37º Encontro Anual da ANPOCS

ST 27 – Ciberpolítica, ciberativismo e cibercultura

Big data: reconstrução e disputa por novos significados de privacidade[1]

Marta Mourão Kanashiro[2]
Fernanda Glória Bruno[3]
Rafael de Almeida Evangelista[4]
Rodrigo José Firmino[5]

1 Este texto também será apresentado no Society for Social Studies of Science Annual Meeting (4S) (outubro, 2013) e foi submetido a Revista Rua com o título "Maquinaria da privacidade". A alteração de titulo reflete uma possibilidade de nova aproximação teórica, discutida no andamento deste trabalho. Explicamos que por maquinaria compreendemos um conjunto de máquinas que funcionam de forma complementar modificando o sentido e a intensidade de uma força.

2 Pesquisadora do Labjor Unicamp, professora plena do Programa de Pos-Graduação em Divulgação Cientifca e Cultural, e professora colaboradora do Programa de Pós Graduação em Sociologia, ambos também da Unicamp. Email: mmk@unicamp.br

3 Professora associada do Programa de Pós-Graduação em Comunicação e Cultura, da Escola de Comunicação da Universidade Federal do Rio de Janeiro (UFRJ). Email: bruno.fernanda@gmail.com

4 Pesquisador do Labjor Unicamp e professor plena do Programa de Pos-Graduação em Divulgação Cientifca e Cultural: rae@unicamp.br

5 Professor associado do Programa de Pós-Graduação em Gestão Urbana e do curso de Arquitetura e Urbanismo da Pontifícia Universidae Católica do Paraná (PUCPR). Email: rodrigo.firmino@pucpr.br

Abstract

It is increasingly difficult to think of communication nowadays untied from the possibility of monitoring and surveillance. This paper addresses this issue and its relationship with new meanings that the notion of privacy is acquiring. The context of this discussion is that of the so-called big data, or the growing possibilities to aggregate and extract value from a massive volume of unstructured and splintered data. From the privacy policies that regulate the use of e-mail services, data storage and social media, and from the privacy requirements by activist groups, we can observe the reconstruction of this concept and the tensions in which it operates. This is an ongoing research that seeks to further scrutinize the debates earlier explored in other three previous studies about: 1) surveillance cameras in Brazil, 2) biometric recognition in the new Brazilian identity scheme, and 3) the mapping of personal data monitoring in Brazil and Mexico. On these occasions, it was observed a series of transformations related to the practice of monitoring, including the destabilization of concepts such as individual, security and democracy. This paper examines the notion of privacy in contemporary everyday life.

Keywords: privacy, technologies of information and communication, ciberculture, social network.

Resumo

É cada vez mais difícil pensar em comunicação na atualidade desvinculada da possibilidade de monitoramento. Este trabalho aborda este tema e sua relação com novos sentidos que a noção de privacidade vem adquirindo. O contexto dessa discussão é o *big data* ou as crescentes possibilidades de agregar e extrair valor de um gigantesco volume de dados esparsos e não estruturados, que cresce em velocidade vertiginosa. A partir dos contratos de privacidade para utilização de serviços de *e-mail*, de armazenamento de dados e redes sociais, e das exigências de privacidade por parte de grupos ativistas, podemos observar a reconstrução deste conceito e o embate no qual se insere. Esta é uma pesquisa em andamento que busca dar continuidade a três estudos anteriores sobre 1) câmeras de vigilância no Brasil, 2) reconhecimento biométrico no novo documento de identidade brasileiro, e 3) um mapeamento de aspectos da vigilância de dados no Brasil e no México. Nessas ocasiões, observou-se um rol de transformações ligadas ao monitoramento, incluindo a desestabilização de conceitos como indivíduo; segurança; democracia. Este trabalho reflete sobre a noção de privacidade no cotidiano contemporâneo.

Palavras-chave: privacidade, tecnologias de informação e comunicação,

cibercultura, redes sociais.

1. Introdução

Palavras, noções e conceitos não são fixos ou estáveis ao longo dos séculos e em diferentes contextos socioespaciais. Por mais banal que possa parecer tal afirmação, sua importância aprofunda-se em tempos de diluição intensa e cotidiana de tantas ideias que estruturaram grande parte dos modos de fazer, de ver e de saber da modernidade. A atual desestabilização de determinados conceitos nos obriga a um questionamento sobre o que está em transformação, sendo desconstruído, disputado, construído ou atualizado. Não se trata, portanto, de uma questão de terminologia, de estudar termos e seu uso, pensar sobre etimologias, e nem do que é reservado ao reino dos glossários. Mas sim, de problematizar as transformações desses conceitos em seu nível operativo e produtivo, assim como também de enfrentar a questão nietzschiana “Que estamos ajudando a fazer de nós mesmos?” reexaminada, dentre outros, por Orlandi (2002).

Dentre os muitos conceitos que mereceriam este tratamento na atualidade, o presente artigo trata de *privacidade* e dos embates que atravessam essa noção. Bruno (2010) ressalta que ainda que essa seja uma ideia que tenha se consolidado jurídica, social e subjetivamente na modernidade, já em seu nascimento era objeto de tensões, deslocamentos e disputas políticas e sociais. Vários autores se voltaram para esse tema (dentre muitos outros, Elias, 1994; Sennet, 1999; Duby e Ariès, 2000; Del Priore, 2011) abordando a construção do privado, da intimidade e da privacidade, suas variações históricas e as tensões políticas e sociais com as quais se vinculavam.

A dimensão do segredo, do escondido, do íntimo, da privacidade ou do privado, tal como se conheceu na modernidade, vem sendo desconstruída, reformulada ou atualizada em diferentes níveis: dos programas televisivos para exposição da intimidade ao que circula nas redes sociais, chegando até qualquer tipo de ação (e seu consequente rastro) na internet e no uso de tecnologias de comunicação (Bruno et al, 2012). Nesse contexto, em que é cada vez mais difícil pensar possibilidades de comunicação desvinculadas da possibilidade de monitoramento, não estamos diante dos limites (e valores) entre a casa e a rua (DaMatta, 1984), entre público e privado (Senett, 1999; Elias, 1994), aqueles da porta fechada ou da alcova, e nem estamos presenciando a fenda na parede ou o buraco da fechadura como transgressão ou transposição de uma demarcação estabelecida.

Recentemente, enquanto uma série de textos jornalísticos vêm anunciando o fim da *privacidade*, e grupos ativistas se empenham em protegê-la, governos buscam regulamentá-la e outros tantos autores (Bauman, 2011; Lyon, 2003 etc) vem apontando o deslocamento dessa noção. Tendo em vista esse panorama, a ideia inicial deste artigo partiu da questão: como se delineia a privacidade da qual se fala hoje, quando se busca constatar seu aniquilamento, protegê-la, ou regulamentá-la diante das novas tecnologias que permitem a comunicação e também o monitoramento, a identificação e a vigilância? O que está sendo produzido ou deslocado nesse processo?

Em seu filme *Imagens da prisão* (2003), o videasta Harun Farocki, aborda elementos da sociedade disciplinar de Foucault (2000) e da sociedade de controle de Deleuze (2000), que espelham muito bem a diluição de conceitos aqui tratada. Podemos assistir com Farocki a passagem do conceito de indivíduo como sujeito e objeto de saber na constituição das disciplinas, para o fluxo de dados e informações, na constituição do controle (Kanashiro, 2006).

No que concerne a privacidade, há em Farocki pistas muito interessantes dessa transformação. Ao apresentar uma recombinação[6] de partes de filmes sobre prisões, em que guardas espiam pelas portas e frestas a sexualidade dos prisioneiros, Farocki parece delinear uma certa concepção disciplinar de privacidade por meio de sua transgressão naquele espaço. Já em outro momento do mesmo filme, o videasta nos mostra a observação pelos guardas de imagens de câmeras de vigilância em uma prisão na Califórnia (EUA), em que os vigilantes criam possibilidades de brigas entre presos nos pátios da prisão para assisti-las pela tela e apostar naquele que venceria, ou naquele que sairia vivo da situação. Do espaço cela ao espaço pátio, do mais fechado, ao mais aberto (ainda que interno a prisão) passa-se da observação da sexualidade como transposição da privacidade para a observação da luta, da competição e da morte[7], e respectivamente do prazer sexual, para o prazer do ganho monetário com a aposta.

O presente artigo pretende percorrer algumas dessas pistas deixadas por Farocki para lançar uma reflexão ainda inicial sobre os embates acerca da privacidade, os deslocamentos e atravessamentos que a compõem e que são produzidos nesse processo. Documentos da política de privacidade da empresa Google são as fontes da análise empírica[8] presentes nesse texto, que parecem expor alguns dos elementos aos quais Farocki nos remete, assim como permitem observar uma parte do que se delineia como privacidade em disputa hoje.

2. A privacidade 2.0

A página de políticas (*policies*) do Google, aonde encontramos *links* para os “Termos de serviços” e para a “Política de privacidade” da empresa, exibe em letras maiores que as do restante da página a seguinte frase: "Estamos comprometidos com a melhoria de sua segurança, com a proteção de sua privacidade e com a criação de ferramentas simples para lhe dar escolhas e controle” (Google, 2013). Nessa mesma página, outras frases procuram expressar a preocupação da empresa com relação a privacidade, mas sempre colocando ao seu lado os termos “proteção” e “segurança”, os quais são relacionados ao usuário, a sua família e contra cibercrimes.

Como os “Termos de serviço” da empresa são alterados periodicamente em função de

---

6 Vale notar que nenhum plano foi filmado pelo videasta e que a obra de Farocki se realiza pelo processo de recombinação de imagens e informações já existentes e finitas. Neste sentido, o próprio filme é processo operatório vigente no controle. Orlandi (2002) ao retomar a pergunta “Que estamos ajudando a fazer de nós mesmos”, aborda as combinações de forças no homem e de forças do fora apontando uma forma dominante em cada configuração histórica, e com relação ao século XX argumenta que independente da forma que é necessário levar em conta o tipo de combinação de forças que o caracteriza. Orlandi, retoma a leitura de Deleuze sobre Foucault e aborda esse processo operatório de recombinações: “*tem-se uma noção das novas forças do fora quando se pensa o finito-ilimitado; é que essas novas forças são aquelas próprias dos conjuntos compostos por um número finito de componentes, mas passíveis de enveredarem por uma diversidade praticamente ilimitada de combinações, o que abre às forças atuantes no homem uma ilimitação de interferências neste ou naquele domínio, como o do código genético*” (Orlandi, 2002: 222)

7 Direito de morte é algo que para Foucault (1988) relaciona ao poder soberano, típico portanto das sociedades de soberania. Ao apontar aqui a morte, não estamos argumentando a presença de elementos de soberania no contexto do controle (apesar de julgarmos interessantes as investigações que se debruçam sobre sobreposições de elementos disciplinares e de controle). A morte aqui se vincula ao extermínio e a competição.

8 Outras fontes desta pesquisa em andamento, mas que não puderam ser detalhadas neste artigo são: política de privacidade do Facebook, da Microsoft, documentos que refletem exigências de privacidade por parte de grupos ativistas internacionais com atuação na América Latina, textos jornalísticos sobre o fim da privacidade e tentativas do governo brasileiro em prover informações sobre privacidade e internet. A partir da contraposição das definições de privacidade presentes nessas diferentes fontes vem sendo possível trazer a tona as tensões que constituem esse campo na atualidade.

mudanças nos próprios serviços, o termo também busca encarregar o usuário de consultar regularmente as novas versões, já que ao concordar com o termo, ele estará submetido as alterações contratuais[9]. Este documento possui um tópico “Proteção à Privacidade e aos Direitos Autorais” que explicita que a política de privacidade aborda (ao lado de direitos autorais) o modo como são tratados os dados pessoais dos usuários e como o Google protege a privacidade, acrescentando que “Ao utilizar nossos Serviços, você concorda que o Google poderá usar esses dados de acordo com nossas políticas de privacidade”. (Google, 2012)

Assim, conforme se procede a leitura do documento é possível notar que o contrato de privacidade apresentado trata fundamentalmente de questões como propriedade, uso e acesso de dados relacionando-os a privacidade, e que ainda assim, está submetido a decisões da empresa sobre como essas políticas serão transformadas no futuro. Isso implica, por exemplo, que limites e controles de privacidade podem ser alterados segundo o interesse da própria empresa, ou seja a maneira com que essas políticas são tratadas admite que o significado de privacidade está entrelaçado a dados pessoais, propriedade , uso e acesso a dados, e passíveis de negociação.

Ainda nos mesmos “Termos de serviço”, o tópico “O seu conteúdo em nossos serviços” afirma que o usuário manterá a propriedade intelectual do conteúdo que é enviado à empresa quando da utilização de seus serviços (alguns exemplos são a rede social Google plus e o serviço de armazenamento Google docs) e acrescenta algo que parece ser uma forma de ironia: “Em resumo, aquilo que pertence a você, permanece com você”. Ao mesmo tempo, a empresa explica nesse mesmo tópico que ao fazer *upload* de conteúdos para os serviços do Google “você concede ao Google (e àqueles com quem a empresa trabalha) uma licença mundial para usar, hospedar, armazenar, reproduzir, modificar, criar obras derivadas (como aquelas resultantes de traduções, adaptações ou outras alterações), comunicar, publicar, executar e exibir publicamente e distribuir tal conteúdo. De acordo com a empresa, os direitos que o usuário concede nesta licença são para os fins restritos de operação, promoção e melhoria e desenvolvimento dos serviços. Essa licença perdura mesmo que o usuário deixe de usar os serviços do Google. O exemplo utilizado no próprio documento é uma listagem de empresas que o usuário adicionou para localização no Google maps.

A página “Política de privacidade” segue a mesma aproximação com relação aos dados do usuário, explicitando quais informações do usuário são coletadas e como são utilizadas pelo Google, além de oferecer ao usuário modos de acesso aos dados coletados pela empresa e formas de atualizar e editar esses dados e configurações. As informações fornecidas pelos usuários têm mais de um nível. São compreendidas como informações pessoais aquelas que identificam o usuário, como nome, endereço de e-mail, número de telefone, do cartão de crédito ou informações de cobrança, deixando a vaga ideia de “outros dados que possam ser razoavelmente vinculados a essas informações pelo Google”. Esse nível de informações que o Google especifica como “fornecidas por você” ainda incluem foto, caso o usuário “queira aproveitar ao máximo os recursos de compartilhamento” oferecidos pela empresa na utilização do Perfil Google. O que parece ser um outro nível dessas informações são aquelas coletadas de forma menos perceptível pelo usuário, e que o Google discrimina como “que solicitamos a partir do uso que você

9 Em função do escopo deste trabalho, não será possível abordar o ponto a seguir que parece bastante interessante, em especial, quando pensado a partir da pesquisa desenvolvida por Rafael Evangelista que trata de cibernética e da ideologia da Califórnia (Evangelista e Kanashiro, 2013). O ponto em questão é o parágrafo final dos Termos de serviço que delega aos tribunais da Califórnia a resolução de possíveis litígios envolvendo o Google, e a possibilidade que as leis da Califórnia também façam precipitar os elementos pesquisados por Evangelista.

faz de nossos serviços". Constituem a grande parte das informações coletadas e processadas aquelas sobre os serviços utilizados pelo usuário, o modo de utilização, que eles explicam: "como quando você visita um *website* que utiliza nossos serviços de publicidade ou quando você vê e interage com nossos anúncios e conteúdo" (Google, 2013). Seguindo a enumeração do próprio documento, pontua-se a seguir as informações incluídas como passíveis de coleta, armazenamento e troca pela empresa:

1) Informações do dispositivo (modelo de hardware, sistema operacional, identificadores exclusivos de produtos[10], e informações de rede móvel, inclusive número de telefone). O Google pode associar seus identificadores de dispositivo ou número de telefone com sua Conta do Google.

2) Quando ocorrer a visualização de conteúdo fornecido pelo Google, a empresa pode coletar e armazenar automaticamente determinadas informações em registros do servidor[11], que podem incluir detalhes de como o usuário usou o serviço, e suas consultas de pesquisa, informações de telefonia, como o número de telefone, número de quem chama, números de encaminhamentos, horário e data de chamadas, duração das chamadas, informações de identificador de SMS e tipos de chamadas.

3) Informações do local vinculadas a utilização de serviços do Google capazes de identificar a localização do usuário, a partir da coleta e processamento de informações a localização real e sinais de GPS enviados por um dispositivo móvel. A empresa também admite a possibilidade de usar várias tecnologias para determinar o local, como dados de sensor do dispositivo do usuário que podem, por exemplo, fornecer informações sobre pontos próximos de acesso Wi-Fi e torres de celular.

4) Números de aplicativos exclusivos e as informações sobre sua instalação. O tipo de sistema operacional e o número da versão do aplicativo são enviados ao Google quando o serviço de aplicativo for instalado, atualizado ou desinstalado, ou quando o serviço contatar o usuário e os servidores Google para atualizações automáticas.

5) O Google pode coletar e armazenar informações localmente no dispositivo do usuário, a partir de mecanismos como armazenamento no navegador da web (inclusive html 5) e *caches* de dados de aplicativo.

6) A empresa pode usar várias tecnologias para coletar e armazenar informações quando o usuário visita um serviço do Google e isso pode incluir o envio de um ou mais *cookies* ou identificadores anônimos para o dispositivo do usuário. Esses mecanismos também são utilizados quando o usuário interage com serviços oferecidos pelo Google a possíveis parceiros, como serviços de publicidade ou recursos do Google que podem aparecer em outros sites[12].

Ainda de acordo com a política de privacidade do Google, o nome do usuário utilizado no

---

10 "Um identificador exclusivo de dispositivo é uma string de caracteres que é incorporada em um dispositivo pelo fabricante e pode ser usada para identificar o dispositivo de modo exclusivo. Diferentes identificadores de dispositivo variam no sentido de serem ou não permanentes, de poderem ou não ser redefinidos pelo usuário e no modo como podem ser acessados. Um determinado dispositivo pode ter diferentes identificadores exclusivos. Identificadores exclusivos de dispositivo podem ser usados para diversos fins, incluindo segurança e detecção de fraudes, sincronização de serviços como a caixa de entrada de um usuário, memorização das preferências do usuário e fornecimento de publicidade relevante". (Google, 2013).

11 De acordo com Google (2013) os "registros do servidor" geralmente incluem a solicitação na web, endereço de protocolo de internet, tipo do navegador, idioma do navegador, a data e a hora da sua solicitação e um ou mais *cookies* que possam identificar exclusivamente seu navegador.

12 Para uma análise abrangente sobre o uso de *cookies* como ferramentas de vigilância e controle, ver Bruno et al, 2012

Perfil Google pode ser utilizado pela empresa nos serviços que exigem uma Conta Google. Por exemplo, o proprietário de um *smartphone* que utilize o sistema operacional Android, necessariamente deve ter uma Conta Google para poder fazer o download e atualização de aplicativos. Se usuário utiliza vários nomes pode ver substituído nomes mais antigos associados com a Conta do Google de modo a ser representado de maneira consistente em todos serviços da empresa. Se outros usuários já tiverem o e-mail deste usuário ou outras informações que o identifiquem, o Google pode mostrar a eles as informações do Perfil do Google desse usuário publicamente visíveis, como nome e foto.

Para não estender muito mais esta apresentação da "Política de privacidade" do Google, vale indicar aqui que esse é um material rico para pesquisas, inclusive porque a empresa disponibiliza várias versões desse documento, sendo possível comparar sua transformação ao longo do tempo. Para concluir a apresentação da política de privacidade atualmente vigente (Google, 2013), é importante ainda abordar o item "Transparência e escolha" no qual a empresa apresenta a possibilidade de o usuário reverter e controlar tipos de informações vinculadas a conta (por meio do serviço Google Dashboard), visualizar e editar preferências de anúncios, por meio da explicitação de categorias de interesse, editar a forma como o Perfil Google é mostrado publicamente ou a alguns indivíduo, controlar o que é compartilhado, obter informações dos serviços da empresa, configurar o navegador para o bloqueio de *cookies* (com o alerta de que alguns serviços podem não funcionar com *cookies* desativados). Vale a pena também ressaltar o item "Acesso e atualização de suas informações pessoais" (ou seja, em parte, aquele primeiro nível de informações), mas que deixa transparecer o outro nível.

Ao solicitar o *download* de seus próprios dados, o usuário é guiado a página *Control your data*[13] Para conseguir este arquivo é necessário utilizar o aplicativo *Take out.* Ao realizar essa experiência é possível acessar, por exemplo, contatos, que não são apenas do Gmail, mas também de telefones celulares armazenados na agenda de usuários de *smartphones*, cruzados com informações de contatos do Google Plus, Orkut etc. Neste caso, pessoas que não sejam usuárias de nenhum serviço da empresa, também podem ter informações no banco de dados da empresa, bastando para isso estarem entre os contatos telefônicos de um alguém que use os serviços do Google.

De acordo com Bruno (2010), é importante, como ressaltado anteriormente, diferenciar duas ordens de dados pessoais geradas em ambientes como esses descritos pelo Google. Na camada mais superficial e visível desses ambientes, há os dados pessoais que os indivíduos geram e disponibilizam voluntariamente e sobre os quais usualmente têm o controle do seu grau de visibilidade e publicidade, por exemplo, sejam aqueles nomeados acima pelo Google como "dados pessoais" ou os que são disponibilizados em redes sociais (como Facebook). Tais dados pessoais voluntariamente publicizados geram uma segunda camada de dados que podem ou não conter meios de identificação dos indivíduos que os geraram. Agregados em bancos de dados e submetidos a técnicas de mineração e *profiling*, tais dados geram mapas e perfis de consumo, interesse, comportamento, sociabilidade, preferências políticas que podem ser usados para os mais diversos fins, do marketing à administração pública ou privada, da indústria do entretenimento à indústria da segurança, entre outros. Neste caso, o controle do indivíduo sobre os seus próprios dados é bem menos evidente e para Bruno (2010), a noção de

13 https://www.google.com/takeout/#downloads "Grabbing a copy of your data? Great! We think it's really important that you have control over your data. If you have time please let us know why it is important to you and how we can improve. If you have decided to take your data elsewhere, please take a minute to research the data export policies of your destination. Otherwise, you might import your data into a service that doesn't let it out. If you ever want to leave the service, you may have to leave important stuff like your photos behind" (Google, 2013).

privacidade (nos seus termos jurídicos) não dá conta da complexidade das questões sociais, políticas e cognitivas envolvidas.

Bruno (2010) nos lembra que Mark Zuckerberg fundador do Facebook fez uma declaração em 2010 afirmando o fim da privacidade (Kirkpatrick, 2010) que ecoava uma afirmação muito similar, pronunciada pelo deputado Donald Kerr, oficial da inteligência estadunidense do governo George W. Bush. O oficial clamava por uma redefinição da privacidade e argumentava que as novas gerações das redes sociais já não a entendiam segundo "velhos termos", uma vez que expunham voluntariamente suas vidas *online*.

Notar neste texto, a proximidade entre propriedade, uso e acesso a dados com a noção de privacidade não significa referendar a redefinição de privacidade, tal como colocadas por Kerr e Zuckerberg, nem de afirmar o fim da privacidade, mas sim, buscar apontar o que esse panorama está produzindo seja no sentido de deslocamento de sentido (significado ou rumo) ou da produção de práticas e saberes.

Não se trata de afirmar que privacidade existe ou deixou se existir, mas de compreender os discursos, forças e práticas que hoje disputam pelo sentido, valor e experiência da privacidade. Essa disputa é especialmente sensível no campo das redes de comunicação distribuída, como a internet. Assim, é preciso entrecruzar a disputa em torno da privacidade e as disputas políticas, econômicas, sociais, cognitivas e estéticas que se travam no âmbito dessas redes, de seus "bens" materiais e imateriais, de seus modelos de comunicação, circulação e produção de informação, conhecimento, cultura.

Em consonância com Bruno (2010), notamos que as mesmas empresas (como o Facebook) que clamam pela redução da privacidade dos seus usuários (uma vez que essa suposta redução é um dos atrativos de seus negócios) reivindicam fervorosamente a sua própria privacidade quando são inquiridas acerca dos usos que fazem da massa de dados pessoais que capturam. É nesses bancos de dados que residem as verdadeiras moedas de seus negócios, suas atividades (e poder de ação), dados pessoais, limites e definições de privacidade (dos usuários e da própria empresa).

3. Big data e alguns elementos para análise

Na passagem da soberania para a disciplina, o direito de morte que detinha o soberano é deslocado para um poder que gera a vida, e passa a vigorar a administração dos corpos e a gestão calculista da vida. (Foucault, 1988). Taxas de nascimento e morte, níveis de saúde, de longevidade surgem como uma série de intervenções e controles reguladores que penetravam os corpos de maneira detalhada e controlavam as populações de modo global, caracterizando aquilo que Foucault chamou de biopolítica das populações. “A estatística como ciência do Estado” ligava a detenção das informações sobre as pessoas pelo Estado e por seus técnicos, e por instituições, hospitais, escolas, exércitos, prisões etc.

A possibilidade de coletar dados[14], arquivar, monitorar, conhecer, reconhecer, identificar, classificar e perfilizar não é mais uma prerrogativa do Estado, nem de seus técnicos e

14 Da mesma forma não é mais possível reconhecer nos saberes produzidos hoje a estatística de que nos falava Foucault (1988). “(...) Estatística e Computação. Essas áreas são como caminhos que em relação com outros ou com áreas distintas, mas reunidos sob a mesma *epistème*, acabam por precipitar-se em outros rumos. São como linhas em uma dança e movimento não retilíneo, que ora se entrecruzam e ora se afastam, e nos momentos em que se tocam, criam várias outras vias, com tonalidades diversas entre si e também diferentes quando compradas com o que as formou” (Kanashiro, 2011: 56).

instituições, tanto quanto não se opera mais por meio de mecanismos disciplinares, mas pelo controle exposto por Deleuze (2000). E da mesma forma, arquivar, conhecer, classificar não têm mais o mesmo sentido ou funcionamento que tiveram em outras épocas.

Estamos lidando com processos automatizados voltados para um gigantesco volume e fluxo de informações, em segundo lugar, com um espraiamento das possibilidades de monitoramento, identificação e classificação que se dão pelo uso cotidiano e corriqueiro de tecnologias de informação e comunicação, dos celulares a internet.

A quantidade e variedade de dados disponíveis na internet e as ferramentas para lidar com esse universo vem sendo chamadas de big data. O tema é tratado de forma geral por especialistas voltados para áreas como marketing, administração, ou aqueles interessados em oportunidade de negócios, aumento da competitividade e inovação. Nesse meio são proclamados como componentes necessários para a definição de big data os 5 Vs: volume, velocidade, variedade, veracidade, valor. Alguns substituem o termo veracidade por viabilidade, mas ambos dizem respeito a importância da autenticidade de dados e da análise dessa informação para que façam sentido. Apesar das diferenças entre as definições de big data, é consensual que ainda não existe infraestrutura, seja em *hardware* ou *software*, para lidar com o volume de dados estruturados e não estruturados produzidos. Mesmo sem essa capacidade, a big data vem sendo defendida como um campo de oportunidades sem precedente para empresas.

Com relação a capacidade de análise e processamento desse volume de informação é consensual que a possibilidade existe, mas é inumana, automatizada. Em menor escala é o que empresas como Amazon, Netflix, Facebook, Google e redes de supermercado já fazem com os dados pessoais de seu usuários, tal como descrito anteriormente. Paralelamente, são constantes as acusações dessas empresas sobre as tentativas de Estados de obterem dados provenientes dessa maquinaria[15].

Com relação a classificação de informações e perfilização, Bruno (2008) aponta que categorias infra-individuais podem ser criadas segundo um modelo *top-down*, utilizando classes pré-estabelecidas – idade, gênero, profissão – ou segundo um modelo *bottom-up*, gerando classes a partir da análise dos dados, como “frequentadores do site Y que clicam nos links de tipo X”; “mulheres solteiras que usam pílula anticoncepcional e frequentam sex shops”. Essa categorização é submetida a um tratamento de segunda ordem, cujos métodos mais usuais são a mineração de dados (*data mining*) e a produção de perfis computacionais (*profiling*), os quais são complementares. A mineração de dados é uma técnica estatística aplicada que consiste num mecanismo automatizado de processamento de grandes volumes de dados cuja função central é a extração de padrões que gerem conhecimento. Não por acaso, este procedimento é chamado *knowledge-discovery in databases*. Tais padrões são constituídos a partir de mecanismos

15 É possível citar aqui, casos como do Programa Prisma, programa de vigilância mantido pela Agência Nacional de Segurança dos Estados Unidos, no qual o Estado obteve de empresas como Google, Skype, Facebook, Apple (dentre outras) informações sobre seus usuários. Outro caso recente, ocorrido no Brasil, foi o convênio firmado entre Tribunal Superior Eleitoral (TSE) para entrega de dados pessoais de eleitores brasileiros ao Serasa, empresa brasileira criada em 1968 pela Federação Brasileira de Bancos (Febraban) para análise e coleta de informações para decisões de crédito e apoio a negócios. A empresa faz projeções do Índice Geral de Preços (IGP) além de outros indicadores econômicos para servirem de referência para o setor de serviços, comércio e indústria. O Serasa faz parte, desde 2007, do grupo Experian, multinacional de gestão de informação e de bancos de dados que opera em diversos países e fornece informações para análises de crédito e de consumo. Em ambos os casos, sinaliza-se o embricamento de atores públicos e empresas privadas para o funcionamento da maquinaria de monitoramento de dados pessoais.

de geração de regras, sendo mais comuns as de tipo associativo (similaridade, vizinhança, afinidade) entre pelo menos dois elementos, que depois diferenciam tipos de indivíduos ou grupos. Esses tipos correspondem a perfis computacionais gerados pelo mecanismo designado *profiling*. A geração de perfis segue uma lógica indutiva que visa “determinar indicadores de características e/ou padrões de comportamento que são relacionados à ocorrência de certos comportamentos” (Bennett, 1996). Os padrões e regularidades daí extraídos permitem visualizar domínios com certa homogeneidade interna e fronteiras externas – de interesses, comportamentos, traços psicológicos – que de outro modo ficariam indefinidos ou fora do nosso campo de atenção.

Com Kanashiro (2001), observamos que aos olhos dessas outras máquinas e dos saberes atuais, não há exatamente o indivíduo das disciplinas, mas dados que a cada cruzamento fazem surgir um indivíduo fugidio para uma situação, uma autenticação, um acesso, uma transação comercial e que logo se dilui e se reconstrói em outra situação. Aquela figura que se formou a partir de determinados cruzamentos de dados e foi impedida de viajar, porque era potencialmente um terrorista, pode diluir-se para depois conformar uma figura que é entendida por determinados órgãos como um ótimo consumidor de alguns produtos, cursos de língua, ou livros, ou potencialmente portador de uma doença genética.

As classificações movem-se conforme os cruzamentos de informações, que podem surgir e ressurgir de infinitos arranjos, tantos que nem a taxonomia fabulosa de Borges (Foucault, 2000) pode imaginar, porque ela não é fixa em categorias, ela é recombinação permanente. Classificações são estabelecidas como possibilidades infinitas, já que oriundas dos processos de recombinação de informações. O humano aparece agora deslocado de sua função de decidir sobre quem é perigoso, doente, beneficiário ou bom consumidor e passa a ensinar e aprender em seu acoplamento com as máquinas essa decisão, porque o trabalho de cruzamento de dados na atual sociedade é inerentemente inumano. O processo automatizado tem a figura humana, o técnico, a ensinar-lhe padrões de reconhecimento, ou seja, que características somadas resultam nessa figura fugidia. (Kanashiro, 2011)

Recentemente, a Google foi acusada coletivamente (Rushe, 2013) por usuários de seu serviço de e-mails, o Gmail, de não respeitar a privacidade, o que o grupo identificou a partir de propagandas presentes em suas caixas postais vinculadas a informações internas das mensagens de e-mails. Sob ação judicial movida por esses usuários, a empresa respondeu que os usuários de e-mail deveriam esperar que seus e-mails sejam sujeitos a processamento automático de análise, já que isso estava expresso nos termos de serviço da empresa, qualificando a ação de tentar “criminalizar práticas comuns de negócios". Erich Schmidt presidente do conselho da empresa ainda acrescentou que “A política do Google é chegar bem perto da linha do inadmissível sem cruzá-la”.

Para além da defesa fundamentada nos termos de serviço, o fato da mineração de dados ser automatizada aparece como argumento em defesa de que a privacidade não está sendo violada por não serem humanas as análises e a triagem de dados. As transposições "aceitáveis" de privacidade e liberdades civis parecem se inserir em uma lógica de sucessivas redefinições.

A atual maquinaria que produz as novas possibilidades de arquivar, monitorar, conhecer, reconhecer, identificar, classificar e perfilizar vincula-se a um jogo de correlações de força

para produção de informação e de conhecimento[16], monitoramento e vigilância.

4. Considerações finais

Entre os anos de 2010 e 2011, foi realizada uma pesquisa comparativa entre Brasil e México, sobre a implementação de câmeras de vigilância, a biometria nos documentos de identificação, até as novas tecnologias de informação e comunicação Firmino et al, 2013; Bruno et al, 2012; Kanashiro, 2011; Kanashiro e Doneda, 2012).

No caso da privacidade, é importante salientar alguns pontos. Em uma pesquisa comparativa sobre a vigilância no Brasil e o México, notou-se que o aumento das possibilidades de vigiar e monitorar não são acompanhadas seja pelo debate público ou pela capacidade de legislar com agilidade sobre o tema da privacidade ou de mecanismos de proteção de dados. Ou seja, até o momento, não é possível dizer que na disputa pelo sentido de privacidade haja uma legislação contundente a esse respeito.

A expressão "invasão de privacidade" ganha, constantemente, novos contornos para se conformar a atividades cada vez mais comuns e inseridas na prática velada e mercadológica da exploração de dados e redes pessoais. A ausência de marcos legais e do debate público sobre esses limites, tende a aumentar o risco para que essas redefinições sejam cada vez e mais facilmente ditadas por interesses privados, a partir dos quais os dados pessoais transformam-se em mercadoria informacional e imaterial de difícil compreensão e com fronteiras de acesso e uso deliberadamente vagas e complexas.

Apesar disso, há movimentos globais levados a cabo por organizações como Electronic Frontier Foundation, Privacy International, dentre outros, que se colocam resistentes diante das possibilidades de invasão de privacidade. A privacidade proclamada por esses grupos muitas vezes ecoou uma noção moderna, aquela transgredida pelo olhar que imiscuia-se pela fresta da parede ou pelo buraco da fechadura.

Este eco fica ainda mais claro nas reclamações de privacidade por parte de usuários, por exemplo, do Facebook em suas páginas pessoais ou preocupações de usuários de redes sociais ou o caso da supracitada ação coletiva movida contra o Google. Em grande parte das vezes, há uma exposição de informações da vida cotidiana e uma preocupação com alguém bisbilhotando essas informações. Neste segundo caso, ainda mais do que no primeiro, não se percebe que não há simplesmente um indivíduo sendo vigiado ou monitorado, já que se trata da big data. Afinal, como já apontamos, empresas como Facebook e Google, por exemplo, alimentam-se dos dados pessoais de seus usuários, dos seus metadados e de todas as atividades que eles realizam em suas plataformas.

Uma vez nelas, tudo o que se faz e se diz torna-se possibilidade de uso e troca, e geração de valor e ativos para essas empresas. O valor econômico e cognitivo desses dados, como já vimos, não consiste apenas no fato de estarem atrelados a indivíduos particulares e identificáveis, mas à possibilidade de recombiná-los para os mais diferentes fins: publicidade direcionada, montagem de perfis de intenção de voto em campanhas

16 Vale ressaltar que táticas e mecanismos característicos do controle deleuziano podem ser colocados em funcionamento junto a instituições entendidas como disciplinares. Este é o caso do uso de celulares por presos (Bumachar, Vicentin e Kanashiro, 2013), no qual um objeto técnico vinculado a novos saberes, mecanismos, técnicas e táticas reconfigura o funcionamento do exercício do poder. Quando o governador do estado de São Paulo afirmou que era dificil coibir o uso de celulares em prisões brasileiras, mas que este equipamento utilizado por presos poderia auxiliar nas investigações da polícia, sinalizava uma atualização de um dispositivo, fazendo-o operar dentro de um novo modelo para produzir algo diferente, nunca visto. O objeto passa de interdito a produtor de conhecimento, passa do repressivo ao permissivo e tolerado como forma de recapturar o objeto celular para um funcionamento que estava fora para dentro do controle do Estado.

eleitorais, projeção de perfis de periculosidade ou criminalidade de indivíduos e grupos, otimização dos próprios serviços oferecidos por estas plataformas etc.

Uma das promessas do big data envolve, inclusive, a promessa de revelação de correlações entre dados jamais imaginadas, tanto por aqueles que os geram ,quanto por aqueles que os capturam (Bruno, 2012). No campo do ativismo pela proteção à privacidade no campo das tecnologias e redes de comunicação contemporâneas, os recentes "Princípios internacionais sobre a aplicação dos direitos humanos na vigilância das comunicações" mostram-se atentos a estas múltiplas camadas de dados geradas pelas ações dos usuários de plataformas, dispositivos e redes digitais, bem como a suas possibilidades de recombinação, mas voltam-se muito mais a possibilidade de monitoramento por parte do Estado. Ainda assim, consideram que "toda informação que inclua, reflita, derive de ou seja sobre as comunicações de uma pessoa e que não seja imediatamente disponível e facilmente acessível pelo público em geral deve ser considerada como "informação protegida", devendo receber adequadamente a mais alta proteção legal." Ainda segundo os referidos Princípios:

"Embora exista desde muito um consenso no sentido de que o conteúdo das comunicações merece proteção significativa por parte da lei devido à sua capacidade de revelar informações sensíveis, é agora claro que outras informações extraídas das comunicações – metadados e outras formas de dados sem conteúdo – podem revelar ainda mais sobre uma pessoa do que o próprio conteúdo, e assim merecem proteção equivalente. Hoje, cada um desses tipos de informação pode, sozinho ou analisado coletivamente, revelar a identidade de uma pessoa, comportamento, associações da qual faz parte, condições físicas ou de saúde, raça, cor, orientação sexual, nacionalidade ou pontos de vista; ou permitir o mapeamento de sua localização, movimento e interações ao longo do tempo,[8], ou mesmo de todas as pessoas de uma certa localidade, incluindo manifestações públicas ou outro evento político".

Da mesma forma, não se observa que há vários níveis de informação ou de dados, que ultrapassam muito questões individuais. No caso das organizações, há uma preocupação geral com relação ao Estado e as informações que podem ser coletadas, armazenadas e trocadas, mais do que com as possibilidades que as corporações têm de realizar esses procedimentos. Neste caso, não se observa tanto os níveis de conexão e de relações entre Estado e corporações, como nos revelam os casos supramencionados do TSE-Serasa e Programa Prisma[17].

Na disputa pelo sentido da privacidade, um elemento importante a ser observado é a vinculação com a dinâmica de acumulação capitalista na atualidade. Vale notar que sob o título de política de privacidade as corporações abordam sobretudo a questão da propriedade intelectual e do acesso e utilização de dados. A noção moderna de privacidade não é por onde se opera essa outra noção que vem sendo construída.

É um universo muito distante da privacidade moderna, e muito mais relacionado as

17 Pelo menos três casos recentes enfatizam elementos importantes do que visam as possibilidades de coletas, armazenamento e troca de dados (criação de bancos de dados sobre a população) entre governos e corporações: 1) as evidências de que o governo brasileiro e as empresas como a Petrobrás têm sido sistematicamente alvo de programas de espionagem da Agência de Segurança Nacional dos Estados Unidos (NSA) apontando o uso estratégico e economico dessa prática; 2) a expansão do uso de tecnologias e práticas de vigilância a fim de responder aos padrões internacionais exigidos pelos megaeventos esportivos que ocorrerão nos próximos anos – Copa do Mundo (2014) e Olimpíadas (2016); e 3) casos recentes de monitoramento, vigilância e criminalização, pelos governos estaduais no Brasil, dos participantes de protestos políticos iniciados em junho de 2013 no país.

apostas e a competição que Farocki (2003) aponta em seu filme. A noção de privacidade é deslocado no sentido de funcionar sob a égide de uma “nova economia” (Lopes, 2008) em que grande parte dos produtos criados, sejam eles informação ou conhecimento, são apropriados por meio da imposição de novos cercamentos.

Referências bibliográficas

Ariès, P. **História social da criança e da família.** Rio de Janeiro: Livros técnicos e científicos, 1981.

Ariès, P.; Duby, G. **História da vida privada**. (org. Paul Veyne). Coleção. São Paulo: Companhia das Letras, 2000.

Bennet, C.J. The public surveillance of personal data: a cross-national analysis. *In*: D. Lyon (org.), **Surveillance as social sorting: Privacy, risk and digital discrimination**. London, Routledge, p. 37-49, 1996.

Biehn, N. The missing Vs in big data: viability and value. **Wired.** Innovation insights community. 05 de junho de 2013 (site) Disponível online: http://www.wired.com/insights/2013/05/the-missing-vs-in-big-data-viability-and-value/ Última consulta: junho de 2013.

Bruno, F.G. “Monitoramento, classificação e controle nos dispositivos de vigilância digital”. **Revista Famecos.** n. 36, agosto de 2008.

Bruno, F. Rastros digitais e teoria ator-rede. **Revista Famecos**. Porto Alegre, v. 19, n. 3, pp. 681-704, setembro/dezembro 2012.

Bumachar, B.L.; Vicentin, D.J; Kanashiro, M.M. Celular phone use in Brazilian prisons. **Annual Meeting of the Society for Social Studies of Science (4S).** San Diego: Estados Unidos. Outubro de 2013.

Bruno, F.G. O fim da privacidade em disputa. **Dispositivo de visibilidade** (blog online), 2010. Disponível em: http://dispositivodevisibilidade.blogspot.com.br/2010/01/o-fim-da-privacidade-em-disputa.html Última consulta: 03 de julho de 2013

Bauman, Z. 2011) **44 Cartas do Mundo Líquido Moderno**. Rio de Janeiro: Zahar, 2011.

Bruno, F.G.; Nascimento, L.C.; Firmino, R.J.; Kanashiro, M.M.; Evangelista, R. Rastros humanos en Internet: privacidad y seguimiento online en sitios web populares del Brasil, **Novática**, v.38, n.217, pp.27-33, 2012.

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, CERT.br. **Cartilha para segurança na internet.** São Paulo: Comitê Gestor para Internet no Brasil, 2012. Disponível online: http://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf Última consulta: 03 de julho de 2013

Colnago, C. **Termos de uso e privacidade: o Facebook.** (blog) Publicado em 11 de

fevereiro de 2011. Disponível online: http://www.colnago.adv.br/termos-de-uso-e-privacidade-o-facebook/ Última consulta 05 de julho de 2013.

DaMatta, R. **A casa e a rua: espaço, cidadania, mulher e morte no Brasil.** São Paulo: Saraiva, 1984.

Del Priore, M. **Histórias íntimas: sexualidade e erotismo na história do Brasil.** São Paulo: Planeta, 2011.

Deleuze, G. "*Post-scriptum* das sociedade de controle" In: **Conversações**, 1972-1990. Rio de Janeiro, Editora 34, 2000.

Doneda, D. "Privacidade, vida privada e intimidade no ordenamento jurídico brasileiro. Da emergência de uma revisão conceitual e da tutela de dados pessoais". **Âmbito jurídico.** (portal) Disponível online:
http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=2460
Último acesso: fevereiro de 2011.

Elias, N. **Processo civilizador.** Rio de Janeiro: Jorge Zahar, 1994.

Evangelista, R. A.; Kanashiro, M.M. "Cibernética, internet e a nova política dos sistemas informacionais". In Giuseppe Cocco (org.) **Gabinete digital: análise de uma experiência.** Corag e Imprensa Oficial do Estado do Rio Grande do Sul: Porto Alegre, 2013.

Farocki, H. **Imagens da prisão**. (vídeo), 2003.

Firmino, R.J.; Kanashiro, M.M.; Bruno, F.G.; Evangelista, R.; Nascimento, L.C. Fear, Security, and the Spread of CCTV in Brazilian Cities: Legislation, Debate, and the Market. **Journal of Urban Technology**, v.20, n.3, 2013.

Foucault, M. **Vigiar e punir: história da violência nas prisões.** (23ª. ed.). Petrópolis: Vozes, 2000.

Foucault, M. **História da sexualidade I; a vontade de saber.** Rio de Janeiro: Edições Graal, 1988.

Facebook. **Declaração de direitos e responsabilidades** (website). Versão 11 de dezembro de 2012. (2012a) Disponível online: https://www.facebook.com/legal/terms Último acesso: 07 de julho de 2013.

Facebook. **Política do uso de dados** (website). Versão 11 de dezembro de 2012. (2012b) Disponível online: https://www.facebook.com/about/privacy/ Último acesso: 07 de julho de 2013.

Facebook. **Princípios do Facebook** (website) Versão 11 de dezembro de 2012. (2012c) Disponível online: https://www.facebook.com/principles.php Último acesso: 07 de julho de 2013.

Google. **Políticas e princípios. Política de privacidade** (website). Versão 24 de junho de 2013. Disponível online: http://www.google.com/intl/pt-BR/policies/privacy/ Último acesso: 07 de julho de 2013.

Google. **Políticas e princípios. Termos de serviço do Google.** (website). Versão 01 de março de 2012. Disponível online: http://www.google.com/intl/pt-BR/policies/terms/ Último acesso: 07 de julho de 2013.

Kanashiro, M.M. **Sorria, você está sendo filmado.** [Dissertação]. Instituto de Filosofia e Ciências Humanas. Unicamp, 2006.

Kanashiro, M.M. "Surveillance Cameras in Brazil: exclusion, mobility regulation, and the new meanings of security" **Surveillance Society,** vol 5, n.3, p. 270-289, 2008.

Kanashiro, M.M. **Biometria no Brasil e o registro de identidade civil: novos rumos para a identificação** [Tese]. Faculdade de Filosofia, Letras e Ciências Humanas. USP, 2011.

Kanashiro, M.M.; Doneda, D. The new Brazilian identification system: unique features of a general transformation. **Surveillance & Society**, vol. 10, n. 1, p. 18-27, 2012.

Kirkpatrick, M. "Facebook's Zuckerberg says the age of privacy is over". **Readwrite** (website). 09 de Janeiro de 2010. Disponível online: http://readwrite.com/2010/01/09/facebooks_zuckerberg_says_the_age_of_privacy_is_ov#awesm=~of6Vj5RJVSgusz. Último acesso 03 de julho de 2013.

Lopes, R.S. "As TICs e a 'nova economia': para além do determinismo tecnológico". **Ciência e Cultura***,* vol.60, n.1, 2008.

Lyon, D. **Surveillance as social sorting: privacy, risk, and digital discrimination**. Psychology Press, 2003.

Microsoft. **Declaração de privacidade 2.0 MBAM.** Versão abril de 2013. Disponível online. http://technet.microsoft.com/pt-br/library/dn186168.aspx Último acesso 03 de julho de 2013.

Microsoft. **Microsoft online privacy statement.** Versão abril de 2012. Disponível online. http://privacy.microsoft.com/PT-BR/fullnotice.mspx Último acesso 03 de julho de 2013.

Minelli, M.; Chambers, M.; Dhiraj, A. **Big data, big analytics: emerging business intelligence and analytic trends for today´s businesses.** Wiley & Sons Inc., 2013. Disponível em: http://onlinelibrary.wiley.com/book/10.1002/9781118562260;jsessionid=1F05C348C35B393EE9B5769D870F6434.d02t02

Orlandi, L. B. "O que estamos a fazer de nós mesmos". In: Margareth Rago, Luiz B. L. Orlandi e Alfredo Veiga-Neto (orgs.) **Imagens de Foucault e Deleuza, ressonâncias nietzschianas** Rio de Janeiro: DP&A, 2002.

Princípios internacionais sobre a aplicação dos direitos humanos na vigilância das comunicações. Vários autores e instituições, 2013. Disponível em https://pt.necessaryandproportionate.org/text

Rushe, D. "Usuários do gmail sabem que não tem privacidade". **Folha de S.Paulo.**

Caderno Mundo. 14 agosto de 2013 (Tradução de matéria publicada no jornal *The Guardian,* texto original disponível online www.theguardian.com/technology/2013/aug/14/google-gmail-users-privacy-email-lawsuit)

Sennett, R. **O declínio do homem público: as tiranias da intimidade.** São Paulo: Companhias das Letras, 1999.

Tech America Foundation. **Demystifying big data: a practical guide to transforming the business of government.** 2012 Disponível em: http://breakinggov.sites.breakingmedia.com/wp

Zikopoulos, P.; Eaton, C.; Deroos, D.; Deustsch, T. , Lapis, G. Understanding Big Data: **Analytics for enterprise class hadoop and streaming data.** McGrawHill., 2012. Disponível em: https://www14.software.ibm.com/webapp/iwm/web/signup.do?source=sw