Ciberespaço, vigilância e privacidade: o caso *Google Street View*

Elisianne Campos de Melo Soares

Universidade de Lisboa (UL)

Resumo

O Google *Street View* é um serviço de mapeamento fotográfico de ruas criado pela multinacional *Google* em 2007. Em maio de 2010, *Google* admitiu que os veículos utilizados para a captura de imagens coletaram, inadvertidamente, dados pessoais (sobretudo mensagens de *e-mail* e vídeos) transmitidos através de redes *wi-fi* privadas. Tendo em vista o problema de um possível atentado à vida privada e à segurança do tratamento de dados pessoais, pretende-se fazer uma breve análise do presente caso, trazendo à discussão algumas ideias tais como as de controle e vigilância no ciberespaço.

Palavras-chave

Cibercultura; Google *Street View*; Internet; Privacidade; Vigilância

Abstract

Google Street View is a street photographic mapping service created by the multinational *Google* in 2007. In May, 2010, *Google* admited that the vehicles used for image capture collected, inadvertently, personal data (especially e-mail messages and videos) transmitted through wi-fi private networks. Considering the problem of a possible attack to private life and personal data treatment security, it is intended to make a brief analysis of the present case, bringing to the discussion some ideas such as control and surveillance in cyberspace.

Keywords

Cyberculture; *Google Street View*; Internet; Privacy; Surveillance

1.0 O que é o Google *Street View*

O Google *Street View* é um serviço de mapeamento fotográfico de ruas criado pela multinacional Google Inc. em maio de 2007. A ferramenta oferece aos utilizadores vistas panorâmicas, ao nível das ruas, de 360° na horizontal e 290° na vertical. As imagens digitais são feitas por câmeras especiais acopladas ao teto de veículos da

empresa que circulam pelas ruas das cidades de vários países do mundo. O equipamento captura e faz corresponder imagens a um local específico através de dispositivos GPS. Ele possui ainda um sistema de coleta de dados de redes sem fio, para formular referências geográficas. Uma vez capturadas as imagens, estas são "costuradas" umas às outras para criar uma panorâmica de 360°. Após o processamento das imagens, Google aplica uma ferramenta que desfoca os rostos dos transeuntes e as matrículas de automóveis que apareçam nas fotografias.

Para visualizar as imagens de ruas, monumentos, etc. basta que o usuário vá ao portal do Google *Street View* na internet, selecione a opção “tilizar”e introduza o endereço desejado. Além de consultar as fotografias, o utilizador do serviço pode fazer marcações e introduzir comentários.

Atualmente, segundo informações do Google, o *Street View* já está inteiramente disponível para quase uma dezena de países na América do Norte, Europa e região Ásia-Pacífico. Portugal está na lista de países cobertos pelo serviço.

2.0 Alguns problemas –os casos da Alemanha, França e Reino Unido

Desde que surgiu, o *Street View* gera questionamentos relativos à privacidade das pessoas fotografadas e à recolha não autorizada de dados circulantes através da internet. No Brasil, por exemplo, alguns portais da *web* reproduziram imagens de pessoas em situações constrangedoras, de nudez ou violência, o que gerou apelações à justiça por parte de quem se sentiu exposto ao ridículo. Inúmeras situações semelhantes também foram registradas em outros países.

Porém, a polêmica maior surgiu quando Google confirmou, em maio de 2010 através de seu blog oficial, que alguns carros da sua frota tinham acidentalmente coletado informações pessoais por meio de conexões *wi-fi*. Segundo a empresa, a descoberta foi feita devido a uma investigação interna realizada a pedido de autoridades alemãs. Google declarou que seus veículos deveriam captar apenas dados abertos (chamados *beacon*), como o nome de redes públicas presentes em um determinado local, por exemplo. Mas acabaram por armazenar, também, dados de identificação de redes privadas e informações particulares (chamadas *payloads*) trocadas por usuários de redes sem fio desprotegidas. Esses dados eram interceptados quando alguém usava uma rede *wi-fi* perto de um carro do *Street View*.

O *Street View* causou reações imediatas na Alemanha, país de lei particularmente protetora da vida privada de seus cidadãos. Depois de longas negociações, Google finalmente disponibilizou um formulário *on-line* que possibilita aos alemães notificarem antecipadamente seu desejo em não ter sua casa identificada nas imagens. Por temerem que a segurança de suas propriedades fosse prejudicada, muitos alemães decidiram fazer valer a ferramenta. A reação impressionou a empresa, que revelou que mais de 250 mil pessoas escolheram utilizar essa função.

" Stasi ficaria verde de inveja se pudesse coletar esses tipos de dados" escreveu o jornal alemão *Frankfurter Allgemeine Zeitung,* em alusão ao órgão de inteligência e polícia secreta da República Democrática Alemã. " que se chamava de 'spionagem estatal'no passado hoje se chama 'oogle *Street View"*" acrescentou.

No Reino Unido, o Conselho de Proteção de Dados e Liberdade de Informação (I.C.O.), órgão supervisor da privacidade dos cidadãos, anunciou que não aplicaria nenhuma multa a Google pela recolha indevida de dados, desde que a empresa se comprometesse a não cometer o erro novamente e submetesse seu pessoal a treinamentos sobre segurança e proteção de dados pessoais. O diretor do I.C.O., Christopher Graham, disse em comunicado que a " ação regulatória mais apropriada e proporcionada"seria receber uma declaração escrita de Google de que a falha não será repetida e conduzir uma auditoria das práticas de proteção de dados da empresa.

Em 19 de novembro de 2010, Google concordou em apagar todas as informações recolhidas indevidamente. Em nota divulgada à imprensa, o escritório da empresa no Reino Unido declarou que não havia consultado nem utilizado os dados coletados em nenhum de seus produtos ou serviços.

Google usou um argumento similar quando foi punido na França pelas mesmas razões. A Comissão Nacional da Informática e das Liberdades (C.N.I.L.), órgão que visa adaptar a proteção das liberdades e da vida privada dos cidadãos franceses à evolução dos aparatos tecnológicos de tratamento de dados, condenou em 17 de março de 2011 Google a pagar uma multa de 100 mil euros pela coleta das informações.

Segundo a C.N.I.L., as irregularidades foram percebidas entre o final de 2009 e o início de 2010, quando o órgão descobriu que Google captava não só fotografias, mas também troca de correio eletrônico, senhas, etc. que circulavam nas redes sem-fio. À época, a C.N.I.L. declarou que essa captura de dados permitiu a Google desenvolver uma base de dados de geolocalização de alta performance, o que levou a empresa a uma

posição dominante no setor. Em abril de 2010 Google declarou à imprensa internacional que não coletava informações pessoais; acabou voltando atrás duas semanas depois, quando reconheceu o fato.

Em 26 de maio de 2010 a C.N.I.L. determinou que Google parasse com as atividades para o Google *Street View* e lhe fornecesse uma cópia integral de todos os dados coletados em território francês. A Comissão analisou as informações recebidas e constatou a coleta de dados de conexão a *websites*, senhas, endereços de correio eletrônico e mensagens de conteúdo sensível (com informações sobre o estado de saúde e a orientação sexual dos indivíduos implicados).

Em sua decisão publicada em março de 2011, a C.N.I.L. afirmou que Google comprometeu-se a cessar a coleta de dados de redes *wi-fi* e a suprimir as informações recolhidas. Porém, o texto afirma que a empresa não renunciou aos dados de identificação dos pontos de acesso das redes *wi-fi*, também mantidos à revelia dos usuários proprietários desses pontos. A Comissão também declarou que Google recusou-se a dar às autoridades acesso ao programa que levou à recolha inadequada de dados. Assim, haveria sempre o risco de que as informações voltassem a ser coletadas ilegalmente. Dadas as deficiências encontradas e à gravidade destas, a C.N.I.L. decidiu pela aplicação da sanção pecuniária no valor de 100 mil euros.

Google manteve-se silente. A empresa alegou que seu serviço de geolocalização não está sujeito à legislação francesa e que por isso se absteve de fazer uma declaração formal à C.N.I.L.. A Comissão obviamente contestou esse ponto de vista. A polêmica continua.

Países como os Estados Unidos e o Brasil enquadraram a atitude de Google com base em leis que proíbem a interceptação, sem autorização judicial, de comunicações telefônicas, de informática ou telemática. No Brasil, o *Information Security Research Team* (Insert), grupo de pesquisa em segurança da informação ligado à Universidade Estadual do Ceará (UECE), recorreu à justiça com base ainda em outro ponto da lei brasileira violado pelos veículos do *Street View*. O artigo 5º, inciso XII, da Constituição Federal determina que o sigilo de correspondência e comunicações seja inviolável.

3.0 Tipos de vigilância e tecnologias de controle

David Lyon (2004) estabelece três grandes categorias de vigilância no ciberespaço, relacionadas com o emprego, a segurança e policiamento e o *marketing*.

No emprego a vigilância caracteriza-se pela monitorização dos *sites* acessados e do correio eletrônico dos funcionários por parte dos diretores e supervisores, com o objetivo de saber se os empregados visualizam conteúdo inadequado (como pornografia, por exemplo) ou utilizam-se do tempo de trabalho para dedicar-se a assuntos *off-work*. Nos Estados Unidos, um estudo público realizado em abril de 2000 indicou que 73,5% das empresas americanas efetuam regularmente algum tipo de vigilância do uso da internet por parte de seus empregados (CASTELLS, 2007, p. 206).

No âmbito da segurança e do policiamento, podemos citar a vigilância proposta por órgãos como Alta Autoridade para a Difusão das Obras e a Proteção dos Direitos na Internet (HADOPI), na França, que promove a luta contra as redes P2P (*peer-to-peer*) e a oferta de *downloads* gratuitos de músicas, filmes e livros protegidos por direitos autorais no universo virtual através da monitorização das atividades dos usuários. HADOPI propõe que os servidores de acesso à internet vigiem a movimentação dos usuários e repassem ao órgão relatórios com a identificação daqueles que infringem os direitos de autor na *web*. Após uma primeira advertência, caso haja reincidência, o utilizador perde o direito de acesso à internet a partir do ponto onde o desrespeito foi cometido e, mesmo assim, continua a pagar pelo serviço ao servidor contratado.

Há também a vigilância conduzida por serviços policiais, como o FBI americano, que em 1995 realizou uma operação batizada de "peração Inocente" ação sob disfarce na America *On-Line* (AOL) envolvendo a interceptação de correio eletrônico de pessoas suspeitas de trocar materiais de pornografia infantil pela *web* (ZUIDWIJK E STEEVES *apud* LYON, 2004, p. 115). O organismo federal também mantém o programa Carnivore, que trabalha em colaboração (voluntária ou não) com fornecedores de acesso à internet, registrando todo o tráfego de correio eletrônico, posteriormente catalogando a informação com base em uma amostra e processamento automatizado de palavras-chave.

Para Terceiro (1996, p. 185), a recolha de dados na internet possibilitou o surgimento de uma nova fonte de lucro: as informações pessoais dos usuários da *web*.

> A utilização das redes de computadores facilita o recolhimento de dados sobre seus usuários, com o que se obtém um sub-produto automático suscetível de utilização e comercialização. O atentado à privacidade das pessoas que supõe essa recolha de dados provoca sérias preocupações em relação à sua proteção, confiada a técnicas de encriptação que até bem pouco tempo pertenciam ao clandestino mundo da espionagem e hoje são moeda corrente no mundo digital.

As informações obtidas pela vigilância direcionada ao *marketing* são massivamente utilizadas, frequentemente de forma indiscriminada, para fins comerciais. Não é novidade que as empresas procurem ter acesso a informações privadas concernentes aos usuários da *web*: tecnologias já foram desenvolvidas unicamente com o intuito de recolher dados que permitam traçar perfis dos internautas. É o caso dos *cookies* (*Client-Side Persistent Information*), espécie de marcadores digitais que os sites colocam automaticamente nos discos rígidos dos computadores que a eles acedem. Uma vez inserido o *cookie* em um computador, todos os movimentos *on-line* realizados a partir dele são gravados automaticamente pelo servidor do *site* que o colocou (CASTELLS, 2007, p. 204). Com o auxílio de tecnologias como essa, empresas de *marketing* e comunicação na *web* vendem os dados pessoais dos seus utilizadores aos seus clientes com fins comerciais ou utilizam-nos eles próprios para os definirem melhor. Portanto, vê-se que as tecnologias de recolha de dados associam-se diretamente à economia do comércio eletrônico. As movimentações dos usuários são monitoradas, na maioria das vezes, à revelia destes. Como diz Rohan Samarajiva (*apud* LYON, 2004, p. 113):

> A chamada "lientela de massa"cria incentivos à recolha de dados pessoais para uso no processo de produção e *marketing*. Os fabricantes ou retalhistas pretendem estabelecer tipos de serviço no relacionamento com os clientes, recolhendo, armazenando ou manipulando informações acerca deles de modo a controlar os seus comportamentos.

Como afirma Rosen (*apud* CASTELLS, 2007, p. 208), "s tecnologias que tornam possível descarregar livros, revistas, músicas e filmes em formato digital para o disco rígido de um computador, permitem às editoras e às empresas de lazer registar e controlar os hábitos de navegação das pessoas para poderem enviar publicidade específica a cada um dos seus clientes"

Na União Europeia, a maior pressão governamental a favor da proteção do consumidor resultou numa lei da privacidade, sob a qual as empresas não estão autorizadas a utilizar os dados pessoais dos seus clientes sem a sua aprovação explícita (CASTELLS, 2007, p. 209). O problema é que muitos *sites* contêm, em seus longos termos de uso, cláusulas que determinam que os dados pessoais fornecidos convertam-se em propriedade legal das empresas de internet e dos seus clientes. Poucos usuários leem integralmente esses termos de uso, concordando com algo que desconhecem –e

muitos desses *sites* só liberam seus serviços e funcionalidades depois que o utilizador aceita as regras propostas.

As oportunidades de negócio parecem ilimitadas neste novo ramo dedicado a comercializar o comportamento privado. Nas eleições do ano 2000, nos Estados Unidos, uma empresa criou uma base de dados chamada Aristotle, que através da recolha de informações e dados de diversas fontes, traçou um perfil político de cerca de 150 milhões de cidadãos. O objetivo era vender esse banco de dados pelas melhores ofertas possíveis, que geralmente eram feitas pelos escritórios eleitorais dos candidatos (CASTELLS, 2007, p. 209).

Manuel Castells (2007) divide as tecnologias de controle em três tipos: tecnologias de identificação, de vigilância e de investigação. As tecnologias de identificação incluem o uso de *passwords*, *cookies* e processos de autenticação –estes últimos utilizam assinaturas digitais que permitem a outros computadores verificar a origem e as características da máquina que se liga à rede; é um protocolo de segurança vastamente adotado por empresas de comércio eletrônico e emissoras de cartões de crédito.

As tecnologias de vigilância interceptam mensagens e colocam marcadores que permitem seguir o fluxo de comunicação a partir de um determinado computador e controlar permanentemente a atividade da máquina. Elas podem identificar um servidor específico na origem de uma mensagem. Valendo-se disso, e através de persuasão ou de coação, os governos, empresas ou tribunais podem obter do servidor de acesso à internet a identificação do usuário suspeito. É o que faz a já anteriormente citada HADOPI.

As tecnologias de investigação, por sua vez, elaboram bases de dados através dos resultados da vigilância e acumulação de informação gravada assiduamente (GARFINKEL *apud* CASTELLS, 2007, p. 205). Constrói-se um perfil agregado a partir dos vários dados recolhidos em formato digital, algo semelhante ao que fazem os estudos de mercado.

O que John Beniger (1986) chama de "evolução do controle"espalha-se por todas as organizações contemporâneas. Como afirma Lyon (2004, pp. 118-119),

> Os empregadores tentam reduzir o risco –de trabalhadores que usam o horário ou o equipamento de trabalho para os seus próprios objectivos, por exemplo –em situações de emprego. A polícia, em conjunto com outras instituições, trabalha no sentido de prevenir o risco da prática de crimes ou, mais genericamente, de comportamentos ameaçadores. E os homens de

> negócios fazem tudo o que estiver ao seu alcance para evitarem os riscos de perder oportunidades, nichos de mercado e, em última instância, lucro. Todos estabelecem procedimentos de recolha de dados para tentarem assinalar riscos (ou oportunidades) e prever resultados. Por conseguinte, a vigilância espalha-se, tornando-se constantemente mais rotineira, mais intensiva (perfis) e extensiva (populações), guiada por forças económicas, burocráticas e agora tecnológicas.

Em relação ao caso Google *Street View*, a ameaça principal é justamente a comercialização ilegal de dados por parte de Google, tanto para benefício de seus parceiros comerciais como da própria empresa. Os internautas que veem na internet um espaço de neutralidade e liberdade absolutas ignoram que, na realidade, o rei está nu: seus movimentos na rede podem estar sendo monitorados, e as informações que trocam, interceptadas por ordem de uma rede de interesses econômicos, mas não só. As técnicas de vigilância não são úteis apenas aos que ganham dinheiro com isso, mas também aos governos, que começam a fazer da *web* um novo território de observação, onde é possível exercer certo controle sobre os movimentos dos cidadãos.

4.0 O ciberespaço, um território informacional

Em seu início de existência global, a internet parecia ser um espaço de libertação. Podia-se fazer muito pouco para controlar o fluxo de informações que transpassam as fronteiras geográficas. Segundo Castells (2007, p. 201),

> A privacidade estava protegida pelo anonimato da comunicação na internet, assim como pela dificuldade de encontrar as fontes e identificar o conteúdo das mensagens transmitidas por meio dos protocolos da internet. Este paradigma da liberdade estava baseado em fundamentos tecnológicos e institucionais. Tecnologicamente, a sua arquitetura, baseada na ligação informática em rede sem restrições, [....] torna bastante difícil –para não dizer impossível –controlá-la.

Mas o desenvolvimento da informática expandiu não apenas as ferramentas libertárias que abriram um maior acesso à informação e à cultura, mas também os meios de controle desse acesso. A tecnologia se mostra uma faca de dois gumes, capaz de facilitar o contato de seu usuário com canais democráticos de participação, porém, ao mesmo tempo, útil aos governos e aos grupos de interesses em sua empreitada pela vigilância das atividades desse usuário na rede. Conforme salienta Castells (2007, p. 203),

> Aplicações de *software* podem configurar-se sobre a internet, permitindo a identificação de rotas de comunicação e conteúdos. Através do uso destas tecnologias, pode-se transgredir a privacidade e, enquanto se chega a relacionar determinados indivíduos com processos de comunicação específicos em contextos institucionais concretos, é possível utilizar todas as formas tradicionais de controlo político e organizativo contra o indivíduo ligado em rede.

Dispositivos móveis, equipamentos informáticos interligados e redes sem fio constituem o território informacional. Entenda-se por território informacional as zonas de controle de informação resultantes da intersecção do espaço físico com o eletrônico. "ensar em termos de território digital permite visualizar a fronteira do fluxo informacional e nos colocar questões políticas relativas à privacidade, ao controle e à vigilância"(LEMOS, 2007). Isto porque "odo território informacional é um lugar social de vigilância de fronteiras, já que ' soberania se exerce nos limites de um território' (FOUCAULT, 2006, p. 27). Os territórios informacionais são lugares onde se exercem controles [....]"(LEMOS, 2007). Em obra posterior, André Lemos (2010), afirma que

> 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: 221).
> 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 "erritório digital ou bolha"(Beslay; Hakala, 2005), "spaço intersticial"(Santaella, 2008), "ealidade 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).

A vigilância no mundo virtual é fruto principalmente da comercialização da *web*. Na criação de sistemas de identificação do usuário, há uma fonte potencial de lucro para empresas de certificação digital e controle de acesso. A questão comercial desse controle também envolve os direitos autorais na internet. Para Castells (2007, p. 203), a implementação de sistemas de vigilância é interessante para os governos, que querem

encontrar alguma forma de instaurar, no ambiente virtual, ferramentas de controle semelhantes às existentes na esfera física:

> A transformação da liberdade e da privacidade na internet é consequência directa da sua comercialização. A necessidade de assegurar e identificar a comunicação na internet para poder ganhar dinheiro graças à rede e a necessidade de proteger os direitos da propriedade intelectual na mesma, resultaram no desenvolvimento de novas arquitecturas de *software* (o que Lessig denomina como "ódigo" que possibilitam o controle da comunicação informática. Os governos de todo o mundo apóiam estas tecnologias de vigilância e apressam-se a adoptá-las, para conseguirem recuperar parte do poder que corriam o risco de perder.

O monitoramento através de autoridades policiais, empresas ou outros órgãos investidos de autorização concedida pelo poder legislativo seriam, conforme Lemos (2007) ressalta, "....] uma forma de 'nvasão'dos territórios informacionais, como entrar na residência seria uma invasão do território residencial. As '*digital borders*'criam, nos territórios informacionais, um *continuum* entre o mundo físico e o espaço das informações eletrônicas" Para Raab (2008, p. 256), a vigilância afeta diretamente alguns importantes pilares da vida social, e pode feri-los se direcionada para fins comerciais, por exemplo: "s práticas de vigilância têm implicações na privacidade e em muitos outros valores importantes: na justiça, na dignidade humana, na autodeterminação, na inclusão social, na segurança, e por aí fora. Alguns destes valores podem ser protegidos se a privacidade estiver salvaguardada"(RAAB, 2008, p. 256).

A vigilância na *web* representa, portanto, mais um exemplo do que Mireille Rosello (*apud* LEMOS, 2010) chama de "ultura da insegurança" de caráter planetário. Além disso, marca o fim da já utópica ideia de um território neutro e livre de controle imaginada nos primórdios da internet. Raab (2008, p. 266), porém, afirma que a informática pode disponibilizar ferramentas que funcionariam como um antídoto contra a insegurança que ela própria possibilitou. Isso seria possível através de tecnologias de filtragem de *cookies*, métodos de encriptação mais potentes, etc. No entanto, é importante salientar que as empresas, os governos e os fabricantes de tecnologia não têm interesse em pôr em marcha essas tecnologias de reforço da privacidade. Sendo assim, os indivíduos que delas quiserem fazer uso deverão empreender esforços adicionais, além de pagar mais para delas se beneficiarem.

5.0 Considerações finais

A recolha e o armazenamento arbitrários de dados digitais se tornaram regra no mundo virtual. Aí se veem os efeitos nefastos do progresso tecnológico (HEUER, 2011, p. 85). O custo do armazenamento de dados em formato digital tornou-se tão baixo que já se mede em *terabytes* (a capacidade de armazenamento de um computador portátil corrente corresponde a pouco mais de metade de um *terabyte*). Há cada vez mais bancos de dados a registrar nossos movimentos na *web* –a Biblioteca do Congresso dos Estados Unidos, em Washington, anunciou recentemente que pretende arquivar todas as mensagens postadas no Twitter desde seu surgimento, em 2006.

De fato nossa vida esteve sempre sob algum tipo de controle –desde a presença em registros de cartórios à identificação em bancos de dados de diversos serviços públicos. O que se alterou com a informatização da sociedade e o advento da internet foi o posicionamento desses registros no espaço. As informações não estão mais fixadas apenas em suportes materiais, livros de atas e papéis de arquivos. Elas estão ao alcance de alguns cliques, mundialmente disponíveis, suscetíveis a cruzamentos, mais sujeitas ao acesso legal ou não autorizado do que nunca. A nova vigilância surgida através das tecnologias digitais é mais sutil, está em todos os lugares e, ao mesmo tempo, em lugar nenhum. Ela é cada vez menos perceptível e mais difusa. Sua fluidez está na invisibilidade e na mobilidade das redes.

Catarina Frois (2008, p. 130) salienta a mudança trazida pela vigilância onipresente da informática:

> Aparentemente, nada disto é exclusivo dos dias de hoje. O propósito das estatísticas, da aglomeração de informação, da recolha de dados pessoais, seja para finalidades de criar perfis de consumo, para fins médicos, para avaliação do sistema de educação, tem como objectivo proporcionar um maior conhecimento sobre uma determinada matéria (Hanson, 1993). Porém, na sociedade contemporânea, a existência de grandes bases de dados informáticas que centralizam informação detalhada dos cidadãos e que é depois cruzada com informação constante noutras bases de dados pessoais ameaça pôr em risco o direito à privacidade, à integridade física e moral, ou mesmo, em última análise, o direito à escolha. [...] O que vemos é uma confluência de dispositivos de reconhecimento da pessoa que abrangem quase todas as esferas da sua vida, desde a sua identidade burocrática e administrativa, a sua história genética e distintividade biométrica e os locais que frequenta, quando e com quem. Neste sentido, é inevitável reconhecer-se que hoje em dia identificar e vigiar são duas acções que andam de mãos dadas. Parece não bastar saber-se quem a pessoa é: urge (quer por parte do Estado, quer por parte de interesses comerciais) saber-se o que quer e o que vai fazer. Poderíamos dizer que na sociedade contemporânea só identificando é possível conhecer-se e só vigiando é possível prever-se.

Para Deleuze (1992), a sociedade do controle era o que Foucault (1984) anunciava como o nosso futuro próximo, o que em termos práticos de vigilância quer dizer que as tecnologias não são mais visíveis e imóveis, mas ubíquas, *pervasives*, "as coisas" não exigindo do indivíduo o confinamento, mas exatamente o contrário: a mobilidade, o que permite um controle dinâmico. Afinal, não podemos esquecer que essas tecnologias têm origem militar. Toda mídia locativa, por seu caráter que associa mobilidade e localização, pode ser usada para monitorar movimentos, vigiar pessoas e controlar ações no dia a dia.

Manuel Castells (2007, p. 215) e diversos outros teóricos da informática e da cibercultura afirmam que a presença em registros e bancos de dados digitais traz às vistas o terrível temor da sociedade vigilante antecipada por George Orwell em seu "984" e pode funcionar como uma forma de repressão à liberdade pela possibilidade do controle constante:

> Não é o *Big Brother* quem nos vigia, mas sim uma multitude de pequenas irmãs (*little sisters*), agências de vigilância e processamento de informação, que registrarão sempre o nosso comportamento, já que estaremos rodeados de bases de dados ao longo de toda a nossa vida [....]. Nas sociedades democráticas onde se respeitam os direitos civis, a transparência das nossas vidas condicionará as nossas atitudes de forma decisiva. Ninguém conseguiu viver jamais numa sociedade transparente. Se este sistema de vigilância e controlo da internet se desenvolver plenamente, não poderemos fazer o que quisermos. Não teremos liberdade, nem um lugar para nos escondermos.

Isso nos leva a um tema que também está na ordem do dia em vários países europeus: o direito ao esquecimento. Um exemplo que ilustra esse direito está na lei francesa de 6 de janeiro de 1978, relativa à informática, aos arquivos e às liberdades, que prevê em seu artigo nº 40:

> Toda pessoa física justificante de sua identidade pode exigir do responsável pelo tratamento de dados que as informações pessoais que lhe concernem sejam retificadas, completadas, atualizadas ou apagadas [....] logo elas sejam inexatas, incompletas, equivocadas, desatualizadas, ou cuja coleta, utilização, comunicação ou conservação seja proibida.

A Comissão Europeia examina a possibilidade de rever a diretiva sobre a proteção de dados de forma a incluir o direito ao esquecimento, como foi anunciado em novembro de 2010 pela comissária da justiça, Viviane Reding (HEUER, 2011, p. 85).

Na Alemanha, governo e parlamento debatem projetos que visam permitir aos cidadãos controlar de forma mais eficaz sua vida digital. Na França, foi adotada em outubro de 2010 uma carta não vinculativa, por iniciativa da secretária de Estado das Tecnologias à época, Nathalie Kosciusko-Morizet. Muitos dos intervenientes franceses na rede assinaram o documento –à exceção do Facebook e, claro, de Google.

Referências bibliográficas e webgráficas

BENIGER, John. **The control revolution**. Cambridge: Harvard University Press, 1986.

CARDOZO, André. **Google coletou dados pessoais por engano por mais de três anos**. Último Segundo. Publicado em: 14 de maio de 2010. Disponível em: < http://tecnologia.ig.com.br/noticia/2010/05/14/google+coletou+dados+pessoais+por+engano+por+mais+de+tres+anos+9485745.html>. Último acesso: 01 de julho de 2011.

CASTELLS, Manuel**. A galáxia internet: reflexões sobre internet, negócios e sociedade**. Lisboa: Fundação Calouste Gulbenkian, 2007.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (C.N.I.L.). **Google "Street View": la C.N.I.L. prononce une amende de 100 000 euros**. Publicado em: 21 de março de 2011. Disponível em: <http://www.cnil.fr/la-cnil/actu-cnil/article/article/google-street-view-la-cnil-prononce-une-amende-de100-000-euros/>. Último acesso: 20 de junho de 2011.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (C.N.I.L.). **Loi du 6 janvier 1978, relative à l'nformatique, aux archives et aux libertés**. Disponível em: <http://www.cnil.fr/fileadmin/documents/approfondir/textes/CNIL-78-17_definitive-annotee.pdf>. Último acesso: 01 de julho de 2011.

DELEUZE, Gilles. *Post-Scriptum* sobre as sociedades de controle. *In*: Deleuze, Gilles. **Conversações**. 1992. Disponível em: <http://www.portalgens.com.br/filosofia/textos/sociedades_de_controle_deleuze.pdf>. Último acesso: 07 de julho de 2011.

O ESTADO DE S. PAULO. **Google vai apagar dados coletados com o Street View no Reino Unido**. Publicado em: 19 de novembro de 2010. Disponível em: <http://blogs.estadao.com.br/link/google-vai-apagar-dados-coletados-com-o-street-view-no-reino-unido/>. Último acesso: 01 de julho de 2011.

FOUCAULT, Michel. **De outros espaços**. 1984. Disponível em: <http://www.virose.pt/vector/periferia/foucault_pt.html>. Último acesso: 07 de julho de 2011.

FROIS, Catarina. Bases de dados pessoais e vigilância em Portugal: análise de um processo em transição. *In*: FROIS, Catarina (org.). **A sociedade vigilante –Ensaios sobre identificação, vigilância e privacidade**. Lisboa: Imprensa de Ciências Sociais, 2008.

GOOGLE. **Nos bastidores**. Disponível em: <http://maps.google.pt/intl/pt-PT/help/maps/streetview/behind-the-scenes.html>. Último acesso: 06 de maio de 2011.

GOOGLE. **Que veículos utilizamos?**. Disponível em: <http://maps.google.pt/intl/pt-PT/help/maps/streetview/behind-the-scenes.html>. Último acesso: 06 de maio de 2011.

HEUER, Steffan. **A rede lembra-se de tudo?**. Courrier Internacional. Publicado em: abril de 2011. Nº 182. Páginas 84-88.

LE MONDE.FR. **Google cesse de photographier les rues allemandes**. Publicado em: 11 de abril de 2011. Disponível em: <http://www.lemonde.fr/technologies/article/2011/04/11/google-cesse-de-photographier-les-rues-allemandes_1505725_651865.html>. Último acesso: 20 de junho de 2011.

LE MONDE.FR. ***Street View*: la C.N.I.L. inflige une amende à Google**. Publicado em: 21 de março de 2011. Disponível em: <http://www.lemonde.fr/technologies/article/2011/03/21/street-view-la-cnil-inflige-une-amende-a-google_1496083_651865.html>. Último acesso: 20 de junho de 2011.

LEMOS, André. Mídia locativa e territórios informacionais. *In*: ARANTES, Priscila; SANTAELLA, Lúcia. **Estéticas tecnológicas**. São Paulo: Editora PUC, 2007.

LEMOS, André. Mídias locativas e vigilância: sujeito inseguro, bolhas digitais, paredes virtuais e territórios informacionais. *In*: BRUNO, F., KANASHIRO, M., FIRMINO, R., **Vigilância e visibilidade - Espaço, tecnologia e identificação**. Porto Alegre: Sulina, 2010.

LYON, David. A *World Wide Web* da vigilância: a Internet e os fluxos de poder *off-world*. *In:* OLIVEIRA, José M.P.; CARDOSO, Gustavo L.; BARREIROS, José J. (orgs.). **Comunicação, cultura e tecnologias da informação**. Lisboa: Quimera, 2004.

MARTINS, Leo. ***Street View* chega ao Brasil. O que fazer com ele?**. Gizmodo Brasil. Publicado em: 30 de setembro de 2010. Disponível em: <http://www.gizmodo.com.br/conteudo/street-view-chega-ao-brasil-o-que-fazer-com-ele/>. Último acesso: 06 de maio de 2011.

MAZZA, Carlos. **Google sob suspeita**. Jornal O Povo. Publicado em: 26 de maio de 2011. Disponível em: < http://www.opovo.com.br/app/opovo/tendencias/2011/05/26/noticiatendenciajornal,2249203/google-sob-suspeita.shtml>. Último acesso: 01 de julho de 2011.

NÃO SALVO. **50 flagras do Google *Street View* que você ainda não viu**. Disponível em: <http://www.naosalvo.com.br/vc/50-flagras-do-google-street-view-que-voce-ainda-nao-viu/>. Último acesso: 06 de maio de 2011.

RAAB, Charles D.. Vigilância e privacidade: as opções de regulação. *In*: FROIS, Catarina (org.). **A sociedade vigilante –Ensaios sobre identificação, vigilância e privacidade**. Lisboa: Imprensa de Ciências Sociais, 2008.

TERCEIRO, José B.. **Sociedad digital: Del homo sapiens al homo digitalis**. Madrid: Alianza Editorial, 1996.