema e colocar *tags* em qualquer coisa, criando conexões à internet e relacionando um objeto a informações históricas, por exemplo. Nesse sentido, *blogs* de coisas podem ser criados e alimentados automaticamente. Outro similar é o "Symbolic Table de Mediamatics", ThingLink de Helsinque. No que se refere à projetos artístico-ativistas de contra-vigilância, temos as ações do grupo americano Preemptive Media, que criou o projeto "Zapped", largando baratas com RFID dentro de um Wall-Mart para criar confusão nos bancos de dados. Há também ações interessantes como o projeto holandês *z25's Data*, de 2005, ou o projeto "Attention please", em Liverpool (Kuitenbrouwer, 2006).

Para Kuitenbrouwer (2006), devemos aproveitar o potencial criativo que é também um dos lados das RFID. O problema é saber negociar a privacidade (não é ter ou não ter privacidade, mas gradações) e agenciar o seu uso. Pode ser interessante, em alguns momentos, abrir mão de alguns dados pessoais para receber informações personalizadas. Por exemplo, ao indicar meu gosto pessoal por música, livros, filmes ou gastronomia, posso ganhar recebendo informações que me interessam diretamente. O mesmo pode ser aplicado às etiquetas RFID. Posso anexá-las em alguns objetos pessoais para que eles tenham um história e uma memória na rede. Elas podem ser assim interessantes plataformas para projetos *bottom-up*, oferecendo formas criativas de agenciamento, transformando as etiquetas em mídias de comunicação e não apenas em dispositivos de vigilância. Trata-se, necessariamente, de um embate político em minimizar as atuais formas de agenciamento (comercial, governamental) que colocam o usuário apenas como um alvo passivo e, na maioria das vezes sem saber, dos serviços de *marketing*, das seguradoras, da publicidade, das polícias. Deve-se incentivar o desenvolvimento de uma RFID 2.0 onde esses mesmos usuários possam produzir conteúdos e indexações próprias. Para Kuitenbrouwer:

> "An 'internet of things' can also increase the experienced value of objects. Things that are tagged can start preserving their own history. (...) Opposition to it from consumer organizations mainly has to do with the ease with which everyone can invent privacy-threatening scenarios in a world crawling with RFIDs. At the same time, the complete disregard by the major market parties of a possible say on the part of consumers and citizens concerning the introduction and applications of RFID is also an important factor. (...) We can leave this to market forces, but it would be better to do it ourselves.

> Just as the Internet after the dotcom implosion has still managed to become the domain of democratic media production, so too can a large-scale implementation of RFID (after the stumbling of RFID 1.0 over privacy issues) become a terrain for a public sphere developing from bottom-up. Not all its content will be relevant, but what's more important is that RFID 2.0 offers a network for new relations between people and things. (...)" (p. 59)

Bluetooth

Telefones celulares também podem ser uma porta de entrada para violação da privacidade ou do anonimato. Artistas do grupo londrino Loca, questionando o uso de redes *bluetooth* e telefones celulares, realizaram a performance "Set to discoverable" onde passantes recebiam mensagens estranhas ao se locomoverem pelas adjacências das ruas onde estavam instalados sensores *bluetooth.* O sistema detectava celulares com redes *bluetooth* abertas e enviava mensagens para os usuários do tipo: "por que você saiu da praça"? "quanto tempo vai ficar sentado nesse banco"?, etc. Os artistas do Loca observavam os passantes e enviavam essas mensagens direto para os respectivos celulares. Interessante notar que os passantes procuravam câmeras de vigilância olhando para cima ou para os lados. A performance visava questionar a invasão de privacidade em plena mobilidade e chamar a atenção para o desconhecimento dos usuários sobre o potencial invasor dessas redes.

Não vamos insistir em outros exemplos. Mostramos como as mídias locativas podem violar fronteiras informacionais ameaçando a privacidade e o anonimato pela via do controle, do monitoramento e da vigilância eletrônicos. Essas fronteiras são invisíveis e muitos usuários não percebem a real dimensão dessa faceta da sociedade de controle: uma vigilância sutil, difusa, deixando o usuário com a sensação de liberdade de produção de informação e de mobilidade. Os exemplos com as câmeras de vigilância, as multissenhas bancárias, os *life-loggs*, as redes sociais móveis, as etiquetas RFID e os celulares com redes *bluetooth* mostram que a computação ubíqua, que a internet das coisas com suas tecnologias, redes e sensores eletrônicos transformam a vigilância panóptica em um controle invisível, modular e distribuído, ao mesmo tempo, em todos e em nenhum lugar.

Antes, as ameaças à privacidade eram visíveis: ou imobilidade ou quebra de fronteiras materiais bem nítidas (casa, trabalho, corpo, prisão, hospital, escola...). Agora, a vigilância locativa é invisível e sutil já que é o próprio usuário que, na maioria das vezes, produz deliberadamente os dados (*data* e *capta*), sentindo-se produtor livre de informação em mobilidade. A violação de fronteiras é agora não mais material, mas eletrônico-digital, trafegando pelas membranas porosas dos novos territórios informacionais. Não há inibição do movimento em confinamentos claros e visíveis, mas coleta, estoque e circulação de informação pessoal em uma nuvem de dados em plena mobilidade. Não é olhando para as fronteiras físicas e concretas dos quartos, casas, hospitais, empresas ou prisões que perceberemos a permeabilidade informacional. A vigilância com as mídias locativas se dá nos invisíveis territórios

informacionais, na violação de fronteiras eletrônicas, invisíveis das "bolhas digitais" ou das "paredes virtuais". Só o reconhecimento dos territórios e fronteiras informacionais poderá garantir o controle cidadão das informações pessoais que manterão o direito à privacidade e ao anonimato na atual cibercultura.

AS BORDAS DOS TERRITÓRIOS INFORMACIONAIS: Bolhas e paredes virtuais

Sociedade de controle, mídias móveis, serviços baseados em localização em interface com o espaço urbano, esse é o quadro atual da vigilância. A circulação de informação em redes, a partir de dispositivos e sensores, ocorre cada vez mais na intersecção dos espaços físicos e eletrônicos. Não se trata de (apenas) circulação de informação no ciberespaço, mas de informação transitando por lugares e objetos do dia a dia, emitindo e coletando informações de pessoas em um espaço urbano hiperconectado pelo desenvolvimento da computação ubíqua, da internet das coisas. A proteção da privacidade só será efetiva com o reconhecimento dessa nova ontologia dos lugares, com o entendimento de que os lugares físicos passam a ser dotados de (novas) funções (heterotopias) informacionais digitais, implicando um processamento automático de dados, memória em bancos de dados e circulação desses mesmo dados em redes telemáticas globais. Ou seja, zonas de controle informacional em meio ao espaço urbano. Como zonas de controle de bordas e fronteiras eletrônicas, essa hibridização cria uma nova territorialidade. Em outro artigo, defini assim os territórios informacionais:

> "Por territórios informacionais compreendemos áreas de controle do fluxo informacional digital em uma zona de intersecção entre o ciberespaço e o espaço urbano. O acesso e o controle informacional realizam-se a partir de dispositivos móveis e redes sem fio. O território informacional não é o ciberespaço, mas o espaço movente, híbrido, formado pela relação entre o espaço eletrônico e o espaço físico. Por exemplo, o lugar de acesso sem fio em um parque por redes *Wi-Fi* é um território informacional, distinto do espaço físico parque e do espaço eletrônico internet. Ao acessar a internet por essa rede *Wi-Fi*, o usuário está em um território informacional imbricado no território físico (e político, cultura, imaginário, etc.) do parque, e no espaço das redes telemáticas. O território informacional cria um lugar, dependente dos espaços físico e eletrônico a que ele se vincula.(...)" (Lemos, 2008, p. 221)

Lugares caracterizam-se justamente pela inter-relação territorial: funções sociais, culturais, imaginárias, subjetivas, econômicas, políticas, suas regras, normas e ritos sociais. Devemos assim, para compreender as ameaças informacionais emergentes nos espaços urbanos, reconhecer uma nova territorialidade, informacional, em interface com as demais territorialidades dos lugares. Não é o fim dos lugares, mas uma "ressignificação" com novas tensões de fronteiras. Por exemplo, ao sentar em um café e falar ao telefone celular, ao usar um *laptop* para enviar e receber informações em rede *Wi-Fi*,

estamos fazendo transitar, por fronteiras invisíveis, informações pessoais que podem ser captadas e usadas sem o nosso conhecimento ou consentimento. Claro, estamos ainda em um café, mas este passa a ser dotado de novas funções informacionais. Vemos aqui uma nova tensão de controle, logo, uma novo território, informacional, criado por redes sem fio e dispositivos digitais nos lugares. Posso assim ser monitorado, controlado ou vigiado nesse café se estiver usando o celular, o *laptop* ou se houver um *reader* que acione a etiqueta RFID da minha caneta. Sem essa camada informacional, sem esse território informacional, não há como circular informação digital e o café seria apenas esse lugar tradicional para se tomar um café ou ler o jornal. Mas trata-se agora de um *ciber*-café. Reconhecer os territórios informacionais, invisíveis, é perceber as novas heterotopias de controle informacional. Esse reconhecimento é fundamental para a conscientização das ameaças da era da computação ubíqua e das mídias locativas.

Vejamos então com as fronteiras dos territórios informacionais podem ganhar a forma de uma "bolha digital" ou de uma "parede virtual". Em ambas as bordas, o que está em discussão é o controle por parte do usuário das informações que passam (saindo ou entrando) nessa bolha ou através dessas paredes. A invasão de privacidade, o controle de movimento, o monitoramento de ações, em suma, a nova vigilância eletrônico-digital se dá hoje em dia na invasão dos territórios informacionais através de suas bordas, sejam elas vistas como bolhas ou paredes.

Bolhas Digitais

É nos territórios informacionais que se exercem controles do fluxo de informação. O controle se dá por senhas de acesso, *firewalls*, permissões de acesso a dados e localização pessoal, controle de emissão de informações a partir de dispositivos e sensores, etc. As bordas invisíveis dos territórios informacionais devem ser controladas pelos próprios usuários, garantindo o nível de privacidade e anonimato desejado: quero que essa informação seja pública, mas não essa outra; que esse pessoa saiba que estou aqui, mas não uma outra; que meu gosto por um determinado assunto possa ser usado por esse sistema, mas não por esse outro, e assim sucessivamente. É negociando as permeabilidades das invisíveis e eletrônicas bordas dos territórios informacionais que podemos manter a privacidade e evitar formas de controle, monitoramento e vigilância indesejadas. Beslay e Hakala (2005) usam a imagem da bolha para definir essa borda do que chamam de "*digital territory*":

> "a temporary defined space that can be used to limit the information coming into and leaving the bubble in the digital domain. It constitutes a digitization of the definition of personal space described by the psychologist Robert Sommer [3] as a soap bubble. The vision of the bubble is defined to gather together all the interfaces, formats and agreements etc. needed for the management of personal, group and public data and

informational interactions."(Beslay; Hakala, 2005, p. 2-3).

Pensar em termos de território digital ou informacional permite visualizar fronteiras, bordas que podem ser ou não permeáveis ao fluxo informacional e garantir políticas relativas a privacidade. A bolha é aqui uma imagem de proteção social, uma forma de isolamento eletrônico do lugar: o território digital é para Beslay e Hakala "a place of information and communication" (2005, p. 1). A noção de território e a imagem da bolha ajudam a reconhecer que há controle (território) e fronteiras (bolha) por onde passam as informações pessoais. Usuários nem sempre se dão conta dessa dimensão e, nesse espaço cotidiano e invisível, dados têm sido coletados à revelia dos sujeitos e usados sem que eles tenham conhecimento, já que as fronteiras entre os espaços privados e públicos têm sido eletronicamente borradas. Consequentemente, "without digital boundaries, the fundamental notion of privacy or the feeling of being at home will not take place in the future information society" (Beslay ; Hakala, 2005, p.1). A nova fase da computação ubíqua, com o ciberespaço "pingando" nas coisas (Russel, 1999), abre possibilidades para violação de fronteiras eletrônicas por onde dados pessoais circulam. Sem reconhecer o território informacional não há como estabelecer uma política da privacidade e um acordo sobre vigilância, monitoramento e controle na era da computação móvel, locativa e distribuída.

A imagem da bolha tem como objetivo criar uma camada de isolamento, de controle informacional, dando aos usuários o poder sobre o que sai ou entra. Beslay e Hakala estão preocupados em fazer com que o espaço pessoal, o espaço da casa, do trabalho ou outros não vazem informações sem autorização e conhecimento dos usuários. Assim, criar uma bolha digital garante a privacidade e o anonimato. O território digital deve ser pensado em vários níveis, com permeabilidades diferenciadas. Bolhas informacionais podem evitar que informações "pinguem" para fora desses níveis. Um primeiro território seria o pessoal (o corpo e a subjetividade). A casa é o segundo nível de isolamento e controle de fronteiras e o espaço público o terceiro nível territorial, onde as pessoas negociam proximidade e distanciamento. O *design* do território digital isolaria os três tipos de espaços protegendo o indivíduo:

> "the vision of digital territory offers the opportunity to introduce the notion of territory, property and space in a digital environment. The objective is to provide a tool that enables users to manage proximity and distance with others in this future ambient intelligence space, both in a legal and a social sense, as is the case in the physical world". (Beslay; Hakala, 2005, p. 2).

Como mostramos, o novo ambiente informacional com a computação ubíqua, coleta, processa e distribui uma grande quantidade de informação: pense no uso do seu telefone celular, no pagamento com cartão de crédito, no acesso a internet de casa, do trabalho ou da rua por redes de telefonia celular

de terceira geração (3G) ou *Wi-Fi*, na sua seguradora coletando dados sobre seus perfis de consumo na internet, da localização de sua posição em sistemas como o Google Latitude; na troca de mensagens de textos por SMS (para *short message service*) entre você, seus amigos e familiares...Os exemplos são banais e mostram as diversas "bolhas" e as respectivas porosidades das esferas pública e privada em relação aos dados informacionais. Reconhecer os novos territórios informacionais (que permitem que as ações acima aconteçam) é a base para o desenvolvimento de formas efetivas de proteção dos dados emitidos, processados, estocados e circulados nessas ações. Para os autores, *"*in the information society, the crucial issue will be to design this digital territory*"* (Beslay; Hakala, 2005, p.2).

As bolhas digitais devem ser vistas como fronteiras dos territórios informacionais, como zonas de controle para garantir privacidade, segurança e proteção. A ameaça à privacidade e ao anonimato na era das mídias locativas emerge da violação das fronteiras dos territórios informacionais, das bolhas. Insistimos, territórios, bolhas digitais e, como veremos, paredes virtuais, devem ser reconhecidas para garantir a proteção à privacidade e a inviolabilidade de dados pessoais, para proteger os cidadãos desavisados dos excessos de controle e de vigilância potencializados com as LBT e os LBS. Como concluem os autores:

> "a growing number of emerging technologies, such as location-based services, fourth generation mobile telephones, closed circuit television, biometrics, etc., tend to establish links and bridges between a specific physical location and digitised knowledge and information. If the added value for the user is obvious, the potential new threats are not always highlighted. (...) Location-based services, radio frequency identification tags, body implants, ambient intelligence sensors, etc. will permit the implementation of a trustworthy environment and therefore the domestication of the ambient intelligence space by the individual. The vision will facilitate the transition through a traditional society that coexists with an information society, to a single society whose citizen have accepted and adopted the fusion of physical and digital realities. In this future society, people will still be able to control and manage distance from others with new tools provided by ambient intelligence space technologies. (Beslay ; Hakala, 2005, p. 7)

Parede Virtual

Conceito similar ao de bolha digital é o de paredes virtuais. Trata-se, mais uma vez, de reconhecer e reivindicar as fronteiras dos territórios informacionais em um ambiente de computação ubíqua com o intuito de proteger a privacidade na era das mídias locativas. Kapadia (2007) trata de ambientes *pervasives* e dos riscos à privacidade com os sensores e dispositivos locativos que fazem com que os usuários deixem "pegadas digitais" (*digital footprints*). As paredes virtuais, pensadas como sistemas interfaces (GUI), devem permitir que os usuários controlem as suas pegadas digitais (geração, estoque e distribuição). Essas paredes virtuais atestam, como as bolhas digitais, a nova territorialidade dos

lugares como zona de controle informacional. O controle entre as bordas eletrônicas que compõem os espaços de lugar devem assim garantir a privacidade, o anonimato e a liberdade em ambientes ubíquos. Como mostram os autores, sensores, como as etiquetas RFID:

> "can record a user's activities and personal information such as heart rate, body temperature, and even conversations. Users may unwittingly leave 'digital footprints' (information about users derived from sensors) that can threaten their privacy. These footprints can be disseminated to applications, or stored for later retrieval, giving rise to useful context-aware applications" (Kapadia et al, 2007, p.162)

A ideia de *virtual wall* está preocupada com a confidencialidade das informações trocadas entre os diversos ambiente e captadas por redes sem fio, dispositivos ou sensores. Os autores partem da constatação de que deve haver o gerenciamento da confidencialidade e da privacidade por parte dos usuários. A confidencialidade é entendida aqui como o acesso/uso de informações apenas por pessoas ou sistemas autorizados. Os autores preferem o termo "impressão digital" por ser mais preciso do que "contexto", deixando antever assim monitoramentos, vigilâncias e controle das pegadas. Para os autores, *"*users will be more motivated to protect the privacy of their 'digital footprints' rather than their 'context." (Kapadia et. al, 2007, p.163). Proteger as pegadas e impressões, esses índices digitais, revela então novas formas de controle da informação entre fronteiras no seio de novos territórios. Aqui as fronteiras dos territórios informacionais tomam a forma de "muros ou paredes virtuais". Vejam a explicação dos autores para o conceito de parede virtual:

> "We propose a policy framework based on the intuitive concept of 'virtual walls' that extends the notion of privacy provided by physical walls into the virtual realm. For instance, users are aware of their physical privacy in a closed room — outsiders cannot see or hear them. In a pervasive environment, however, their virtual privacy could be quite the opposite. Digital footprints from a videocamera and a microphone could expose their privacy in the virtual world, where other users can see and hear them by accessing their footprints (...). Using virtual walls, users can 'bolster' physical walls by specifying intuitive policies that control access to all their personal footprints in a way that is consistent with their notion of physical privacy. Virtual walls also relieve the burden of specifying separate policies for several footprints, which would be cumbersome in sensor-rich environments." (Kapadia et al, 2007, p.163)

Tecnicamente essa parede virtual é uma interface que pode ser usada em diversos sistemas eletrônicos. Ressaltarei aqui apenas algumas característica importantes para a sua compreensão. A porosidade ou negociação do que passa ou não pelas paredes virtuais é definida em níveis: transparente, translúcido e opaco*,* revelando possibilidades de trocas controladas pelos usuários entre as membranas. Transparente significa permissão de ver todos os dados; translúcido, apenas alguns dados e opaco, nenhum. Define-se assim níveis de privacidade e de confidencialidade mostrando que o usuário pode

escolher o tipo de controle informacional, do que sai ou entra no seu território informacional de acordo com os níveis de permeabilidade:

> "In keeping with the metaphor of privacy afforded by physical walls, transparent virtual walls allow queries to access any footprints, even a user's personal information (such as their heart rate or whether they are speaking); opaque walls block access to all footprints originating from within the wall; and translucent walls allow queriers to access only general information such as room temperature and the presence of motion. To add flexibility, users may create walls of varying transparencies for different queriers." (Kapadia et al, 2007, p.166)

Interessante ver como o modelo dos autores define os conceitos de "lugar", "pegadas", "enquete" e "paredes virtuais". Por "lugar" os autores fazem referência a espaços físicos utilizados pelos usuários: salas e prédios que teriam etiquetas de identificação. O usuários "colocam" paredes virtuais em lugares específicos de acordo com os níveis de permissão citados acima. Isso mostra mais uma vez como os territórios informacionais redefinem e dão novos significados aos lugares. Uma parede virtual pode ser aplicada a qualquer lugar. No que concerne às "pegadas ou impressões", elas são originadas nos lugares a partir de sensores ou dispositivos eletrônicos de coleta de dados. Por exemplo, uma gravação de voz em um quarto é uma "pegada digital" originada no "lugar" quarto. Os autores as categorizam em "geral", que não revelam informações pessoais, como a temperatura do quarto; e "pessoal", que contém dados que identificam de alguma forma o usuário. O modelo de "enquete" assume que o usuário pode pesquisar sobre as pegadas a partir de uma combinação de variáveis: lugar, tempo, movimento, dono...Por fim, as "paredes" ou muros virtuais podem ser definidos como proteções eletrônicas permitindo ao usuário controlar a visibilidade de suas pegadas digitais nos lugares:

> "Virtual walls protect the privacy of users by allowing them to control the visibility of their personal footprints and general footprints in their vicinity. In our implementation, users create virtual walls through a GUI. The context server records walls in a persistent database and uses them to enforce the user's access control policies". (Kapadia et al, 2007, p.168).

O sistema foi testado com alguns usuários de *softwares* sociais. Os autores concluem, a partir desse estudo, que o modelo de paredes virtuais é fácil de usar e de compreender, e que os usuários conseguem traduzir as preferências de privacidade em paredes virtuais.

CONCLUSÃO

O regime de vigilância pela (in)visibilidade, de controle e monitoramento de movimentos, bem como de serviços e tecnologias baseados em localização nascem de pesquisas militares e servem aos

poderes estatais, policiais, comerciais e industriais de longa data. Os projetos com LBT e LBS acionam um registro de vigilância, controle e monitoramento de dados há muito instituído no complexo militar-industrial. Mostramos nesse artigo com as mídias locativas e o desenvolvimento da "internet das coisas" ameaçam a vida privada oferecendo possibilidades performativas de monitoramento, vigilância e controle.

O ambiente computacional ubíquo, transformando tudo em "pegadas digitais", é o pano de fundo da insegurança, da emergência do "*sujet insécure*" (Rosello, 2008). Isso faz do reconhecimento dos territórios informacionais uma barreira técnica e política (proteção por lei) contra a vigilância difusa e invisível da atual fase da cibercultura. As visões e projetos de "*digital bubble*" (Beslay; Hakala, 2005) e "*virtual wall*" (Kapadia, 2007) mostram as bordas dos territórios informacionais e se colocam como formas de proteção da privacidade nos domínios técnico, regulatório e sociológico. Os exemplos dados nesse artigo comprovam a amplitude e a seriedade das formas atuais de vigilância: locativa, móvel, invisível e sutil. Esta alimenta-se de maior liberdade e mobilidade informacional dos usuários e não do confinamento e da imobilidade da sociedade disciplinar, embora essa figura não tenha de todo desaparecido.

Como mostra David Lyon (2001), deve-se buscar uma visão ética da privacidade que considere o indivíduo com um todo, contra a tendência de digitalização de "representações" dos sujeitos em sistemas de processamento e mineração de dados, contra formas de violação das fronteiras dos territórios informacionais. Um conceito global da pessoa implicaria assim um controle mais efetivo das bordas, das bolhas e paredes virtuais do território informacional, no reconhecimento do "sujeito inseguro" e na necessidade de garantir a autonomia do sujeito sobre o que se faz e como se produz informações que lhe dizem respeito. Para Lyon:

> "The chain of events that connects Cartesian disengagement with the amoral actuarial surveillance of the twenty-first century can be broken. The first step is to understand how such surveillance systems operate and with what social and personal consequences. Articulated with this, the second step is to find agreement on what constitutes the human dignity and the social justice that may be compromised by those systems. I suggest that embodied, social, personhood provides such a starting point. Until the body is brought back in, and the face is recalled to its rightful place, surveillance systems will continue to haunt us with Cain's impertinent and fateful question."(Lyon, 2001)

REFERÊNCIAS

ALBRECHT, K; MCINTYRE, L. *Spychips. How majors corporations and government plan to track your every purchase and watch your every move.* New York: Plume Book, 2006.

BENFORD, S. *Future location-based experiences*. JISC Tech Report, 2005.

BENFORD, S.; FLINTHAM, M.; DRODZ, A. *The design and experience of the location-based performance uncle roy all around you*. Vol. 14, n. 3. Disponível em: <http://leoalmanac.org/journal/Vol_14/lea_v14_n03-04/roy.asp>, Acesso em: 10 de novembro de 2006

BESLAY, L., HAKALA, H. *Digital territory: Bubbles*. Draft Publication, European Community, Disponível em: <http://cybersecurity.jrc.es/docs/DigitalTerritoryBubbles.pdf>. Acesso em: 11 de novembro de 2005.

BRUNO, F. Monitoramento, classificação e controle nos dispositivos de vigilância digital. *Famecos,* Porto Alegre, n. 36, p. 10-16, 2008.

DELEUZE, G. *Post-Scriptum sobre as sociedades de controle.* In: DELEUZE, G., *Conversações: 1972-1990*, Editora 34, pp. 219-226, 1992. Disponível em: <http://netart.incubadora.fapesp.br/portal/midias/controle.pdf>, Acesso em: 03 de junho de 2008.

DELEUZE, G. ; GUATTARI, F. *Mille plateaux. Capitalisme et schizophrénie.* Paris: Les Editions de Minuit, 1980.

DODGE, M., KITCHIN, R. Outlines of a world coming into existence: pervasive computing and the ethics of forgetting**.** *Environment and planning B: Planning and design 2007*, v. 34, pp. 431 – 445, 2007.

FOUCAULT, M. De outros espaços. In: *Architecture, mouvement, continuité,* 1984. Disponível em: <http://www.rizoma.net/interna.php?id=169secao=anarquitextura> Acesso em: 25 de fevereiro de 2007.

GOW, G. *Privacy and ubiquitous network societies***.** Background Paper, ITU, 2005.

KAPADIA, A; HENDERSON, T; FIELDING, J; KOTZ, D. Virtual walls: Protecting digital privacy in pervasive environments. *Pervasive 2007*, pp. 162-179, Springer-Verlag Berlin Heidelberg. Disponível em: <http://www.springerlink.com/content/a651245g33k62p72/fulltext.pdf>, Acesso em: 15 de

outubro de 2008.

KELLERMAN, A. *Personal mobilities.* New York: Routledge, 2006.

KUITENBROUWER, K. *The cultural and social possibilities of RFID,* 2006. n. 11, Disponível em <http://www.skor.nl/id.php/KUITENBROUWERENGELSOPEN11> Acesso em: 15 de outubro de 2008.

LEMOS, A. Cidade e mobilidade. Telefones celulares, funções pós-massivas e territórios informacionais*. Matrizes, Revista do Programa de Pós-Graduação em Ciências da Comunicação.* USP, ano 1, n.1, São Paulo, 2007, ISSN 1982-2073, p.121-137, 2007.

_____. Comunicação e práticas sociais no espaço urbano: as características dos Dispositivos Híbridos Móveis de Conexão Multirredes *(DHMCM)*. *Revista Comunicação, Mídia e Consumo***,** São Paulo, v. 4, n. 10, p. 23-40, 2007a.

_____ . Mídias locativas e territórios informacionais. In: SANTAELLA, L., ARANTES, P. (ed) *Estéticas tecnológicas. Novos modos de sentir.* São Paulo: EDUSC., p. 207-230, 2008.

LYON, D. Facing the future: Seeking ethics for everyday surveillance. *Ethics and Information Technology*, v. 3, p. 171-181, 2001. Disponível em: <http://csalt.education.ecu.edu.au/projects/cyberspace/lyon/ethics_surveillance.pdf> Acesso em: 15 de outubro de 2008.

MANN, S.; NOLAN, J.; WELLMAN, B. Sousveillance: inventing and using wearable computing devices for data collection in surveillance environments". *Surveillance & Society*, Newcastle, v. 1, n. 3, p. 331-355, 2003.

MANOVICH, L. *The poetics of augmented space: Learning from Prada*. 2005, Disponível em: <http://www.noemalab.org/sections/ideas/ideas_articles/manovich_augmented_space.html>
Acesso em: 15 de outubro de 2008.

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

MONAHAN, T. *Surveillance and security. Technological politics and power in everyday life*. NY: Routledge, 2006.

POPE, S. The shape of locative media. *Mute Magazine***,** n. 29, 2005. Disponível em: <http://www.metamute.com/look/article.tpl?IdLanguage=1&IdPublication=1&NrIssue=2 9NrSection=10NrArticle=1477> Acesso em: 15 de outubro de 2008.

ROSELLO, M. *Culture de l'insecurité*. Disponível em: <http://www.cerium.ca/Insecurite-linguistique-et.>Montréal, Université de Montréal 2008.

RUSSEL, B. A Headmap Manifesto. Headmap.Org, 1999. Disponível em: <http://www.headmap.org>. Acesso: 15 de outubro de 2007

SACK, R. *Human territoriality: Its theory and history*. Cambridge: Cambridge University Press, 1986.

SANTAELLA, L. A estética política das mídias locativas. *Nómadas***.** Colombia: Universidad Central, n. 28, abril, 2008.

Scientific America. The future of privacy, special issue: Will technology kill privacy. NY, September, 2008. Disponível em: <http://www.sciam.com>

VAN KRONENBURG, R. *The internet of things. A critique of ambient technology and the all-seeing network of RFID.* Amsterdam: Waag Societt/Institute of Network Cultures, 2008.