

## Do panóptico ao “Big Brother”

Por **Ariel G. Foina** Advogado e diretor de Projetos da ONG Universidade Cidadã, Brasília

### **Data da publicação:**

Julho de 2009

Em 1785 Jeremy Bentham concebeu uma estrutura arquitetônica voltada para a edificação de penitenciária com fins a reduzir os custos do controle dos prisioneiros, denominada panóptico. Nesta nova forma de prédio, havia um centro de onde os detentos poderiam ser vigiados de tal forma que eles mesmos não pudessem ver quem os vigiava (ou saber se quem deveria vigiá-los estava efetivamente lá). Jeremy Bentham não era arquiteto, era um filósofo utilitarista e seu trabalho decorria de uma reflexão sobre eficiência do controle. O sucesso do panóptico provinha do fato de que ali, naquele modelo, havia um controle simbólico imposto 24 horas por dia – afinal, pelo fato de os detentos não conseguirem ver quem os vigiava no centro da estrutura, sentiam-se vigiados o tempo todo, estando presente o vigilante ou não.

Alguns séculos depois, em 1975, Michel Foucault publicou “Vigiar e Punir”, onde aborda o debate filosófico sobre a punição em nossa sociedade, correlacionando, por um lado, escolas, presídios e hospitais, e por outro, a vigilância e a punição como forma de adestramento/educação e controle social.

É inegável que alguns aspectos sociais mudaram desde a concepção destas estruturas/idéias até os dias de hoje. Em algum ponto da transição da modernidade<sup>1</sup> para a “sociedade pós-moderna”<sup>2</sup>, o pesadelo de Foucault tornou-se o sonho do consumidor médio de bens de entretenimento, viabilizando-se os assim denominados “reality shows”.

Não é incomum encontrar indivíduos, nos dias de hoje, dispostos a expor sua privacidade cotidiana, a colocar-se em verdadeiros aquários humanos integralmente vigiados - os reality shows no estilo “Big Brother”, em troca de uma chance de obter alguma quantia em dinheiro. Mesmo que o prêmio financeiro não seja conquistado, a participação nestes espetáculos é, inegavelmente, associada à possibilidade da “fama” e à consequente exposição pública deste indivíduo, mesmo após o fim do reality show – um processo que redundava numa sucessiva e crescente renúncia à privacidade e à intimidade.

Essa renúncia à privacidade parece ser impulsionada por estímulos financeiros, em maior ou menor grau, o que resulta no fato de que este bem denominado “privacidade” – que até pouco tempo atrás parecia tão precioso – hoje está disponível para ser negociado, a maior ou menor preço, pela grande maioria dos indivíduos que compõem nossas sociedades ocidentais contemporâneas. É como reduzir o debate do “se a ex-brother vai posar para a revista de conteúdo erótico” a uma questão apenas de “por quanto”.

O exemplo anterior é retórico, o usuário médio da Internet não vai posar para revista<sup>3</sup>, mas sua renúncia à privacidade parece seguir no mesmo curso do exemplo que demos no parágrafo anterior. As pessoas não parecem estar muito preocupadas com o “a que custo”, desde que em troca da renúncia à privacidade lhe sejam oferecidos, por exemplo, vários gigabytes gratuitos de espaço para sua caixa de correio eletrônico.

### **URBANIZAÇÃO E PRIVACIDADE**

A sociologia clássica, se lida como forma de entendimento de contextos históricos anteriores ao nosso, parece poder elucidar algo da possível causa deste “barateamento” da privacidade. A partir da leitura de vários trabalhos sociológicos fica a impressão de que perda da privacidade está relacionada com o processo de urbanização.

Mais do que o aspecto óbvio – de que uma casa isolada em uma área rural remota é capaz de oferecer mais privacidade do que uma casa em uma cidade; de que esta pode oferecer mais privacidade do que um apartamento, e este pode oferecer mais privacidade do que um quarto em uma república universitária –, existe algo do urbano que é introjetado pelo indivíduo e que o impulsiona a flexibilizar seus critérios de limite na intromissão externa à sua esfera de intimidade e, conseqüentemente, à sua privacidade. Mais do que isto, no meio urbano existe o chamado comportamento blasé, onde o indivíduo urbano precisa ignorar outros indivíduos urbanos, dada a impossibilidade de se estabelecer com todos sucessivos processos de socialização - sendo tal comportamento recíproco entre os demais indivíduos urbanos (na prática significa dizer que ma pessoa não pode cumprimentar todos os estranhos que passam por ela numa rua movimentada, aprendendo a ignorá-las. Isso a sociologia urbana do início do século passado chamou de comportamento blasé).

Sem aprofundar-nos na teoria, cabe destacar apenas que, se por um lado existe uma gradativa renúncia à privacidade, por outro lado existe uma certa expectativa de que aquilo de privado que se expõe seja parcialmente ignorado sempre que esteja de acordo com o comportamento médio. Não se tem certeza sobre qual variável influenciaria o indivíduo a flexibilizar sua exigência de privacidade - mas, seja pelo contato mais intenso com outros indivíduos, seja pela redução do espaço, seja pelo aumento na organização do tempo e sua consequente escassez, ou então, seja pelo mero “agravamento” do processo de urbanização<sup>4</sup>, o fato é que todas estas variáveis parecem suscetíveis aos impactos das novas Tecnologias de Comunicação e Informação.

Com a globalização e, mais recentemente, com a intensificação do uso da Internet, a construção social de conceitos como tempo e espaço se modificaram para se adequar a novos sítios e ritmos de interação. Conceitos sociais como o de distância (construído tendo como referência o tempo que se leva para percorrer um espaço), parecem ter sofrido modificações drástica<sup>5</sup>, que podem ser comumente percebidas, por exemplo, pelos critérios com que os indivíduos utilizam expressões como “aqui” e “ali”, ou pela proximidade que se estabelece entre pessoas em relações mediadas por computadores.

## **PRIVACIDADE E O SISTEMA JURÍDICO BRASILEIRO**

Assim sendo, a questão da privacidade de dados no Brasil, especialmente quando se fala de privacidade na Internet ou em sistemas eletrônicos – excetuada a transmissão de dados<sup>6</sup> – costuma ser reduzida a dois aspectos fundamentais: as relações de consumo, com o consequente direito à informação, e a correção das informações armazenadas em bancos de dados.

Tal redução geralmente decorre de uma situação jurídica brasileira muito singular, se observados outros países: o fato de que as únicas ferramentas legais que tratam de privacidade de informações no Brasil serem o Código de Defesa do Consumidor e a Constituição Federal quando trata das garantias e da via do hábeas-data. Desta mingua de normas, resulta a frequente posição, comum entre juristas e operadores do direito, de que há a necessidade de se estabelecer critérios e leis que ditem como, para que e quais as informações relativas ao comportamento do indivíduo e seus dados pessoais podem ser armazenadas.

Denúncias de que uma ou outra empresa rastreia o comportamento de seus clientes ou de usuários de Internet para lhes oferecer determinados produtos ou publicidade, ou, simplesmente, para vender os dados a terceiros (tudo sem o conhecimento dos usuários), são muito comuns e normalmente recaem na discussão sobre o que está ou não está previsto nos Termos de Uso do Serviço - ou se houve ou não houve informação clara ou anuência prévia do consumidor quanto a tal conduta.

Este debate é necessário e relevante, mas não deve ser o único. Como apontamos anteriormente, existem indícios de que a questão da privacidade vem sendo relegada a uma posição de menor relevância pelos próprios usuários de redes digitais, fruto de um processo social que vem traçando seu curso histórico desde muito antes da existência dos computadores, e cuja tendência nos parece ser de agravamento.

Esta crescente renúncia à proteção da própria privacidade, se por um lado é motivada por um benefício imediato ao indivíduo frente a uma enxurrada de serviços gratuitos, e intensificada pelo descaso na atenção à maioria dos Termos de Uso de Serviço – extensos, complexos, mal traduzidos, e pouco inteligíveis – por outro lado implica em custos sociais ainda pouco experimentados no Brasil.

## **POR UMA POLÍTICA PÚBLICA DE PRIVACIDADE**

Violações de grandes bancos de dados já foram realizadas para os mais variados fins - desde perturbações

meramente comerciais, mediante oferta de serviços por concorrentes que deliberadamente copiaram bases de dados de clientes, passando por esquemas de chantagem e extorsão operados pela máfia do Leste Europeu decorrentes da obtenção da base de clientes de sítios web pornográficos, chegando ao crime de “roubo de identidade”, ainda pouco falado no Brasil mas já famoso em países onde o número de bancos de dados com informações de consumidores é muito maior do que em nosso país.

Não é razoável se esperar do usuário médio uma leitura atenta de todos os Termos de Uso de Serviço, nem se esperar de todos os prestadores de serviço um cuidado exacerbado com a privacidade da informação do usuário - uma vez que isso implica em custos muitas vezes maiores do que aqueles incorridos com as consequências da divulgação não autorizada dos dados armazenados.

Assim sendo, mais do que definir leis que estabeleçam formas aceitáveis de aquisição de dados, com prévia autorização dos usuários, é necessário que o país acorde para uma questão mais ampla – devemos pensar não apenas em entregar aos cidadãos um acervo de recursos para a proteção da privacidade (que, por desinteresse, pressa ou desinformação, poderia não ser utilizado); mas também em criar, nas esferas jurídica e administrativa, formas de controle e regras que permitam a redução dos danos nos casos de vazamento e comprometimento de bancos de dados com informações privadas.

É hora de nos perguntarmos se é correto que um sítio web comercial armazene dados como número de RG, data de nascimento, nome, endereço, telefone, sexo, etc. - quando seria necessário, para fins fiscais, apenas o nome e o C.P.F. de seus usuários. Da mesma forma, deveríamos nos perguntar para que um órgão público deveria compor bases de dados que incluem, numa mesma ficha de registro, o nome do indivíduo, o nome dos pais, a data de nascimento, o número de diversos documentos (entre eles, passaporte ou identidade, C.P.F.), o endereço residencial, o número da CNH - apenas para nos outorgar uma habilitação para condução de veículos automotivos.

Independente da resposta, é certo que deveria haver uma preocupação pública quanto aos motivos que levam ao crescente armazenamento dos dados, a real necessidade deste armazenamento, a finalidade para a qual foram compostos os bancos, os níveis de segurança adequados a cada tipo de cadastro e a possibilidade e forma de sua negociação, se for o caso.

Outros países como o Canadá, os Estados Unidos, a Inglaterra e a França<sup>7</sup>, entre outros, já têm legislações que visam delimitar as práticas de retenção e armazenamento de dados, relevando-se aí muitas diferenças culturais. Em alguns casos, existem até comissões ou órgãos da administração pública especialmente dedicados à fiscalização, padronização e estudo de bancos de dados com informações de cidadãos e consumidores. No Brasil não se escuta muito falar sobre este tema. Talvez por uma questão de cultura, não estamos acostumados a questionar a real necessidade do registro de uma extensa quantidade de informações sobre nós em diversos e redundantes cadastros nacionais. Especialmente num país como o nosso - onde dados inquestionavelmente sigilosos e privados, como os da Declaração de Imposto de Renda de Pessoa Física, até pouco tempo atrás, encontravam-se à venda no mercado informal - o debate sobre a forma de funcionamento, os limites de uso, o armazenamento e a segurança dos bancos de dados com informações de cidadãos, consumidores e usuários parece uma preocupação cada vez mais urgente. Este debate deve ser promovido, não só com fin acadêmicos, mas também com vistas à necessária regulação estatal.<sup>8</sup>

Por fim, devemos considerar a hipótese de violação cotidiana da privacidade como fato dado e praticado pelos mais diferentes meios, com perspectivas de agravamento. Portanto, cabe ao Estado e à sociedade civil se preocupar em definir de forma clara e urgente um número de questões que não foram apreciadas pelo nosso sistema legal, tampouco por outras esferas da sociedade, como por exemplo: o que se tem feito efetivamente com os dados coletados? Por quem são manipulados? O que é registrado? O que deve ser registrado? Por quanto tempo? A quem se deve prestar contas? Qual nível de segurança adequado a cada tipo de dado? O que é comercializado? O que pode ser comercializado? Para que fim?

A lista não se esgota aí. Há várias outras questões ainda em aberto. Esta é uma discussão que não pode mais ser adiada.

---

1. Termo aqui entendido de forma similar ao que outros autores denominam como “sociedade industrial”, “modernidade sólida” e se refere ao período histórico cujo fim se identifica entre as décadas de 60 e 80 do século passado.

2. Sem entrar no debate quanto à existência ou não de uma pós-modernidade, aqui nos referimos à Sociedade Pós como sendo o mesmo período também denominado como “Sociedade pós-industrial”, “pós-moderna”, “modernidade tardia”, “modernidade líquida” ou qualquer conceito que denomine uma nova configuração social historicamente delimitada após a década de 60, seja no entendimento de que se trata de um novo modelo, ou de mera fase de transição.

3. Esta frase também é em boa parte retórica, considerando-se fenômenos como o “sexting” e a possibilidade deste tipo de comportamento extrapolar as faixas etárias mais jovens. O fato é que não é possível afirmar de forma categórica qual será (ou se haverá) um limite à renúncia à privacidade e que aspectos da privacidade tal limite (ou a falta dele) pode vir a afetar.

4. Desenvolvemos um ensaio teórico sobre este tema: Foina, A. G. O urbano na rede: Como a Teoria Sociológica Urbana Pode Ler as Cidades do Ciberespaço, Urbanidades, 2002  
<http://www.unb.br/ics/sol/urbanidades/arielfoina.htm>

5. Ver Bauman, z . Globalização: as consequências humanas, no capítulo denominado “Tempo e Espaço”, Jorge zahar Ed., 1999.

6. A privacidade da transmissão de dados tem proteção constitucional, e existe uma expectativa entre a maioria dos cidadãos de que tal proteção é efetiva - tendo em vista, inclusive, a legislação específica para regular as hipóteses e os meios de quebra de tal proteção mediante ordem judicial. Mesmo assim, este debate possui nuances complexas que não vamos abordar aqui - a questão da transmissão de dados não é objeto deste trabalho.

7. Entre várias normas e instituições que podem ser citadas, temos na União Europeia: Diretiva 2002/58/EC e Diretiva 95/46/EC de Privacidade Eletrônica e Proteção Geral de Dados, respectivamente; no Reino Unido: Data Protection Act 1998; na França, desde 1978 há a Commission Nationale de l’Informatique et des Libertés.

8. Mesmo motivado pelos bancos de dados eletrônicos, o debate é (e deve ser) estendido aos dados coletados ambientalmente, como no caso de informações decorrentes de RFIDs (Radio-Frequency Identification ou Identificação por Rádio Frequência), dados biométricos e leitores de imagem e faciais, bem como o armazenamento de dados de DNA e informações genéticas, restando ainda muito o que ser debatido e, eventualmente, regulado.

Categoria:

- [poliTICS 4](#)