XXIX CONGRESSO NACIONAL DO CONPEDI BALNEÁRIO CAMBORIU - SC

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS I

LITON LANES PILAU SOBRINHO

LUIZ ERNANI BONESSO DE ARAUJO

AIRES JOSE ROVER

FERNANDO GALINDO AYUDA

D597

Direito, governança e novas tecnologias I [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Aires José Rover; Fernando Galindo Ayuda; Liton Lanes Pilau Sobrinho; Luiz Ernani Bonesso de Araujo.

– Florianópolis: CONPEDI, 2022.

Inclui bibliografia
ISBN: 978-65-5648-629-1
Modo de acesso: www.conpedi.org.br em publicações
Tema: Constitucionalismo, Desenvolvimento, Sustentabilidade e Smart Cities

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direito. 3. Governança e novas tecnologias.

XXIX Congresso Nacional do CONPEDI Balneário Camboriu - SC (3: 2022: Florianópolis, Brasil).

CDU: 34

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

XXIX CONGRESSO NACIONAL DO CONPEDI BALNEÁRIO CAMBORIU - SC

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS I

Apresentação

Direito, Governança e Novas Tecnologias.

O presente Grupo de Trabalho, baseia-se na problemática dos impactos das novas tecnologias, a partir de sua regulação, interferências e impactos da Governança. O objetivo do mesmo é ampliar as discussões e reflexões acerca das pesquisas realizadas sobre a temática com a finalidade de buscar a difusão do conhecimento científico para a melhoria e para o benefício da sociedade atual. O paradoxo das novas tecnologias e seus impactos no sistema jurídico vislumbram uma necessidade de readequação e mostram-se preocupantes, pois nos últimos anos a velocidade e a quantidade de acontecimentos observados no mundo inteiro dão um tom dramático à sensibilidade e impactos das novas tecnologias nas relações de governança e regulação. O desenvolvimento tecnológico tem trazido grandes avanços e, em contrapartida, uma insegurança em relação aos limites impostos as relações do sistema jurídico e da governança. Vivencia-se uma crise paradoxal, principalmente pela incerteza dessas relações. Com todos os avanços e o desenvolvimento de novas tecnologias na área jurídica e de governança, se está diante de um paradoxo, ou seja, o Estado cada vez mais reduzindo o investimento em pesquisas e deixando para a iniciativa privada dominar o campo das novas tecnologias. Assim, resta a dúvida de qual é o papel do Estado, uma vez que, em assim sendo, a sociedade fica à mercê do mercado. Nesse sentido, faz-se necessário repensar a dinâmica dessas relações. Outrossim, os trabalhos apresentados neste GT tratam dessas reflexões necessárias para o amadurecimento e para a assimilação de seus impactos. Os organizadores agradecem a todos os colegas pesquisadores e autores que contribuíram com seus excelentes trabalhos, estes que compõem esta publicação. Sendo assim, constata-se que houve comprometimento na investigação das mais diversas temáticas aqui trabalhadas, o que permitirá ao leitor uma leitura acurada e esclarecedora dessa obra.

PRIVACIDADE NAS CIDADES INTELIGENTES: PROPOSTAS ENTRE A UTOPIA E A DISTOPIA

PRIVACY IN SMART CITIES: PROPOSALS BETWEEN UTOPIA AND DYSTOPIA

Caitlin Mulholland [1]
Frederico Boghossian Torres [2]

Resumo

A instituição das cidades inteligentes, que se propõem a promover a melhoria da qualidade de vida dos cidadãos a partir da tecnologia, mobiliza a discussão pública. De um lado, temos o discurso hegemônico, propagandeado pelo setor privado, que defende a cidade inteligente como um caminho universal rumo ao progresso. Do outro, temos a reação alarmista aos danos causados pela tecnologia à privacidade, que assemelha a cidade inteligente a uma distopia marcada pela erosão da privacidade. No presente artigo, rejeitamos a assunção de que estamos diante de uma escolha entre a utopia e a distopia, buscando propor a análise concreta do fenômeno em questão. Assim, abordaremos a instituição da cidade inteligente a partir da origem deste discurso criador, que acaba por desconsiderar contextos locais e por promover uma versão universalizante de urbanismo. Em seguida, serão estudados os efeitos negativos que a arquitetura da cidade inteligente pode causar na privacidade e proteção de dados dos cidadãos. Ao final, como forma de equacionar as promessas da cidade inteligente com as preocupações relacionadas à privacidade, serão oferecidas, de forma não exaustiva, soluções que ajudam a mitigar o dano causado à intimidade dos cidadãos.

Palavras-chave: Cidades inteligentes, Privacidade, Proteção de dados, Lei geral de proteção de dados, Urbanismo

Abstract/Resumen/Résumé

The institution of smart cities, which aim to promote the improvement of citizens' quality of life through technology, mobilizes public discussion. On one hand, we have the hegemonic discourse, propagandized by the private sector, which defends the smart city as a universal path to progress. On the other, we have the alarmist reaction to the damage to privacy caused by technology, which likens the smart city to a dystopia marked by the erosion of privacy. In this paper, we reject the assumption that we are faced with a choice between utopia and dystopia, seeking to propose a concrete analysis of the phenomenon in question. Thus, we will approach the institution of the smart city from the origin of this creative discourse, which ends up disregarding local contexts and promoting a universalizing version of urbanism. Next, the negative effects that the smart city architecture can cause on citizens' privacy and

[1] Doutora em direito civil, pela Universidade do Estado do Rio de Janeiro. Professora do Departamento de Direito da PUC-Rio, onde atualmente exerce o cargo de Diretora do Departamento de Direito.

[2] Mestre em Teoria do Estado e Direito Constitucional, PUC-Rio.

data protection will be studied. Finally, as a way to equate the promises of the smart city with privacy concerns, we will offer, in a non-exhaustive way, solutions that help mitigate the damage to citizens' privacy.

Keywords/Palabras-claves/Mots-clés: Smart cities, Privacy, Data protection, Data protection general law, Urbanism

1. INTRODUÇÃO

As cidades, desde o primeiro assentamento registrado há cerca de nove mil anos, movimentam o imaginário da humanidade. A saída do campo para a cidade é temática comum na literatura, assim como os perigos e experiências oferecidos pelos ambientes urbanos. As cidades também são palco dos principais embates políticos, a exemplo da conexão entre a democracia grega e a arquitetura da *polis* (HAROUEL, 2004). No presente, as cidades seguem no centro das discussões sobre a política e a economia, hoje pautadas pelo uso das novas tecnologias em um mundo em transição para a chamada economia movida a dados pessoais, na qual a extração e processamento de informações tornam-se processos de primeira relevância econômica e política (FRAZÃO, 2020).

Esta nova lógica opera com base na questionável suposição de que existe uma livre troca da privacidade individual por serviços, operada entre as pessoas e as empresas produtoras de tecnologia (ZUBOFF, 2021). De um lado, cedemos nossos dados pessoais para serem tratados por aplicações inovadoras. Do outro, recebemos serviços mais rápidos, eficientes e capazes de promover melhorias em nossa qualidade de vida. É neste cenário que se inserem as cidades inteligentes, que, mediante o uso da tecnologia, prometem revolucionar os serviços urbanos, apesar dos evidentes riscos à privacidade dos cidadãos (KITCHIN, 2015).

Por outro lado, as cidades contemporâneas enfrentam os principais problemas humanos do século XXI: fluxos migratórios, mudanças climáticas, desastres naturais, superpopulação, gestão de resíduos, entre outros. Tais desafios muitas vezes precisam ser enfrentados em escala municipal, o que põe o gestor público diante de uma tarefa ingrata: resolver problemas complexos por meio de orçamentos frequentemente escassos. Além de complexas, as cidades estão em franco crescimento populacional, o que evidencia a necessidade de novas formas de solução de problemas. Segundo as Nações Unidas, a população urbana, entre 1950 e 2018, passou de 750 milhões para 4,2 bilhões. Mantida tal tendência de crescimento, acredita-se que mais de 70% da humanidade viverá em cidades até o ano de 2050 (UNITED NATIONS, 2018).

Ou seja, por mais que a inserção da tecnologia no tecido urbano seja motivo de justas preocupações quanto à expansão da vigilância, fato é que a humanidade se vê obrigada a buscar soluções eficientes para conseguir promover um desenvolvimento urbano justo e sustentável. Por esse motivo, além do *lobby* privado que existe pela promoção de *smart cities,* estas também se inserem na agenda global de sustentabilidade e desenvolvimento promovida pela ONU-

Habitat através da chamada Nova Agenda Urbana (NAU), que dedica uma de suas sessões à necessidade de criação de cidades mais resilientes e inteligentes (REIA, 2019).

Tendo em vista a antítese posta entre a necessidade de utilização da tecnologia pelas cidades e os riscos inerentes à expansão, no cenário urbano, da economia movida a dados, o presente artigo busca adotar uma postura crítica e construtiva. É certo que os desafios postos são de difícil solução, mas a adoção de discursos alarmistas não nos permite debater a melhor forma de implementar a tecnologia nas cidades.

Assim, buscaremos expor o que a cidade inteligente tem a nos oferecer a partir do estudo das tecnologias nelas utilizadas, da criação de um discurso global pelas cidades inteligentes e da dificuldade de definição sobre o que é uma *smart city*. Em seguida, analisaremos os riscos que a expansão da tecnologia pelas cidades representa para a privacidade, a partir de uma comparação com princípios consagrados pelas leis de proteção de dados mais avançadas. Por fim, buscando rejeitar uma visão maniqueísta, exemplificaremos, de forma breve, sugestões para promover o avanço das *smart cities* de uma maneira que mitigue os danos causados ao direito fundamental à proteção de dados pessoais.

2. A UTOPIA: SURGIMENTO DE UM DISCURSO PARA AS SMART CITIES

A relevância dos dados pessoais não é recente, mas hoje vivemos uma alteração que se dá em escala exponencial, como expõe a Lei de Moore, que narra que a capacidade dos microchips dobra a cada dois anos (MOORE, 1998). Tal aceleração possibilita o surgimento de imensos bancos de dados que podem ser analisados de forma rápida e precisa, permitindo o tratamento de dados pessoais em escalas antes inimagináveis. Esses fatores evidenciam que estamos diante da quarta revolução industrial, que se distingue das anteriores por seu crescimento exponencial. Indo além da substituição da força humana pela máquina, a revolução 4.0 busca a substituição da capacidade mental humana de organização pelos computadores, se distinguindo através de funcionalidades como a inteligência artificial, a computação em nuvem, a Internet das Coisas (IoT) e o *big data* (BARBOSA; COSTA; PONTES, 2020).

Essas novas ferramentas imediatamente passam a influenciar nosso cotidiano, fazendo-nos receber e compartilhar informação em frequências muito superiores. Como forma de tornar mais atrativo esse drástico processo de mudança nas relações sociais e econômicas, os produtos de nova geração passaram a ser chamados de *smart*, ou seja, inteligentes. Primeiro vieram os *smartphones*, que rapidamente foram seguidos pelos relógios inteligentes, eletrodomésticos dotados de conectividade e uma variedade de outros objetos *smart*.

Segundo Evgeny Morozov e Francesca Bria (2019), o termo "*smart*" se transformou em uma marca de irreverência, avanço e disrupção. Tais produtos inteligentes seriam inerentemente superiores aos anteriores, que se tornaram inadequados e devem ser substituídos. Entretanto, os autores destacam que não existe debate sobre o que significa tal adjetivo, mas tão somente a categorização, pelos próprios criadores, de que tais dispositivos ou projetos são inteligentes. No contexto das cidades inteligentes, essa polissemia pode ser perigosa, já que locais diferentes possuem prioridades distintas, afetando diretamente o que cada população percebe como a melhor opção de *smart city*.

Hoje, o "selo *smart"* é um ativo valioso, capaz de tornar uma cidade globalmente relevante e apta a atrair investimentos e mão de obra qualificada. Diversas organizações avaliam as cidades de acordo com a sua "inteligência", elaborando *rankings* e estimulando a competição entre essas, que buscam atrair parceiros privados para seus projetos (ECKHOFF; WAGNER, 2018). Ainda, propaga-se a relação das novas tecnologias com a promoção dos Objetivos para o Desenvolvimento Sustentável estabelecidos pelas Nações Unidas, como promoção de energia renovável, crescimento econômico inclusivo e sustentabilidade (REIA, 2019).

Porém, apesar de se acreditar que a discussão sobre a cidade inteligente é espontânea e decorrente de um avanço tecnológico natural, é possível datar o início do discurso hegemônico sobre as *smart cities*. Assim como o discurso *smart* mencionado, a divulgação do sonho da cidade inteligente tem origem em uma estratégia de *marketing* direcionada a criar uma agenda positiva sobre um novo mercado, que se inicia com o programa "*Smarter Cities*", patenteado pela empresa IBM no ano de 2009 (DIRK; KEELING, 2009). A empresa, após a crise de 2008, decide reorientar seus serviços para um mercado ainda pouco explorado pelas empresas de informática: as cidades. Através do programa, a IBM assume a posição de criadora de uma nova realidade urbana que, no presente, influencia o rumo do urbanismo em todo o planeta.

É essa a posição que, em geral, o setor privado assume: definir o tipo de "inteligência" que será adotado nas cidades. Ser inteligente, então, não necessariamente significa dar prioridade às necessidades reais da cidade e do cidadão, mas sim adotar as ferramentas difundidas por aqueles que definem o que é *smart*. A narrativa, desde o início, se molda para tornar as grandes empresas de tecnologia pontos de passagem obrigatórios para a promoção das cidades inteligentes (SÖDERSTROM et al., 2014). Deste modo, o discurso não somente narra o que as empresas são capazes de produzir, mas também as coloca como atores centrais da gestão urbana. Este processo de divulgação tem fundamento na chamada teoria do ator-rede (LATOUR, 2000), na qual os atores criam os interesses em que são capazes de agir, tornando-se peças essenciais de um sistema por eles criado.

Em meio à difusão das cidades inteligentes pelo mundo, ainda é incipiente o debate sobre o que efetivamente significa o conceito. A falta de precisão sobre o que é uma *smart city* favorece que modelos iguais de cidade se espalhem por locais com realidades e necessidades variadas, podendo agravar o fenômeno chamado solucionismo (MOROZOV; BRIA, 2019). Ao fornecer definições de cidade inteligente separadas em sistemas estáticos (transporte, moradia, energia, etc.) e soluções universais para cada sistema, o discurso da *smart city* inverte o fluxo ideal de solução de problemas coletivos. Ou seja, em vez da identificação de um problema real ser sucedida pela busca pela solução correta e adotada de forma dialógica, o solucionismo consiste na oferta de produtos que abordam questões pré-definidas, atravessando os pontos de passagem obrigatórios da indústria (KITCHIN; CARDULLO; DI FELICIANTONIO, 2018).

Não se trata de vilanizar o discurso adotado pelas empresas. Estas naturalmente irão buscar a expansão do seu mercado consumidor e divulgar versões de cidades que se amoldam aos seus produtos. Entretanto, é importante termos ciência de que a utopia da *smart city* como conhecemos é baseada em um processo que busca despolitizar a forma como se constrói a cidade (MOROZOV; BRIA, 2019), oferecendo soluções precipitadamente consideradas "inteligentes" sem que haja um debate sobre: (i) o que significa ser inteligente; (ii) as reais necessidades de cada local e (iii) os riscos para a privacidade dos cidadãos.

É por esses motivos que a discussão sobre o significado de "cidade inteligente" é extremamente relevante, já que a pluralidade de significados permite a mobilização de sonhos de natureza distinta. A definição, contudo, não é fácil. Desde a primeira menção ao termo nos anos 1990 até o presente, existem pelo menos 27 definições distintas sobre o termo (MOURA; DE ABREU E SILVA, 2019). Entendemos que essa polissemia não se origina somente da abertura da linguagem, mas da disputa em torno de qual modelo queremos para o futuro.

Nesse sentido, o foco escolhido por um conceito irá variar de acordo com o objetivo de quem nomeia. As definições de cidade inteligente trazidas pelo setor privado costumam focar no ideal de cidade digital, dando protagonismo à aplicação concreta da tecnologia e na divulgação de aplicações que se destinam a cada setor específico, à semelhança de um panfleto comercial (MOURA; DE ABREU E SILVA, 2019). As definições apresentadas pelas empresas são importantes para conhecermos as tecnologias, mas não são úteis para uma reflexão crítica sobre que modelo de cidade queremos adotar. As conceituações trazidas pelo setor público também elencam aplicações possíveis da tecnologia no tecido urbano, mas costumam ser mais centradas nos interesses do cidadão. É o caso da definição trazida pela Carta Brasileira para Cidades Inteligentes (CBCI), que define uma estratégia nacional para a construção de cidades inteligentes. Segundo a Carta, cidades inteligentes são:

> (...) cidades comprometidas com o desenvolvimento urbano e a transformação digital sustentáveis, em seus aspectos econômico, ambiental e sociocultural, que atuam de forma planejada, inovadora, inclusiva e em rede, promovem o letramento digital, a governança e a gestão colaborativas e utilizam tecnologias para solucionar problemas concretos, criar oportunidades, oferecer serviços com eficiência, reduzir desigualdades, aumentar a resiliência e melhorar a qualidade de vida de todas as pessoas, garantindo o uso seguro e responsável de dados e das tecnologias da informação e comunicação. (BRASIL, 2019)

A definição enfrenta dois problemas que costumam ser pontos cegos nas definições correntes: o solucionismo e a desconexão com a realidade de cada local. Dessa forma, a CBCI entende que a cidade inteligente deverá enfrentar "problemas concretos" e "reduzir desigualdades", trazendo conceito centrado na promoção da qualidade de vida da participação.

Em linhas gerais, todos os conceitos de cidade inteligente possuem um fio condutor: a melhoria da qualidade de vida urbana por meio do uso da tecnologia mais avançada disponível. Desse modo, Eckhoff e Wagner (2018) sumarizam as áreas que podem ser abordadas em: mobilidade, sustentabilidade, economia, utilidades, serviços públicos, saúde, construção civil, governança e cidadania. Para ilustrar como se dá a cidade inteligente, cabe trazer breves exemplos de aplicações concretas. É o caso da uso de câmeras dotadas de reconhecimento facial para prevenção de crimes, de postes de iluminação dotados de sistemas de economia de energia. Cidades também podem ampliar participação popular a partir de mecanismos digitais de consulta pública, assim como gestores podem adotar sistemas inteligentes para potencializar a eficiência da administração (LISDORF, 2020).

A utopia da cidade inteligente oferece promessas como: (i) fomentação da atividade econômica através da inovação; (ii) governo mais eficaz, capaz de tomar decisões informadas, promover a participação e assumir maior *accountability;* (iii) redes inteligentes de mobilidade urbana; (iv) economia de recursos e maior sustentabilidade; (v) maior segurança e eficiência nas habitações inteligentes; (vi) empoderamento da população, tornando-a mais capaz de obter informação e de exercer sua cidadania e empreendedorismo e (vii) enfrentamento mais inteligente e menos letal de ameaças de segurança pública (KITCHIN, 2015).

Entretanto, Kitchin (2015) também destaca que este sonho é acompanhado de palpáveis preocupações, como a despolitização do urbanismo a partir de um discurso universalista que descontextualiza a vida urbana local, a reprodução de vieses discriminatórios a partir do uso de tecnologias deficientes ou a propagação do solucionismo. Contudo, neste artigo dedicaremos especial atenção a outro risco mapeado pelo autor: a possibilidade de expansão da vigilância e de erosão da privacidade dos cidadãos.

3. A DISTOPIA: HAVERÁ PRIVACIDADE NAS CIDADES INTELIGENTES?

Apesar de a relação entre privacidade e tecnologia ser uma das principais discussões jurídicas e políticas do presente, a maioria dos rankings que medem a "inteligência" nas cidades não utiliza a privacidade como um indicador relevante (ECKHOFF; WAGNER, 2018). A ausência de destaque dada à privacidade nos põe diante de um risco de que, para obtermos os benefícios dos serviços de *smart cities*, precisemos trocá-los pela expansão da vigilância.

Apesar de a discussão pública sobre as cidades inteligentes ainda ser desvinculada da política, a forma de conformação do território urbano tem relação direta com o exercício do poder. O pensador francês Michael Foucault (2008), em seus estudos sobre governamentalidade, demonstra que, durante o processo de racionalização do poder do Estado, a forma como os governantes veem a cidade ideal se altera de acordo com as suas necessidades. Se, no período medieval, as ameaças principais vinham de fora e justificavam o levantamento de muralhas, a Europa industrializada prioriza um urbanismo capaz de gerir as massas urbanas e os problemas por essas gerados, como as epidemias ou as grandes manifestações públicas.

Hoje, nas cidades inteligentes, é possível falar em governamentalidade algorítmica, que potencializa a influência dos poderes sobre o comportamento humano a partir de mecanismos tecnológicos praticamente invisíveis e onipresentes (ROUVROY; BERNS, 2018). Pode-se entendê-la como um modelo de "*racionalidade governamental baseado na coleta em grande escala, na mineração dos dados e na elaboração de perfis com visada preditiva, conformando ambientes e direcionando a ação humana*" (ALVES, 2019, p. 245). A ubiquidade dos sensores permite que os mecanismos de poder se façam invisíveis, a ponto de "*poderem permanecer anônimos e de não serem controláveis*" (ROUVROY; BERNS, 2018, p. 112).

A inserção da cidade inteligente na lógica da economia movida a dados tem, então, evidentes contornos políticos. Uma figura repetida ao se debater privacidade é o panóptico, adaptado à realidade urbana por Finch e Tene (2016), que batizam a cidade vigiada de "*metróptico*". O panóptico é um modelo de prisão idealizado por Jeremy Bentham no século XVIII, no qual um agente posicionado ao centro é capaz de observar todas as celas ao seu redor. O modelo, também aplicável a hospitais, fábricas e escolas, influenciou o estudo sobre o poder, evidenciando a aplicação de técnicas de vigilância para além da esfera penal. São evidentes as coincidências do panóptico com a cidade inteligente, em que cidadãos são facilmente identificáveis e localizáveis através de controles centralizados.

Essa capacidade de gerar dados a partir da interação com sensores é interessante tanto para o setor público quanto para o setor privado. O primeiro se vê diante de dados que podem

ser utilizados tanto para reforçar o controle quanto para ter "acesso direto"[1] a informações úteis para a prestação de serviços à sociedade (ANTONIALLI; KIRA, 2020). Já o setor privado obtém dados que representam bens valiosos, que tanto podem ser utilizados para gerar lucro e aprimoramento de produtos quanto podem ser transmitidos para outros atores do mercado.

Neste processo, é importante ressaltar que, ao contrário de uma transação tradicional, a escolha por interagir com uma aplicação que coleta e armazena dados não significa a conclusão de um contrato. É tão somente o início de uma relação entre o cidadão e o serviço, na qual o primeiro se posiciona cada vez menos como um consumidor que recebe um serviço e mais como um "gerador" de dados que retroalimentam este sistema. Munidos desses dados, os agentes de tratamento conseguem traçar perfis, treinar algoritmos e interagir com os titulares de maneiras cada vez mais invasivas (ANTONIALLI; KIRA, 2020).

É evidente, então, que é necessário pensarmos modelos para que a cidade inteligente se desenvolva sem que isso resulte em vigilância exacerbada. De modo a pensar soluções para potencializar o a proteção de dados nas cidades, Lilian Edwards (2016) adota definição de cidade inteligente a partir das tecnologias mais utilizadas nos projetos de *smart city*:

- **Internet das coisas:** aplicação de sensores aos mais variados objetos do mundo real, com objetivo de permitir a interação entre eles em um contexto de hiperconectividade (MAGRANI, 2018)
- ***Big data*:** tratamento de dados em alto volume, velocidade, variedade, veracidade (SILVA RIBEIRO, 2020).
- **Computação em nuvem:** infraestrutura de alta capacidade que permite o armazenamento e interconexão de quantidades massivas de dados (EDWARDS, 2016)

Apesar de serem fenômenos amplamente estudados, a combinação dos três mecanismos em escala massiva é recente, demandando atenção diante do crescimento das populações urbanas e da relevância política global das cidades. A difusão de sensores pelo território urbano a partir da internet das coisas produz uma quantidade massiva de dados que trafegam em tempo real (*big data*) com amparo em uma robusta estrutura de computação em nuvem. Tal arquitetura comporta graves riscos à privacidade e conflita diretamente com os princípios adotados pelas mais modernas leis de proteção de dados, como veremos adiante.

[1] Uma das grandes críticas realizadas à economia movida a dados é que o acesso a informações coletadas sobre tal assunto não significa ter acesso à "verdade" sobre este objeto, haja vista que sistemas são dotados de algoritmos criados por seres humanos, podendo importar vieses destes, além de conter falhas em sua execução. Ou seja, qualquer base de dados naturalmente irá traduzir uma verdade que pode ser, na melhor das hipóteses, incompleta e, na pior das hipóteses, mentirosa (ROUVROY; BERNS, 2018).

Os desafios impostos pela cidade inteligente põem em evidência o fato de que o vocabulário jurídico tornou-se limitado em sua capacidade de oferecer soluções para mitigar o dano à privacidade dos cidadãos. Inicialmente, a construção teórica do direito à privacidade buscava proteger o indivíduo somente em seu espaço íntimo. Ainda assim, a massificação das cidades permitia que o indivíduo gozasse de relativa anonimidade e privacidade em público. Ou seja, na sociedade do início do século XX, o cidadão gozava da privacidade em seu lar e da anonimidade na cidade.

Nas *smart cities*, a lógica se inverte. Tanto a opacidade do espaço privado quanto a anonimidade do indivíduo em público são alteradas pelas novas tecnologias. Estas coletam informações dentro do lar (a exemplo de eletrodomésticos dotados de IoT) e permitem localização e identificação de um indivíduo em meio à multidão (a partir câmeras, reconhecimento facial, geolocalização, etc). Se os espaços públicos eram entendidos como locais que permitiam a agregação de anônimos, hoje podem ser permeados por sensores que coletam informações pessoais (EDWARDS, 2016).

Ou seja, as cidades inteligentes representam um desafio no que diz respeito aos limites da intimidade humana, deixando dúvida sobre o que é a esfera privada. Hoje, informações privadas fluem em ambientes públicos, seja a partir do monitoramento de nossos corpos ou a partir dos dispositivos pessoais que portamos, como telefones celulares e computadores. Além disso, ambientes privados tornam-se cada vez mais "públicos", na medida que a *smart home* expande a possibilidade de vigilância dentro do lar. Por exemplo, uma casa conectada à rede inteligente de energia (*smart grid*) pode ter seu padrão de consumo energético estudado, de modo a mapear o comportamento dos habitantes com precisão (SETO, 2015).

Koops (2014) sintetiza que vivemos em um mundo de "lares em evaporação" e "rastreabilidade ubíqua". Enquanto a vida privada escorre para o espaço público, essas informações privadas são conectadas com novos dados gerados pelos indivíduos em público. Ainda, no sentido contrário, as atividades registradas em público revelam aspectos da vida privada que se reservavam aos locais íntimos. Isto permite que se conheça a vida privada sem intromissão física em nenhum espaço privado, tornando a relação do conceito de privacidade com o de espaço cada vez mais defasada.

Ou seja, a defesa da privacidade torna-se cada vez mais difícil. Assim, as legislações contemporâneas de proteção de dados buscam ir além do direito negativo de proteção da intimidade contra as intromissões indesejadas, conferindo ao titular de dados o poder de, ativamente, exigir seus direitos. Para isso, estas leis estabelecem um rol de princípios cuja

obediência torna-se praticamente impossível nas cidades inteligentes. É o caso dos princípios da necessidade, finalidade, qualidade e transparência previstos no art. 6º da LGPD.

O primeiro, também conhecido como princípio da minimização, determina que os controladores devem tratar somente o mínimo necessário de dados para atingir suas finalidades. Contudo, a interação entre IoT e *big data* conflita com este objetivo. Segundo Edwards (2016), cientistas de dados tendem a coletar o maior número possível de dados, sendo mais fácil e menos custoso coletar todos os dados do que realizar a filtragem para que sejam coletados apenas os necessários. Além do volume de dados, a grande quantidade de dispositivos espalhados pela cidade coleta dados de forma constante, o que produz uma imensa quantidade de dados colaterais. Uma câmera de trânsito, por exemplo, irá registrar todo tipo de dado pessoal além de captar imagens de veículos (ECKHOFF; WAGNER, 2018). A inserção de tais limitações no código das tecnologias urbanas é um desafio tecnológico que demanda um investimento que ainda parece ter pouco estímulo para a sua realização.

Por sua vez, o princípio da qualidade determina que os dados utilizados devem ser exatos, atualizados e claros. É inevitável que as cidades inteligentes gerem quantidades impressionantes de dados, já que os sensores espalhados pela cidade irão interagir constantemente com a população. Este processo gera bases de dados com uma grande quantidade de informações incompletas, imprecisas ou conflitantes e retirar conclusões valiosas pode ser um desafio. Entretanto, as cidades devem ser responsáveis, haja vista que as consequências das análises afetam as vidas das pessoas, podendo determinar o redirecionamento de recursos ou o rumo de políticas públicas (FINCH; TENE, 2016).

Tais deficiências na qualidade de dados advém principalmente do fato de que essas bases são geradas sem finalidade específica, o que se traduz em violação ao princípio da finalidade, que exige que toda atividade de tratamento seja vinculada a um objetivo lícito. O ato de coletar por coletar, comum na ciência de dados, faz com que o *big data* seja coletado sem finalidade específica, sendo reutilizado para diversas intenções. Isso fará com que o resultado das análises seja de baixa qualidade, já que os dados usados não são específicos para o fim proposto. Nas cidades, é comum que uma tecnologia seja implementada com uma finalidade original que se expande, pondo em risco os direitos dos cidadãos (CHRISTOFI, s.d.). Pensemos na instalação de câmeras inteligentes para detecção de uso de máscaras durante a pandemia do novo coronavírus. Passado o contexto, tais ferramentas não devem ser utilizadas para outras finalidades, como a prevenção de crimes.

Ademais, ao tratarmos das bases legais previstas pela LGPD, a configuração de um consentimento lícito para o tratamento de dados é difícil nas cidades inteligentes. Conforme

mencionado, a coleta de *big data* costuma ser feita de forma indiscriminada e agregada, o que dificulta estabelecimento de um consentimento prévio para fins específicos (EDWARDS, 2016). A coleta de dados em espaços públicos também dificulta o consentimento livre. Estes espaços são destinados a serem usados para finalidades públicas, mas com a presença de sensores, o uso desses bens será vinculado à coleta de informações, não havendo uma verdadeira escolha por parte do cidadão. Isto evidencia o desequilíbrio de poder entre titular e controlador nas cidades, já que tanto o Estado quanto as empresas possuem capacidade de tratar dados de modo que não comporta a oposição do titular (CHRISTOFI, s.d.).

Logo, a realidade é que a maioria dos controladores optará por bases legais distintas do consentimento. O risco é que, no contexto urbano, o consentimento seja deixado de lado e que o tratamento de dados seja baseado em prerrogativas públicas ou no interesse legítimo do controlador, o que gera riscos de tratamentos pouco transparentes, mal justificados e capazes de violar direitos (EDWARDS, 2016). Mais do que isso, essas bases legais podem ser usadas, caso não haja fiscalização, para dar novas finalidades aos dados coletados.

Por sua vez, o princípio da transparência obriga que os controladores sejam capazes de demonstrar, aos titulares, como e para que utilizam seus dados. Na cidade inteligente, tal transparência é de difícil atendimento, haja vista que o cidadão tem pouca visibilidade sobre quais sistemas estão operando ou sobre qual é o fluxo de seus dados pessoais ou seu local de armazenamento. Ainda mais grave é a falta de visibilidade quanto ao compartilhamento de dados entre o Estado e o setor privado, já que o último fornece a grande maioria das tecnologias implementadas na cidade.

Para promover a transparência, é possível que a cidade se estruture de modo que permita conhecer e entender as formas como os dados são tratados nela. Com o crescente entendimento de que é difícil a plena adequação da cidade inteligente à legislação de proteção de dados (EDWARDS, 2016), a transparência é entendida como o principal fator de redução de danos e promoção da confiança da sociedade (FINCH; TENE, 2016). A efetivação dessa transparência depende de medidas que vão muito além da previsão de princípios e direitos em lei, sendo necessárias medidas concretas variadas que serão abordadas a seguir.

Por fim, cabe mencionar também que a ausência de uma norma que regule o tratamento de dados pessoais para fins de segurança pública no Brasil representa um grave risco nas cidades inteligentes. Cada vez mais, é difundida utilização de tecnologia para fins de policiamento, como o uso de sistemas de reconhecimento facial. Na falta de uma lei específica, a LGPD cria uma exceção demasiadamente perigosa para o estruturamento de cidades inteligentes, qual seja, a sua não incidência sobre temas de segurança pública, defesa nacional,

segurança do Estado e atividades de investigação e repressão penal (art. 4º, III). Faz-se urgente, então, o preenchimento de tal lacuna legislativa pelo Congresso Nacional.

4. COMO EQUACIONAR "INTELIGÊNCIA" E PROTEÇÃO DE DADOS NAS CIDADES?

Como se vê, não são poucas as tensões entre a cidade inteligente e a proteção de dados pessoais dos cidadãos. O risco de que a *smart city* signifique um dano demasiadamente grave à privacidade é real, o que nos obriga a pensar formas de mitigar a expansão da vigilância enquanto buscamos a melhoria em nossa qualidade de vida. Neste capítulo, exploraremos, de forma breve e não exaustiva, algumas alternativas para a harmonização entre as demandas das legislações de proteção de dados e os projetos de cidade inteligente.

4.1. Encarregado de dados

A função de encarregado de dados, prevista na LGPD, é equivalente à figura do *data protection officer* (DPO) previsto pelo GDPR. Trata-se de figura chave para a garantia da governança de dados e do cumprimento da LGPD dentro da estrutura de um controlador, sendo definida pela lei (art. 5º, VIII) como: "*pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)*" (BRASIL, 2018).

A LGPD prevê que o Poder Público deverá nomear encarregado quando realizar operações de tratamento de dados (art. 23, III). Mais que isso, existem pesquisas que sugerem, além da nomeação de encarregados específicos dentro de órgãos ou projetos públicos, seja nomeado um agente para atuar como encarregado no âmbito da cidade como um todo. Tal solução pode ser uma eficiente maneira de reduzir a opacidade das formas de tratamento de dados em cidades inteligentes, centralizando as solicitações das autoridades e dos titulares em uma figura específica, munida de comitê ou equipe especializada no assunto.

Van Zoonen (2016) explica que a complexidade da governança de dados em cidades tem feito com que municípios adotem a figura do *chief data officer,* que se responsabiliza pela gestão dos dados tratados pela cidade, facilitando a compreensão popular de temas como o fluxo de dados em projetos de *smart cities.* Nos Estados Unidos, já existem dezenas de CDO nomeados em âmbito estadual e municipal, com a incumbência de promover a governança de dados no âmbito da administração pública (GOVTECH, 2018).

A proliferação de posições de governança evidencia que a crescente dependência tecnológica das cidades demanda que este processo seja acompanhado por especialistas. Nos EUA, a figura do encarregado não existe na legislação, mas se assemelha ao *chief privacy*

officer (CPO), que representa um agente público de alto escalão, responsável pela fiscalização das normas de privacidade, pelo atendimento de demandas de titulares e pela promoção de boas práticas. Além do CDO e do CPO, cidades americanas tem adotado outras posições, como o *chief innovation officer* e o *chief technology officer*, responsáveis pela inovação, privacidade e tecnologia (FINCH; TENE, 2018). Essas posições demonstram a necessidade de interação multidisciplinar do encarregado, sendo um exemplo a ser seguido pelas cidades brasileiras.

A Índia, um dos países mais engajados na criação de projetos de cidades inteligentes, criou sua versão do *city data oficcer*, que atua como um encarregado de dados municipal. Hoje, o país conta com 100 encarregados distribuídos por 100 cidades inteligentes A posição é definida como um profissional sênior capaz de gerir um programa de governança de dados e de interagir com atores públicos e privados. Em sua gestão, o *city data officer* é obrigado a publicar uma política municipal de dados (*city data policy*), revisada mensalmente em contato com os atores relevantes nos projetos de cidade inteligente (GOVERNMENT OF INDIA, 2018).

No Brasil, tal movimento ainda é incipiente. Apesar disso, algumas iniciativas locais merecem destaque, como a Lei Ordinária nº 7.012 de 2021 no Rio de Janeiro, que instituiu o Conselho Municipal de Proteção de Dados e da Privacidade. A lei determina que o Conselho auxilie o Município na elaboração de uma Política Municipal de Proteção de Dados e acompanhe os processos de adequação da Prefeitura à LGPD. O Conselho também possui função de promover a cultura e conscientização sobre proteção de dados na cidade, realizando eventos e estudos junto à população do município do Rio de Janeiro. Ainda que o Conselho não possua capacidade de atuar como ponto de interação com os titulares de dados e de estabelecer diretrizes obrigatórias para projetos de cidades inteligentes, a possibilidade de promoção da cultura de proteção de dados na população do município pode ser um fator importante para a conscientização do cidadão sobre o funcionamento das *smart cities*.

4.2. Relatório de Impacto à Proteção de Dados (RIPD)

Uma das principais características da legislação adotada no Brasil é a abordagem que visa a minimização de riscos e a promoção da transparência das operações de tratamento de dados pessoais. É com este objetivo que a LGPD inaugura o instituto do Relatório de Impacto à Proteção de Dados (RIPD), definido pela norma brasileira (art. 5º, XVII) como: "*Documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco*;" (BRASIL, 2018). No que diz respeito ao seu conteúdo, a LGPD é silente, mas entende-se que este deve conter, pelo menos,

a descrição do tratamento, a finalidade deste, a descrição dos riscos, as medidas de mitigação e segurança adotadas e a avaliação de proporcionalidade da operação.

Na Bélgica, o projeto SPECTRE (*Smart city Privacy: Enhancing Collaborative Transparency in the Regulatory Ecosystem*) realizou estudos avaliando a aplicação dos RIPD na cidade inteligente. Dentre as principais conclusões do projeto, entende-se que a elaboração do RIPD é essencial para que sejam promovidas a transparência, a responsabilização dos atores e a confiança do cidadão. Além disso, o RIPD é importante pois evidencia o caráter múltiplo das iniciativas de *smart city,* servindo como oportunidade para reunir os atores públicos e privados no processo de atribuição de responsabilidades e definição de fluxos. Quanto à melhor forma de inserção das avaliações na realidade das cidades, concluiu-se que: (i) o RIPD deve ser elaborado previamente; (ii) a elaboração do RIPD deve envolver os cidadãos e todos os agentes envolvidos; (iii) a avaliação de impacto não é um processo único e finito, devendo ser revisitada e atualizada periodicamente (BREUER, HEYMAN, 2019).

Em vez de ser visto como um empecilho, o RIPD pode ser entendido, pelos administradores municipais e atores privados, como uma oportunidade de descobrir ineficiências e beneficiar o projeto como um todo, gerando confiança por parte do cidadão (BREUER, HEYMAN, 2019). Ainda que o custo de elaboração possa ser elevado, cabe à Administração Pública determinar que a elaboração prévia de RIPD é obrigatória nas *smart cities,* tendo em vista a larga escala dos projetos e do número de titulares afetados.

É possível, inclusive, que os resultados dos RIPDs realizados sejam divulgados ao público, com atenção às limitações relativa ao segredo comercial e industrial, que podem e devem ser tratadas como confidenciais. É o caso da Prefeitura de Seattle já realizou mais de 100 avaliações de privacidade (RIPD), sendo 19 dessas disponibilizadas publicamente (CITY OF SEATTLE, 2022). Dentre esses, incluem-se RIPDs sobre serviços diversos, que contém informações sobre a atividade de tratamento e sobre os atores privados envolvidos, o que serve para promover tanto a transparência quanto a confiança dos cidadãos.

4.3. Promover a confiança do cidadão

Um erro comum ao avaliar projetos que envolvem o tratamento de dados é achar que estes variam somente de acordo com o volume, sendo mais ou menos arriscados aqueles que tratarem mais ou menos dados. Nas cidades inteligentes, existe uma grande variedade de operações de processamento de dados que variam não só em volume, mas em finalidade, complexidade, transparência e muitos outros indicadores. Em grandes cidades, é difícil acompanhar com precisão todas essas variáveis, o que se torna ainda mais desafiador tendo em conta que estão envolvidos atores públicos e privados (VAN ZOONEN, 2016).

Outro erro é acreditar que a solução para os danos à proteção de dados nas cidades inteligentes passa somente pela tecnologia, já que ambientes urbanos são compostos também por pessoas. Assim, é essencial entender o que este cidadão pensa sobre a cidade inteligente, verificando se este se sente seguro para interagir com a cidade conectada. O elemento humano é, então, tão importante quanto o tecnológico, sendo imperativo entender de que maneira o indivíduo vê a cidade inteligente e de que maneira podemos fazê-la mais confiável e atrativa.

Nas cidades, é possível que um projeto seja desenhado de forma mais ou menos invasiva à privacidade. Tendo essas variações em mente, o administrador urbano deve, antes da adoção de uma iniciativa inteligente, avaliar de que forma o cidadão se relaciona com tal atividade de tratamento e de que forma a legislação a regula. Após essa análise, é possível elaborar uma política urbana capaz de não somente cumprir a lei como também estimular a participação cidadã, evitando usos desnecessários ou ilegais dos dados pessoais (VAN ZOONEN, 2016).

Além do estudo das preocupações da sociedade, existem outras maneiras de se promover a confiança. É o caso da garantia do direito de acesso, previsto pela LGPD, que determina que todo titular de dados deve ter acesso aos dados tratados pelos agentes. À medida que o cidadão for mais familiarizado com a forma de processamento, o local de armazenamento e as finalidades da coleta, este será mais capaz de entender a cidade inteligente e de se sentir mais seguro dentro dela. Ainda, isto permite que o titular de dados saiba a quem recorrer caso considere que suas informações estão sendo tratadas de forma ilícita (FINCH; TENE, 2016).

Por fim, outro caminho para aproximar o cidadão do gestor público nas cidades inteligentes é fazer com que a população se beneficie da coleta de dados. Na chamada *data featurization* (FINCH; TENE, 2016), o gestor busca dar aos indivíduos informações úteis, além de permitir que o cidadão possa acessar a informação coletada pela cidade e usá-la como bem quiser. Tais iniciativas buscam transformar os dados gerados pela cidade inteligente em informações que podem ser utilizadas pela sociedade civil, de maneira que estimule a inovação, o empreendedorismo e a participação cidadã.

4.4. Efetivando a transparência

Um dos caminhos para a promoção da confiança acima mencionada é garantir que as cidades inteligentes sejam transparentes em seu funcionamento. Nas cidades inteligentes, tais iniciativas de transparência podem ser variadas, incluindo por exemplo, medidas de transparência algorítmica ou de transparência administrativa.

A demanda por maior entendimento sobre o funcionamento das tecnologias contemporâneas advém do fato de que boa parte das aplicações com as quais interagimos

cotidianamente funciona de forma pouco clara para os usuários. Via de regra, não sabemos quais dados são coletados, como estes são utilizados, que tipos de inferências são feitas com base neles e qual é o impacto que este processo causa. Essa opacidade é ainda mais evidente em sistemas de inteligência artificial capazes de tomar decisões automatizadas, o que respalda a edição de normas que preveem o direito de revisão a decisões automatizadas (MULHOLLAND; FRAJHOF, 2020).

Uma das principais formas de se promover a transparência algorítmica é a estruturação de plataformas para a criação, divulgação e utilização de sistemas baseados em códigos abertos ou não proprietários (*open source*). A potencialização da democracia digital a partir da inovação pode ser promovida pela permissão da criação colaborativa de sistemas de código-fonte aberto a serem aplicados na cidade (MOROZOV; BRIA, 2019). Exemplos de uso de *softwares* livres podem ser verificados na cidade de Barcelona, que utiliza a plataforma Sentilo, uma plataforma cooperativa de cidades inteligentes, utilizando código livremente acessível para que a cidade seja menos dependente de plataformas proprietárias e de funcionamento obscuro[2].

O desenvolvimento de soluções *open source* não só promove a transparência como permite a colaboração para a inovação, potencializando a participação popular e estimulando o progresso científico. Ainda, a elaboração de soluções locais tende a se basear em diagnósticos realizados também de forma local, por pessoas que vivem os problemas que buscam solucionar. Dessa maneira, é possível reduzir a dependência de soluções universais, que nem sempre irão se amoldar às realidades locais.

Já a transparência administrativa ou organizacional depende da criação de documentos que esclarecem o funcionamento da *smart city*. O entendimento de que existe um desequilíbrio informacional entre agentes de tratamento e titulares demanda que os primeiros forneçam informações claras e acessíveis. A medida mais evidente é a publicação de políticas de privacidade, contendo detalhes sobre as atividades de uma organização. Em regra, as políticas costumam listar: os tipos de dados tratados, as finalidades de tratamento, as bases legais atribuídas, os limites do compartilhamento com terceiros, os canais para atendimento aos titulares, as medidas de segurança adotadas, os períodos de retenção de dados, entre outros.

Nas cidades inteligentes, estes documentos são essenciais para a centralização das informações sobre cada serviço prestado no ambiente urbano. Ressalte-se que a norma ISO nº 37.156/2020, que estabelece padrão para comunicações de dados em cidades inteligentes, recomenda a elaboração de políticas de privacidade pelas *smart cities*. Segundo a norma, o ideal

[2] A Sentilo se define como um sensor de código aberto desenhado para se encaixar na arquitetura de Smart City de qualquer cidade que busca a abertura e a fácil interoperabilidade (SENTILO, 2022).

é que estas cubram tanto a cidade como um todo quanto os serviços específicos nela prestados, tendo atenção à multiplicidade de formas de processamento de dados na cidade (ISO, 2020). Sendo assim, a promoção da transparência de uma cidade inteligente pode ser feita através de uma política de centralizada, que explique os fluxos de dados dos principais serviços da cidade. Esta iniciativa é importante para que o cidadão saiba quais fornecedores são utilizados pela cidade, permitindo que este busque as políticas de cada um destes, além de possuir um canal direto de contato com essas para exercitar seus direitos.

Importante ressaltar que estes documentos dificilmente irão cumprir sua função se forem excessivamente longos e técnicos, devendo ser acompanhados de versões que privilegiem a acessibilidade e experiência do usuário. A linguagem técnica é uma barreira à compreensão sobre o funcionamento de serviços que irão impactar a população (FINCH; TENE, 2018). Por isso, a criação de plataformas interativas, vídeos, cartilhas e outros recursos são iniciativas importantes para o sucesso da transparência organizacional nas cidades. Também é relevante determinar onde esses documentos e plataformas serão localizados. Como exemplo, é possível que o *link* ou código de acesso seja disponibilizado em áreas monitoradas por câmeras, respeitando os direitos dos cidadãos filmados. Ademais, uma estratégia de comunicação bem desenhada é essencial para o sucesso destes projetos, devendo a administração da cidade elaborar campanhas que promovam a conscientização (FINCH; TENE, 2018).

Como exemplo, merecem destaque as políticas da cidade estadunidense de Seattle. Com a intenção de conciliar inovação e privacidade, a cidade inaugurou um robusto programa de adequação dos projetos de *smart city* aos melhores padrões de proteção de dados, com a intenção de encontrar o equilíbrio entre coletar dados para prestar serviços e a necessidade de proteção da privacidade. Neste processo, a cidade adotou seis princípios para o tratamento de dados no ambiente urbano, consolidados nos *City of Seattle Privacy Principles* (CITY OF SEATTLE, 2015), que determinam que: a privacidade deve ser um valor chave para a cidade; a cidade deve coletar o mínimo de dados para seus projetos; a cidade deve sempre elencar suas finalidades e se responsabilizar pelos resultados; a cidade deve informar os cidadãos sobre o compartilhamento de dados e os dados coletados devem ser precisos e de boa qualidade.

5. CONSIDERAÇÕES FINAIS

O presente trabalho objetivou discutir, de maneira concreta, o cenário que as cidades inteligentes representam para a privacidade dos cidadãos. Em primeiro objetivamos expor que

a *smart city* é, diante dos desafios enfrentados pelos cidadãos e gestores urbanos, um caminho inevitável, haja vista a necessidade de soluções para problemas crescentes e complexos. Partindo desse pressuposto, definimos que é importante que a cidade inteligente seja estudada de forma responsável, que rejeite tanto a utopia propagandeada pelo discurso hegemônico quanto o temor exacerbado que não favorece um debate acadêmico propositivo que busque investigar formas mais sustentáveis de avanço das *smart cities*.

Em seguida, expusemos como se estruturou o discurso despolitizante e tecnicista de divulgação do ideal de cidade inteligente, o que acaba por criar uma utopia capaz de esconder verdadeiros riscos para a privacidade dos cidadãos e para a sua participação na construção da cidade. Tal discurso possui conexão evidente com a promoção da economia movida a dados e com a expansão da vigilância sobre o cotidiano das pessoas. Por isso, buscamos delimitar de que forma a cidade inteligente pode representar um risco para a privacidade dos cidadãos, conflitando diretamente com os princípios da legislação de proteção de dados.

Por fim, para cumprir com o compromisso de estabelecimento de um debate propositivo, elencamos, de forma não exaustiva, medidas que podem ser adotadas para mitigar o dano à proteção de dados nas cidades inteligentes. Com este objetivo, exploramos a figura do encarregado de dados, a criação de RIPDs e de mecanismos capazes de promover a transparência organizacional e algorítmica.

Ressalte-se que, sendo a cidade inteligente um fenômeno multifacetado e sendo o direito à proteção de dados uma categoria que permite diversos pontos de vista, o presente artigo não pretende exaurir os debates sobre a interação entre *smart city* e privacidade. Ademais, existem fatores de natureza técnica que se mostram essenciais para a promoção de uma cidade inteligente mais responsável, dentre os quais se destacam as chamadas PETs (*privacy enhancing technologies*) ou tecnologias potencializadoras da privacidade. A exploração de tais medidas técnicas ou de outras medidas de natureza administrativa faz-se urgente para que a discussão sobre a privacidade no ambiente urbano seja aprofundada.

REFERÊNCIAS BIBLIOGRÁFICAS

ALVES, M. A. S. Cidade inteligente e governamentalidade algorítmica: liberdade e controle na era da informação. **Philósophos - Revista de Filosofia**, v. 23, n. 2, 7 jan. 2019.

ANTONIALLI, D.; 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**, 12 fev. 2020, p. 1-25.

BARBOSA, A.; COSTA, J.; PONTES, R. Cidades Inteligentes no contexto da quarta revolução industrial. In: CZYMMECK, A. (ED.). **A quarta revolução industrial: inovacões, desafios e oportunidades.** Botafogo, Rio de Janeiro, RJ: Konrad Adenauer Stiftung, 2020, p. 9-34.

BRASIL. **Carta Brasileira de Cidades Inteligentes**, 2019. Disponível em: https://www.gov.br/participamaisbrasil/carta-brasileira-para-cidades-inteligentes4. Acesso em 10 de setembro de 2022.

BREUER, J.; HEYMAN, R. Mapping DPIA (best) practices in Smart Cities (D.2.1). **SPECTRE Research Project**, Bruxelas: FWO, 2019. Disponível em: https://spectreproject.be/. Acesso em 25 de março de 2022.

CHRISTOFI. A. Smart cities and the data protection framework in context. **SPECTRE Research Project**, Bruxelas: FWO, s. d. Disponível em: https://spectreproject.be/. Acesso em 23 de março de 2022.

CITY OF SEATTLE. **Privacy Statement.** Seattle, WA: Seattle Information Technology, 2022. Disponível em: https://www.seattle.gov/tech/initiatives/privacy/privacy-statement. Acesso em 17 de Setembro de 2022.

CITY OF SEATTLE. **Seattle Privacy Principles**. Seattle, WA: Seattle Information Technology, 2015. Disponível em: https://www.seattle.gov/tech/initiatives/privacy/privacy-statement. Acesso em 17 de Setembro de 2022.

DIRKS, S.; KEELING, M. **A vision of smarter cities: How cities can lead the way into a prosperous and sustainable future**. IBM Institute for Business Value – Executive Report, Nova Iorque: IBM Global Business Service, 2009.

ECKHOFF, D.; WAGNER, I. Privacy in the Smart City—Applications, Technologies, Challenges, and Solutions. **IEEE Communications Surveys & Tutorials**, v. 20, n. 1, p. 489–516, 2018.

EDWARDS, L. Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective. **European Data Protection Law Review (Lexxion),** SSRN E. J., 2016.

FINCH, K.; TENE, O. Smart Cities: Privacy, Transparency, and Community. In: SELINGER, E.; POLONETSKY, J.; TENE, O. (EDS.). **The Cambridge Handbook of Consumer Privacy**. 1. ed. [s.l.] Cambridge University Press, 2018, p. 125-148.

FINCH, K.; TENE, O. Welcome to the Metropticon: protecting privacy in a hyperconnected town. **Fordham Urban Law Journal**, v. 41, n. 5, article 4, pp. 1581-1615, 2016.

FOUCAULT, M.; SENELLART, M. **Segurança, território, população: curso dado no Collège de France (1977-1978).** São Paulo (SP): Martins Fontes, 2008.

FRAZÃO, A. Fundamentos da proteção de dados pessoais – Noções introdutórias para a compreensão da importância da LGPD. In: FRAZÃO, A.; DONATO OLIVA, M.; TEPEDINO, G. (coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.** 2ª ed. São Paulo: Thomson Reuters Brasil, 2020, p. 23-52.

HAROUEL, J.-L. **História do urbanismo.** Campinas: Papirus, 2004.

ISO 37156:2020 - **Smart community infrastructures — Guidelines on data exchange and sharing for smart community infrastructures.** Geneva: ISO, 2020.

KITCHIN, R. Promises and perils of smart cities. **SCL – Society for Computers and Law**, 8 jun. 2015. Disponível em: https://www.scl.org/articles/3385-the-promise-and-perils-of-smart-cities. Acesso em 15 ago. 2022.

KITCHIN, R.; CARDULLO, P.; DI FELICIANTONIO, C. **Citizenship, Justice and the Right to the Smart City.** [s.l.] SocArXiv, 19 out. 2018. Disponível em: <https://osf.io/b8aq5>. Acesso em: 15 setembro de 2022

KOOPS, B. J., 'On legal boundaries, technologies, and collapsing dimensions of privacy', **3 Politica e Società**(2), 2014, p. 247-264

LATOUR, B. **Ciência em ação: como seguir cientistas e engenheiros sociedade afora.** São Paulo: Unesp, 2000.

LISDORF, A. **Demystifying Smart Cities: Practical Perspectives on How Cities Can Leverage the Potential of New Technologies**. Berkeley, CA: Apress, 2020.

MAGRANI, E. **A internet das coisas**. 1a ed. Rio de Janeiro, RJ, Brasil: FGV Editora, 2018.

MOORE, G. E. Cramming More Components onto Integrated Circuits. **Proceedings of the IEEE**, v. 86, n. 1, jan. 1998, p. 82-85.

MOROZOV, E.; BRIA, F. **A cidade inteligente: Tecnologias urbanas e democracia.** São Paulo: Ubu Editora, 2019.

MULHOLLAND, C.; FRAJHOF, I. Inteligência Artificial e a Lei Geral de Proteção de Dados Pessoais: breves anotações sobre o direito à explicação perante a tomada de decisões por meio de machine learning. In: FRAZÃO, A.; MULHOLLAND, C. (coord.). **Inteligência Artificial e Direito.** 2ª edição. São Paulo: Thomson Reuters Brasil, 2020, p. 267-292.

REIA, J. O Direito à Cidade (Inteligente): Tecnologias, Regulação e a Nova Agenda Urbana. In: SILVA, A. et al. **Horizonte Presente: tecnologia e a sociedade em debate**. Belo Horizonte: Casa do Direito. Fundação Getúlio Vargas, 2019, p. 140-170.

ROUVROY, A.; BERNS, T. Governamentalidade algorítmica e perspectivas da emancipação: o díspar como condição de inviduação pela relação? In: BRUNO, F. et al. (EDS.). **Tecnopolíticas da vigilância: perspectivas da margem**. 1ª edição ed. São Paulo, SP: Boitempo, 2018, p. 107-140.

SETO, Y. Application of Privacy Impact Assessment in the Smart City. **Electronics and Communications in Japan**, Vol. 98, No. 2, 2015, p. 52-61.

SILVA RIBEIRO, C. J. Big data no contexto da quarta revolução industrial: transformações no processo de Pesquisa & Desenvolvimento (P&D). In: ACZYMMECK, A. (ED.). **A quarta revolução industrial: inovações, desafios e oportunidades.** Botafogo, Rio de Janeiro, RJ: Konrad Adenauer Stiftung, 2020.

SÖDERSTRÖM, O.; PAASCHE, T.; KLAUSER, F. Smart cities as corporate storytelling. **City, v. 18**, n. 3, p. 307–320, 4 maio 2014.

UNITED NATIONS. **World Urbanization Prospects: The 2018 Revision, Online Edition, 2018.** Disponível em: <https://esa.un.org/unpd/wup/Publications/Files/WUP2018-KeyFacts.pdf>. Acesso em: 15 setembro de 2022.

VAN ZOONEN, L. Privacy concerns in smart cities. **Government Information Quarterly**, v. 33, n. 3, p. 472–480, jul. 2016.

ZUBOFF, S. **A era do capitalismo de vigilância: a luta por um futuro na nova fronteira de poder**. 1ª edição. Rio de Janeiro: Intrínseca, 2021 (edição digital).