PLANEJAMENTO URBANO DO FUTURO, DADOS DO PRESENTE: A PROTEÇÃO DA PRIVACIDADE NO CONTEXTO DAS CIDADES INTELIGENTES

Dennys Marcelo Antonialli[* a,e,f]
Beatriz Kira[** b,c,e,f]

* InternetLab (Centro de Pesquisa Independente em Direito e Tecnologia), São Paulo, SP, Brasil.
** Universidade de São Paulo, Faculdade de São Paulo, São Paulo, SP, Brasil.

Resumo

As cidades ao redor do mundo vivenciam hoje experiências nas quais uma quantidade cada vez maior de dados gerados pelos cidadãos é usada para fins de gestão e planejamento urbano, com potencial para estimular o engajamento e a participação cidadã, promover a inclusão e tornar as comunidades mais eficientes, habitáveis e justas. Ao mesmo tempo, os avanços na ciência da reidentificação, nos mercados de dados e na análise de big data, trazem consigo preocupações quanto a atividades de coleta, uso, compartilhamento e descarte de dados, processos que devem estar cercados de cautela. À medida que novas tecnologias geram mais dados do que nunca, como aproveitar as oportunidades trazidas para as cidades, preservando a privacidade individual e construindo a confiança do público? Quais as experiências vivenciadas por cidades que depararam com esse desafio? E como as cidades brasileiras podem navegar entre iniciativas de uso de dados que acarretam benefícios aos cidadãos, como a economia de recursos e o aumento de eficiência da administração pública das cidades, mas que podem cobrar um custo significativo de privacidade? Este artigo busca explorar essas questões, apoiando-se na discussão de experiências internacionais e nacionais em que se faz presente a tensão entre o crescente uso de dados pelas chamadas cidades inteligentes e a proteção da privacidade dos cidadãos.

Palavras-chave

Cidades inteligentes; Dados pessoais; Privacidade; Políticas públicas; Planejamento urbano.

a. fundamentação teórico-conceitual e problematização; b. pesquisa de dados e análise estatística; c. elaboração de figuras e tabelas; d. fotos; e. elaboração e redação do texto; f. seleção das referências bibliográficas.

THE FUTURE OF URBAN PLANNING IS IN DATA FROM THE PRESENT: THE PROTECTION OF PRIVACY IN THE CONTEXT OF SMART CITIES

Dennys Marcelo Antonialli[*]
Beatriz Kira[**]

* InternetLab (Centro de Pesquisa Independente em Direito e Tecnologia), São Paulo, SP, Brasil.
** Universidade de São Paulo, Faculdade de São Paulo, São Paulo, SP, Brasil.

Abstract

Cities around the world today deal with situations in which an ever-increasing amount of citizen-generated data is used for urban planning and management purposes, with the potential to stimulate citizen engagement and participation, to promote inclusion, and to make communities more efficient, liveable and just. At the same time, advances in the science of re-identification, trade of personal data, and big-time analytics bring with them concerns about the collection, use, sharing, and disposal of data, processes that must be surrounded by caution. As new technologies generate more data than ever before, how to seize the opportunities brought to the cities, while preserving individual privacy and building public confidence? What experiences have been brought by cities that have faced this challenge? And how can Brazilian cities navigate between data-use initiatives that bring benefits to citizens, such as resource savings and increased efficiency of city government, but which can come with a significant cost of privacy? This article seeks to explore these issues, discussing international and national cases, in which the tension between the growing use of data by the so-called smart cities and the protection of citizens' privacy is present.

Keywords

Smart cities; Personal data; Privacy; Public policy; Urban planning.

PLANEJAMENTO URBANO DO FUTURO, DADOS DO PRESENTE: A PROTEÇÃO DA PRIVACIDADE NO CONTEXTO DAS CIDADES INTELIGENTES

Dennys Marcelo Antonialli
Beatriz Kira

1. Introdução

De censores que geram registros minuciosos sobre as atividades que acontecem no espaço urbano a veículos autônomos que se deslocam de forma otimizada pelas vias públicas, a tecnologia promete revolucionar a vida nas cidades. Nesse contexto, o conceito de *cidades inteligentes* (ou *smart cities*), de difícil delimitação, abrange um conjunto bastante heterogêneo de iniciativas e projetos. Um relatório da IBM identifica no conceito de *smart cities* um instrumento para criar dados que poderiam oferecer maior eficiência nos serviços públicos, interconectando diferentes pontos da cidade e viabilizando a tomada de decisões mais subsidiadas a respeito das demandas da gestão pública (IBM INSTITUTE FOR BUSINESS VALUE, 2009). Já Townsend (2013) defende que cidades inteligentes são espaços onde se combinam informações sobre todos os aspectos da cidade para responder aos problemas sociais, econômicos e ambientais. O centro de pesquisa em tecnologia Gartner identifica a base das *smart cities* como o fluxo inteligente de trocas de informação entre os diferentes subsistemas, para um ambiente mais eficiente e sustentável (VELOSA; RYAN-TRAZ; ANAVITARTE; FERNANDO, 2011). O Relatório do Parlamento Europeu as conceitua como a maneira inteligente de as cidades utilizarem informação e tecnologia da informação (ICT) com o propósito de endereçar seus desafios (PARLAMENTO EUROPEU, 2014).

Em comum entre essas definições, parece estar o uso de tecnologias de informação e comunicação para a transformação de dinâmicas urbanas, tais como o planejamento urbano e territorial, o engajamento e a participação cidadã, as políticas de mobilidade, habitação, entre outras.[1] Para tanto, é fundamental que a administração pública tenha a possibilidade de utilizar dados cada vez mais completos e precisos. São novas oportunidades de análise, que permitem ao gestor público otimizar de maneira revolucionária a formulação de políticas públicas (BLOOMBERG, 2014).

A multiplicação de dispositivos conectados à internet ("internet das coisas"), os menores custos de armazenamento de dados, a popularização dos *smartphones* e das técnicas de análise de *big data* são algumas das novidades que contribuíram para que uma quantidade cada vez maior de dados estivesse à disposição dos gestores públicos. Ao mesmo tempo, a criação de bancos de dados complexos, que congregam registros sobre a vida dos cidadãos, pode representar uma ameaça para a privacidade individual. Nesse contexto, a pergunta de pesquisa que enfrentamos neste artigo é: como aproveitar as oportunidades trazidas para as cidades, preservando a privacidade dos cidadãos e construindo a confiança do público?

Inicialmente, serão exploradas experiências internacionais e nacionais na intersecção de novas tecnologias adotadas por cidades, privacidade e proteção de dados, além de desenvolvimento urbano. Em seguida, serão examinados os recentes esforços de algumas cidades para regular e coletar informações valiosas para o planejamento urbano geradas por aplicativos de transporte de passageiros, como a Uber e a 99Taxi, e o modo como eles refletem o uso de dados tanto do setor público como do privado em cidades inteligentes. Por fim, serão abordados os dilemas emergentes para as cidades encontrarem equilíbrio entre seus compromissos com as iniciativas de acesso à informação e dados abertos, que ajudam a promover um governo transparente, mas que podem expor informações pessoais, e aqueles relacionados com a proteção da privacidade dos cidadãos.

2. Gestão pública "inteligente": o uso de dados pelas cidades ao redor do mundo

O crescimento das cidades,[2] por um lado, e o surgimento de novas tecnologias, por outro, têm encorajado líderes locais a procurar formas inovadoras de servir ao

1. Sobre o ciclo de vida das políticas públicas, ver Farah (2001).

2. Segundo dados da World Health Organization (2017), em 2014, 54% da população mundial total vivia em cidades, em comparação a 34% em 1960, e essa porcentagem continua a crescer. Estima-se, que em 2017, mesmo em países menos desenvolvidos, a maioria das pessoas já vivia em áreas urbanas.

interesse público (BLOOMBERG, 2014). No centro desse movimento, parece estar a crescente habilidade de utilizar dados para melhorar os serviços oferecidos pelos governos locais. Apesar de o uso, pelo poder público, de dados gerados e coletados pelos cidadãos não ser novo – sistemas mais antigos tradicionais, como as linhas de emergência e disque-denúncia, já possibilitavam a contribuição dos cidadãos, com informações para a melhoria dos serviços públicos –, novas plataformas tecnológicas permitem que a coleta e a análise desses dados ocorram em escalas muito maiores: com maior abrangência territorial, em mais quantidade e muito mais rapidamente (BATTY, 2015).

Com isso, novos horizontes se apresentam para o planejamento urbano e cresce o interesse dos gestores públicos em ter acesso a esses dados. Experiências ao redor do mundo mostram que o *uso inteligente* de tais dados pode contribuir para promover a inclusão e tornar as comunidades mais eficientes, habitáveis e justas, com a criação de estatísticas sobre o ambiente urbano e o mapeamento de problemas. Alguns gestores argumentam, inclusive, que estaríamos vivendo em uma "revolução digital", que coloca à disposição da administração pública ferramentas tecnológicas para informar a tomada de decisões estratégicas, contribuindo para a alocação mais eficiente e efetiva de recursos. Com algumas dessas ferramentas é possível, por exemplo, que comunidades e servidores públicos descubram informações sobre bairros e regiões que antes ou demandariam muito tempo ou custariam muito dinheiro para serem obtidas. Além disso, permitem que os próprios moradores forneçam quantidades enormes de dados que os governos antes não tinham como reunir ou acessar (BLOOMBERG, 2014).

A prefeitura de Chicago, por exemplo, desenvolveu um algoritmo para otimizar as inspeções sanitárias dos restaurantes da cidade. Para identificar quais dos mais de 15 mil estabelecimentos locais estavam mais suscetíveis a problemas, um time de analistas desenvolveu um algoritmo utilizando dados variados sobre os restaurantes e o contexto urbano no qual eles estavam inseridos. Informações como o tempo de existência do empreendimento, o clima da região e a quantidade de roubos registrados no bairro foram consideradas para apontar maior ou menor probabilidade de riscos à saúde. O algoritmo parece ter contribuído para o aumento da eficiência das inspeções, pois, após sua implementação, o número de violações sanitárias identificadas aumentou em 15%, enquanto o número de reclamações de problemas de saúde relacionados a elas permaneceu estável (TOTTY, 2017).

Em Washington DC, graças ao programa *Grade.DC.gov*, os munícipes podem avaliar instantaneamente a qualidade dos serviços oferecidos por órgãos públicos, bem como os canais de atendimento à população (311 e 911). O programa, lançado em junho de 2012, possibilita que usuários enviem notas e comentários sobre ser-

viços públicos utilizados, tanto por meio de mensagens de texto como pelo site. O sistema coleta ainda comentários de redes sociais, como Facebook, Yelp, Twitter e *blogs* sobre os serviços da cidade em geral. Todas essas informações são analisadas com a ajuda de um algoritmo, que atribui uma nota geral a cada serviço. O programa contribui para que o governo local identifique com mais precisão a qualidade dos serviços, de acordo com os cidadãos, e foque sua atenção e recursos onde eles são mais necessários (GOLDSMITH; CRAWFORD, 2014).

Em Nova York, foram usados dados para a identificação de terrenos subutilizados de propriedade da prefeitura. O projeto, chamado *596 Acres*, disponibiliza um mapa interativo *on-line*, que mostra lotes públicos espalhados pela cidade. Clicando em um determinado lote vago, são exibidos detalhes sobre o terreno – como seu endereço e o órgão público responsável por ele. Outras funções de filtragem mostram, por exemplo, todos os lotes públicos vagos perto de um dado endereço, ou lotes públicos vagos que já são objeto de esforços de utilização. Além disso, como resultado de uma interação com a ferramenta *Google Street View,* o *site* permite que usuários explorem as proximidades dos terrenos. Segundo dados do programa, sua implementação propiciou o desenvolvimento de mais de cem iniciativas para que as áreas públicas passassem a ser utilizadas pela comunidade local (GOLDSMITH; CRAWFORD, 2014).

Recentemente, a cidade de São Paulo também foi palco de algumas experiências interessantes com o uso de dados. Em 2016, a Prefeitura, na gestão de Fernando Haddad, decidiu tornar públicos dados de todos os cerca de 3,3 milhões de imóveis da cidade, reunidos no cadastro do Imposto Territorial e Predial Urbano (IPTU), disponibilizando o nome da pessoa física e/ou jurídica proprietária, a metragem dos imóveis, o tipo de construção, o tipo de uso, entre outras informações (PREFEITURA DE SÃO PAULO, 2016). A relação foi publicada na plataforma *on-line* GeoSampa,[3] que reúne informações da cidade em um mapa georreferenciado. A disponibilização desse banco de dados, em formato aberto,[4] permitiu o desenvolvimento de uma série de estudos sobre a propriedade imobiliária na cidade de São Paulo, como a pesquisa *São Paulo: a corrupção mora ao lado* (TRANSPARÊNCIA INTERNACIONAL BRASIL, 2017), desenvolvida por uma equipe de pesquisadores da Transparência Internacional (TI), uma organização sem fins lucrativos de combate à corrupção.

3. Disponível em: <http://geosampa.prefeitura.sp.gov.br/PaginasPublicas/_SBC.aspx>. Acesso em: 2 maio 2017

4. Dados abertos podem ser entendidos como "dados que podem ser livremente usados, reutilizados e redistribuídos por qualquer pessoa – sujeitos, no máximo, à exigência de atribuição da fonte e compartilhamento pelas mesmas regras", segundo definição da Open Knowledge Foundation, Open Data Handbook, disponível em: <http://opendatahandbook.org/guide/ pt_BR/what-is-open-data/>. Acesso em: 2 maio 2017

Partindo da premissa de que a ocultação de bens é uma das formas mais comuns de investir recursos obtidos ilicitamente, ou seja, de que a aquisição de imóveis é bastante utilizada para se lavar dinheiro (OECD, 2007), os pesquisadores da TI usaram o banco de dados do IPTU para investigar o uso de estruturas corporativas pouco transparentes nas quais o beneficiário final é desconhecido – em geral, *offshores*[5] constituídas em paraísos fiscais ou jurisdições secretas – para a compra de imóveis na cidade.

Cruzando as informações do cadastro do IPTU, que revelavam os imóveis registrados no nome de pessoas jurídicas e o respectivo CNPJ, com informações obtidas no site da Junta Comercial do Estado de São Paulo (Jucesp), a pesquisa revelou que 3452 propriedades da capital paulistana estavam registradas em nome de 236 empresas controladas ou vinculadas. Essas propriedades têm o valor médio de 2,5 milhões de reais cada e, ao todo, são avaliadas em mais de 8 bilhões de reais, com base no valor venal – o valor de mercado pode ser ainda maior. A pesquisa concluiu que existe uma lacuna de transparência no setor imobiliário da capital paulista, pois não é possível identificar o beneficiário final das empresas que detêm essas propriedades em São Paulo, ou seja, se desconhecem os verdadeiros proprietários desses imóveis milionários, o que deve ser visto como sinal de alerta em relação ao combate à corrupção, finalizando com algumas recomendações de melhores práticas à Prefeitura.[6]

Situações como essas ilustram os novos potenciais do uso de dados para desenvolver ferramentas eficientes e confiáveis para informar decisões de gestores urbanos – especialmente de políticos locais, urbanistas e tomadores de decisão – a partir de informações antes indisponíveis ou muito difíceis de reunir e analisar. A redução de custos para a administração pública, o aumento de eficiência na alocação de recursos e a diminuição de filas para serviços públicos são alguns dos possíveis benefícios, os quais contribuem diretamente para a melhoria da vida dos munícipes (BATTY, 2015).

Entretanto, apesar dos benefícios que podem propiciar para a vida nas cidades, as atividades de coleta e tratamento de dados levantam preocupações com a privacidade dos cidadãos. Isso porque potencializam significativamente as possibilidades de utilização desses dados para finalidades que atendam aos interesses de diversos outros atores, tanto do setor público como do setor privado.

---

5. O estudo da Transparência Internacional Brasil (2017) traz a ressalva de que empresas *offshore* podem operar no Brasil e não são necessariamente ilegais. Mas, por terem como principal vantagem o sigilo, elas protegem o nome do beneficiário final do escrutínio público e, justamente por isso, são utilizadas também para esconder ganhos advindos de atos ilícitos, o que justifica os sinais de alerta.

6. Mais informações ver Transparência Internacional Brasil (2017).

No caso do setor privado, a possibilidade de construção de perfis detalhados dos hábitos e preferências das pessoas (HOOFNAGLE, 2012) e do desenvolvimento de algoritmos preditivos[7] permitiu repensar as formas de aproximação e de interação com os consumidores, além de abrir caminho para novos modelos de negócio e estratégias de monetização de informações pessoais, sobretudo aquelas baseadas na publicidade comportamental. De posse de dados que revelam características tão sensíveis e detalhadas a respeito de sua personalidade, o cidadão fica cada vez mais exposto ao poder de manipulação que esses atores podem exercer, influenciando de maneira cada vez mais poderosa suas decisões.[8]

Já no caso do setor público, a possibilidade de ampliação do aparato de vigilância e controle dos cidadãos tem sido vista como uma oportunidade para o aumento da segurança pública e como uma alternativa para o aperfeiçoamento dos mecanismos de gestão. Crescem, assim, as iniciativas de acesso e utilização de dados pessoais e biométricos para a identificação de pessoas e o controle de fraudes em serviços públicos, como o de transporte,[9] o monitoramento de manifestações, protestos e eventos públicos,[10] a fiscalização da veracidade de declarações e pagamento de impostos (MINISTÉRIO DA ECONOMIA, 2017) e até mesmo a localização de pessoas (ABREU; VALENTE, 2017).

Nesse contexto, à medida que o setor público e as empresas aproveitam mais dados do que nunca, como avaliar os riscos e as oportunidades das novas tecnologias, preservando a privacidade individual e construindo a confiança do público?

A pergunta exige a consideração de diversos elementos, como os aspectos regulatórios, culturais e tecnológicos ligados à arquitetura desses produtos e serviços. Legislações de proteção de dados ou políticas públicas que visem preservar a segurança da informação, bem como o sigilo e a confidencialidade no acesso a dados de usuários, são exemplos de como a regulação pode impactar esses usos.

---

7. Algoritmos preditivos são modelos matemáticos capazes de realizar inferências sobre usuários, geralmente como subsídio a processos de tomada de decisão automatizada (CRAWFORD; SCHULTZ, 2014).

8. Um estudo sugere, por exemplo, que anunciantes de cosméticos e produtos de beleza concentrem seus esforços publicitários na parte da manhã das segundas-feiras, quando, de acordo com as conclusões da pesquisa, as mulheres se sentem menos atraentes (CALO, 2013, p. 996).

9. Cf. Santos. "Ônibus municipais terão sistema de reconhecimento facial em Santos, SP". *G1*. Disponível em: <https://www1.folha.uol.com.br/cotidiano/2019/07/metro-de-sp-tera-vigilancia-com-reconhecimento-facial.shtml?loggedpaywall> e Agência Brasil, "Reconhecimento facial combate fraudes no transporte em Curitiba". Disponível em: <http://agenciabrasil.ebc.com.br/geral/noticia/2018-08/reconhecimento-facial-ajuda-combater-fraudes-no-transporte>.

10. Cf. UOL TAB, "*Scanner* facial abre alas e ninguém mais se perde no Carnaval (e fora dele)". Disponível em: <https://tab.uol.com.br/noticias/redacao/2019/03/11/carnaval-abre-alas-para-o-escaner-facial-reconhece-milhoes-e-prende-seis.htm?utm_source=facebook&utm_medium=social-media&utm_campaign=tab&utm_content=geral>.

Da mesma forma, a conscientização da população a respeito dos riscos que as atividades de coleta e tratamento de dados podem oferecer para sua privacidade repercute na sua disposição para consentir ou se insurgir contra determinadas tecnologias. Por fim, é possível incorporar padrões de proteção à privacidade na arquitetura do próprio sistema ou produto em desenvolvimento: no Reino Unido, por exemplo, o desenvolvimento de medidores "inteligentes" do consumo de energia elétrica, capazes de coletar muitas informações sobre as rotinas diárias dos cidadãos britânicos, tentou incorporar princípios de "*privacy by design*" para minimizar os impactos que a sua introdução acarretaria para a privacidade dos cidadãos (BROWN, 2013).

O presente artigo pretende analisar a pergunta que norteou a pesquisa do ponto de vista brasileiro. Para tanto, utilizaremos a experiência de compartilhamento de dados entre aplicativos de transporte e a administração pública municipal no Brasil como estudo de caso com o objetivo de identificar as principais questões que precisam ser consideradas na formulação de políticas públicas e na implementação de iniciativas que empreguem a tecnologia e envolvam o compartilhamento de dados pessoais para a gestão das cidades brasileiras.

3. A regulamentação de aplicativos de transporte nas cidades brasileiras: o compartilhamento de dados como "moeda de troca"

Nesta seção, serão discutidos alguns casos nos quais a administração pública usou instrumentos regulatórios para obter acesso a dados coletados por empresas privadas com o propósito de informar políticas públicas de mobilidade urbana. A ênfase é dada aos riscos à privacidade que determinados arranjos regulatórios ensejam e a possíveis alternativas para que o tratamento dos dados seja adequado à finalidade. É necessário esclarecer, inicialmente, o modelo regulatório de privacidade e proteção de dados no Brasil em vigor na época da implementação desses instrumentos regulatórios e de que modo sua evolução pode impactar iniciativas similares no futuro.

3.1. Os modelos regulatórios de privacidade e proteção de dados pessoais

A tutela do direito à privacidade evoluiu de maneira significativamente diferente ao redor do mundo, dando origem a diferentes modelos regulatórios. Isso se justifica, em parte, porque as concepções a respeito do papel do Estado na tutela de direitos e na regulação do mercado variam bastante de país para país. Nos Estados Unidos, por exemplo, Stephen Kobrin (2004) assinala que o Estado costuma conferir maior deferência à livre iniciativa e à autonomia privada, ao passo que, na Europa, prevaleceriam as preocupações com os direitos individuais e o bem-estar social.

Nesse sentido, esse autor esclarece que, em geral, nos Estados Unidos, as garantias individuais impõem limites à atuação do Estado, privilegiando a livre concorrência do mercado e a sua autorregulação. Isso teria influenciado a regulação sobre privacidade no país, que, ao se desenvolver com base nessas premissas, teria adquirido contornos muito mais "reativos" e direcionados a setores específicos (*issue-specific*) (KOBRIN, 2004, p. 115)

No caso da Europa, a privacidade seria considerada segundo seu valor social, isto é, sua função de garantir o desenvolvimento livre e pleno da personalidade dos cidadãos.[11] Nessa perspectiva, a regulação desse direito teria evoluído de forma a reconhecê-la como um direito fundamental e inalienável.[12] Ao contrário, nos Estados Unidos, "a privacidade é vista como uma coisa alienável sujeita ao mercado. Disputas sobre informações pessoais e os mecanismos para sua proteção são postos em termos econômicos". (KOBRIN, 2016, p. 116)[13]

Essas diferentes concepções a respeito do valor do direito à privacidade deram origem a modelos regulatórios diferentes. Enquanto nos Estados Unidos não há uma lei geral de proteção de dados pessoais, apenas regulações setoriais, na União Europeia vigora o modelo que convencionamos chamar de "legislativo", por se basear em leis de proteção de dados pessoais. Nesse modelo, adota-se um marco regulatório de proteção de dados pessoais genérico, que estabelece parâmetros mínimos que devem ser respeitados para a coleta e o tratamento de tais dados. Até 2018, vigorava na União Europeia a Diretiva 95/46/CE, com parâmetros mínimos para as atividades de coleta e tratamento de dados pessoais. A partir de maio de 2018, passou a vigorar o Regulamento Geral de Proteção de Dados Pessoais, diretamente aplicável a todos os países-membros da União Europeia.

O modelo europeu teve forte influência no regime regulatório adotado em outros países. Para se adequar às exigências da legislação europeia e permitir a transferência internacional de dados, mais de cem países seguem legislações de proteção de dados pessoais.[14]

---

11. Paradigmática, nesse sentido, foi a decisão do Tribunal Constitucional alemão em 1983 (BVerfGE 65, 1), no caso envolvendo uma lei que previa a realização de um censo populacional, introduzindo o conceito de "autodeterminação informacional", segundo o qual deve ser reconhecido aos cidadãos um poder de controle sobre seus dados pessoais. Para uma discussão aprofundada a respeito do conceito e de suas repercussões para o desenvolvimento da regulação do direito à privacidade na União Europeia (BIONI, 2016).

12. Gregory Shaffer (2000, p. 19) aponta, nesse sentido, que a privacidade não seria objeto de nenhum tipo de "barganha".

13. "Safe harbours are hard to find: the trans-Atlantic data privacy dispute, territorial jurisdiction and global governance" [Tradução da autor].

14. É o caso, por exemplo, de Canadá, México, Nova Zelândia, África do Sul, Austrália, Argentina, Colômbia, Chile etc. Para uma lista completa dos países que adotam legislações de proteção de dados pessoais ver Graham Greenleaf (2015).

No Brasil, apesar de o direito à intimidade e à vida privada estar assegurado na Constituição Federal e de existirem regras esparsas sobre a sua proteção na legislação infraconstitucional, como no Marco Civil da Internet e no Código de Defesa do Consumidor, a discussão sobre a adoção de uma lei geral de proteção de dados pessoais levou muitos anos.

Em 14 de agosto de 2018, foi aprovada a Lei Geral de Proteção de Dados (LGPD, Lei nº. 13.709). A sanção pelo então presidente Michel Temer envolveu uma série de vetos e a lei foi objeto da Medida Provisória nº. 869/2018, que introduziu mudanças significativas na lei, especialmente no que tangia à criação da Autoridade Nacional de Proteção de Dados (ANPD), órgão competente para fiscalizar as atividades de coleta e tratamento de dados pessoais no país. A Medida Provisória foi então discutida e apreciada pelo Congresso Nacional, dando origem à Lei nº. 13.853 de 2019, sancionada pelo presidente Jair Bolsonaro em 8 de julho de 2019, também com uma série de vetos, e que finalmente cria a ANPD.

Embora aprovada em 2018, a LGPD só entrará em vigor no Brasil em agosto de 2020, razão pela qual ela não foi aplicada às experiências de compartilhamento de dados entre aplicativos de transporte e a administração pública, que comentaremos a seguir. Vale destacar, ainda, que a LGPD não se aplica ao tratamento de dados pessoais realizado exclusivamente para fins de segurança pública, defesa nacional e segurança de Estado (art. 4º, III), o que diminui o grau de proteção que será aplicável a iniciativas nessas áreas.

Até agora, portanto, as cidades brasileiras abrigam exemplos constantes da tensão entre os interesses daqueles que veem na coleta e tratamento de dados oportunidades únicas para promover o desenvolvimento urbano, com os interesses daqueles que advogam por limites a essas capacidades como condição para a tutela da privacidade. Esse debate pode ser ilustrado pelos recentes casos envolvendo empresas que oferecem aplicativos de transporte e prefeituras municipais brasileiras, como relatamos a seguir.

3.2. O caso Uber em São Paulo

Em 2014, a empresa Uber iniciou suas atividades em São Paulo, inaugurando na cidade um modelo de negócios que oferece serviço de intermediação de corridas entre motoristas e passageiros por meio de um aplicativo de celular, e trouxe consigo uma série de conflitos regulatórios. Em São Paulo, a exemplo do que ocorreu em várias cidades ao redor do mundo, o início das operações da empresa aqueceu o debate acerca da regulação do transporte individual de passageiros e levou a movimentações importantes, no âmbito municipal, dos poderes Executivo e Legislativo (ZANATTA; KIRA; DE PAULA, 2015). Tal cenário se tornou ainda mais

complexo com a entrada de outras empresas, com modelos de negócios similares, como é o caso da modalidade POP da 99Taxis e da Cabify.

Em dezembro de 2015, a Prefeitura de São Paulo lançou consulta pública, colocando em debate uma minuta de decreto que trazia uma proposta inovadora de regulação de um novo modelo de transporte individual para a cidade. A consulta ficou no ar por trinta dias, período em que foram recebidas 5865 contribuições pela plataforma disponibilizada na internet.[15] Após a consolidação das sugestões, em 10 de maio de 2016, a Prefeitura de São Paulo publicou o Decreto nº 56.981/2016, criando novos contornos regulatórios para o uso do viário urbano municipal. [16]

O decreto aprovado estabelece uma série de regras que regulamentam as chamadas Operadoras de Tecnologia de Transporte Credenciadas (OTTCs), definidas amplamente como "operadoras de tecnologia credenciadas que sejam responsáveis pela intermediação entre os motoristas prestadores de serviço e os seus usuários".[17] Para atuarem na cidade, a Prefeitura exigiu que essas empresas utilizassem créditos, em quilômetros, cujo preço público seria estabelecido pelo poder público, de acordo com critérios como horários de utilização, área de atuação na cidade e distância percorrida.

Além disso, e elemento importante para o objeto do presente artigo, o decreto, sobretudo por meio da Resolução no 1 do Comitê Municipal de Uso do Viário (CMUV), posteriormente reeditada pela Resolução no 5, criou a obrigação de compartilhamento de certos dados pelas OTTCs credenciadas, o que inclui informações sobre as viagens (origem e destino, tempo de duração, trajeto etc.), sobre os motoristas (identificação e avaliação do serviço prestado) e sobre os veículos. Essas exigências, fundadas na necessidade de monitoramento e aplicação das regras de uso dos créditos, trouxeram algumas preocupações em relação à proteção da privacidade de usuários e motoristas.

Em resposta a essas questões, levantadas por algumas empresas do setor, o CMUV, ente responsável pelo monitoramento das OTTCs, publicou, em 16 de setembro de 2016, a Resolução CMUV nº. 10/2016 (COMITÊ MUNICIPAL DE USO DO VIÁRIO, 2016), que regulamentou o Decreto no 56.981/2016 em relação à segurança e ao tratamento das informações recebidas ou geradas pelas OTTCs. A resolução, que, entre outras medidas, colocou os dados comerciais das empresas e os dados e

15. Disponível em: <http://consultausointensivoviario.prefeitura.sp.gov.br/>. Acesso em: 2 maio 2017.

16. O Decreto no 56.981/16 foi alterado pelo Decreto nº 58.595, de 4 de janeiro de 2019, que estabeleceu requisitos adicionais para a inscrição de condutores e veículos, por exemplo. O cerne da estrutura regulatória introduzido pelo Decreto nº 56.981/16 foi mantido.

17. Prefeitura de São Paulo, Decreto nº 56.981/2016, art. 3º, §1º.

informações pessoais de passageiros e condutores sob sigilo legal, era aguardada e foi bem recebida pelo setor empresarial. Ao que parece, as novas regras atenderam não apenas demandas relacionadas à proteção da privacidade de usuários, mas também de segredos de negócios e vantagens competitivas das empresas.

O contentamento durou pouco. Apenas três dias após a publicação da regulamentação, foi publicada a Resolução CMUV nº. 11/2016, revogando a resolução anterior. Tal guinada, segundo alguns veículos de imprensa (RIBEIRO; LEITE, 2016) teria ocorrido por conta de incompatibilidade entre a resolução anterior com o Decreto nº. 56.519/2015, que regulamenta as regras de sigilo de informações da Prefeitura. Por esse decreto, seria necessário ouvir a Comissão Municipal de Acesso à Informação, responsável por classificar as informações em qualquer grau de sigilo.

Nesse contexto de oscilação regulatória, a proteção conferida aos dados gerados e coletados pelas OTTCs entrou novamente no campo da incerteza. Se, por um lado, quando se trata de dados do poder público, o acesso à informação e a transparência da gestão são essenciais para o controle e *accountability* dos atos da administração pública, por outro, quando se trata de dados pessoais, o centro de gravidade da regulação deve ser a proteção dos direitos fundamentais. Assim, ao mesmo tempo que políticas de dados abertos são iniciativas interessantes e condizentes com gestões responsáveis e responsivas, o tratamento oferecido aos dados pessoais também merece atenção dos gestores.

Para além de uma questão econômica, relacionada a segredos de negócios, ou formal, relativa à identificação do órgão competente para classificação dos dados como sigilosos, a questão de fundo sobre proteção à privacidade parece ter sido pouco explorada pelos grupos envolvidos no debate. É importante lembrar que, quanto mais as pessoas compartilham dados com plataformas, maior é o risco de exposição de sua privacidade e intimidade. A depender do tipo de dado coletado ou gerado (informações como horários de deslocamentos, trajetos, opiniões sobre os motoristas etc.), é possível montar perfis detalhados dos usuários, com suas rotinas e preferências. Em 2018, o escândalo envolvendo a consultoria política Cambridge Analytica e o Facebook é um exemplo de situação em que dados pessoais foram apropriados e utilizados sem o controle e o conhecimento dos usuários da rede social, para finalidades, no mínimo, suspeitas – e, sob muitas legislações, ilegais.

Casos como esses, que colocam a proteção da privacidade dos usuários na linha de frente, geram preocupações legítimas que deveriam ser consideradas pelo regulador de forma ampla, ao considerar os arranjos de políticas públicas das cidades inteligentes. A discussão acerca da proteção de dados pessoais no contexto da chamada economia digital e, em especial, na economia do compartilhamento

ganha, assim, cada vez mais relevância, principalmente em um cenário de maior interesse do poder público na regulação de novos modelos de negócios.

No caso de São Paulo, em 25 de novembro de 2016, o CMUV aprovou uma nova resolução sobre proteção dos dados de OTTCs. A Resolução nº. 13 do CMUV estabeleceu o regime de tratamento e proteção, pela Administração Pública Municipal, dos dados recebidos ou gerados a partir das atividades de transporte individual remunerado de passageiros. A resolução, entre outras medidas, criou o cargo de gestor da informação, responsável por assegurar o sigilo dos dados protegidos legalmente e zelar sobre seu compartilhamento entre entes da administração municipal. A resolução determinou que são protegidos por sigilo legal todos os dados pessoais de passageiros e condutores ou aqueles que possam ferir sua privacidade, de acordo com a Lei nº. 12.527/2011, bem como dados operacionais das empresas.

Apesar da criação desse marco regulatório, sua implementação ainda era incerta. Em 2017, um novo prefeito, João Doria Jr., assumiu a Prefeitura de São Paulo. No entanto, a indicação de uma pessoa para o cargo de gestor de informação, figura central para que os dispositivos previstos na Resolução nº. 13 da CMUV sejam aplicados e supervisionados adequadamente, ainda não tinha ocorrido.

Foi com base na ausência de indicação de um gestor de informação e no descumprimento dos requisitos estabelecidos pela Resolução nº. 13 da CMUV que a empresa Uber obteve uma decisão judicial suspendendo a obrigatoriedade de compartilhamento de dados com a Prefeitura de São Paulo.[18] Em janeiro de 2018, a Justiça de São Paulo decidiu em caráter liminar que, diante do risco de que os dados sigilosos sejam indevidamente acessados por terceiros, e "na medida em que eles se constituem em fonte de planejamento estratégico e comercial da empresa", o município só poderá exigir o compartilhamento dos dados após comprovar que tomou as providências necessárias para garantir o sigilo e a segurançan das informações.

As Resoluções nº. 9 e 15 da CMUV passaram, então, a admitir que a verificação do valor do preço público a ser pago pelas empresas (calculado com base na quilometragem da OTTC) seja feita por meio de auditoria independente, eliminando, desta forma, a obrigação de entregar à Prefeitura informações específicas sobre cada viagem.

Recentemente, durante a gestão do prefeito Bruno Covas, a Prefeitura cumpriu os requisitos estabelecidos na Resolução nº. 13, ficando, portanto, apta a exigir

18. Cf. Portal Migalhas, "Uber não é obrigado a compartilhar dados pessoais com Prefeitura de São Paulo". Disponível em: <https://www.migalhas.com.br/Quentes/17,MI273078,101048-Uber+nao+e+obrigado+a+compartilhar+dados+pessoais+com+prefeitura+de+SP>.

o compartilhamento direto de informações das empresas. A Resolução no 16 da CMUV, posteriormente alterada pela Resolução nº. 18, criou o Cadastro Municipal de Condutores (Conduapp), que impõe um cadastro obrigatório para motoristas de OTTC, o qual deve ser compartilhado com a Prefeitura.

A Resolução nº. 19 determina o método de envio dos dados à Prefeitura, estabelecendo duas modalidades de compartilhamento possíveis, a remota, mediante a instalação de sistema que dá acesso direto, pela Prefeitura, aos dados solicitados, e a eletrônica, que depende do envio de arquivos no padrão estabelecido pela Prefeitura. São três grupos de dados: (i) sobre as chamadas; (ii) sobre os condutores; e (iii) sobre os veículos. No caso das chamadas, a Prefeitura exigia o ID da chamada, a data, o tempo de viagem, a distância percorrida em metros, assim como a localização de origem e destino da chamada, informada com base no CEP.

A Resolução nº. 21 da CMUV, atualmente em vigor, extingue a possibilidade de envio de relatórios por meio de auditoria independente e exige a entrega direta de dados das empresas para a Prefeitura. Além disso, introduziu uma mudança importante nas informações sobre a origem e o destino das chamadas: elas devem incluir dados de latitude de origem e destino em WGS84 com três casas decimais, o que significa um grau de precisão de até 110m (ZANG, 2014).

Ao abandonar a referência de CEP e exigir as informações de latitude com grau de precisão de três casas decimais, a Prefeitura ganha acesso a dados detalhados sobre os deslocamentos das chamadas na cidade. Estudos demonstram que técnicas de engenharia reversa e de cruzamento de dados tornam possíveis, com base nesses dados, a identificação de usuários e a descoberta de endereços como residência e local de trabalho, por exemplo. Em um estudo conduzido em 2013, pesquisadores concluíram que registros de mobilidade humana são altamente únicos. Com informações de tempo e de localização com grau de precisão de quatro casas decimais, foi possível identificar 95% do total de indivíduos, que foi de 1,5 milhão (MONTJOYE, 2013).

Em outro exemplo, explorando as deficiências na forma de anomização de dados, quando foi liberado um banco de dados de todas as viagens de táxi feitas na cidade de Nova York em 2013, contendo registros de 173 milhões de viagens – incluindo locais de origem e destino e horários, além do número de licença, placa e outros metadados – , pesquisadores foram capazes de desanonimizar todo o conjunto e assim reidentificar números de licença e placa para cada viagem com relativa facilidade (PANDURANGAN, 2014).

Para além das questões ligadas aos dados que são compartilhados pelas empresas com a Prefeitura, no caso de São Paulo, o tratamento dado à questão pela gestão municipal tem gerado polêmicas. Em entrevista, o então titular da Secre-

taria de Transportes da Prefeitura (SPTrans), Sérgio Avelleda, revelou o número total de carros da Uber e dos outros três aplicativos que operam na capital paulista – dado mantido sob sigilo na gestão do ex-prefeito Fernando Haddad (DIÓGENES, 2016). Polêmicas declarações foram dadas também com relação à venda de dados do Bilhete Único municipal, que registra informações sobre os trajetos dos usuários, como parte da agenda de privatizações da Prefeitura.

Foi durante o evento *World Government Summit 2017*, em Dubai, que o então prefeito João Doria Jr. anunciou seu programa de desestatização (SECRETARIA ESPECIAL DE COMUNICAÇÃO, 2017), que incluiria a comercialização da base de dados dos bilhetes do sistema de transporte público de São Paulo, para "*cross selling opportunities*". O evento reuniu diversos outros prefeitos e governantes, com o objetivo de atrair investimentos internacionais para a cidade, e, desde seu anúncio, ainda não foram fornecidas mais informações sobre como esse compartilhamento de dados se daria, em que circunstâncias nem com quais finalidades.

A proposta apresentada por João Doria Jr. utilizaria a base de dados dos usuários do Bilhete Único, que concentra hoje informações de cerca de 15 milhões de cartões já emitidos pela Secretaria Municipal de Transportes (SPTrans). As informações armazenadas pela Prefeitura são os dados cadastrais que o usuário deve obrigatoriamente fornecer para a emissão do bilhete, tais como nome, endereço, CPF, RG, nome da mãe e foto (LEMOS, 2017).

Como consequência da proposta, o art. 9º, I, da Lei Municipal nº. 16.703, de 4 de outubro de 2017, que disciplina as concessões e permissões de serviços, obras e bens públicos que serão realizadas no âmbito do Plano Municipal de Desestatização da Cidade de São Paulo, autorizou a exploração econômica, por meio do regime de concessão, do sistema de bilhetagem eletrônica de transportes, que compreende a gestão do Bilhete Único. Registre-se, nesse sentido, que o Bilhete Único reúne grande quantidade de informações sobre seus usuários, tais como dados de biometria facial, CPF, idade, sexo, endereço, e que não há o consentimento livre, específico e informado de seus usuários para a exploração econômica dessas informações.

A possibilidade de comercialização dessa ampla base de dados coloca, portanto, em risco a privacidade dos mais de 15 milhões de usuários ativos da rede de transporte público da Grande São Paulo, pois forneceria à empresa dados detalhados sobre a origem e o destino dos usuários. Ademais, os dados pessoais sobre deslocamento são gerados pelos usuários e entregues à administração pública de

forma involuntária, sem que estejam em vigor termos de uso que exijam a manifestação do consentimento dos munícipes e que estabeleçam regras claras a respeito de como o tratamento dessas informações se dará.[19]

3.3. O caso 99Taxis no Distrito Federal

Medidas como a regulamentação paulistana também têm sido questionadas em outros locais, e por outras empresas que oferecem serviço similar ao Uber. Em 2018, a 99Taxis ingressou com ação perante a 4ª Vara da Fazenda Pública do Distrito Federal contestando a constitucionalidade e a legalidade da Lei nº. 5.691/2016 do Distrito Federal e de suas regulamentações – Decreto nº. 38.258/2017 e Portarias nº. 54/2017 e nº. 77/2017 –, que regulam o serviço de transporte individual privado de passageiros por aplicativos no DF. A empresa questionava a adequação e a proporcionalidade das regras, que incluem a obrigação de coletar e encaminhar ao poder público dados pessoais dos veículos e dos motoristas cadastrados, além de informações sobre viagens realizadas, segundo a empresa, sem que tivessem sido adotadas medidas para a proteção dos dados.

Em 15 de março de 2018, a justiça do DF negou o pedido liminar, alegando que não há inconstitucionalidade nem ilegalidade na regulação. Segundo o magistrado, as informações sobre as viagens realizadas seriam instrumentos relevantes para a cobrança de tributos pela administração pública e para a melhoria do planejamento de trânsito e transporte público. Além disso, nos termos da decisão, as informações exigidas não seriam dados pessoais, mas sim dados objetivos sobre o serviço prestado, que não atingem a intimidade ou a privacidade dos usuários, nem violam o sigilo de dados estabelecido no Marco Civil da Internet. A 99 recorreu, mas o pedido foi novamente negado. A decisão, no entanto, não é definitiva e pode ser modificada no decorrer do processo.

As regras do Distrito Federal têm como base a Lei Federal nº. 13.640/2018, que altera a Política Nacional de Mobilidade Urbana (Lei nº. 12.587/2012) para regulamentar o transporte remunerado privado individual de passageiros. Aprovada no início de 2018, após meses de debates no Congresso Nacional, a nova lei estabelece algumas regras em nível nacional, mas delega aos municípios a competência para regulamentar e fiscalizar o serviço. De lá para cá, várias cidades aprovaram regras para disciplinar a atividade, estabelecendo regras locais para o oferecimento do serviço. A exigência de compartilhamento de dados aparece em várias delas.

---

19. No Rio de Janeiro, há também a preocupação com a forma como os dados fornecidos para o Bilhete Único, o RioCard, estão sendo tratados, se estão sendo compartilhados, em decorrência da falta de transparência do governo carioca.

4. Boas práticas e proteção de dados pessoais nas cidades: um debate necessário

Como os casos acima relatados ilustram, a abundância cada vez maior de ferramentas de coleta e tratamento de dados à disposição do poder público levanta sérias preocupações em relação à privacidade dos cidadãos nas cidades inteligentes. Diante da tarefa de regular iniciativas inovadoras, que trazem novos desafios para o direito regulatório tradicional, a tendência é de que, cada vez mais, o regulador queira acesso aos dados disponibilizados e produzidos pelas plataformas.

Empresas têm desenvolvido ferramentas para colaborar com o poder público e, ao mesmo tempo, preservar a privacidade de usuários. Destaca-se o *Uber Movement*, serviço lançado pela Uber que permite mostrar, por meio de um mapa de fluxo de movimento, informações sobre os lugares e horários em que há maior demanda do serviço de transportes, o tempo médio de viagem entre dois pontos e outros dados referentes à mobilidade em centros urbanos.[20] Segundo a empresa, todos os dados são anonimizados e agregados, ou seja, nenhum dado ou informação sobre o comportamento de uma pessoa individualmente identificada ou identificável pode ser revelado por meio da plataforma. O serviço foi lançado em São Paulo e já opera em grandes centros urbanos ao redor do mundo, incluindo Nova York e Boston, nos Estados Unidos, e Bogotá, na Colômbia.

A divulgação desses dados agregados, similar àquela feita pelo aplicativo Waze por meio do programa *Connected Citizens*, permite o acesso às informações em tempo real, buscando aprimorar a gestão das cidades. O objetivo, segundo a Uber, é ajudar os planejadores urbanos a tomar decisões subsidiadas sobre suas cidades com base nos dados coletadas com as viagens (GILBERTSON; SALZBERG, 2017). Apesar da iniciativa, a empresa ainda tem recebido diversos pedidos de prefeituras para que divulgue as informações sobre os locais onde se iniciam e finalizam as viagens dos passageiros, o que a Uber tem mantido em sigilo (DAVIES, 2017). Diferentes estratégias têm sido desenvolvidas para lidar com essa questão. O uso exclusivo de dados agregados ou anonimizados e a exigência de consentimento explícito do munícipe para que a cidade os utilize são algumas das proteções possíveis. Chicago, por exemplo, alega que as informações coletadas pelos sensores urbanos instalados serão anonimizadas, mas em outros locais os gestores públicos enfrentam mais dificuldades (GOLDSMITH; CRAWFORD, 2014).

Nesse contexto, é importante que os reguladores tenham cautela em relação a quais tipos de dados devem ser exigidos e ao modo como devem ser armaze-

20. Disponível em: <https://canaltech.com.br/noticia/apps/uber-movement-conheca-o-novo-servico-de-monitoramento-de-trafego-do-app-86988/>. Acesso em: 2 maio 2017.

nados. No caso da regulamentação do Distrito Federal, muitas das informações requeridas são consideradas dados agregados, o que significa que o poder público não está exigindo acesso a informações individuais sobre motoristas ou passageiros, mas sim a um conjunto de dados não identificados, o que é positivo. É o caso, por exemplo, da exigência de envio da quantidade total de viagens realizadas mensalmente pela plataforma e da quantidade total, em quilômetros, da distância percorrida entre locais selecionados pela Secretaria de Mobilidade do Estado (Semob).

Em termos de legislação, há princípios constitucionais de proteção da privacidade e princípios da administração pública que se confrontam com o interesse regulatório por mais dados. Perguntas como "que tipo de dados são estritamente necessários para colocar a regulação em prática?" devem fazer parte da racionalidade regulatória. Ademais, com a entrada em vigor da Lei Geral de Proteção de Dados (Lei nº. 13.709/2018), é importante que os dados exigidos pelas regulamentações locais não excedam sua finalidade.[21] Isso significa dizer que o poder público deve requerer apenas as informações estritamente necessárias para colocar a regulação em prática e para fiscalizar as atividades das empresas. Informações individuais, como horários de deslocamentos, trajetos específicos, opiniões sobre os motoristas etc. – que possibilitam a montagem de perfis detalhados de usuários, suas rotinas e preferências – estariam fora do escopo. Nesse sentido, o envio mensal de uma planilha listando todos os motoristas, o número de CPF, o nome da mãe, o telefone celular e o endereço de *e-mail*, são exemplos de dados excessivos exigidos pela Portaria nº 77 do Distrito Federal.

Pode ser verdade que, quanto maior a quantidade de dados coletados, melhor será a compreensão do cenário no geral – o que pode contribuir para uma gestão mais eficiente das políticas públicas –, mas é preciso lembrar que a proteção dos dados de usuários é um limite que não deve ser transposto.

Nota-se, ainda, que um dos grandes desafios do desenho regulatório eleito pelas administrações municipais para lidar com as questões ligadas à privacidade, à proteção de dados e à confidencialidade de informações é o fato de, muitas vezes, por meio de atos administrativos como resoluções e portarias, serem estabelecidos instrumentos normativos de competência exclusiva do Executivo, cujas revogação e alteração podem ser feitas a qualquer tempo – a exemplo do que aconteceu na cidade de São Paulo. Quando as garantias em relação à privacidade e proteção de

21. A versão do projeto de lei aprovado pelo Congresso Federal (PLC nº. 53/2018) criava regras específicas para a coleta e o tratamento de dados pelo poder público, que proibiam, por exemplo, a transferência a entidades privadas de dados pessoais constantes das bases de dados a que se tenha acesso. Tais dispositivos, entretanto, foram vetados pela Presidência da República.

dados estão exclusivamente previstas nesses atos, elas podem ser facilmente revogadas, especialmente quando ocorrem mudanças de governo. Assim, os dados que foram entregues à administração pública sob determinado regime, podem ter seus usos e finalidades alterados ou seu grau de proteção simplesmente redefinido. Com a entrada em vigor da LGPD em agosto de 2020, espera-se que haja maior uniformidade no tratamento dessas questões por parte das administrações locais.

5. Conclusão

Este artigo discutiu como a abundância de dados sobre as dinâmicas urbanas e seus cidadãos, gerada por empresas de tecnologia, tem despertado o interesse do poder público em diferentes cidades ao redor do mundo, cujas administrações buscam acesso a tais informações para fins de desenvolvimento de políticas públicas e planejamento urbano, visando à construção de "cidades inteligentes". Em seguida, argumentou-se que, a despeito dos evidentes benefícios trazidos pelo uso de dados pelos governos locais, determinados arranjos regulatórios que exigem o compartilhamento de dados pessoais acarretam enormes riscos à privacidade dos cidadãos. Para ilustrar o argumento, foram apresentados alguns conflitos envolvendo prefeituras brasileiras e empresas de tecnologia e elencados os desafios envolvidos na necessidade de conciliar o acesso a dados importantes para o desenvolvimento das cidades, mas preservando direitos fundamentais.

Com isso, fica claro que os debates sobre privacidade e proteção de dados precisam acompanhar todas as iniciativas regulatórias encampadas pelo poder público que envolvam a adoção de tecnologias e o compartilhamento de dados com empresas do setor privado. Se, de um lado, legislações de proteção de dados, como a LGPD, estabelecem parâmetros e balizas que buscam minimizar os riscos das atividades de coleta e tratamento de dados praticadas pelos setores público e privado, de outro, também crescem as pressões de gestores públicos, urbanistas e profissionais ligados ao planejamento urbano pelo acesso a dados que permitam compreender as dinâmicas urbanas contemporâneas para possibilitar a formulação de políticas mais eficientes.

Nos casos das regulamentações envolvendo os aplicativos de transporte, fica claro que o compartilhamento de dados entre as empresas e as prefeituras serve a finalidades diferentes, como o cálculo do preço público em São Paulo, ou a fiscalização da condição dos veículos e do preenchimento de determinados requisitos pelos condutores. Contudo, também se percebe que as exigências de compartilhamento de dados excessivos podem ser encaradas como uma moeda de troca que, mais do

que submeter as empresas à instalação de mecanismos custosos e sofisticados para a disponibilização dos dados, acabam expondo os cidadãos a vazamentos e abusos.

Por essas razões, nessas empreitadas, para preservar a privacidade e a segurança das informações pessoais dos cidadãos, é preciso enfrentar questões complexas do ponto de vista regulatório: como o acesso aos dados será monitorado e restringido, como cidadãos poderão optar por não terem seus dados coletados, por quanto tempo a informação será mantida, como os abusos serão punidos, como os dados serão efetivamente anonimizados, entre outras (GOLDSMITH; CRAWFORD, 2014).

Mas há outras frentes de ação, que precisam estar concatenadas com os aspectos regulatórios. Uma delas se refere à conscientização dos cidadãos a respeito do valor de sua privacidade e do modo como a administração das cidades lida com essa questão. Além de fomentar políticas de transparência e informação a respeito da coleta e da utilização de dados, a administração pública deve promover campanhas e materiais de formação que orientem e preparem os cidadãos para essa nova realidade.

Por fim, vale destacar a necessidade de engajamento com a comunidade técnica e de desenvolvedores, que podem incorporar nas tecnologias e produtos utilizados pelas cidades o conceito de *privacy by design*, minimizando os riscos de violações e abusos em relação aos dados dos cidadãos e propondo soluções de compartilhamento que adotem técnicas robustas de segurança da informação, como a criptografia forte, e ainda métodos sofisticados de anonimização de dados pessoais.

Uma vez que as tecnologias de coleta e análise de dados ainda são relativamente novas, assim como seus usos pela cidade, este é o momento oportuno para lidar com as implicações de privacidade, para que as cidades do futuro não incorram em erros do passado.

Referências bibliográficas

ABREU, J. S.; VALENTE, M. Cuidado por onde andas, usar o celular te faz suspeito. Blog Deu nos Autos, Link, *Estadão*, 9 de março de 2017. Disponível em: <https://link.estadao.com.br/blogs/deu-nos-autos/cuidado-com-onde-andas-usar-o-celular-te-faz-suspeito/>

BALDWIN, R.; CAVE, M.; LODGE, M. *Oxford Handbook of Regulation*. Oxford: Oxford University Press, 2010.

BATTY, M.. Does Big Data Lead to Smarter Cities? Problems, pitfalls and opportunities. *Journal of Law and Policy*, v. 11. p. 133, 2015.

BIONI, B. *Autodeterminação informacional*: paradigmas inconclusos entre a tutela dos direitos da personalidade, a regulação dos bancos de dados eletrônicos e a arquitetura da internet. Dissertação de mestrado. São Paulo: Universidade de São Paulo, 2016.

BLOOMBERG, M. Foreword. In: GOLDSMITH, S.; CRAWFORD, S. *The Responsive City*: Engaging Communities Through Data-Smart Governance. Nova York: Jossey Bass, 2014.

BROWN, I. Britain's smart meter programme: a case study in privacy by design. *International Review of Law, Computers & Technology,* v. 28, n. 2, p. 172-184, 2013.

CALO, R. Digital Market Manipulation. *The George Washington Law Review,* v. 82, 2013.

CRAWFORD, K.; SCHULTZ, J. Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms (October 1, 2013). *Boston College Law Review*, v. 55, n. 93, 2014;

DAVIES, A. Uber's mildly helpful data tool could help cities fix streets. *Wired*, 1 de agosto de 2017. Disponível em: <https://www.wired.com/2017/01/uber-movement-traffic-data-tool/>. Acesso em: 31 ago. 2018.

DIÓGENES, J. Total de carros da Uber e outros aplicativos supera número de taxistas em SP, diz Doria. *O Estado de São Paulo*, São Paulo, 04 de fev. de 2016. Disponível em <http://sao-paulo.estadao.com.br/noticias/geral,total-de-carros-da-uber-e-outros-aplicativos-supera-numero-de-taxistas-em-sp-diz-doria,70001653256>. Acesso em: 30 maio 2017.

FARAH, M. F. S. Parcerias, novos arranjos institucionais e políticas públicas no nível local de governo. *RAP – Revista de Administração Pública*, v. 35, n. 1, p. 119-145, jan.-fev. 2001.

FINANCIAL ACTION TASK FORCE. *Money Laundering and Terrorist Financing through the Real Estate Sector*. Paris: OECD, 2007. Disponível em: <https://www.fatf-ga.org/media/fatf/documents/reports/ML%20and%20TF%20through%20the%20Real%20Estate%20Sector.pdf>. Acesso em: 2 maio 2017.

GILBERTSON, J.; SALZBERG, A. Introducing Uber Movement. Uber Newsroom, 8 de janeiro de 2017. Disponível em: <https://newsroom.uber.com/introducing-uber-movement/>. Acesso em: 30 abril 2017.

GOLDSMITH, S.; CRAWFORD, S. *The Responsive City:* Engaging Communities Through Data-Smart Governance. Nova York: Jossey Bass, 2014.

GREENLEAF, G. Global Data Privacy Laws 2015: 109 Countries, with European Laws Now a Minority (January 30, 2015). *UNSW Law Research Paper*, n. 2015-21, 2015. Disponível em SSRN: <https://ssrn.com/abstract=2603529>. Acesso em: 2 jan. 2017.

HOOFNAGLE, C. J. *et al.* Behavioral Advertising: The Offer You Cannot Refuse. *Harvard Law and Policy Review*, 6, 2012.

IBM INSTITUTE FOR BUSINESS VALUE. *A Vision of Smarter Cities.* Somers: IBM, 2009. Disponível em: <https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GBE03227USEN>. Acesso em: 30 maio 2017.

KOBRIN, S. J. Safe harbours are hard to find: the trans-Atlantic data privacy dispute, territorial jurisdiction and global governance. *Review of International Studies*, 30, 2004, p. 111-131.

MACHADO, J. Prefeito Dória anuncia a venda de dados dos usuários do Bilhete Único. *Colab*, São Paulo, 16 de fev. de 2017. Disponível em <http://colab.each.usp.br/?p=587>. Acesso em: 30 maio 2017.

MINISTÉRIO DA ECONOMIA. Receita Federal analisa as informações de redes sociais. *Receita Federal - Notícias*, 14 de março de 2017. Disponível em: <http://receita.economia.gov.br/noticias/ascom/2017/marco/receita-federal-analisa-as-informacoes-de-redes-sociais>.

MONTJOYE, Y-A. *et al.* Unique in the Crowd: The Privacy Bounds of Human Mobility, *Scientific Reports,* 3, 1376, Mar. 23, 2013. Disponível em: <http://www.nature.com/articles/srep01376>.

NATUSCH, I.; FELIZI, N.; VARON, J. Bilhete Único: concentração de dados e dinheiro no transporte público do Rio. *Chupadados*, Rio de Janeiro, 12 de set. de 2017. Disponível em: <https://chupadados.codingrights.org/com-o-riocard-seus-dados-passeiam-pelo-rj-e-ninguem-sabe-onde-vao-descer/>. Acesso em: 30 maio 2017.

PANDURANGAN, V. On Taxis and Rainbows, Lessons from NYC's improperly anonymized taxi logs, *Medium*. Jun 22, 2014. Disponível em: <https://tech.vijayp.ca/of-taxis-and-rainbows-f6bc289679a1>.

PARLAMENTO EUROPEU. *Mapping Smart Cities in the EU. Relatório do Parlamento Europeu.* Policy Department: Economic and Scientific Policy, União Europeia, 2014. Disponível em: <http://www.europarl.europa.eu/studies>.

RIBEIRO, B.; LEITE, F. Haddad diz que sigilo a dados da Uber e outras firmas é irregular e manda revogar resolução. *O Estado de São Paulo*, São Paulo, 17 de set. de 2016. Disponível em: <http://sao-paulo.estadao.com.br/blogs/por-dentro-da-metropole/haddad-diz-que-sigilo-a-dados-da-uber-e-outras-firmas-e-irregular-e-manda-revogar-decreto/>. Acesso em: 30 maio 2017.

SÃO PAULO. PREFEITURA MUNICIPAL. Prefeitura disponibiliza base do IPTU em formato aberto no GeoSampa. *Gestão Urbana SP*, 05 de maio de 2016. Disponível em: <http://gestaourbana.prefeitura.sp.gov.br/noticias/prefeitura-disponibiliza-base-do-iptu-em-formato-aberto-no-geosampa>. Acesso em: 2 maio 2017.

SÃO PAULO. SECRETARIA ESPECIAL DE COMUNICAÇÃO. Prefeito vai a evento internacional para atrair investimentos em SP, *Notícias*, 14 de fev. de 2017. Disponível em <http://capital.sp.gov.br/noticia/prefeito-vai-a-evento-internacional-para-atrair-investimentos-em-sp>. Acesso em: 30 maio 2017.

SÃO PAULO. SECRETARIA MUNICIPAL DE TRANSPORTES. COMITÊ MUNICIPAL DE USO DO VIÁRIO. Resolução nº 10, de 30 de agosto de 2016. *Diário Oficial da Cidade de São Paulo*, São Paulo, 16 de set. de 2016. Disponível em: <https://www.migalhas.com.br/arquivos/2016/9/art20160919-03.pdf>. Acesso em: 2 maio 2017.

_____. Resolução nº 11, de 19 de setembro de 2016. *Diário Oficial da Cidade de São Paulo*, São Paulo, 20 de set. de 2016. Disponível em: <http://www.docidadesp.imprensaoficial.com.br/NavegaEdicao.aspx?ClipID=DAI3AO1T7N876eCRKNJ38K9TP3A&PalavraChave=revoga>. Acesso em: 20 maio 2017.

_____. Resolução nº 13, de 18 de novembro de 2016. *Diário Oficial da Cidade de São Paulo*, São Paulo, 25 de nov. de 2016. Disponível em <https://www.internetlab.org.br/wp-content/uploads/2016/11/resolucao_CMUV_protecao_dados.pdf>. Acesso em: 30 maio 2017.

SHAFFER, G. C., Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Data Privacy Standards. *Yale Journal of International Law*, v. 25, pp. 1-88, 2000. Available at SSRN: <https://ssrn.com/abstract=531682>

TOTTY, M. The Rise of the Smart City. *Wall Street Journal*, Nova York, 16 de abril de 2017. Disponível em: <https://www.wsj.com/articles/the-rise-of-the-smart-city-1492395120>. Acesso em: 2 maio 2017.

TOWNSEND, A. *Smart Cities*: Big Data, Civic Hackers, and the Quest for a New Utopia. Nova York: W. W. Norton & Company, 2013.

TRANSPARÊNCIA INTERNACIONAL BRASIL. *São Paulo*: a corrupção mora ao lado? Empresas offshore e o setor imobiliário na maior cidade do hemisfério sul. São Paulo: Transparency International, 2017. Disponível em: <http://quemmoraaolado.org/qmal/index.php>. Acesso em: 2 maio 2017.

UBER. *Metodologia de cálculo do Uber Movement*. Disponível em: <https://movement.uber.com/_static/76002ded222a46a02ae89f207e91e335.pdf> Acesso em: 30 maio 2018.

_____. *Uber Movement Frequently Asked Questions*. Disponível em <https://movement.uber.com/faqs>. Acesso em: 30 maio 2017.

VELOSA, A.; RYAN-TRAZ, B.; ANAVITARTE, L.; FERNANDO, H. Market Trends: Smart Cities Are the New Revenue Frontier for Technology Providers. *Gartner Research*, 01 de abril de 2011. Disponível em: <https://www.gartner.com/doc/1615214/market-trends-smart-cities-new>. Acesso em: 30 maio 2017.

ZANATTA, R.; KIRA, B.; PAULA, P. de. A regulação do transporte individual em São Paulo: o que está em jogo? *InternetLab*, 12 de jan. de 2016. Disponível em: <http://www.internetlab.org.br/pt/opiniao/a-regulacao-do-transporte-individual-em-sao-paulo-o-que-esta-em-jogo/>. Acesso em: 2 maio 2017.

ZANG, S. Quão preciso é um grau de longitude ou latitude?. *Gizmodo Brasil*, 8 de setembro de 2014. Disponível em <https://gizmodo.uol.com.br/quao-preciso-e-um-grau-de-longitude-ou-latitude/>. Acesso em: 2 maio 2017.

Bases de dados

GEOSAMPA. *Geosampa*. Disponível em: <http://geosampa.prefeitura.sp.gov.br/PaginasPublicas/_SBC.aspx>. Acesso em: 2 maio 2017.

OPEN KNOWLEDGE FOUNDATION. *Open Data Handbook*. Disponível em: <http://opendatahandbook.org/guide/pt_BR/what-is-open-data/>. Acesso em: 2 maio 2017.

WORLD HEALTH ORGANIZATION. *Global Health Observatory*. Disponível em: <http://www.who.int/gho/urban_health/situation_trends/urban_population_growth_text/en/>. Acesso em: 2 maio 2017.

Dennys Marcelo Antonialli

Doutor em Direito Constitucional pela Universidade de São Paulo, onde também atuou como professor do Departamento do Estado (DES-FDUSP). Possui mestrado em Direito pela Stanford Law School (EUA) e mestrado profissional em Law and Business, conjuntamente oferecido pela Bucerius Law School e pela WHU Otto Beisheim School of Management (Alemanha). É diretor do InternetLab, centro independente de pesquisa em direito e tecnologia.

Email: dennys@internetlab.org.br
ORCID: 0000-0001-6382-2712

Beatriz Kira

Mestra em Ciências Sociais da Internet pela University of Oxford. Doutoranda em Direito Econômico pela Universidade de São Paulo e pesquisadora sênior na Blavatnik School of Government, University of Oxford.

Email: beatriz.kira@usp.br
ORCID: 0000-0002-7078-8193

Submissão: 23 de dezembro de 2018.

Aprovação: 11 de setembro de 2019.

Como citar: ANTONIALLI, D. M.; KIRA, B. Planejamento urbano do futuro, dados do presente: a proteção da privacidade no contexto das cidades inteligentes. *Revista brasileira de estudos urbanos e regionais*. v.22, E202003, 2020. DOI 10.22296/2317-1529.rbeur.202003

Artigo licenciado sob Licença Creative Commons CC BY-NC 4.0.
https://creativecommons.org/licenses/by-nc/4.0/deed.pt_BR