NOTAS DE CONJUNTURA

Da privacidade à transparência: desafios da interação entre agentes públicos e privados na gestão de informações pessoais

From privacy to transparency: challenges of the public and private interactions in the management of personal information

De la privacidad a la transparencia: desafíos de la interacción entre agentes públicos y privados en la gestión de informaciones personales

Jamila Venturini | *jamila.venturini@fgv.br*
Fundação Getúlio Vargas, Centro de Tecnologia e Sociedade. Rio de Janeiro, Brasil.

Resumo

Preocupações com a proteção da privacidade marcaram a construção da jovem democracia brasileira. Regras de transparência e publicidade complementam as garantias presentes na Constituição Federal visando garantir controle social sobre as atividades do Estado e prevenir abusos como os ocorridos durante a ditadura militar. Contraditoriamente, porém, com o avanço das tecnologias digitais e da internet assim como das iniciativas de cidades inteligentes, a balança parece estar invertida: as atividades do Estado - inclusive na área de segurança pública e vigilância - seguem secretas e pouco sujeitas a escrutínio público, enquanto cidadãos encontram-se cada vez mais expostos a agentes públicos e privados. Ao mesmo tempo, crescem as preocupações com o poder de vigilância adquirido pelas empresas de tecnologia da informação e comunicação. Esta nota discutirá a questão, trazendo exemplos de como a interação público-privada traz novos riscos à privacidade, inclusive no que diz respeito a seu aspecto de bem social.

Palavras-chave: informação; privacidade; direitos fundamentais; proteção de dados pessoais; transparência.

Abstract

Concern about the protection of privacy marked the construction of the young Brazilian democracy. Transparency and publicity rules complement the guarantees contained in the Federal Constitution to guarantee social control over State activities and prevent abuses like the ones occurred during years of military dictatorship. Contradictorily, however, with the advancement of digital technologies and the internet and of smart city initiatives, the situation seems to be reversed: State activities - including those developed in the area of public security and surveillance - remain secret and little subject to public scrutiny, while citizens are increasingly exposed to public and private actors. At the same time, concern about the surveillance power acquired by information and communication technology companies is growing. This paper will discuss this issue, bringing examples of how public-private interaction brings new risks to privacy, including with regard to its aspect of social good.

Keywords: information; privacy; fundamental rights; personal data protection; transparency.

Resumen

Preocupaciones por la protección de la privacidad marcaron la construcción de la joven democracia brasileña. Normas de transparencia y publicidad complementan las garantías presentes en la Constitución Federal para garantizar el control social sobre las actividades del Estado y evitar abusos como los ocurridos durante los años de la dictadura militar. Paradójicamente, sin embargo, con el avance de las tecnologías digitales e de la Internet y de las iniciativas de ciudades inteligentes, la situación parece estar invertida: mientras las actividades del Estado – incluso con respeto a la seguridad y la vigilancia - siguen secretas y poco sujetas al escrutinio público, los ciudadanos tienen su privacidad cada vez más sin protección frente a agentes privados y públicos. Al mismo tiempo, existe una creciente preocupación por el poder de vigilancia adquirido por las empresas de tecnología de información y comunicación. Este artículo discutirá este tema, presentando ejemplos de cómo la interacción público-privada trae nuevos riesgos para la privacidad, incluso con respecto a su aspecto de bien social.

Palabras clave: información; privacidad; derechos fundamentales; protección de datos personales; transparencia.

INFORMAÇÕES DO ARTIGO

Contribuição dos autores: A autora é responsável por todo o texto.

Declaração de conflito de interesses: nenhum

Fontes de financiamento: não houve

Considerações éticas: nada a declarar

Agradecimento/Contribuições adicionais: nada a declarar

Histórico do artigo: Submetido: 28 out.2016 | Aceito: 01.nov.2016 | Publicado: 23.dez.2016

A preocupação com a privacidade perpassa a construção da jovem democracia brasileira. Depois da experiência de um Estado autoritário que se valia de suas estruturas de inteligência para infiltrar-se no mais íntimo da vida das pessoas em busca de "inimigos internos"[i], os brasileiros colocaram a proteção da privacidade e intimidade entre seus valores mais protegidos ao redigir a Constituição Federal de 1988. As garantias e limitações constitucionais às atividades de inteligência, porém, não impediram que abusos seguissem acontecendo no período democrático e os escândalos sobre o uso extensivo da vigilância das comunicações por parte do Estado brasileiro são recorrente[ii].

Somando-se às preocupações com intrusões à privacidade por parte do Estado, as denúncias de Edward Snowden sobre as práticas de vigilância em massa pela inteligência estadunidense e seus parceiros[3] evidenciaram o papel cada vez maior que cumprem as corporações privadas nessas atividades. Para além da indústria militar e de segurança, ficou clara a capacidade de novos agentes – marcadamente do setor de tecnologias da informação e comunicação - de coletar e processar uma quantidade cada vez maior de informações sobre hábitos e costumes de populações inteiras.

Quando se trata do mundo online, uma quantidade de informações e registros é gerada a cada interação. Elas são deixadas voluntariamente - em cadastros ou com a publicação de conteúdos -, mas também de forma involuntária durante a navegação, com o uso de tecnologias de coleta automatizada como os cookies[4]. Quando agregadas e organizadas logicamente, essas informações permitem a criação de perfis acurados e de "um vasto, dinâmico e polifônico arquivo de nossas ações, escolhas, interesses, hábitos, opiniões etc."[5], que se torna valioso não só para os negócios baseados na venda de anúncios personalizados, por exemplo, mas também para a vigilância e o controle estatal.

A situação se agrava com o advento da chamada 'Internet das Coisas', que torna objetos cotidianos capazes não só de coletarem informações e interagirem com o mundo físico, mas de se conectarem uns aos outros para o intercâmbio de dados e informações sem necessidade de intervenção humana. O mesmo acontece com as ditas cidades "inteligentes", que prometem incrementar a eficiência na gestão pública[6] a partir da coleta e do processamento de grandes volumes de dados, inclusive pessoais. Tais dados podem ser obtidos tanto diretamente - por meio de pesquisas e da interação das pessoas com os serviços públicos digitais ou objetos inteligentes instalados na cidade (como sensores e câmeras, por exemplo) -, quanto indiretamente de concessionárias de serviços públicos ou com o estabelecimento de acordos com empresas privadas.

Nesse contexto, práticas corriqueiras implicam (ou passarão a implicar) o intercâmbio de dados entre cidadãos, empresas e poder público, trazendo novos riscos e desafios para a proteção da privacidade: acender uma luz ou desligar o ar condicionado; utilizar um aplicativo de trânsito; compartilhar um comentário ou denúncia por meio de uma rede social; locomover-se pela cidade utilizando um telefone móvel; utilizar um cartão nos sistemas de transporte coletivo, ou mesmo circular em ambientes monitorados por câmeras ou radares de velocidade. Podem ser identificadas ao menos quatro dimensões do conceito de privacidade que podem ser envolvidas no desenvolvimento das cidades inteligentes: (i) a privacidade das informações pessoais; (ii) a privacidade das pessoas; (iii) a privacidade de comportamento e (iv) a privacidade das comunicações pessoais[7]. Segundo a classificação, a privacidade das informações pessoais consiste no direito de controlar,

---

[i] Durante a ditadura militar, o foco do antigo Sistema Nacional de Inteligência (SNI) constituía o combate ao "inimigo interno", de acordo com os princípios da Doutrina de Segurança Nacional, que orientou as atividades de inteligência nas ditaduras militares em diversos países da América Latina1. Com a transição democrática, as acusações de repressão e tortura contra o SNI diminuíram, mas denúncias de violações de direitos, principalmente à privacidade, com o monitoramento de correspondências e conversas telefônicas, continuaram até o governo Sarney. Os alvos incluíam trabalhadores em greve e partidos de esquerda. Cabe ressaltar que tanto militares quanto as forças policiais (federal, militar e civil) dos diferentes estados estavam desde a ditadura envolvidos nas atividades de vigilância de comunicações[2].

[ii] O país chegou a ser condenado pela Corte Interamericana de Direitos Humanos por realizar interceptações consideradas ilegais para vigiar ativistas ligados ao Movimento Sem Terra (ver caso Escher e outros vs. Brasil). Além disso, ao menos desde 2013, organizações de direitos humanos continuamente denunciam o uso de novas tecnologias para o monitoramento de ativistas no contexto da realização de megaeventos como a Copa do Mundo da FIFA e os Jogos Olímpicos[2].

acessar, excluir e corrigir dados relacionados à pessoa; a privacidade da pessoa está relacionada ao direito de controlar o próprio corpo; a privacidade de comportamento seria o direito de salvaguardar de terceiros o conhecimento sobre suas atividades e escolhas; e a privacidade de comunicações pessoais o direito de se comunicar sem estar sujeito à vigilância, monitoramento ou censura.

As preocupações com a privacidade no contexto de coleta e processamento maciço de dados, portanto, se multiplicam e a própria ideia de privacidade se amplia: não se trata apenas de proteger cidadãos das intrusões do Estado na vida privada, mas de garantir que o tratamento de dados por parte do setor privado obedeça a princípios básicos que incluem adequação, necessidade, transparência, segurança, não discriminação, entre outros. O respeito a tais princípios e ao direito à privacidade busca preservar a autonomia e a liberdade e se torna ainda mais central para o funcionamento da democracia e o respeito aos direitos fundamentais.

O conflito público *versus* privado na gestão da informação

São diversas as justificativas para o interesse do Estado no acesso aos dados coletados e armazenados pelas empresas de tecnologia da informação e comunicação. Em primeiro lugar estão as preocupações com a defesa nacional, que legitimaram programas como o PRISM nos Estados Unidos, nos quais o governo tinha acesso direto aos sistemas de grandes corporações estadunidenses como Google, Facebook, Apple, entre outras[3]. Preocupações com a segurança pública e a defesa civil também motivam parcerias visando ao acesso a dados para combater a criminalidade ou até prever futuros crimes.

No caso das cidades inteligentes[iii], alega-se que o acesso a dados pode contribuir com a gestão pública em setores como mobilidade, sustentabilidade, segurança, acesso à educação e saúde, entre outros, e que as empresas na internet são fontes valiosas para obtê-los. O Centro de Operações Rio (COR), da Prefeitura do Rio de Janeiro, por exemplo, estabeleceu uma parceria com o aplicativo *Waze* visando oferecer informações sobre as condições do trânsito na cidade. A Prefeitura usaria os dados oferecidos pela empresa para identificar engarrafamentos, retenções e acidentes em tempo real[9].

Por outro lado, volumes cada vez maiores de dados coletados para subsidiar a gestão pública demandam investimentos altos em infraestrutura e capacidade de armazenamento e processamento com os quais o Estado, principalmente em países periféricos como o Brasil, nem sempre pode se comprometer[iv]. Com isso, parcerias com empresas privadas de tecnologia se tornam não só atrativas como quase necessárias para sustentar cidades ou órgãos públicos que se pretendam 'inteligentes'. O cenário é interessante também para o mercado, que encontra consumidores cativos para seus serviços e produtos e se apresenta como alternativa mais eficiente e segura para a gestão da informação.

Além disso, numa economia fortemente baseada em dados, o interesse das empresas em estabelecer parcerias com o setor público é grande, mesmo que num primeiro momento não resultem em benefícios econômicos. Por meio delas as corporações podem ter acesso a informações que dificilmente poderiam obter. Depois de entrar em escolas[11] e universidades[12], o Google, por exemplo, por meio de seu braço de inteligência artificial Deep Mind, estabeleceu uma parceria com um hospital britânico para liberar o tempo

[iii] O termo "cidades inteligentes" representa "um modelo de desenvolvimento urbano conceitual baseado na utilização do capital humano, coletivo e tecnológico para o reforço do desenvolvimento e da prosperidade nas aglomerações urbanas". No entanto, "o planejamento estratégico para o desenvolvimento de uma cidade inteligente consiste em uma ideia bastante abstrata por várias razões, incluindo o fato de que se refere a campos ainda inexplorados e, em grande parte, interdisciplinares. As partes interessadas (governos locais, instituições de pesquisa, movimentos populares, fornecedores de tecnologia, promotores imobiliários, etc.) muitas vezes são movidas por interesses conflitantes. A tendência a acreditar que a instrumentação tecnológica inovadora transforma automaticamente uma cidade em 'inteligente', bem como o uso tendencioso da palavra 'smart' de maneiras fragmentadas ou superficiais, prejudica o esclarecimento do assunto"[8].

[iv] Borgman[10] relativiza as vantagens do *big data* ao considerar que dados não possuem valor em si mesmos e que são poucos os agentes que têm a capacidade para o gerenciamento e processamento de bases tão grandes.

gasto pelos médicos com "burocracia" de modo que possam se dedicar aos "cuidados com o paciente". O acordo implica no compartilhamento de dados pessoais de mais de 1,6 milhão de pacientes por ano com a empresa[13].

As parcerias entre Estado e empresas de tecnologia, portanto, parecem marcar o cenário de prestação de serviços públicos na era digital e elas avançam de forma quase invisível para a maioria da população. Mais grave: quando se trata da regulação da coleta e uso desses dados, o Brasil não conta com uma lei geral de proteção de dados pessoais. Normas setoriais abrangem o tema, tanto com relação ao tratamento de dados pessoais por parte de agentes públicos, quanto privados; porém as regras existentes são poucas, dispersas e não dão conta dos desafios trazidos pelas novas tecnologias e as propostas de 'cidades inteligentes'.

Um exemplo é que ainda que existam restrições quanto à divulgação de informações pessoais detidas por órgãos públicos, não há na legislação limites à coleta de dados por parte do Estado[14] ou um detalhamento sobre as medidas de segurança necessárias para prevenir o acesso indevido às bases de dados. O país tampouco dispõe de uma autoridade independente capaz de fiscalizar se o tratamento dos dados é adequado do ponto de vista das normas e princípios vigentes.

Quando se trata do setor privado, a aceitação aos chamados "Termos de Uso" - condição necessária para a interação com a maioria das plataformas online e, portanto, para o exercício de uma série de direitos na rede[15] - parece ser uma carta em branco que autoriza qualquer tipo de processamento de dados pessoais. Se no mundo offline contratos como os Termos de Uso poucas vezes são lidos, no ambiente online essa situação parece se agravar: segundo um estudo da Universidade de Carnegie Mellon, nos Estados Unidos, um usuário deveria reservar 8h diárias em 76 dias de um ano para ler somente as Políticas de Privacidade de uma média de 1.462 páginas visitadas[11]. Ainda assim, se os usuários quisessem se informar lendo esses documentos, eles poderiam se decepcionar com seu conteúdo: estudo recente que analisou os Termos de Uso de 50 plataformas aponta que, apesar de longos e aparentemente detalhados, esses documentos costumam ter cláusulas genéricas autorizando o compartilhamento de dados com diversos agentes e políticas complacentes em relação a pedidos de compartilhamento de dados com governos[16]. É extremamente preocupante, portanto, que, num contexto de intensa interação público-privada para a gestão da informação, a regulação através de contratos possa substituir ou se sobrepor às políticas públicas, preenchendo os vazios regulatórios e se impondo também nas relações entre cidadãos e Estado.

Para ir além das falsas dicotomias: transparência

Aprovar um marco legal abrangente de proteção de dados pessoais é fundamental para superar inseguranças jurídicas - prejudiciais para os negócios e a economia nacional - e garantir as devidas proteções à população. Nesse momento, o Brasil tem a oportunidade concreta de fazê-lo com a aprovação do Projeto de Lei nº 5276/2016, que após um longo processo de consultas públicas tramita na Câmara dos Deputados. No entanto, esse é apenas um primeiro passo. Fica evidente a necessidade de mais transparência no que diz respeito às iniciativas existentes quando o que se observa hoje é um desequilíbrio no qual as atividades do Estado - inclusive na área de segurança pública e vigilância - seguem secretas e pouco sujeitas a escrutínio público, enquanto os cidadãos encontram-se cada vez mais expostos[17]. Adotar medidas de acesso à informação e transparência, assim como de proteção de dados pessoais são tarefas centrais e demandam esforços coordenados para a construção de políticas amplas de gestão da informação. Cabe também refletir ainda sobre as limitações de uma compreensão da privacidade como direito individual e quais as consequências de se "trocar" a privacidade por outros bens nas democracias contemporâneas[18]. Repensar a privacidade enquanto bem social é fundamental no momento de sopesar interesses conflitantes. Não se pode negar os benefícios sociais que as iniciativas de digitalização e processamento de dados podem trazer, mas é necessário que haja escrutínio público e um debate aberto sobre as garantias e limitações que serão necessárias para que elas sejam implementadas.

Referências

1. Alves MHM. Estado e oposição no Brasil (1964-1984). Bauru: Edusc; 2005.
2. Cepik M, Antunes P. Brazil's new intelligence system: an institutional assessment. International Journal of Intelligence and Counterintelligence 2005, 16(3):349-373.
3. Greenwald G, MacAskill E. NSA Prism program taps in to user data of Apple, Google and others. The Guardian. 2013. [citado 25 nov. 2016] Disponível em: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.
4. Louzada L, Venturini J. A regulamentação da proteção de dados pessoais no Brasil e na Europa: uma análise comparativa. 2015. [citado 01 nov. 2016] Disponível em: http://lavitsrio2015.medialabufrj.net/anais/#theme-1
5. Bruno F. Máquinas de ver, modos de ser: vigilância, tecnologia e subjetividade. Porto Alegre: Sulina; 2013.
6. Paroutis S, Bennett M, Heracleous L. A strategic view on smart city technology: The case of IBM Smarter Cities during a recession. Technological Forecasting and Social Change 2014, 89:262-272. [citado 17 ago. 2016] Disponível em: http://www.sciencedirect.com/science/article/pii/S0040162513002266
7. Bartoli A. Hernandez-Serrano J, Soriano M, Dohler M, Kountouris A, Barthel D. On the ineffectiveness of today's privacy regulations for secure smart city networks. Paper presented at: Smart Cities Congress, 2012, Barcelona; set. 2012
8. Vicente JP. Como as Olimpíadas ajudaram o Brasil a aumentar seu aparato de vigilância social". Motherboar. [citado 25 nov. 2016] Disponível em: http://motherboard.vice.com/pt_br/read/como-o-brasil-aprimorou-seu-aparato-de-vigilancia-social-para-as-olimpiadas
9. Machado A. Prefeitura começa a usar Waze no Centro de Operações Rio. O Globo. 2013. [citado 04 nov. 2016] Disponível em: http://oglobo.globo.com/sociedade/tecnologia/prefeitura-comeca-usar-waze-no-centro-de-operacoes-rio-9152370
10. Borgman C. Big data, little data, no data: scholarship in the networked world. Cambridge; The MIT Press; 2015.
11. Guimarães SP. Google lança ferramenta de ensino para alunos e professores. Exame. 2014. [citado 25 nov. 2016] Disponível em: http://exame.abril.com.br/tecnologia/google-lanca-ferramenta-de-ensino-para-alunos-e-professores
12. Schmidt S. Comunidade acadêmica pede transparência sobre parceria entre Google e Unicamp. Lavits. 2016. [citado 25 nov. 2016] Disponível em: http://lavits.org/comunidade-academica-pede-transparencia-sobre-parceria-entre-google-e-unicamp/?lang=pt
13. Bloch-Budzier S. 2016. NHS using Google technology to treat patients. BBC News. 2016. [citado 25 nov. 2016] Disponível em: http://www.bbc.com/news/health-38055509
14. Dahlmann A, Venturini J, Dickow M, Maciel M. Privacy and surveillance in the digital age: a comparative study of the Brazilian and German legal frameworks. 2015. [citado 27 nov. 2015] Disponível em: https://www.academia.edu/18159512/Privacy_and_Surveillance_in_the_Digital_Age_a_comparative_study_of_the_Brazilian_and_German_legal_frameworks.
15. McDonald AM, Cranor LF. The Cost of Reading Privacy Policies. ISJLP 2008, 4, 543. Disponível em: http://moritzlaw.osu.edu/students/groups/is/files/2012/02/Cranor_Formatted_Final.pdf. 01 nov. 2016.
16. Burle C, Venturini J, Barros M, Córdova Y. Os degraus da implementação efetiva no Brasil: como as regulamentações locais de acesso à informação impactam na implementação de portais de dados abertos e transparência Paper presented at: ConDatos, Santiago do Chile; set. 2015
17. Cohen JE. What privacy is for. Harvard Law Review 2013, 126:1-24. [citado 01 nov. 2016] Disponível em: http://ssrn.com/abstract=2175406
18. Angelidou, M. Smart city policies: A spatial approach. Cities 2014 41, S3–S11. [citado 16 de nov. 2015] Disponível em: http://www.sciencedirect.com/science/article/pii/S026427511400095X