A Lei Geral de Proteção de Dados nas Plataformas de Mobilidade Urbana no Contexto da Economia e do Urbanismo Orientados por Dados

The General Data Protection Act in the Urban Mobility Platforms Within the Context of Data-Oriented Economy and Urbanism

MATEUS DE OLIVEIRA FORNASIER[1]
Universidade Regional do Noroeste do Estado do Rio Grande do Sul, Brasil.

NORBERTO MILTON PAIVA KNEBEL[2]
Universidade Regional do Noroeste do Estado do Rio Grande do Sul, Brasil.

RESUMO: O objetivo deste artigo é de analisar a aplicabilidade da Lei Geral de Proteção de Dados (LGPD) – Lei nº 13.709/2018 – como marco de proteção de dados pessoais, no contexto de um urbanismo orientado por dados que disciplinam os sistemas de mobilidade urbana. Os aplicativos de transporte público ou coletivo e as demais aplicações que se utilizam da geolocalização constituem plataformas que geram e trabalham os dados dos usuários – e, nesse contexto, é a informação gerada por cada usuário que constrói algoritmos e modelos para governança da mobilidade urbana. Sua hipótese é de que os dados não constituem mais mera informação para a decisão, mas sim determinantes dos modelos de decisão algorítmicos – o que só é possível por meio do aprendizado de máquinas e das inteligências artificiais, sugerindo uma economia que tem nos dados um ativo importante em si e a formação de padrões estratégicos forjados na análise em tempo real desses dados. Objetos específicos: i) analisar a aplicabilidade da LGPD no contexto das plataformas de mobilidade urbana sob o ponto de vista da proteção da privacidade e da transferências de dados pessoais entre agentes privados; ii) interpretar sistematicamente a LGPD, com vistas aos princípios constitucionais e ao contexto socioeconômico. Resultado: a cultura de proteção de dados promete ser o principal legado da LGPD, influenciando organizações a possuir um sistema protetivo para garantir sua confiabilidade e competitividade, pois o cenário do *big data* invoca desafios à regulação que observe direitos fundamentais que fogem do Estado e pressupõem formas de normatividade que contemplem a realidade econômica, social e política da sociedade orientada por dados. A dinâmica complexa da mobilidade urbana e a massividade de dados produzida por ela indica essa dificuldade para a regulação atender àquilo que só as inteligências artificiais conseguem. Quanto à metodologia, utilizamos o método de procedimento hipotético-dedutivo, com abordagem qualitativa e técnica bibliográfico-documental.

1 Orcid: <http://orcid.org/0000-0002-1617-4270>.
2 Orcid: <http://orcid.org/0000-0003-0674-8872>.

PALAVRAS-CHAVE: Lei Geral de Proteção de Dados; plataformas de mobilidade urbana; economia digital; urbanismo; privacidade.

ABSTRACT: The purpose of this paper is to analyze the applicability of the General Data Protection Act (LGPD) – Lei n. 13.709/2018 – as a mark of personal data protection, in the context of a data-driven urbanism that disciplines urban mobility systems. Public and mass transit apps and other applications that use geolocation are platforms that generate and work user data – and, in this context, the information generated by each user is what builds algorithms and models for urban mobility governance. Its hypothesis is that the consideration of the consent of individuals to whom data are collected – LGPD's core principle in this regard – may be insufficient for effective privacy protection, given that the way in which such data are managed and operationalized in practice distances itself from the simple gathering of data and its impediment. Specific objects: i) to analyze the applicability of LGPD in the context of urban mobility platforms from the point of view of protecting privacy and the transfer of personal data among private agents; ii) to systematically interpret LGPD, with a view to constitutional principles and the socioeconomic context. As a result, data protection culture promises to be LGPD's main legacy, influencing organizations to have a protective system to ensure their reliability and competitiveness, as the big data scenario invokes regulatory challenges that observe fundamental rights that escape the state and presuppose forms of normativity that contemplate the economic, social and political reality of data-driven society. The complex dynamics of urban mobility and the mass of data produced by it indicate such difficulty for regulation to meet what only artificial intelligences can achieve. Methodology: hypothetical-deductive procedure method, with qualitative approach and bibliographic-documentary technique.

KEYWORDS: General Data Protection Act; urban mobility platforms; digital economy; urbanism; privacy.

INTRODUÇÃO

A proteção jurídica dos dados no Brasil tem seu marco normativo na Lei Geral de Proteção de Dados (Lei nº 13.709/2018), instituída em 2018, mas que entrou em vigor em 2020. Essa lei, conforme seu primeiro artigo, dispõe sobre os dados pessoais, de pessoa natural ou jurídica, tendo o objetivo de proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade. O contexto dessa forma de mobilidade urbana é a economia orientada por dados, que transforma a economia informacional ao incorporar a gestão das informações e análise da massiva *big data*, que só é capaz por meio do aprendizado de máquinas e das inteligências artificiais, sugerindo uma economia que tem nos dados um ativo importante em si e a formação de padrões estratégicos forjados na análise em tempo real desses dados – algo que só as máquinas são capazes de fa-

zer. Portanto, os dados não são mais mera informação para os processos de decisão, mas determinante ao compôr os modelos de decisão algorítmicos.

Esta pesquisa se justifica pela importância de se compreender a LGPD dentro do cenário da economia e do urbanismo orientados por dados, tendo em vista apontar contradições, vácuos ou forças da lei que entrará em vigor ao analisar os conceitos e os dispositivos legais. Do ponto de vista constitucionalista, trata-se de entender como direitos fundamentais na ordem jurídica brasileira estão sendo regulamentados por atos normativos elaborados em um contexto socioeconômico imprevisto quando da promulgação da Lei Maior.

Considerou-se, para a elaboração deste trabalho, o seguinte problema de pesquisa: a proteção de dados pessoais prevista na LGPD é aplicável à mineração de dados promovida pelas plataformas de mobilidade urbana? Em relação a tal questionamento, a hipótese apresentada é a de que os dados não constituem mais mera informação para a decisão, mas sim determinantes dos modelos algorítmicos – o que só é possível por meio do aprendizado de máquinas e das inteligências artificiais, sugerindo uma economia que tem nos dados um ativo importante em si e a formação de padrões estratégicos forjados na análise em tempo real desses dados. Nesse sentido, a consideração do consentimento dos indivíduos sobre quem os dados são coletados – princípio nuclear da LGPD neste tocante – pode ser considerada insuficiente para uma efetiva proteção da privacidade, tendo-se em vista que o modo de gerenciar e operacionalizar tais dados na prática se distancia da simples obtenção de dados, ou do seu impedimento – o consentimento não tem sentido nesses contextos, de complexas técnicas de tratamento de dados, constituindo, assim, uma rendição completa sobre sua informação (Solove, 2004, p. 51).

O objetivo geral deste artigo é analisar a aplicabilidade da LGPD como proteção de dados pessoais sob o contexto de um urbanismo orientado por dados que disciplinam os sistemas de mobilidade urbana. Os aplicativos de transporte público ou coletivo e as demais aplicações que se utilizam da geolocalização constituem plataformas que geram e trabalham com os dados dos usuários; nesse contexto, a informação gerada por cada usuário, usada para treinar e construir algoritmos e modelos para governança da mobilidade urbana. Já os seus objetivos específicos, sendo cada um traduzido em um dos subtítulos deste trabalho, são: i) a análise da aplicabilidade da lei no contexto das plataformas de mobilidade urbana sob o ponto de vista da proteção da privacidade e da transferências de dados pessoais entre agentes privados; e ii) a leitura sistemática da LGPD, tendo em vista

os princípios constitucionais e o contexto econômico e social, que vêm à tona no questionamento do conceito de consentimento que será aplicado pela lei, bem como os limites de sua efetiva substancialidade no cenário do dirigismo informacional.

A fim de tornar factíveis tais objetivos, o artigo faz uma reflexão que parte de uma lógica dedutiva e de abordagem qualitativa, pois foi abstraída de uma revisão bibliográfica ampla i) da análise doutrinária da LGPD, ii) da proteção jurídica de dados, iii) da economia orientada por dados e iv) do urbanismo orientado por dados, uma resposta sobre a aplicabilidade dos conceitos da LGPD no cenário da mobilidade urbana.

1 A ECONOMIA ORIENTADA POR DADOS E A PROTEÇÃO JURÍDICA DOS DADOS NO BRASIL

A estrutura jurídica que normatizou a proteção aos dados está inserida no contexto de uma economia orientada por dados (*data driven economy*), também chamada de economia digital/informacional. Esse contexto de transformação digital corresponde à criação de um novo tipo de economia, orientada pelos dados gerados na rotina do dia a dia urbano, conectando digitalmente indivíduos e máquinas (Ciuriak, 2018, p. 12). Configura-se, assim, uma tendência de conversão de todas as práticas da vida social, política e econômica em dados, os quais podem, consequentemente, ser monitorados e manipulados. É um cenário na qual Zuboff (2019, p. 222) identifica uma rendição da experiência da vida cotidiana aos dados rentáveis – um mecanismo tecnológico que transforma os hábitos e os comportamentos ativos economicamente valiosos e complexos.

Pensar a regulação na sociedade informacional perpassa, então, pela compreensão da economia política das plataformas orientadas por dados, sujeitas ao seu potencial monopolista e de inviabilidade de competição quanto à gestão do espaço digital. A noção de plataforma é importante, pois indica que o poder, a funcionalidade e os recursos nela envolvidos dependem de arquiteturas que incorporam e extrapolam os limites de organizações formais ou Estados – eis que permitem a interação paralela entre pessoas, máquinas (mormente inteligências artificiais e algoritmos) e empresas. Essa complexidade das práticas informacionais surge como ameaça ao direito de privacidade e à capacidade cidadã de acessar, manipular, redistribuir, discutir e rearticular informações importantes (Hildebrandt, 2018, p. 2-3).

Do ponto de vista do desenvolvimento econômico, a economia orientada por dados sugere um novo modelo, baseado na transformação das

estruturas, que pode ser traduzida como a transição da economia baseada no conhecimento (*knowledge-based economy*) para a economia orientada por dados (*data driven economy*, ou *DDE*) (Ciuriak, 2018, p. 13), tendo esta última como principais características: i) a assimetria como fundação; ii) a industrialização do aprendizado por meio das inteligências artificiais; iii) a concentração de mercado e monopólio das grandes empresas; iv) a monetização dos dados; v) os riscos sistêmicos.

A ideia de que a sociedade informacional iria proporcionar o conhecimento para todos é confrontada com a realidade do *big data*, em que a quantidade massiva de dados impossibilita sua interpretação pela mente humana e pelas práticas individuais, dependendo de estruturas computacionais poderosas, preparadas para extrair sistematicamente dados importantes a partir de algoritmos dirigidos. Sobre a manipulação assimétrica do *big data*, além da relação desigual entre as grandes corporações informacionais e as pessoas, também é possível inferir que a administração e a interpretação dos dados digitais massivos instituam uma desigualdade entre o Estado e as pessoas[3], em razão da qual "o *big data* pode se transformar no *big brother*" (Cukier; Mayer-Schoenberger, 2013, p. 30).

O paradigma do *big data* traz consigo um elemento importante, que revela cada vez mais a assimetria entre usuários e controladores de dados: a tecnologia da informação sensível ao contexto – e razão da qual a gestão e a criação de dados digitais se adapta à entrada e à saída de dados no contexto do usuário e de seu ambiente. Ou seja: não se trata de dados simples (informações básicas de local ou tempo), mas sim de dados geridos e categorizados conforme o contexto e a relação entre os usuários em tempo real (o que também inclui a relação entre objetos autônomos conectados à internet, a chamada "internet das coisas")[4].

Essa possibilidade, independentemente de considerações sobre se ela se origina a partir das ações das empresas ou do Estado, indica a era da mineração de dados (*data science*), em que o direito à privacidade ganha nova relevância. As formas de proteção dos dados alcançam formas digitais

3 Também entre Estados que se relacionam conforme a orientação centro-periferia, em que a desigualdade do ponto de vista da economia política institui um uso de dados baseado em uma hierarquia de capacidade técnica para lidar com o *big data,* mesmo que traçando interesses humanitários, conforme destaca a pesquisa de Mann (2018, p. 35) ao criticar o desajuste estrutural na análise de dados por entidades norte-americanas e europeias em trabalhos voluntários na África.

4 A capacidade de interagir no contexto de *big data* é de diálogos entre máquina-máquina, processando em conjunto o comportamento humano. É a receita dos mecanismos inteligentes que conseguem processar dados em tempo real, algo que não seria possível com intervenção humana (Chen, 2012, p. 383).

de preservação das identidades anônimas após os dados serem publicados; sendo assim, torna-se necessário que informações sensíveis (informações sobre saúde, genética etc.) sejam impossibilitadas de serem reidentificadas. Todavia, conforme a tendência estrutural de monetização dos dados, o mercado adere a uma perspectiva contratualista, em que o uso dos dados em detrimento da privacidade pode se dar, desde que haja devida compensação aos indivíduos pelos coletores de dados (Xu *et al.*, 2015, p. 1256).

A informação sempre foi importante para as transações mercantis (dados relativos aos preços, principalmente). Sempre foi vital para a governança estratégica das empresas e das economias nacionais, e essa dimensão da gestão de dados já é bem compreendida e consolidada. Entretanto, na economia orientada por dados, ela ascende à categoria da valorização e da monetização dos próprios dados – o que faz com que estes deixem de ser um elemento auxiliar nos negócios, tornando-se uma grande plataforma em que a negociação de dados pessoais (conexões, opiniões. preferências e padrões de consumo) tem valor em si mesmo (Mayer-Schonberger; Cukier, 2013, p. 82-83). E a competição das grandes empresas nada mais é que uma competição pela capacidade de despossessão dos usuários, ou seja, pela potência de seus algoritmos usados para extrair dados cada vez mais valiosos (Zuboff, 2019, p. 155).

Essa mercantilização dos dados permite o surgimento de uma nova indústria, em que corretores de dados ("*data brokers*") operam obtendo informações de usuários e as negociam conforme os interesses das corporações, tanto ao adquirirem dados coletados por empresas e governos quanto ao coletarem por si próprios e organizarem informações públicas a respeito de pessoas ou grupos. Essa função revela a assimetria do controle dos dados, justamente porque a capacidade de proteger a privacidade depende da capacidade técnica e econômica de geri-los e interpretá-los. O conjunto dessas informações úteis e valiosas constitui, assim, mercadoria traduzida nos dados na economia digital (Crain, 2018, p. 90-91).

A economia orientada por dados também possui uma efetiva transformação em campos pessoais como a capacitação para o trabalho e o conhecimento, devido ao processo de "industrialização do aprendizado" efetivado na ascensão das inteligências artificiais em detrimento ao trabalho humano (Ciuriak, 2018, p. 13). Com isso, máquinas capazes de aprenderem a executar tarefas cotidianas e cada vez mais complexas tendem a mudar a organização do trabalho – assim, mesmo que não sejam responsável pelo fim do trabalho humano, tal forma de industrialização tende a expor uma nova divisão de tarefas – em que máquinas serão responsáveis pelas ativi-

dades mais longas e repetidas, enquanto os humanos somente executarão tarefas altamente especializadas[5].

A capacidade assimétrica de lidar com os dados, a industrialização do aprendizado por quem possui as tecnologias de inteligências artificial e a possibilidade de mercantilizar os dados marcam uma tendência estrutural de concentração de mercados na economia orientada por dados, em que as escalas da economia mundial e das redes interligadas mundialmente sugerem a expansão dos lucros e incentivam o comportamento estratégico (Ciuriak, 2018, p. 14). A intensidade da expansão lucrativa desse capitalismo baseado em dados é demonstrado pelo sucesso sem precedentes das *big techs* – caminhando das operações econômicas até novos territórios da experiência humana, nas quais a intervenção sobre os comportamentos significa também a nova fronteira dos lucros (Zuboff, 2019, p. 176).

Do ponto de vista da economia política, Zuboff (2019, p. 222-244), ao acreditar que essa economia resulta em um "capitalismo de vigilância", compreende os mecanismos de extração de dados como instrumentos que trabalham e manipulam os comportamentos dos usuários em prol de um mercado de futuros, no qual dados preditivos capazes de moldarem comportamentos são ativos essenciais. Ou seja, mais do que informações completas acerca do comportamento dos usuários, sofrem um tratamento intenso e em tempo real de dados que importa no direcionamento de comportamentos e regula incentivos, principalmente aqueles relacionados ao consumo. Ainda, é um mecanismo considerado injusto, tendo em vista que ocorre a rendição dos dados do usuário em troca de melhorias nas aplicações, mas sendo ocultado um processo de valorização desses dados no qual os usuários são expropriados.

Essa tendência de concentração pode vir a causar a extinção de iniciativas menores, resultando numa "competição" dentro de um núcleo monopolista global realizada entre gigantes como Apple, Alphabet (Google), Microsoft, Amazon e Facebook. Todavia, o desafio da regulação antitruste tem sido relacionado ao comprometimento com o desenvolvimento tecnológico, diretamente relacionado a essas grandes empresas. Por isso, a tomada de decisão de proteção jurídica enfrenta a escolha entre garantir a com-

5 Conforme Fava (2018), há uma intrínseca relação entre educação, trabalho e as inteligências artificiais. Por isso, é preciso atentar e monitorar a adesão às tecnologias, porquanto é preciso evitar o fetiche pela tecnologia ao mesmo tempo que a tecnofobia.

petitividade[6] e não impor óbices à inovação tecnológica (Nuccio; Guerzoni, 2019, p. 12).

A economia orientada por dados revela um novo paradigma regulatório, tendo em vista a necessidade de dar atenção a riscos sistêmicos, como os atinentes à privacidade dos dados pessoais, à manipulação política/eleitoral e à (in)segurança digital. No ínterim dessa verdadeira revolução digital da economia orientada por dados, a qual acarreta mudanças na vida e no mundo cada vez mais notáveis, é preciso responder às questões democráticas e tomar decisões contextualmente corretas. A programação do trabalho e da economia não pode fazer com que a sociedade se torne apenas um emaranhado de "cidadãos" programados aguardando catástrofes pré-programadas. As tecnologias manipulativas são capazes de influenciar a liberdade de escolha, mesmo que sejam perfeitamente eficientes para a economia – por isso, é necessário elaborar regulações que contemplem a autonomia privada, ao mesmo tempo que estejam conscientes da assimetria entre cidadãos e as inteligências artificiais de grandes empresas no que tange à manipulação de dados (Helbing *et al.*, 2018, p. 77-80).

Assim, o *big data*, referência dessa nova economia, precisa ser regulado para que a sociedade não seja regulada por ele (Mayer-Schonberg; Cukier, 2013, p. 138-141). É necessário conceber uma normatividade que governe a expansão no âmbito da informação e da circulação de dados, considerando que a sua massividade já está transformando os cotidianos individuais sobremaneira. Mudanças legislativas pontuais não vão abarcar essas mudanças e mitigar os danos causados pelo lado negativo do *big data* – como a violação da privacidade –, tornando-se imperativo desenvolver novos agentes e instituições, capazes de interpretar e analisar esses algoritmos complexos em prol dos vulneráveis à economia digital.

Nesse cenário, o intuito legislativo de criar um marco jurídico de proteção de dados deveria vir na insurgência de uma cidadania digital que exige a concretização do direito fundamental à privacidade, por meio da autodeterminação informativa e da proteção da dignidade da pessoa humana (Mendes; Doneda, 2016, p. 36), a qual necessita atender as necessidades acarretadas: i) pela competitividade econômica/inovação cônscias da realidade da economia orientada por dados; e ii) pela vulnerabilidade dos

6 Também, tendo em vista a estrutura da economia digital, a ausência de competitividade não é vista como problema porque não reflete necessariamente em impacto de preço aos consumidores – não levando em conta outros aspectos negativos dessas concentrações de mercados (Zanatta; Abramovay, 2019, p. 433).

cidadãos/consumidores frente à também tão real desigualdade da apropriação e gestão dos dados.

Os princípios da LGPD atentam para a necessidade do desenvolvimento econômico, inovação tecnológica e da livre iniciativa/concorrência (art. 2º, V, VI). A realidade da economia orientada por dados é da importância da gestão e da análise de dados como ativos e peças-chave nos mercados. Essa face da lei traz a necessidade de o Brasil ser economicamente competitivo quanto aos dados, pois a natureza regulatória desses dispositivos pode trazer uma cultura de proteção de dados para as organizações que agregam fatores importantes, como reputação e confiança (Bioni, 2019, p. 32-33).

Quanto aos consumidores, a LGPD aponta para a importância do consentimento como hipótese em que os dados pessoais podem ser tratados, sendo que a lei o define, no seu art. 5º, XII, como "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada". E seu art. 7º, I, afirma a obrigatoriedade do consentimento do titular dos dados pessoais para o seu tratamento. Ou seja, há um ato exigido do consumidor, em razão do qual este fornecerá suas informações às empresas que praticam a gestão de dados. Ainda, para os dados que a legislação considera "pessoais sensíveis"[7], no art. 11, o fornecimento de consentimento do titular precisa destacar as formas e finalidades específicas e destacadas para seu uso.

A noção de consentimento como defesa de direitos privados não foi utilizada pela primeira vez na LGPD, mas sim no Marco Civil da Internet (Lei nº 12.965/2014), tendo já naquela oportunidade constituído um dos pilares de segurança conferidos aos usuários da internet, marcados pela ligação entre acesso à rede e exercício da cidadania[8]. Naquela lei já estava consolidado o conteúdo do termo "consentimento expresso e inequívoco" – que consiste na obrigação dos provedores de aplicativos ou *sites* em facultar ao usuário o consentimento para transferência a terceiros de seus dados pessoais. É preciso, assim, que o provedor disponibilize canais que exponham

7 A definição legal do art. 5º, II, da LGPD é "dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural".

8 No art. 7º, VII, a lei proíbe o fornecimento de dados pessoais a terceiros, salvo mediante consentimento; no art. 7º, IX, aponta a necessidade de consentimento expressos em caso de contratos que tratem de coleta, uso, armazenamento e tratamento de dados pessoais; o art. 16, I, define que é vedada a guarda de registros de acesso em aplicativos, sem consentimento; também, no art. 16, II, que é vedada a guarda de dados para fins alheios ao consentimento do titular (Brasil, 2014).

a clara e esclarecida pergunta sobre consentimento e a possibilidade de sua futura revogação por parte do titular das informações coletadas (Oliveira, 2014, p. 6-7).

Todavia, ao analisar esse percurso legislativo do consentimento, como fez Bioni (2019b, p. 345) ao apontar a ambivalência na visão do cidadão protagonista do consentimento, aprofunda-se a noção de consentimento para o Direito. A primeira visão é puramente normativa, pois apregoa a importância da capacidade do cidadão em controlar seus dados; já uma segunda perspectiva indica uma (hiper)vulnerabilidade que precisa ser protegida, pois a intensidade informacional é capaz de dirigir comportamentos – principalmente em relação ao consumidor. Portanto, há uma dualidade na proteção aos dados, que se trata da importância da autonomia privada e da proteção da dignidade da pessoa humana num contexto em que a proteção da privacidade precisa ultrapassar a esfera contratual.

A leitura da LGPD à luz da Constituição Federal de 1988 permite enxergar o valor da privacidade como direito fundamental, disposto no art. 5º, X e XII, da Carta Magna. Portanto, há uma garantia da privacidade que impõe ao Estado agir em defesa dela, orientando o conteúdo das leis privadas, devendo estar as normas contratuais vinculadas a esses direitos fundamentais em seu conteúdo. Esse processo de constitucionalização do direito privado sugere desdobramentos do direito à privacidade também como o "direito ao esquecimento", o qual aponta para a necessidade de intervenção pela defesa da privacidade em nome da dignidade da pessoa humana (Souza, 2019, p. 12-13).

A preocupação com possíveis abusos promovidos por plataformas de mídias sociais deve constituir um panorama de proteção aos dados considerando a dignidade da pessoa humana e a possibilidade de autodeterminação informativa, cujo objetivo deve ser o empoderamento do usuário/titular de dados como gestor de seus dados pessoais, que deve ser capaz de incluir, controlar ou excluir seus dados de bases digitais. Portanto, sugerem-se formas regulatórios complementares às vedações legais, mas que promovam a cidadania digital ativa (Bioni, 2019b, p. 66).

A proteção jurídica dos dados pessoais indica a importância do consentimento, mas também que se deve ir para muito além de tal exigência. Torna-se preciso, assim, contemplar a liberdade e a autonomia privada como princípios. Entretanto, a realidade desigual da gestão de dados revela a assimetria de infraestrutura e a interpretação das informações massivas. Na era do *big data*, o papel central do indivíduos na formação de leis ati-

nentes ao direito privado é colocado em xeque, justamente pela dificuldade (ou impossibilidade) de se obter consentimento informado sobre algo que os usuários sequer sabem como funciona – principalmente porque essas análises são feitas por inteligências artificiais inexplicáveis, opacas (Mayer-Schonberger; Cukier, 2013, p. 124-128).

Dessa forma, a LGPD instaura uma nova perspectiva da proteção de dados ainda em movimento, que possibilita uma articulação maior em nome dos direitos da personalidade e do exercício de direitos fundamentais. A manipulação dos dados digitais, que se tornaram um significativo ativo de mercado, deve estar compreendida nessa estrutura jurídica de proteção da LGPD, ao mesmo tempo em que é lida com as lentes dos princípios constitucionais e firma caminho para a efetividade, também, do Código de Defesa do Consumidor (Miragem, 2019, p. 27-28). Trata-se esse do cenário pretendido pela LGPD, em construir uma mudança na cultura regulatório em prol de uma interpretação e aplicação sistemática da proteção aos dados atenta ao desenvolvimento tecnológico (Doneda; Mendes, 2019, p. 322).

2 URBANISMO ORIENTADO POR DADOS E A PROTEÇÃO AOS DADOS NAS PLATAFORMAS DE MOBILIDADE URBANA

O contexto da sociedade informacional ganhou destaque nas teorias do planejamento urbano ao orientar o que se chama de cidades inteligentes (*smart cities*), servindo às empresas e aos governos que descrevem cidades a partir do crescimento dos usos das tecnologias da informação e comunicação (TICs) na natureza, na estrutura e na vida urbanas. E com a ascensão do *big data* como novo paradigma informacional, os dados gerados pelo comportamento geral de cada indivíduo e comunidades no viver urbano ultrapassam o papel de informar a Administração Pública, e passando a orientar a cidade em tempo real (Kitchin, 2014, p. 3).

A economia orientada por dados encontra uma derivação no planejamento urbano, que é o urbanismo orientado por dados (*data driven urbanism*). Embora não seja novidade que a informação e os dados tenham guiado o entendimento da vida urbana e a formação das políticas públicas, ocorre atualmente uma transformação desse urbanismo informado pelos dados: até há pouco tempo, utilizados como apoio para as tomadas de decisão; agora, base e orientação do urbanismo, sendo conectados em redes operacionais de governança via plataformas. Em outras palavras, trata-se da instrumentalização autônoma dos dados digitais na infraestrutura e nas práticas das cidades (Kitchin, 2015, p. 2).

Tal e qual a reorganização proporcionada pela economia, o urbanismo orientado por dados supera os limites do *small data*, que representavam a coleta e análise de dados por meio de métodos agora obsoletos – como as enquetes, grupos focais e entrevistas, insuficientes pela periodicidade infrequente, imprecisão, incompletude, subjetividade e vieses nos resultados. Também, na limitação temporal e local que os dados menores proporcionaram, dando largo espaço para a discricionariedade, tendo agora a possibilidade de reconstruir a definição dos problemas urbanos a partir de uma massiva gama de informações (Bibri, 2019, p. 269).

O urbanismo orientado por dados traz à tona a proliferação de infraestruturas computacionais nos ambientes urbanos e a possibilidade de novas formas de interação entre as comunidades e as pessoas. Nas mais recentes "cidades inteligentes", esse urbanismo experimental tem funcionado na combinação de infraestruturas em rede com o desenvolvimento estratégico (empresarial), em plataformas que produzem a cidade em tempo real, aliadas à ubiquidade da computação na vida cotidiana – em uma nova concentração de agentes produtores do espaço urbano contemplando uma governança urbana de plataformas digitais (Coletta; Heaphy; Perng; Waller, 2017, p. 15).

Essa expansão dos agentes de produção da cidade na era do *big data* representa a maior gama de intérpretes em tempo real dos dados, que incluem, segundo lista de Kitchin (2016, p. 2): a) empresas de serviços públicos – que utilizam dados sobre o uso de eletricidade, gás e água; b) provedores de transporte/mobilidade – que identificam a localização/movimentação e os destinos dos usuários; c) operadoras de internet e telefonia – que, assim como as empresas de internet e telefonia, fornecem a localização dos usuários, dados acerca do uso de aplicativos e demais metadados comportamentais dos seus usuários; d) *sites* e aplicativos de viagem – auxiliando na catalogação dos padrões de consumo e interesses gerais dos usuários; e) mídias sociais – registrando e classificando perfis a partir de opiniões, fotos, informações pessoais gerais e localização; f) Administração Pública – serviços públicos e audiências públicas; g) instituições financeiras – também auxiliando na construção de perfis de consumo e na localização dos seus clientes; h) empresas de segurança – localização e comportamento; i) serviços de emergência – segurança, criminalidade e policiamento; j) aparelhos domésticos conectados à internet – comportamento e padrões de consumo.

Essas informações sempre foram produzidas nesses campos de atuação; entretanto, com a ascensão das tecnologias da informação, tornaram-se

muito mais frequentes e, principalmente, passaram a ter valor econômico próprio – o fenômeno da mercantilização dos dados pessoais característico da economia orientada por dados. Por isso, o *big data* representa para o urbanismo também a transformação da informação para a era em que ela é determinante nos processos de produção da cidade. Um grande campo de atuação para o urbanismo orientado por dados é o da mobilidade urbana, tendo em vista a produção em tempo real das trajetórias espaço-temporais das pessoas nas cidades.

Os dados para a mobilidade servem de fundamento para uma alta gama de aplicações que são fundamentais para o desenvolvimento de protocolos de análise e implementação de sistemas urbanos de mobilidade, contemplando massivas informações quantidades e qualitativas – capazes de realizar experimentos de simulação que conseguem descrever um modelo de dia na cidade[9]. A cidade passa ser um grande campo de tratamento de dados, em que os hábitos diários das pessoas podem fornecer um grande campo de experimentação para o desenvolvimento dos sistemas de mobilidade urbana. A implementação desses sistemas passa pela programação de protocolos e aplicações móveis capazes de interpretar dados de grandes redes de automóveis, celulares e outros componentes (como os passes de ônibus inteligentes)[10]; de explorar as correlações e divergências dessas diversas fontes de dados e de promover a eficiência da mobilidade (medida pelo fator tempo, principalmente)[11].

A mobilidade urbana dirigida por dados indica um uso intensivo das informações e das tecnologias para coleta e tratamento dessas informações que a cidade produz a todo o tempo por meio de sensores (câmeras de vigilância instaladas nas ruas, por exemplo) e outras fontes de dados (mormente aquelas geradas de forma pessoal em plataformas digitais). Constituem o núcleo desse pensamento urbanista o poder dos dados e a conectividade em rede da vida na sociedade informacional, e tal urbanismo pode influenciar a gestão urbana do tráfego de automóveis, do estacionamento, do passeio público, do transporte público (Akerkar, 2019, p. 106) – ou seja, pode passar

9 Como descreve, por exemplo, a pesquisa de Pappalardo e Simini (2017, p. 805) ao estudar a trajetória do GPS de celulares sob um modelo matemático criado para contemplar as variedades de trajetórias e identificar padrões.

10 A ferramenta do *smart card* tem sido um objeto de análise dos dados de mobilidade, por conseguir apontar dados de trajetórias em tempo real que as inteligências artificiais podem interpretar para reordenar a disponibilidade do transporte público em tempo real (Mahrsi; Côme; Oukhellou; Verleysen, 2017, p. 712).

11 Um exemplo é a pesquisa chinesa sobre a aplicação *"mPat"*, que contempla os dados do sistema urbano da cidade de *Shenzen*, que indicou uma aplicabilidade em tempo real reduzindo o tempo de viagem dos cidadãos em 36% (Zhang et al., 2018, p. 671).

a determinar o sistema de mobilidade urbana, orientando o planejamento urbano com os modelos e algoritmos gerados, não mais sendo utilizados os dados somente para informar a gestão pública.

A mobilidade urbana pode ser verificada por sensos ubíquos e em tempo real, como, por exemplo, na observação dos telefones celulares, que é capaz de estimular a densidade das aglomerações urbanas, as diferentes atividades em diversas partes da cidade, os padrões de mobilidade, detectar eventos e analisar a geografia das redes sociais (divisão regional e comunicações inter-regionais) (Calabrese; Ferrari; Blondel, 2014, p. 14). Entretanto, o desafio para esse urbanismo informacional orientado por dados é conceber máquinas inteligentes que consigam administrar a mobilidade e torná-la mais eficiente lendo e processando o máximo de dados possíveis.

Entretanto, essa ubiquidade da computação e dos dados (tanto da produção pessoal deles como da análise e tratamento) traz consigo dilemas éticos para as cidades inteligentes e implicam reflexões para sua regulação. Essas questões são apresentadas por Kitchin (2016, p. 5-11) por meio de dois temas: i) a "datificação" da vida urbana e a privacidade e ii) o uso, a distribuição e o reaproveitamento dos dados.

A privacidade reconhecida como direito corresponde a diversas formas inter-relacionadas, sendo as mais significativas as privacidades de identidade, do corpo, territorial, de localização e mobilidade, da comunicação e das transações econômicas. Portanto, sua proteção no contexto das cidades inteligentes perpassa o reconhecimento das dificuldades trazidas pela datificação e pela vigilância pelos dados – em que a ubíqua mediação digital dos principais aspectos da vida urbana exige cada vez mais formas específicas e diversas de identificação de subjetividades humanas para serem usadas plataformas digitais. Assim, a razão tecnocrática que sustenta o urbanismo orientado por dados conforma um discurso político que se choca com valores democráticos ao sustentar que sistemas automatizados podem planejar a cidade atuando como vigilantes em detrimento da privacidade e da liberdade pessoais (Tironi Rodó, 2019, p. 24-28).

A possível inferência e a previsibilidade de comportamentos ou identidades pelo tratamento de dados em tempo real podem revelar ou prever informações que são consideradas sensíveis ou pessoais em razão da ubíqua e incessante coleta e análise de dados. Em outras palavras, quando as inteligências artificiais demonstram serviço eficiente ao categorizarem um indivíduo em determinado grupo ou padrão de comportamento, violam a

privacidade de informação sensível, e, quando erram, podem provocar a estigmatização e o julgamento baseado nessa antecipação[12].

Além disso, a *big data* urbana torna impossível a anonimização ou a reidentificação – já que o imenso controle sobre os dados e a massiva produção pessoal deles vincula cada indivíduo ao perfil identificável a partir de seus dados tratados; e não possuir qualquer identidade digital (ou ainda, tentar alterar o perfil que foi construído a partir de seus dados) é algo independente da vontade individual. Esse problema se traduz, assim, na ofuscação e no controle reduzido das pessoas sobre seus próprios dados pessoais e sensíveis, e a circulação dos dados entre plataformas e algoritmos faz ser impossível identificar como se organizam os próprios dados.

Ainda, e fundamentalmente, o consenso torna-se algo vazio, ou até mesmo inexistente. A expansão das tecnologias nas cidades inteligentes promove uma ubiquidade dos dados que torna o consentimento um ato meramente formal, já que o dia a dia urbano está tomado por formas tecnológicas que produzem dados e governam vivências mediante o uso de algoritmos. A mobilidade urbana produz dados para todos que circulam pela cidade e orientam diretamente os serviços públicos e privados de transporte, o controle do tráfego e a locomoção das pessoas em geral, passando o cidadão a significar nada mais do que um usuário de plataformas de serviços.

A proteção jurídica dos dados e, consequentemente, da privacidade precisa atentar para esses fenômenos para sua efetiva regulação. A LGPD indica uma aplicação calcada na observância do direito fundamental à privacidade, primeiramente ao apontar a diferença entre dado pessoal e dado pessoal sensível (art. 5º, I e II), concebendo a indisponibilidade da privacidade nos dados sensíveis de uma pessoa natural – obrigando o Estado de Direito a protegê-la, restando ao consentimento somente a autorização para finalidades específicas e destacadas (art. 11, I) que devem ser fiscalizadas.

Essa diferença é importante para garantir o direito de titularidade da pessoa natural sobre seus próprios dados, afirmada na LGPD (art. 17), pois a responsabilidade sobre os dados no marco normativo brasileiro supera a visão contratualista, tratando o consentimento obrigatório, mas não absoluto e garantidor da liberdade plena dos controladores e operadores de dados. Conforme a leitura de Bioni (2019b, p. 291- 292), essa tendência é de con-

12 O exemplo prático utilizado por Kitchin (2016, p. 8) é de que a plataforma, ao rastrear dados de alguém que frequenta regularmente um estabelecimento considerado "LGBTI", passa a considerar por inferência que essa pessoa é LGBTI.

sideração substancial do consentimento e se consubstancia na necessidade de tratar a proteção de dados para além desse ato da autonomia privada.

Um método de aplicação contextual do consentimento na LGPD identificado sistematicamente por Bioni (2019b, p. 324-327) é de verificação (teste) da proporcionalidade do legítimo interesse de quem trata os dados, tendo em vista que balanceia os interesses do titular dos dados com os controladores/operadores. Primeiramente i) verifica-se a legitimidade do interesse na situação concreta e finalidade legítima; logo após, a ii) necessidade – utilização mínima dos dados, somente o necessário para a finalidade expressa; em seguida, o iii) balanceamento – observância das expectativas do titular e dos direitos e liberdades fundamentais; e, em sequência, observando-se iv) salvaguardas – o dever de transparência, a observância dos mecanismo de oposição (o direito do titular dos dados de retirar seus consentimento) e a mitigação de riscos do titular.

Dessa forma, aplicando-se esse modelo de verificação da legitimidade, o ato de consentimento em aplicativos de mobilidade urbana resta esvaziado frente à dinâmica da locomoção das cidades, pois todo movimento é registrado e processado, quedando-se a vida cotidiana submetida ao processamento por algoritmos. Por isso, é preciso proteger o cidadão do abuso na gestão dos dados em razão da assimetria do seu poder em relação àqueles que tratam os seus dados (Estados, empresas etc.). A finalidade legítima que o planejamento da mobilidade urbana sustenta ao ser orientada por dados não pode ser, portanto, considerada um "cheque em branco" em prol da concessão de todas as informações relativas à locomoção urbana.

A utilização de aplicativos de transporte privado (como o Uber) e os aplicativos de localização (como o Google Maps e o Waze) não possuem maneiras de contemplar essa forma jurídica de consentimento justamente pela quantidade massiva de dados em tempo real que os suportam. O consentimento formal dos termos de aceite de uso não tem substância ou conteúdo de consentimento, pois suas finalidades não claras – jamais conseguindo comprovar necessidade –, até mesmo pelo contexto exposto do tratamento de dados sob o *big data*, em que sequer é possível identificar o papel dos dados produzidos por um só cidadão dentro do dinâmico e em constante aprendizado mundo das inteligências artificiais.

A proteção ao titular dos dados e a necessidade de exigência de substância no consentimento de concessão de informações nos meios digitais é fruto dos dilemas éticos trazidos pelas práticas de *big data*, em que a privacidade e a liberdade requerem novas e eficazes formas de regulação.

Ainda, existem os dilemas relativos ao uso, à circulação e à distribuição de dados relativos ao processo de mercantilização dos dados pessoais, em que o conjunto de informações produzidas no dia a dia possui valor em si e é alvo de negócios que constituem um mercado de dados pessoais digitais (Kitchin, 2016, p. 10).

A prática mercantil de coordenar e reorganizar dados para venda – assim criando produtos derivados da produção de dados original – é uma prática comum no mercado, surgindo a figura do corretor de dados (*data broker*), que não tem na LGPD seu papel consagrado: a lei determina como agentes de tratamento de dados, apenas, as figuras do controlador e do operador, sendo o primeiro há quem pertencem os dados e o segundo aquele que apenas opera em nome do primeiro[13]. É possível apontar, portanto, um vazio regulatório na função de quem intermedeia o negócio dos dados, que é uma realidade de mercado.

A transferência de dados é tratada na LGPD como i) "uso compartilhado de dados"[14] e ii) "transferência internacional de dados"[15]. O primeiro se refere ao termo geral que representa qualquer prática em que os dados não sirvam à primeira ordem pela qual foram coletados, como a transmissão entre empresas dos dados dos consumidores – para a qual a LGPD exige consentimento, legítimo interesse e finalidade do uso dos dados. Já quanto aos dados administrados pelo Poder Público, é vedado transferi-los a entidades privadas, a menos que sejam publicamente acessíveis ou para a execução de serviços públicos (arts. 7º, III, e 26).

O uso compartilhado de dados entre entidades privadas é reconhecido como prática de mercado ao se identificar que se trata de direito do titular de dados obter informações acerca do uso compartilhado por meio do controlador que cedeu os dados (art. 9º, V); e, na hipótese de mudança de finalidade incompatível com o consentimento original, o titular pode requerer ao controlador original que retire todos os seus dados em circulação, contatando as outras operadoras (art. 18, § 6º). Ainda, é vedado o uso

13 O art. 5º da LGPD define: "VI – controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referente ao tratamento de dados pessoais; VII – operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador".

14 Definido pelo art. 5º, XVI, da LGPD como "comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados; [...]".

15 Definido pelo art. 5º, XV, como "transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro".

compartilhado de dados sensíveis à saúde quando envolvido o objetivo de obter vantagem econômica (art. 11, § 4º).

A transferência internacional de dados é regulada pela LGPD ao se permitir a transferência para países ou organismo internacionais que tenham um grau de proteção com conteúdo adequado ao da própria lei (art. 33, I)[16] e entre controladores que consigam garantir o cumprimento dos princípios da proteção estipulada na lei – por meio de cláusulas que determinam finalidade específica, normas corporativas globais e selos ou certificados de garantia reconhecidos (art. 33, II e III). Portanto, há uma política de cooperação entre nações que buscam se assemelhar nas leis locais, enquanto que as práticas das corporações transnacionais reconhece a normatividade das ordens não estatais e os *compliances* corporativos.

Entretanto, esse tratamento contratual da proteção dos dados não contempla a cotidianidade das plataformas de mobilidade urbana no contexto do *big data*, pois a produção e tratamento de dados se dá em tempo real – principalmente devido à ubiquidade da geolocalização –, sendo o *machine learning* instantâneo e refletido imediatamente noutras decisões tomadas pelas inteligências artificiais que atuam na governança urbana orientada por dados. Não há um momento destacado em que as plataformas internacionalizam ou compartilham os dados, e, dentro do contexto explicado da economia dirigida por dados, essas informações já compõem, constroem e transformam algoritmos que controlam a cidade. A dinâmica intensa da mobilidade urbana não permite rastrear os próprios dados pessoais – e esse é o fundamento do paradigma chamado *big data*.

A vigilância pelos dados (*dataveillance*) por meio dos dados de geolocalização – que permitem identificar onde o usuário está, para onde foi e quanto tempo demorou pra chegar – é a preocupação mais candente na proteção aos dados nas plataformas de mobilidade urbana, pois seu fluxo intenso em tempo real e comparável com todos os outros usuários pelas inteligências artificiais tem dinâmica cotidiana e não parece ser invasivo à primeira vista, justamente porque a funcionalidade de um algoritmo urbano eficiente depende de dados massivos, o que pressupõe um uso comparti-

16 Esse nível de adequação é medido pelo disposto no art. 34 da LGPD: "O nível de proteção de dados do país estrangeiro ou do organismo internacional mencionado no inciso I do *caput* do art. 33 desta lei será avaliado pela autoridade nacional, que levará em consideração: I – as normas gerais e setoriais da legislação em vigor no país de destino ou no organismo internacional; II – a natureza dos dados; III – a observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares previstos nesta lei; IV – a adoção de medidas de segurança previstas em regulamento; V – a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais; e VI – outras circunstâncias específicas relativas à transferência".

lhado instantâneo e internacional. Sendo os dados pessoais, sensíveis ou não, incorporados ao aprendizado artificial que constitui as plataformas de governança urbana, tem-se que, mesmo sem o consentimento do usuário, seus dados já serviram para o treinamento instantâneo das inteligências artificiais.

Ademais, esses mecanismos de proteção de dados se mostram insuficientes para coibir a violação da privacidade e do abuso na gestão de dados pelos controladores e operadores frente à realidade que é a economia orientada por dados, inserida no fenômeno da globalização, do surgimento de novos agentes não estatais e da expansão da tecnologia da informação (Menezes Neto; Morais; Bezerra, 2017, p. 196). O desafio da regulação nesse contexto passa pela verificação de novas responsabilidades que transpassam o Estado-Nação e reconhecem a transnormatividade exercida por esses agentes não estatais na gestão do *big data*.

Como aplicação possível, há o disposto no art. 11, § 3º, da LGPD, segundo o qual a autoridade nacional de proteção de dados pode vedar a utilização compartilhada de dados pessoais sensíveis em casos cujo objetivo seja obter vantagem financeira e a prática venha a ferir direitos fundamentais. Todavia, a aplicabilidade desse dispositivo depende do estabelecimento de estruturas de proteção jurídica e política, que só poderão ser verificadas quando for possível empiricamente. Isso é mais do que parece afirmar o "espírito" da LGPD, mas, como apontaram Doneda e Mendes (2019, p. 322), isso pode corresponder ao papel que a LGPD pode assumir, de instigar uma cultura jurídica, social e política de proteção de dados, ao reconhecer a economia e o urbanismo orientado por dados e seus agentes.

CONCLUSÃO

A atualidade da sociedade informacional aponta para uma economia orientada por dados, em que o paradigma do *big data* ascende ao marco do tratamento de dados, pois o papel deles não é mais apenas de informar as decisões. Assim, em razão da massividade do volume de dados e da velocidade do seu tratamento, em tempo real, as decisões passam a ser tomadas pelas máquinas que aprendem a partir deles, e essas inteligências artificiais passam a orientar processos econômicos, sendo os dados pessoais transformados não mais apenas em suporte, mas também em ativos econômicos significativos no mercado.

Esse fenômeno tem por consequência o desenvolvimento de uma forma derivada de urbanismo, também orientado por dados, em que as plata-

formas constituem o viver urbano devido à sua ubiquidade e à constante cessão de dados pelos usuários – já que cada vez mais a cidade se relaciona socialmente mediante serviços disponíveis, ou não, aos usuários. No âmbito da mobilidade urbana, em específico, as plataformas se utilizam a todo momento das referências de geolocalização das pessoas, forjando em tempo real as decisões sobre o tráfego de veículos e sobre o deslocamento das pessoas.

Por isso, o desafio de aplicação de instrumentos jurídicos de proteção de dados é conseguir obliterar o rastreamento dos dados pessoais de cada usuário frente à veloz e gigantesca rede de informações geradas e interpretadas em tempo real. Nesse sentido, ao mesmo tempo que os dados são gerados, já incorporam o contexto dos próximos dados que virão a ser tratados (pois as tecnologias usadas para tal são sensíveis ao contexto). Não há maneira de identificar para onde os dados vão e no que se transformam, exatamente, assim.

A LGPD estipula o conceito de consentimento como fundamental para a o uso e transferência dos dados pelos controladores e operadores. É um direito do titular, portanto, mas a mesma lei reconhece que, no caso dos dados sensíveis, é preciso destacar a finalidade específica para o uso dos dados, sendo obrigatória a constante informação. Portanto, no marco da LGPD, o consentimento depende de legítimo interesse de quem irá utilizar esses dados – ou seja, foge-se da noção de um consentimento meramente formal, exigindo-se dele substância.

Pensar a aplicabilidade do consentimento de fato utilizando o teste de proporcionalidade do legítimo interesse no caso da mobilidade urbana permite antecipar a ilegalidade das plataformas de mobilidade orientadas por dados, justamente porque os administradores destas, no atual *status quo*, não conseguem comprovar o legítimo interesse e a necessidade dos dados que obtêm, já que a vigilância de dados é constante e a referência da geolocalização é ubíqua. E as inteligências artificiais que tomam decisões nas plataformas interagem com todos os dados, independentemente do consentimento, que acaba servindo apenas para evitar a divulgação de dados relativos à localização ou à locomoção, mas não de sua utilização.

As plataformas precisam e sabem da localização de todos os dispositivos, e consequentemente de seus usuários, determinando, assim, os processos de ocupação dos espaços ao administrar a mobilidade em tempo real. Ao angariar padrões pessoais e de grupo, os algoritmos permitem inferências para as plataformas efetivarem seus objetivos de eficiência da

mobilidade urbana: por isso, o tratamento de dados em tempo real é um constante e indetectável movimento de transformação de algoritmos e modelos, tornando impossível perceber o papel de cada usuário na geração de novos dados.

Ainda, a LGPD pressupõe uma cooperação jurídica baseada numa tendência mundial de proteção de dados por parte dos Estados e pelas grandes corporações, segundo a qual a transferência de dados entre controladores só pode ser exercida em relações jurídicas que sejam adequadas ao paradigma de proteção do Brasil e possam garantir os direitos fundamentais relativos aos dados. Entretanto, tal e qual ocorre em relação à dificuldade imposta ao consentimento, determinar as transações internacionais de dados é algo impossível frente à realidade da *data science*, em que os dados, ao mesmo tempo em que são informados, já passam a compor modelos e algoritmos aplicados no mundo todo.

Dessa forma, a cultura de proteção de dados promete ser o principal legado da LGPD, influenciando as organizações, no sentido de lhes obrigar sistemas protetivos confiáveis e protetores de sua competitividade, pois o cenário do *big data* invoca desafios à regulação que observe direitos fundamentais que fogem do Estado e pressupõe formas de normatividade que contemplem a realidade econômica, social e política da sociedade orientada por dados. A dinâmica complexa da mobilidade urbana e a massividade de dados produzida por ela indica essa dificuldade para a regulação atender aos que só as inteligências artificiais conseguem.

REFERÊNCIAS

AKERKAR, Rajendra. Privacy and security in data-driven urban mobility. In: DAMONT, J.; LOUDCHER, S. (Org.). *Utilizing big data paradigms for business intelligence*. Hershey, PA: IGI Global, p. 106-128, 2019.

BIBRI, Simon Elias. The unfolding and soaring data deluge for transforming smart sustainable urbanism: data-driven urban studies and analytics. In: BIBRI, Simon Elias (Org.). *Big data science and analytics for smart sustainable urbanism*. Springer, Cham, p. 253-272, 2019.

BIONI, Bruno Ricardo. Inovar pela Lei. *Gv/Executivo*, v. 18, n. 4, jul./ago. 2019. Disponível em: <http://bibliotecadigital.fgv.br/ojs/index.php/gvexecutivo/article/download/79978/76432>. Acesso em: 14 set. 2019.

_____. *Proteção de dados pessoais*: a função e os limites do consentimento. São Paulo: Forense, 2019b.

CALABRESE, Francesco; FERRARI, Laura; BLONDEL, Vincent D. Urban sensing using mobile phone network data: a survey of research. *ACM Computing Surveys (CSUR)*, v. 47, n. 2, p. 1-25, 2015.

CHEN, Yen-Kuang. Challenges and opportunities of internet of things. In: *17th Asia and South Pacific design automation conference*, IEEE, p. 383-388, 2012.

CIURIAK, Dan. The economics of data: implications for the data-driven economy. In: *Data Governance in the digital age*: special report. Canada: Centre for International Governance Innovation, p. 12-19, 2018.

COLETTA, Claudio; HEAPHY, Liam; PERNG, Sung-Yueh; WALLER, Laurie. Data-driven cities? Digital urbanism and its proxies: Introduction. *Tecnoscienza*, v. 8, n. 2, p. 5-18, 2017.

CRAIN, Matthew. The limits of transparency: Data brokers and commodification. *New Media & Society*, v. 20, n. 1, p. 88-104, 2018.

CUKIER, Kenneth; MAYER-SCHOENBERGER, Viktor. The rise of big data: How it's changing the way we think about the world. *Foreign Affairs*, v. 92, p. 28, 2013.

DONEDA, Danilo; MENDES, Laura Schertel. Um perfil da nova Lei Geral de Proteção de Dados brasileira. In: BELLI, Luca; CAVALLI, Olga. *Governo e regulações da internet na América Latina*: análise sobre infraestrutura, privacidade, cibersegurança e evoluções tecnológicas em homenagem aos dez anos da South School on Internet Governance. Rio de Janeiro: Escola de Direito do Rio de Janeiro da Fundação Getúlio Vargas, p. 309-324, 2019.

FAVA, Rui. *Trabalho, educação e inteligência artificial*: a era do indivíduo versátil. Porto Alegre: Penso, 2018.

HILDEBRANDT, Mireille. Primitives of legal protection in the Era of data-driven platforms. *Georgetown Law Technology Review*, 2018. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3140594>. Acesso em: 14 set. 2019.

KITCHIN, Rob. Data-driven, networked urbanism. 2015. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2641802>. Acesso em: 14 set. 2019.

_____. The real-time city? Big data and smart urbanism. *GeoJournal*, v. 79, n. 1, p. 1-14, 2014.

MANN, Laura. Left to other peoples' devices? A political economy perspective on the big data revolution in development. *Development and Change*, v. 49, n. 1, p. 3-36, 2018.

MAYER-SCHONBERGER, Vyktor; CUKIER, Kenneth. *Big Data*: a revolution that will transform how we live, work, and think. Boston; New York: Houghton Mifflin Harcourt, 2013.

MENDES, Laura Schertel; DONEDA, Danilo. Marco jurídico para a cidadania digital: uma análise do Projeto de Lei 5.276/2016. *Revista de Direito Civil Contemporâneo – RDCC*, v. 9, p. 35-48, 2017.

MENEZES NETO, Elias Jacob de; MORAIS, Jose Luis Bolzan de; BEZERRA, Tiago José de Souza Lima. O projeto de lei de proteção de dados pessoais (PL 5.276/2016) no mundo do *big data*: o fenômeno da *dataveillance* em relação à utilização de metadados e seu impacto nos direitos humanos. *Revista Brasileira de Políticas Públicas*, v. 7, n. 3, p. 184-198, 2018.

MIRAGEM, Bruno. A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o Direito do Consumidor. *Revista dos Tribunais*, v. 1009, nov. 2019.

NUCCIO, Massimiliano; GUERZONI, Marco. Big data: hell or heaven? Digital platforms and market power in the data-driven economy. *Competition & Change*, v. 23, n. 3, p. 312-328, 2019.

OLIVEIRA, Carlos Eduardo Elias de. Aspectos principais da Lei nº 12.965, de 2014, o Marco Civil da Internet: subsídios à comunidade jurídica. *Texto para Discussão*, Brasília: Núcleo de Estudos e Pesquisas/Senado, n. 148, abr. 2014. Disponível em: <http://www1.tjrs.jus.br/export/poder_judiciario/tribunal_de_justica/centro_de_estudos/doutrina/doc/lei_12625_comentarios.pdf>. Acesso em: 14 set. 2019.

PAPPALARDO, Luca; SIMINI, Filippo. Data-driven generation of spatio-temporal routines in human mobility. *Data Mining and Knowledge Discovery*, v. 32, n. 3, p. 787-829, 2018.

SOLOVE, Daniel. *The digital person*: technology and privacy in the information age. Nova Iorque: NYU Press, 2004.

SOUZA, Liege Alendes de. A constitucionalização do direito privado: o direito ao esquecimento como um novo direito fundamental. *Disciplinarum Scientia | Sociais Aplicadas*, v. 15, n. 1, p. 1-14, 2019.

TIRONI RODÓ, Martín. Experimentando con lo urbano: políticas, discursos y prácticas de la ciudad inteligente y la datificación. *Athenea Digital: Revista de Pensamiento e Investigación Social*, v. 19, n. 2, p. 18, 2019.

XU, Lei et al. Privacy or utility in data collection? A contract theoretic approach. *IEEE Journal of Selected Topics in Signal Processing*, v. 9, n. 7, p. 1256-1269, 2015.

ZANATTA, Rafael A. F.; ABRAMOVAY, Ricardo. Dados, vícios e concorrência: repensando o jogo das economias digitais. *Estudos Avançados*, v. 33, n. 96, p. 421-446, 2019.

ZHANG, Desheng et al. Urban-Scale Human Mobility Modeling With Multi-Source Urban Network Data. *IEEE/ACM Transactions on Networking (TON)*, v. 26, n. 2, p. 671-684, 2018.

ZUBOFF, Shoshana. *The age of surveillance capitalism*: the fight for a human future at the new frontier of power. Nova Iorque: Profile Books, 2019.

Sobre os autores:

Mateus de Oliveira Fornasier | *E-mail:* mateus.fornasier@gmail.com
Professor do Programa de Pós-Graduação *Stricto Sensu* (Mestrado e Doutorado) em Direitos Humanos da Universidade Regional do Noroeste do Estado do Rio Grande do Sul (Unijuí), Doutor em Direito Público (Unisinos), com Pós-Doutorado pela University of Westminster (Reino Unido).

Norberto Milton Paiva Knebel | *E-mail:* norberto.knebel@gmail.com
Doutorando Programa de Pós-Graduação *Stricto Sensu* (Mestrado e Doutorado) em Direitos Humanos da Universidade Regional do Noroeste do Estado do Rio Grande do Sul (Unijuí), Mestre em Direito pela Universidade La Salle.

Data de submissão: 26 de setembro de 2019.

Data do aceite: 9 de outubro de 2020.